CYBER HERO
FRONTLINE

magazine by THREATLOCKER®

Defend against SMB attacks
Protect file shares with effective policy enforcement

Counter the AI crimewave
Vibe hacking demands a new cybersecurity approach

Supply chains resilience
Shipping security solutions for the future of logistics

THREATLOCKER® IN 2025

Highlights of what's been an eventful year at the company

GROWING WITH THE ZERO TRUST SHIFT

Zero Trust is actively being adopted around the world. As that shift accelerates, we are even more determined and driven to give customers the support they need and the flexibility to deploy Zero Trust in ways that work for their environment.

In 2025, that meant expanding the ThreatLocker team and infrastructure globally, with a new data center in Riyadh, Saudi Arabia, a new office in Brisbane, Australia, and opening a second headquarters in Orlando, FL, U.S. Our team grew from 500 to over 600 employees, and we expect that momentum to continue as demand for practical Zero Trust solutions keeps rising.

EXPANDING THE PLATFORM

Attackers don't stand still, which means we have to stay diligent and proactive to keep them out. ThreatLocker has been doing just that throughout 2025, expanding our Zero Trust platform with new capabilities and solutions, including Insights, Patch Management, User Store, Web Control, Cloud Control, Detect dashboard, and Defense Against Configurations (DAC).

These additions all maintain the singular purpose of empowering security teams to stay ahead of attackers with more agile solutions, which will ultimately reduce their burdens whilst streamlining defenses. As the platform evolves, so does our commitment to delivering protections that are easier to deploy and manage as well as being more effective in day-to-day operations. You can expect even more straightforward, purpose-built protections in 2026 and beyond.

ZERO TRUST WORLD 2025—AND LOOKING AHEAD

In 2025, ThreatLocker welcomed 1,800 attendees from 28 countries to Orlando for the fifth edition of Zero Trust World. The event brought together practitioners from across industries for hands-on labs, deep technical training, and real-world Zero Trust discussions.

This issue arrives alongside Zero Trust World 2026, and we hope those who join us walk away with a stronger, more practical understanding of how Zero Trust principles apply in real environments. If you couldn't attend this year, we'd love to see you in 2027.

INTRODUCING CYBER HERO® FRONTLINE

2025 also marked the launch of Cyber Hero Frontline magazine with the simple goal of cutting through the noise and placing focus on what Zero Trust looks like in practice. We want our readers to make actionable use of these tips to defend better and keep attackers at bay. Each issue shares insights, strategies, and lessons you can apply immediately.

It's one more way we're working to support defenders on the front lines. We hope the practical knowledge within these pages makes a real difference—whether you're refining policies, tightening controls, or building a lower-risk environment that's harder for attackers to move through.

WELCOME NOTE

Hello and thank you for exploring our third edition of Cyber Hero® Frontline magazine. The path to Zero Trust begins with strong awareness. The more you know, the more empowered you are to strengthen your defenses. And we hope this magazine continues to serve as a catalyst, helping you act with more confidence as you harden your environment.

APPLYING ZERO TRUST CONTROL TO YOUR NETWORK RESOURCES

Multi-factor authentication (MFA) has been a long-established additional security measure, thought to be one step ahead of would-be hackers: A user within an organization needs to sign-in to an affiliated network resource (think a SaaS, like Salesforce, or a cloud-based service like Microsoft Office 365) with a username and password, and then they're required to enter a one-time code (OTC) sent to their assigned device for further identity verification.

Unfortunately, this process is not as secure as you would like to think. If a user is willing to enter their credentials, they are also likely willing to provide their OTC. All an attacker needs to do is get a single user in an organization to click on one of their phishing links, sending the user to a website that looks exactly like the service they normally log into.

The attacker can then forward those credentials to the actual service in real time but remain in the middle. Once a user signs in, the attacker has access to the service as that user for as long as the token lasts.

Tokens can be valid for as little as an hour if set up properly, or as long as a year, but administrators rarely change the default settings. This period grants successful attackers unobstructed access to your organization's resources, along with all the key information contained within.

Whatever the amount of time they're inside, it will be more than enough to do damage. But what if there was an additional layer of approval required for your organization, beyond an authentication layer based on individual credentials from device to device?

We've solved this challenge. We are happy to share ThreatLocker® is expanding its protection suite to include features that will make environments resistant to these phishing attacks.

Like how Application Allowlisting blocks everything in your environment by default, you'll be able to harden your environment at the end-user level and gain more granular control over which user devices can access the network resources available to your organization.

IT teams can allow specific trusted devices to connect to a secure network managed by ThreatLocker, where they can then connect to a SaaS or cloud resource. This means that even if an attacker extracts a user's credentials and OTC, they wouldn't be able to sign-in to the account.

This is going to lead to a drastic reduction in the risk of successful phishing attacks that malicious actors use to extract or tamper with key data.

We look forward to sharing more details and demonstrating this solution in action.

ZERO TRUST WORLD 2026

Adopting Zero Trust is becoming standard practice across leading organizations in both the government and the private sector. Learning as much as you can, as quickly as possible, to efficiently deploy these controls has become mission-critical. It's crucial not to get left behind.

This is why, for the sixth year in a row, we are hosting Zero Trust World (ZTW) in Orlando, FL.

As the title implies, ZTW is geared toward raising strong awareness and a practical understanding of something we hold dear as our core operating principle: A strong Zero Trust framework is the most effective way to keep threats from impacting your environment.

Our goal is for all participants to achieve a strong working knowledge of Zero Trust cybersecurity during the event, with which they'll feel equipped to take immediate action to harden their environments.

We're confident that anyone who takes part in ZTW—past, present, or future—will find real value and enjoyment, heading home galvanized with new skills that make their day-to-day work easier and their environments more secure.

In the meantime, we invite you to dive into this latest edition of Cyber Hero Frontline and gain actionable insights from within its pages.

Yours,

Sami Jenkins
COO and Co-founder, ThreatLocker

Danny Jenkins
CEO and Co-founder, ThreatLocker

TABLE OF **CONTENTS**

INDUSTRY FOCUS

SECURITY INSIGHTS

GLOBAL POLICY

LIFESTYLE

TRENDING

PEACE OF MIND

ON MY **MIND**

BY DANNY JENKINS

When we launched ThreatLocker® in 2017, our goal was to change the ways we approached cybersecurity and make the pathway to a secure environment as straightforward as possible. We are continuing to make huge strides towards that goal and look forward to rolling out our latest solutions. With that in mind, here are some of the key topics I have been thinking about lately

1 BASIC CONTROLS CAN KEEP OUT RAPID ATTACKS

Attacks can happen unbelievably quickly.

However, introducing some basic controls to your environment can also be incredibly effective. By placing limitations on what even your most trusted applications can do and shutting down ports on the firewall, you are proactively limiting attack vectors for cybercriminals.

Taking steps like limiting application-to-application interactions, deploying allowlisting to decide and oversee which applications are allowed to run in your environment, and shutting down ports on the firewall can block out the overwhelming majority of threats.

“

By placing limitations on what even your most trusted applications can do and shutting down ports on the firewall, you are proactively limiting attack vectors for cybercriminals

2

MAKING ZERO TRUST WORLD A FANTASTIC EDUCATIONAL OPPORTUNITY

Getting into the core values of what it means to have a Zero Trust policy is at the heart of what we do here at ThreatLocker. For us, the effective deployment of a Zero Trust framework is crucial to a future in which cybersecurity risks are always lower.

That's why we host our annual event, Zero Trust World (ZTW). The aim is to provide attendees with both a great learning experience and an opportunity to leave more skilled in Zero Trust policies than when they arrived.

We have been hard at work to ensure we provide three days of immense value for attendees, with industry leaders on hand to deliver talks, training sessions, and valuable face time with fellow cyber professionals. If you have attended ZTW26 this year, I hope you left with a handful of solid tips and strategies to harden your environment immediately.

3

WORKING TO SECURE APPLICATIONS WE HAVE NO CONTROL OVER

Cloud services present a different security challenge than a typical on-premises application. While organizations cannot enforce execution-level controls within software-as-a-service (SaaS) platforms, strong identification protocols, along with access and data controls, can still reduce risk.

From a Zero Trust perspective, this starts with enforcing secure authentication: Protection must rely on compensating controls. Phishing-resistant multi-factor authentication (MFA), conditional access policies, and least-privilege administration reduce the blast radius and limit the impact of management-layer abuse.

Because cloud applications sit outside traditional endpoint control boundaries, the most effective way to harden their use today is to apply Zero Trust principles to everything that interacts with them: users, devices, identities, and data uploaded.

ThreatLocker continues to expand protections around cloud usage and access patterns. In the meantime, reducing trust at endpoints and enforcing least privilege remain critical layers in protecting cloud-based workflows.

> **AI is a new and ever-expanding payload development tool for malware and ransomware that's only going to get more relentless—but we can keep them out and render cybercriminal actions irrelevant**

4

ATTACKERS ARE STILL OUTPACING DEFENSES

Threats continue to evolve, and attackers will continue to find ways around defenses. AI is a new and ever-expanding payload development tool for malware and ransomware that's only going to get more relentless—but we can keep them out and render cybercriminal actions irrelevant.

We have to go one step further than having a list of trusted applications, although that's a great start. By placing blocks on even your organization's most trusted applications and keeping permissions only at the business-critical level, you're not going to give any would-be hackers much breathing room.

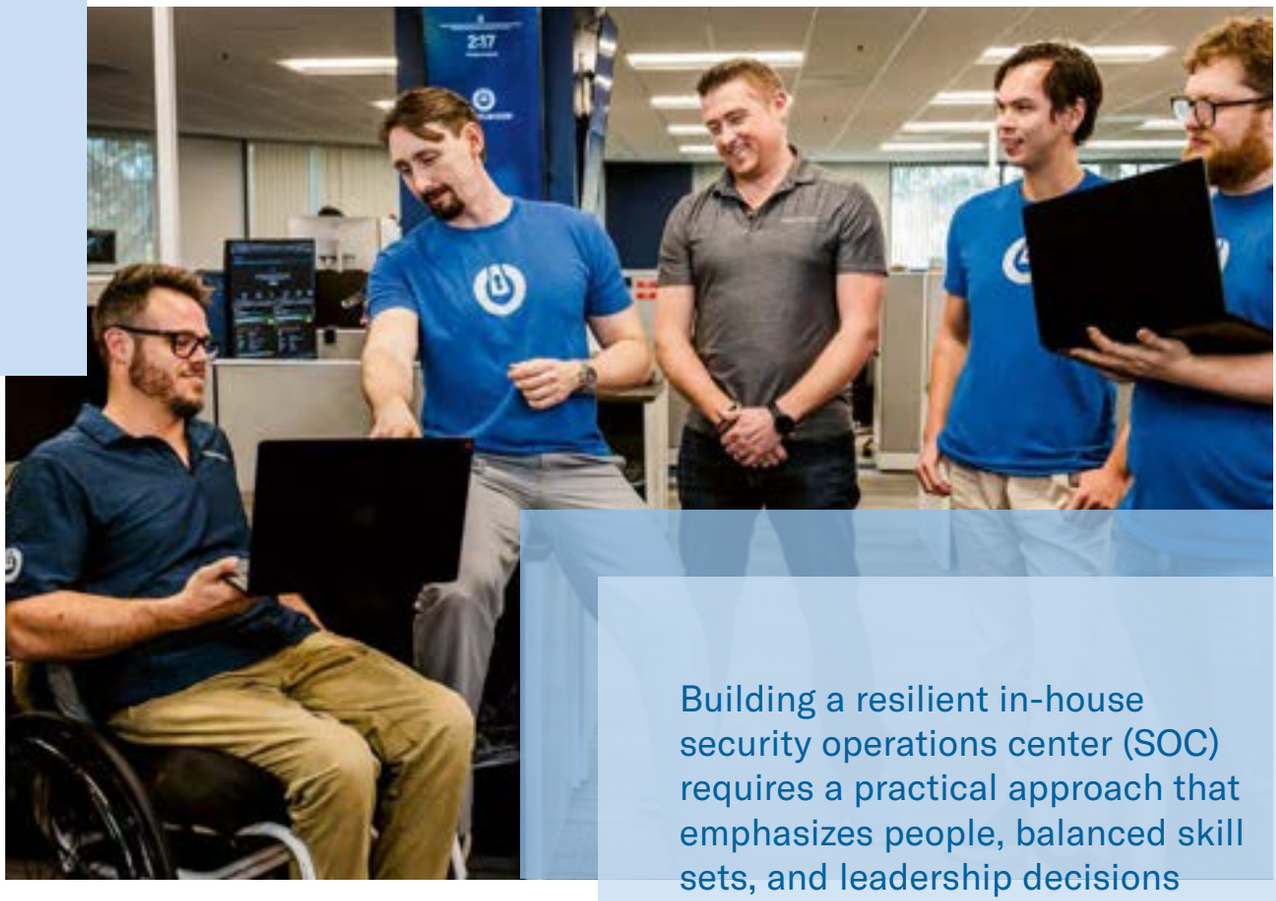
The ThreatLocker platform enables this exact level of granular control. Our solutions allow you to decide how applications interact within your environment, rather than granting them the same permissions as an end-user. This ultimately reduces the vulnerabilities introduced when an application is weaponized.

THREATLOCKER TIP

Watch the latest video from ThreatLocker, because a fast response isn't fast enough

STAFF A RESILIENT **IN-HOUSE SOC**

By John Lilliston, CISSP,
Detect Product Director, ThreatLocker



Building a resilient in-house security operations center (SOC) requires a practical approach that emphasizes people, balanced skill sets, and leadership decisions aligned with tools and policies

Cybersecurity often advertises its technology first. Vendors talk about smarter analytics, faster detection, and automated responses—tools that learn, scale, and never sleep. The truth is that none of these are effective without rules and policies anchoring them and molding their abilities into an effective security program. Furthermore, that structure only works if the right people support it.

A SOC depends on human judgment more than most outsiders assume. Alerts may start with dashboards and detections, but the choices that follow—what to escalate, what to ignore, and what needs immediate attention—belong to analysts. A strong team shapes the character of an entire security program. Building such a group requires intention—not only about what skills candidates bring, but also about how they complement one another.

A practical philosophy for team design

It is all about building a mix. The healthiest SOCs blend versatility with deeper pockets of expertise. That does not mean every analyst must know everything, but each person should have the range to handle common alerts and the depth to contribute something distinctive. Think of it as a practical balance: Enough breadth to stay flexible and enough mastery to remain effective when problems get complicated.

This philosophy matters because cybersecurity work rarely follows a neat script. Attackers move fast and their methods change. Business needs shift, networks expand, and tools get replaced or reconfigured. A team that relies too heavily on a handful of specialists becomes brittle, while a team made entirely of generalists struggles with complex investigations. The right mix gives a SOC both stability and momentum.

The security professional baseline

Whatever a candidate's eventual specialty, certain competencies form the entry point for all analysts:

- **Confident response:** Alerts like phishing reports, endpoint detections, and account anomalies are the everyday signals a SOC must triage. Analysts must be able to determine whether the alert is worth actioning. This skill develops through exposure, but it starts with clear expectations and steady practice.
- **Running business-critical tools:** Analysts do not need deep engineering knowledge of every platform, but they should know how to perform the essentials. When a critical user is locked out of an application, the SOC must troubleshoot quickly, apply exceptions when appropriate, and document the decision. Small operational tasks often prevent big operational disruptions.
- **Acting independently:** Many incidents begin when staffing is thin. An analyst who works the late shift cannot rely on an entire team for backup, so they need a solid grasp of response procedures and escalation paths. Leadership must reinforce those expectations and offer frequent opportunities for hands-on practice.

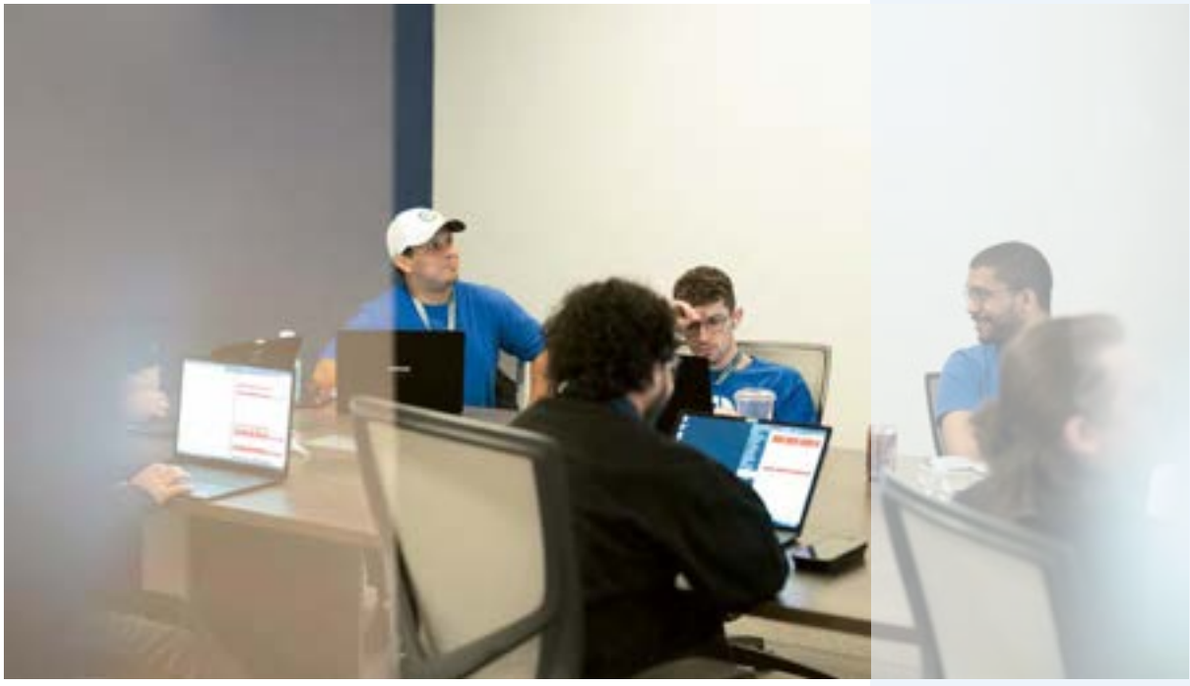
It is all about building a mix. The healthiest SOCs blend versatility with deeper pockets of expertise

These shared skills create resilience because if one person cannot step in when needed, the whole structure wobbles. A SOC becomes dependable only through a reliable and consistently applied baseline.

How specialization adds strength

With the basics covered across all staff, specialization multiplies the power of the team. Analysts should pursue the areas where they naturally excel to offer the SOC capabilities that pure generalists cannot match. Some strengths prove especially valuable:

- **Networks and infrastructure:** Analysts with a strong IT background often excel at deciphering complex traffic patterns or permission issues. They know how identity systems behave, how segmentation works, how misconfigurations open doors to attackers, and how rigid policy management keeps them closed.
- **Forensics and programming:** Some gravitate toward the hacker end of the spectrum. They might work on reversing malware, writing scripts



Hiring for potential rather than standout skills takes patience, but creates teams that adapt to evolving threats

to streamline investigations, or reconstructing the steps of a breach. Their work often answers the "how" behind an incident—context that improves both detection and prevention.

- **Organizational specialties:** Cloud security, threat intelligence, identity monitoring, and compliance are areas that grow as an organization grows. They require dedicated focus and deep expertise, and while these responsibilities are often shared, every SOC benefits from an expert voice.

Strong leadership recognizes these emerging strengths early. A good manager encourages analysts to pursue in-depth learning without drifting away from the fundamentals. When everyone maintains an ambitious baseline, and a few people also develop exceptional abilities, you end up with a mature SOC.

A SOC staffed entirely by lateral hires can stay afloat, but one that grows its own talent becomes resilient

A more realistic hiring playbook

Ambition in SOC building requires grounding in realistic hiring practices. Security hiring often fails before the interviews begin. Job descriptions describe entry-level roles that demand years of experience, a stack of certifications, and familiarity with obscure tools that most universities do not cover. This approach discourages exactly the creative and adaptable learner who thrives in SOC work.

An ambitious yet sustainable model groups candidates to find those who fit all aspects of the SOC. It looks for a small set of seasoned experts who can anchor technical direction and mentor others, solid mid-level analysts to keep day-to-day operations reliable, and early-career hires with strong IT fundamentals and the drive and personality to grow in their roles.

This layered structure enables ambitious growth without unrealistic expectations. It also mirrors how effective technical teams have grown for decades—through steady development and deliberate planning. When leaders invest in junior hires, the payoff is long-term loyalty and a pipeline of internal specialists shaped by the organization's actual needs. Realism is the foundation that makes ambitious security programs sustainable.

Modern SOCs succeed when they blend shared skills with individualized strengths

How big should a SOC be?

There is no universal answer to the optimal team size. It depends on the organization's scale, the expectations set in its policies, and the budget available to meet them. What can be said with confidence is that 24/7 monitoring carries real staffing implications, even when a rigid software layer is in place to help.

Late-night and early-morning hours are often when serious incidents surface. Relying on a lone analyst for those shifts creates unnecessary risk. Two-person minimum coverage is a safer standard and gives analysts a sounding board during stressful investigations.

Shift structure matters as well. Rotational models distribute off-hour work more evenly but can disrupt sleep cycles. Fixed shifts provide stability but require people willing to embrace permanent nights or weekends. Whichever model a SOC chooses, leadership should match its promises with the resources to deliver them. A team tasked with providing all-day, everyday coverage cannot do so responsibly without adequate staffing.

The talent pool

Despite the negative narrative of a cybersecurity shortage, the truth is that more potential candidates are now entering the field than ever before. Universities offer cybersecurity programs, community colleges have caught up quickly, and online training has lowered barriers to entry. What is often missing is clarity, rather than talent.

Organizations struggle to articulate what "entry level" should mean, and therefore bypass capable candidates who lack experience with niche tools but have strong fundamentals in systems, networking, or scripting. Those candidates, once trained, often become standout analysts because they approach the work with curiosity rather than checklist thinking.

Hiring for potential rather than standout skills requires patience. But over time, it builds teams that understand the environment deeply and adapt as threats evolve. A SOC staffed entirely by lateral hires can stay afloat, but one that grows its own talent becomes resilient.

Building teams that endure

Modern SOCs succeed when they blend shared skills with individualized strengths. When analysts understand the essentials, they can keep operations running even under pressure. When they pursue deeper specialties, the team gains the insight needed to unravel complex attacks. And when leadership commits to thoughtful hiring and realistic staffing, the SOC becomes steady enough to support the business through inevitable change.

THREATLOCKER TIP

Strong SOC leadership is built on trust. Empowered analysts respond to threats faster and make smarter decisions

RECOVERY SYSTEMS

DEMAND RESILIENCE FIRST

Safe Mode disables endpoint security tools when systems need troubleshooting. Modern defenses must assume failure and limit the damage

A critical system crashes, throws a blue screen, and the only way back in is Safe Mode. In many ways, this path to recovery will come as a relief; it suggests that all is not necessarily lost. In the right hands, Safe Mode offers useful respite. In the wrong hands, though, Safe Mode provides a way in. If a machine can be forced to blue screen and pulled out of regular operation, it can be tampered with.

Safe Mode is not a secure environment. By design, it disables most third-party drivers and services, including endpoint security tools. The techniques that cyber professionals rely on—endpoint detection and response (EDR), application allowlisting, behavioral analysis, and related controls—are typically rendered inactive. Safe Mode is a necessary troubleshooting tool, but also a security blind spot.

ACCEPTING THE INEVITABLE

So, what should organizations do when an attacker forces a system into Safe Mode, or exploits the window of reduced protection during recovery? Organizations must assume Safe Mode incidents will occur. Searching for security tools that enforce policy within Safe Mode proves futile.

The solution is pragmatism, understanding that Safe Mode cannot be secured in the traditional sense, and we cannot pretend otherwise.

If it is assumed that a system will, at some point, blue screen, and that Safe Mode will, in turn, be breached, the professional obligation becomes obvious. Only by designing resilient networks and endpoints can we ensure that attackers gain nothing of value—even when they have their hands on a deliberately permissive operating environment.

In practice, reducing the impact of Safe Mode abuse depends on two non-negotiable controls. First, everything that happens in standard operation must be governed by strict Zero Trust principles. Applications must be authorized, privileges tightly constrained, access controlled, and persistence mechanisms blocked.

REDUCING THE BLAST RADIUS

If an attacker is not given the opportunity to stage tools, modify behavior, or establish a network foothold, Safe Mode becomes far less exploitable. The potential for attackers to use Safe Mode to interfere with a machine directly is reduced, as is their ability to force target machines into a failure state in the first place.

The second control surrounds data. Specifically, endpoint data must be protected independent of

HOW THREATLOCKER® REDUCES THE RISK OF SAFE MODE ABUSE

Safe Mode disables most security software, but it is important to remember that successful Safe Mode attacks are almost always prepared in advance. ThreatLocker limits that preparation by enforcing Zero Trust controls during standard operation—at the very moment attackers are attempting to stage tools, modify configurations, and establish persistence.

Application Allowlisting ensures that only explicitly authorized applications, scripts, and libraries can execute, preventing attackers from introducing offline tools or boot-time payloads that could cause a system to fail.

Elevation Control removes local admin rights by default, limiting the ability to alter boot settings, drivers, or recovery configurations.

Ringfencing™ restricts how approved applications can interact with files, credentials, and system resources, reducing opportunities to harvest sensitive data or move laterally.

On servers and critical endpoints, **ThreatLocker Storage Control** adds a safeguard by blocking unauthorized access to sensitive directories.

When combined with full-disk encryption, these controls ensure that while Safe Mode may disrupt operations, it should not expose data or compromise the network.

For years, security teams have sensibly focused on controlling who has administrative access, but far less attention has been paid to what administrators can do once that access is granted

the operating system state. Servers are a common target because they are perceived as stable, trusted, and always-on.

Domain controllers, file servers, application servers, and virtualization hosts often hold the most sensitive data in the environment and operate with elevated privileges by necessity. When these systems are forced into Safe Mode, the consequences are amplified: A single compromised server can expose credentials, disrupt authentication, or provide a pivot point into the wider network.

Full-disk encryption with BitLocker is not optional. If forcing a machine into Safe Mode provides access to files, credentials, or confidential data, it means your security procedures have failed long before a crash. Safe Mode abuse still disrupts operations on encrypted systems, but its impact is far less damaging.

DISRUPTION VS. CATASTROPHE

To keep these two pillars aloft, security leaders must be honest about the tradeoffs they will need to make. There is an element of accepting fate, admitting that Safe Mode incidents will happen and disrupt business continuity. Security teams will need to intervene manually to bring machines back up, and the recovery process may be long-winded.

But only to an extent: Recovery from a Safe Mode attack, among a well-protected network, is a matter of hours, not days.

And perhaps most importantly, that recovery can be measured in time, rather than the vast cost of breach notifications, regulatory penalties, or network-wide disruption. Ultimately, the inconvenience of putting a single system back online is insignificant compared to the impact of an attacker gaining free access to an unprotected network.

The argument for Zero Trust is not a technical debate but a professional baseline standard. Security professionals know about the dangers of Safe Mode, and if forcing a machine into Safe Mode is enough to compromise it, the problem is not the blue screen; it is the security architecture that allowed that to happen in the first place. There is no excuse for ignoring a glaring vulnerability.

TRY BEFORE YOU APPLY

ThreatLocker rule simulation is designed to give administrators clarity to avoid security controls failing due to enforcement without context. When administrators have a clearer insight before rules are put into action, controls will be more effective thanks to better informed and intentional enforcement decisions

Security controls fail when they are enforced without context. ThreatLocker rule simulation is designed to give administrators clarity before those rules are put into action, ensuring enforcement decisions are informed, intentional, and disruption-free.

Application Control is a powerful security measure, but moving to enforcement too quickly can introduce unnecessary risk and cause unintended downtime.

Even the most well-managed environments have blind spots, and it can be difficult to understand the way proposed policies will behave; rule simulation basically provides a pre-enforcement checkpoint, allowing security teams to observe policy outcomes without changing the way systems operate.

Rather than focusing on approval or installation, simulation is centered on impact analysis. It reveals which files, applications, or processes would be denied if Secure Mode were enabled. This gives administrators the opportunity to validate their rules against real activity instead of relying on assumptions. Administrators can identify and address potential issues early, before they affect productivity or business continuity.

At the heart of this process are Simulate Deny logs. These logs show every execution that would have been blocked in practice, helping administrators focus their attention where it matters most

From a governance perspective, rule simulation supports a more disciplined rollout. Security teams gain confidence in their policies, leadership gains assurance that risk has been assessed, and end-users are protected from abrupt changes

At the heart of this process are Simulate Deny logs. These logs show every execution that would have been blocked in practice, helping administrators focus their attention where it matters most.

The system clearly and consistently surfaces unusual application behavior, frequent file changes, and software that does not align with static rulesets. With this visibility, teams can investigate why a denial would occur and determine whether it represents legitimate behavior or unacceptable risk.

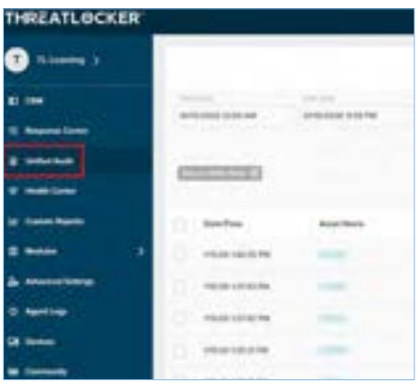
Many business-critical applications regularly update components, generate new dynamic-link libraries (DLLs), or dynamically compile files at runtime. From a security standpoint, this behavior can appear suspicious, even though it is technically expected. In simulation, these patterns can be reviewed calmly and methodically, without the pressure of live enforcement.

Simulation also plays an important role in identifying unnecessary exposure. Non-business software, legacy utilities, or unauthorized tools often appear during this phase, and it provides a natural opportunity to clean up the environment before instituting policy changes. This strengthens overall policy quality while reinforcing the value of Application Control.

From a governance perspective, rule simulation supports a more disciplined rollout. Security teams gain confidence in their policies, leadership gains assurance that risk has been assessed, and end-users are protected from abrupt changes. The point is that policy enforcement should be a deliberate step, not an experiment.

By separating validation from enforcement, ThreatLocker Simulation Mode enables organizations to introduce strong application control with confidence, achieving protection that is both effective and operationally sound.

Simulating a deny operation with ThreatLocker



Navigate

In the ThreatLocker Portal, navigate to the Unified Audit page in the left bar

Simulate

Using the Advanced Search function, opt to run a deny simulation

Confirm

Review the simulation outcome with a detailed audit, then confirm your choice

INSTALLATION MODE GRANTS CONTROLLED FLEXIBILITY

ThreatLocker® Installation Mode eliminates the guesswork from software deployment—capturing every dependency automatically so teams stay secure without workflow disruption

Application control is most effective when it is precise. Precision is not always easy to come by, particularly when installing complex or unfamiliar software, but ThreatLocker Installation Mode is an invaluable assistant.

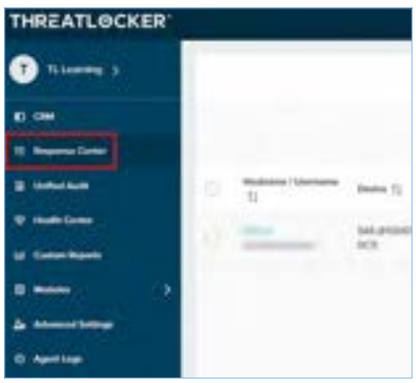
Installation Mode is designed to safely bridge the gap between strict security and operational reality. This solution allows teams to install software or updates while automatically capturing everything those applications do, as well as everything required for them to function.

Installation Mode temporarily relaxes application restrictions on a specific endpoint while closely monitoring system changes. During this window, ThreatLocker tracks every executable, dynamic-link library (DLL), script, and dependency introduced or modified by the installer.

Once the installation is complete, those components are automatically cataloged and added to the appropriate allowlist. This will ensure that the application can run normally moving forward, without permanently weakening security controls.

Installation Mode is highly practical. Ideally, new software is approved using built-in applications or verified in a controlled testing environment. In the real world, however, that is not always feasible. Some enterprise applications include thousands of files and dependencies that are difficult to predefine. Others cannot be easily replicated in a lab or test environment due to licensing, infrastructure complexity, or business constraints.

Installation Mode with ThreatLocker



Alert

To respond to a user's request for application installation, head to the Response Center

Response

The application can be approved in Installation Mode, temporarily lowering restrictions

Installed

Once approved, the user is informed on the endpoint and can run the application

In these scenarios, manually approving each component would be time-consuming and error-prone. But with Installation Mode, they can be automatically cataloged and allowed, while security teams scrutinize those components for potential issues.

Installation Mode is particularly useful for large-scale updates, where installers touch vast numbers of system files. It is also valuable when dealing with vendor software that updates frequently or behaves differently across environments.

Rather than guessing which components will be required, administrators can allow the installation to run once under supervision and subsequently let ThreatLocker learn what is needed.

Instead of permanently broadening application permissions, Installation Mode grants temporary flexibility with a clear purpose and defined scope

Importantly, Installation Mode is not a blanket bypass. It is time-bound, deliberate, and auditable. Protection is partially relaxed for the duration of the installation, and only the files and changes observed during that window are trusted afterward. This reduces the risk of abuse and ensures that security posture returns to its regular state as soon as the task is complete.

From a security perspective, this approach aligns with the principle of least privilege. Instead of permanently broadening application permissions, Installation Mode grants temporary flexibility with a clear purpose and defined scope. The result is a balance between operational efficiency and strong application control.

This is a functionality that exists for the moments when traditional approval methods are not practical. Installation Mode provides a controlled, secure way to handle complex installations while preserving the integrity of a Zero Trust security model, making it an essential tool for administering real-world IT environments.

HOW TO DEFEND AGAINST SMB ATTACKS

Server Message Block (SMB) is probably the most common network file sharing protocol. It is ripe for abuse, but enforcing the right policies can make it safe

Modern endpoint security policies do an excellent job of stopping malware from running locally. Controlling application access, privilege elevation, and the execution of scripts and exploits make it extremely difficult for an attacker to deploy ransomware directly on a protected machine.

But many organizations overlook quieter, just as dangerous, off-machine attack paths that may not be covered by standard endpoint controls.

Ransomware does not always need to run on a server to cause damage. An untrusted device, which could be anything from an Internet of Things (IoT) system to a compromised personal laptop, could access shared folders over SMB and encrypt files remotely. In this scenario, the server itself remains clean, but the damage to it is just as severe.

By combining default-deny networking with identity-based trust validation, ThreatLocker® Network Control protects file servers from one of the most common and damaging ransomware techniques

The ThreatLocker Network Control solution is designed to close this gap. Rather than assuming that everything on the internal network is trustworthy, it enforces a Zero Trust approach to network access. The goal is simple: Only trusted, managed devices should ever be allowed to communicate with sensitive services like file servers, and even then, within strict guardrails.

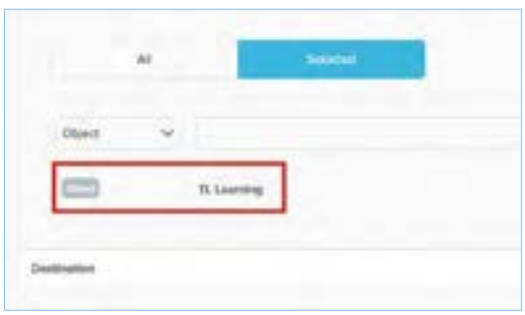
Creating a default-deny policy with Network Control

Create

Go to ThreatLocker Network Control, and click the button to create a new policy

Block

Set the action to “Deny,” leaving all other options blank, and click “Create”



Override

Allow ThreatLocker-protected devices as exceptions as and when required

The most effective strategy starts by blocking inbound network access by default. Servers and workstations typically do not need to accept unsolicited connections. By denying inbound traffic, especially through high-risk services like SMB, you dramatically reduce the attack surface available to ransomware and lateral movement.

Of course, file servers still need to be accessible, so a policy-driven approach is critical. Instead of opening SMB ports broadly or relying on IP-based allowlists, access can be limited strictly to trusted devices within the organization. This eliminates reliance on static IP addresses, which are unreliable in Dynamic Host Configuration Protocol (DHCP)-based environments and frequently exploited by attackers with a foothold on the network.

ThreatLocker validates trust dynamically. When a device attempts to access a protected server, the server verifies in real time that the connecting system is a managed, trusted endpoint. If it is, access is permitted. If it is not, the server is effectively invisible, leaving no opportunity to remotely encrypt data.

This model prevents unmanaged or rogue devices from ever reaching SMB services, even if they are physically connected to the same network—a vital protection given SMB’s continuing history of exploitation and compromise.

It also ensures continuous enforcement of trust. If ThreatLocker is somehow removed, disabled, or tampered with on an endpoint, that device immediately loses access to network resources.

By combining default-deny networking with identity-based trust validation, ThreatLocker Network Control protects file servers from one of the most common and damaging ransomware techniques. It shifts network security away from assumptions and toward verification, ensuring that only the right devices in the correct state can ever touch critical data.

THE ZERO TRUST SHORTCUT

Bahrain Maritime & Mercantile International (BMMI) is one of Bahrain's longest-established and most diverse listed companies. That diversity creates a security reality in which "one size fits all" controls rarely fit anyone—different users, roles, systems, and endpoints travel between offices, sites, and homes, creating a vast attack surface. For BMMI Senior IT Manager Ali Al Jabal, the solution was not to wait for a major incident; it was to deliberately raise security maturity and build a stable foundation for a broader Zero Trust journey

For readers who don't know BMMI, what kind of organization are you securing, and what makes it challenging to protect?

BMMI is one of the oldest companies in Bahrain. We operate across retail, hospitality, and logistics, including major global brands. We also run one of the best-known supermarket brands here.

From an IT operations perspective, we support the entire group, from user endpoints through to servers and cloud services. We support warehouse systems during stock takes, retail infrastructure, and even weighing scales for food items. The environment is broad, and the endpoint estate is highly varied.

That diversity is important. The commonalities between users can be quite short because the business units are different. When you have many user types, tools, and workflows, security becomes harder to standardize and monitor.

How does digitalization change the security picture when you're dealing with logistics and cross-border operations?

Logistics has historically run on legacy infrastructure. When we talk about digitalizing that part of the operation, the scope extends outside borders to shipments and services connecting across regions and continents.

That creates a challenge: streamlining security operations while expanding the operational footprint and relying on systems that may not be under our direct control. As the scope grows, you need security controls that remain consistent, even when the endpoints are remote or moving between locations.

This is where ThreatLocker® becomes relevant, because the policy enforcement sits with the endpoint. You can operate across different places and configurations while still maintaining strong control. In logistics, you don't want your security posture to depend on whether a device is "inside" a particular network perimeter.

Roughly, how large is the endpoint estate you're protecting today?

We're talking about hundreds of endpoints—around 800 for computer endpoints alone. That doesn't include Internet of Things (IoT). The key point is that it's not small, and it's not static. Some endpoints travel between office and home. Mobility matters because it affects how you design security controls.

Established in Bahrain in 1883, BMMI is a global group operating across retail and distribution, hospitality, and contract services

> “ThreatLocker stands apart clearly after you experience the operational gaps of legacy tools. For mature security teams, the difference is decisive

What pushed you toward a Zero Trust approach—and why ThreatLocker?

Zero Trust on endpoints was a first step towards a broader Zero Trust architecture. But ThreatLocker gave us a shortcut that allowed us to move faster.

When you evaluate endpoint security, built-in tools can appear sufficient on paper. The difference shows up when you need mature security reporting, close monitoring, and real investigation workflows. In those conditions, you start realizing where built-in or legacy tools create operational friction or visibility gaps.

ThreatLocker stands out in environments where security maturity matters. If you haven’t lived through the limitations of other tools, you may not immediately appreciate why it’s different. But when you have, the advantage becomes clear.

The choice to use ThreatLocker wasn’t difficult. Application Allowlisting and endpoint-level security rules reduce overhead by following the endpoint wherever it goes. You don’t want continuous alerting just to be confident that endpoints are behaving. It’s a complete endpoint security solution, which consolidates controls that would otherwise be spread across multiple systems.

What’s the major difficulty of built-in tools?

For the IT team, consolidation matters. One portal, one solution, where you can see the security aspects of endpoints without adding unnecessary complexity.

The issue is whether they provide what a mature security operation needs. Take Windows Firewall. Microsoft will tell you it’s there and can lock down the network. But it can’t give you high-level feedback; built-in tools often don’t reflect the way security teams work.

There’s also the operational reality of large vendor ecosystems. When security tooling is consolidated into a giant tenant, a platform-wide update can introduce subtle configuration drift. You want your security controls to stay consistent even when you upgrade to a bigger service.

BMMI specializes in the distribution, wholesale, and retail of food and household goods

> When people hear “complete endpoint security solution” they expect complexity. But consolidating multiple controls into one platform made it more peaceful to operate

What convinced you ThreatLocker would deliver?

When we started talking to ThreatLocker, I already knew the questions I had in mind about protecting our infrastructure. So, I asked those questions upfront and translated them into features: reporting, administration capability, investigation support, and policy control.

ThreatLocker committed to addressing the gaps we had experienced with previous tools. They demonstrated key requirements through a proof of concept. The proof of concept mattered because it’s one thing to read claims, but another to see whether the tool behaves as you need it to.

What was important was not only capability, but also whether it would be manageable. When you consolidate application, network, storage, and Ringfencing™ controls into a single system, someone might assume it becomes harder to operate. In our experience, it became easier because it’s integrated and consistent.

Zero Trust often requires a mindset shift. How did your team adapt?

ThreatLocker helped us consolidate. Because of the business’ diversified nature, the diversity of users could have made it difficult to move toward Zero Trust. ThreatLocker brought that diversity to an acceptable level from a security perspective.

Before ThreatLocker, some of these controls were not available in our environment, or they weren’t used properly. That creates a lot of after-the-fact work like monitoring, follow-up, and reporting to management.

With ThreatLocker, moving toward Zero Trust felt like switching from unsecured to secured mode—a cleaner transition, with less reliance on constant manual oversight. Importantly, we didn’t wait for an attack; we wanted to elevate our level proactively and reduce the risk of roaming devices bringing malware from outside environments.

What difference has it made operationally?

I will give you a practical example. I don’t manage ThreatLocker administration day to day, but when our lead ThreatLocker engineer went on annual leave, I didn’t even have a formal handover session. I had only seen the interface a few times, but I was able to jump in. I could navigate it, respond to requests, handle approvals, and continue operations without disruption.

When people hear “complete endpoint security solution” they expect complexity. But consolidating multiple controls into one platform made it more peaceful to operate. Previously, these controls were spread across three or four systems, each with its own complexity. Now they’re unified.

> With ThreatLocker, moving toward Zero Trust felt like switching from unsecured to secured mode—a cleaner transition, with less reliance on constant manual oversight

FEATURE PROFILE

Ali Al Jabal is the Senior Manager of Information Technology for BMMI Group, leading an expert team covering the company's broad spectrum of IT assets across multiple divisions and diverse business activities.

His team oversees system engineers and support staff responsible for end-user environments, servers, cloud services, and operational systems supporting everything from warehouses to retail infrastructure. A veteran of the IT industry with a special interest in organizational transformation, Al Jabal began his career helping to establish the next generation of IT experts as a lecturer at the Bahrain Training Institute. Since then, he has directed IT operations at major businesses, including the National Bank of Kuwait, BMI Bank, and SNB Capital.

The BMMI Shipping Services division delivers reliable solutions for ports, cargo, and marine services across industries

And I must highlight the experience we have with support. The ThreatLocker Cyber Hero® Team has been consistently available and responsive. We raised requests that other vendors might call "non-standard," but nothing was dismissed.

If I had to summarize it for peers, ThreatLocker stands apart clearly after you experience the operational gaps of legacy tools. For mature security teams, the difference is decisive. And it gave us the breathing room to strengthen other security controls across the organization, not just endpoints.

NEXT PAGE

Without rigid cybersecurity, rapidly digitalizing global supply chains are vulnerable to attack. Find out how Zero Trust changes the game for logistics

SUPPLY CHAIN RESILIENCE **MATTERS**

The next chapter of global logistics depends on shipping cybersecurity solutions that fit the bill

The container ships, aircraft holds, heavy goods vehicle (HGV) yards, and parcel hubs of the logistics industry keep the global economy running, and if something goes wrong, they bring it to a halt. In what is now an overwhelmingly digital world, cyber-attacks can strike anywhere and can have a knock-on impact that stretches all the way through the supply chain. When logistics stops, the world notices. Logistics has moved fast to match the demands of the connected world.

Even pre-pandemic, the rush to full digitalization was seen as a necessity. Talking to the Wall Street Journal in 2018, then-CEO of Maersk, Søren Skou called the idea of smart transportation "more than moving cargo from A to B. Digitization within the transport and logistics sector means seamless service to our customers, visibility in the supply chain, and driving a more efficient business."

USD 9 trillion

in value is estimated to have been unlocked by transport digitalization across the G7‡

CHOKEPOINTS, PHYSICAL AND DIGITAL

The speed and breadth of logistics' growth have left the industry brittle, not just to infamous incidents like the 2021 blockage of the Suez Canal by the stranded *Ever Given*—a disaster which cost an estimated USD 400 million per hour in trade‡—but also to digital disruption, which could be equally damaging.

A cyber shutdown may not be as visible as a grounded container ship, but the financial drag can be comparable. As route planning, terminal operations, customs clearance, fleet telematics, warehouse robotics, and shipment tracking now depend on connected software, contributing greatly to increased revenue in the sector, a cyberattack on a logistics operator means more than it ever has.

Containers sitting on quays, trucks stuck in depots, and production lines waiting for parts—these hit the reputation of logistics operators, cause backlogs that efficient just-in-time facilities are often unable to accommodate and have a massive impact on the world at large.

Transportation represents a high-value target for attackers, and criminal attention is growing. IBM X-Force reports a sharp rise in the share of cyber incidents between 2023 and 2024, with transportation services leapfrogging government and healthcare targets to become the fifth-most attacked sector.

THE MALWARE WAKE-UP CALL

A look back at the 2017 *NotPetya* malware campaign highlights the fragility of the sector even in its early days of digitalization. Maersk was hit by the wiper malware, with critical systems disrupted and around a third of its shipping lines frozen for weeks—the company estimated the incident cost between USD 200-300 million‡ in lost revenue, though it has been heavily speculated that those figures were reported on the low side.

FedEx was forced to implement a temporary halt on market trading of subsidiary, TNT Express, after *NotPetya* brought down the networks of domestic and regional distribution centers.‡ Destroyed records at consumer goods company Reckitt Benckiser forced it to halt production and shipping, causing its growth to contract.‡

This fragility served as a lesson. "The state-sponsored investment in some of these weapons is beyond the capability even of global companies like ours to defeat," stated Maersk CISO Andy Powell at a maritime conference following the incident, suggesting that businesses "will not stop every attack [...] What you have to develop is your ability to respond."‡

Maersk was not unprepared, either—only by virtue of an offline backup stored in Lagos was it able to restore systems within nine days.

LOGISTICS IN THE FIRING LINE

NotPetya was not an outlier. In the years since, cyberattacks have repeatedly demonstrated how tightly wound modern logistics has become. In 2021, South Africa's state-owned Transnet declared force majeure after being hit by ransomware. The attack halted operations at key container terminals, including the country's largest, Durban, and caused extensive traffic queues at the terminals' closed gates.

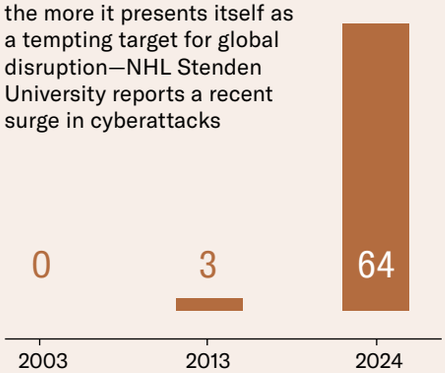
In July 2023, the Port of Nagoya—responsible for moving more than 2.5 million twenty-foot equivalent units (TEUs) of container traffic and over 150 million tons of cargo through Japan annually—was paralyzed for days when ransomware froze its container management platform, leaving haulers unable to collect or drop off freight.‡

The industry's growing dependence on third parties only amplifies the risk. Research from the World Economic Forum's Global Cybersecurity Outlook 2025 identifies supply-chain interdependency as the top cyber risk for large organizations, with 54% of global businesses citing vulnerabilities among third-party partners as their biggest barrier to resilience.

What makes logistics unique is that these vulnerabilities appear in the middle of live operational workflows. When Expeditors International, a USD 16 billion freight forwarder, was hit by a cyberattack in 2022, the company shut most of their operating systems down around the world to contain the breach, causing global delays—all because the data was not where it was supposed to be.

MARITIME CYBERATTACKS‡

The more connected the maritime sector has become, the more it presents itself as a tempting target for global disruption—NHL Stenden University reports a recent surge in cyberattacks



WHERE OT MEETS IT

Logistics operations touch everything, and everything is critical: information systems (IS), operational technology (OT), automation, physical movement, and, most importantly, people. It is a blend of physical and digital dependency which, when compromised, can directly impact worker safety. A disabled port crane or an unpredictable conveyor line puts operators directly at risk.

Beyond the obvious dangers of malfunctioning equipment, a compromised digital workflow can create subtler hazards, and even small deviations from expected behavior can be dangerous. When attacks alter the integrity of data, they threaten the humans working around the machines executing that data.

This is why cyber incidents in logistics routinely escalate beyond straightforward technical issues. They become safety issues, liability headaches, and continuity crises. A breach can mean shut gates, stalled machinery, unsafe conditions, and a chain reaction across customers, carriers, suppliers, and end-consumers.

> “
>
> More than moving cargo from A to B, digitization within the transport and logistics sector means seamless service to our customers, visibility in the supply chain, and driving a more efficient business

OPERATIONAL CHANGE FOR GOOD

Zero Trust is now being embraced as operational doctrine and a commercial necessity. In essence, warehouses and ports are classic flat networks. They feature enormous address spaces. A compromise on one forklift terminal or a single handheld scanner could move rapidly into core systems. Zero Trust reverses the assumption that devices on the network (or in that warehouse, or port) are safe. Instead, every user, device, and application is treated as untrusted until proven otherwise—and even then, only within the limits of what it specifically needs to do.

In broad terms, Zero Trust already maps directly onto the structure of the logistics industry. Forklifts are restricted to lanes; only approved personnel can drive the forklifts; cranes obey defined zones; drivers follow assigned routes; automated systems operate within programmed tolerances. These things should be constrained, predictable, and incapable of wandering into areas they have no reason to access—and digital systems should behave in the same way.

By applying Zero Trust principles, logistics operators secure all users, devices, and systems to enhance efficiency and reliability

Zero Trust secures warehouses by restricting access and movement, ensuring safe operations within defined boundaries

EMPHASIZING CONTAINMENT

Keeping attackers out is vital, a deny-by-default approach, means that what gets allowed into a network is a carefully considered exception, which should eliminate any vector of attack. However, if an intrusion does occur—and the Zero Trust framework broadly assumes that it already has—its impact must be tightly contained. But frameworks do not enforce themselves.

Logistics operators need tools that can apply those principles directly onto fast-moving, always-on environments—across OT gateways, terminal servers, warehouse PCs, port systems, fleet devices, and the myriad third-party integrations that tie them together.

The ThreatLocker® solutions closely align with operational reality. By defining exactly what each device, user, and application is permitted to do—and blocking everything else by default—ThreatLocker translates Zero Trust from theory into day-to-day control.

It gives logistics operators the ability to lock down execution, restrict communications, protect critical data, and isolate compromised assets before they can trigger the kind of cascading failures that have defined the industry's worst cyber incidents.

80%

of transport leaders have increased investment in technology since 2020‡

THREATLOCKER: ZERO TRUST THAT WORKS AT THE SPEED OF LOGISTICS

The policy-based model of ThreatLocker supports the always-on nature of logistics. It protects OT, IT, cloud, and IoT systems without demanding downtime or interrupting live operations—essential in ports, hubs, and distribution centers where seconds matter.

Application Allowlisting
Lock down warehouse PCs, management servers, and OT gateways so they run only approved applications. Unknown executables, ransomware loaders, and unauthorized scripts simply cannot run—even if an attacker gets inside.

Ringfencing™
WMS applications may need to access a database, but not the internet. Label printers have no business spawning PowerShell. Enforce strict behavioral boundaries, contain compromised processes, and stop them from pivoting across the network.

Storage Control
Protect critical operational data: manifests, customs documents, routing tables, and inventory records. Only authorized applications and authenticated users can alter them, blocking both mass encryption and subtle manipulation of supply-chain data.

Network Control
Replace flat networks with granular, software-defined segmentation. Forklift terminals should talk only to their operational servers; port-side OT systems stay isolated from office networks; contractor laptops access only the asset they are responsible for.

Elevation Control
Give engineers the exact privileges they need—for a specific task, for a specific time window—and no more. Remove standing admin rights across distributed sites and prevent attackers from abusing elevated accounts.

Centralized audit and visibility
ThreatLocker monitors the entire logistics estate, providing a clear audit trail for investigations and helping demonstrate compliance with frameworks including the International Standards Organization/International Electrotechnical Commission (ISO/IEC) 27001, Network and Information Security (NIS)2, Customs-Trade Partnership Against Terrorism (CTPAT), and customer-driven security requirements.

CONTROL BEATS TRUST

Modern attacks abuse trusted admin tools. Locking down execution—not just tool access—is now an essential component of endpoint security

Successful breaches increasingly exploit legitimate tools. Attackers overwhelmingly live-off-the-land, abusing legitimate administrative tools that already exist on every Windows system. Command shells, scripting engines, and built-in management utilities are trusted, powerful, and almost always unrestricted.

In other words, the most dangerous software on your network is not something attackers bring with them; it is already inside the environment.

As attackers' tactics have changed, defensive strategies must evolve with them. For years, security teams have sensibly focused on controlling who has administrative access, but far less attention has been paid to what administrators can do once that access is granted. This blind spot has quietly become one of the most reliable paths to compromise.

TARGETING TOOLS, NOT USERS

Tools such as PowerShell, WMI, PsExec, certutil, and rundll32 exist to help administrators manage systems efficiently. Unfortunately, they also provide attackers with everything they need to move laterally, disable security controls, exfiltrate data, and establish persistence without ever dropping a traditional malware payload.

Once an attacker gains admin access—through common methods like phishing, credential reuse, token theft, or multi-factor authentication (MFA) fatigue—a standard environment often assumes those actions are legitimate. Traditional security models implicitly trust administrators, even though attackers actively target such accounts to abuse that trust. But since admin tools are high-risk assets, treating them as universally safe simply because they are built into the operating system is no longer defensible.

FROM TRUST TO CONTROL

Modern environments require a different mindset that assumes compromise is inevitable. The focus is on reducing what an attacker can do after that happens. That means a move away from blanket admin access toward explicit, automated, and contextual control over admin activity, making administrative capability intentional, not default.

Admin tools should be available only when they are needed, only for the task at hand, and only under the right conditions. Everything else should be denied

by default. This approach reduces the reliance on guesswork and human discretion in security decisions. Administrators do not need to tread carefully at every moment. Security teams do not need to rely on perfect behavior. The controls enforce the rules automatically.

LOCKING DOWN WITHOUT BREAKING IT

Control starts with understanding what is being used. Many organizations do not know which admin tools are regularly used versus those that are simply present because they have always been there. Once usage is understood through a thorough audit, meaningful restrictions can be applied.

Application control plays a critical role in setting the rules. PowerShell, for example, does not need to be universally available in interactive mode. It can be restricted to signed scripts, limited to specific workflows, or blocked entirely for users with no legitimate need for it. Command shells can be tied to specific parent processes or administrative tasks instead of being freely accessible.

Equally important is how privilege is granted. Permanent local admin rights dramatically increase the risk and give attackers unlimited time to operate. Application-based, time-limited elevation provides a more robust approach, granting admin privileges only for a specific action and automatically revoking them once the task is complete. When access expires, so does the opportunity for abuse.

AUTOMATE ADMIN TOOL RESTRICTION WITH THREATLOCKER®

ThreatLocker enables organizations to lock down admin tools without relying on manual processes or user discipline:

ThreatLocker Application Control for admin tools
Explicitly control PowerShell, command shells, scripting engines, and system utilities, even when launched by administrators.

Just-in-time privilege elevation
Grant admin rights only when they are needed, for specific applications or tasks, and automatically revoke them when no longer required.

Context-aware policies
Apply stricter rules for remote locations, unmanaged networks, or high-risk scenarios without impacting normal operations.

Auditability and control by design
Every elevation request and admin tool execution is logged, reviewed, and enforced automatically. No assumptions, no shortcuts.

Admin tools should be available only when they are needed, only for the task at hand, and only under the right conditions. Everything else should be denied by default

DESIGNING FOR EDGE CASES

It is not always easy to deviate from the status quo, given the potential for any change to introduce operational friction. Many cite remote workers, IT staff, and emergency scenarios as reasons why admin controls would not work in practice. That view is short-sighted; in reality, these are the exact scenarios where stronger controls are needed.

Admin tool usage from remote or untrusted locations should carry higher scrutiny. An administrator working from a secured corporate network does not present the same risk profile as one connected from a hotel or home network. Context-aware controls can enforce stricter restrictions, require additional approval, or block specific tools entirely based on location or device trust.

Time-locking is another underused but powerful safeguard. If an administrator needs elevated access for 20 minutes to complete a task, that is fine, but that access should not persist for the rest of the day. Time-bound permissions dramatically reduce attacker dwell time and limit the potential damage caused by compromised credentials. Even emergency or “break-glass” access can be handled safely when it is auditable, tightly scoped, and automatically revoked.

HUMAN-AWARE SECURITY

While administrators are skilled professionals, they are also human. They click links, reuse passwords, and make mistakes under pressure. A security strategy that depends on perfect behavior will eventually fail, and the practice of controlling admin tools accepts this reality. It assumes compromise has already happened, and limits what can happen next.

When attackers lose access to the tools they rely on most, breaches become harder to execute, easier to detect, and far less damaging. In today’s threat landscape, controlling admin access is fundamental. Controlling admin tools is what turns Zero Trust into real-world protection.

ALL HANDS ON DUCK

The USB Rubber Ducky has been a potent threat for over 15 years—innocent on the surface but paddling fast underwater

Tired of performing repetitive tasks in his IT job in 2010, Hak5 Founder Darren Kitchen took a creative route to efficiency.

Using USB hardware modified to pose as a standard keyboard, Kitchen used scripting and keystroke injection to automatically send commands to the servers and printers he was administering. The idea quickly morphed into the USB Rubber Ducky, the first commercially available keystroke injector.

Despite looking like an innocent USB flash drive, the Ducky could inject 1,000 words per minute, automatically firing when plugged in.

"You plug it in, and it acts like a keyboard," explained Kieran Human, ThreatLocker® Special Projects Engineer and head of Rubber Ducky labs at Zero Trust World. "Anything you can do with a keyboard, this can do. It can open PowerShell, delete files, exfiltrate data, or encrypt it. You don't even need elevated privileges to fire any of this stuff off, because you're technically not executing scripts. You (or, more correctly, the Ducky) are just typing."

Because the device identifies itself as a standard human interface device (HID), the operating system grants it the same level of trust and access as a user's actual keyboard. No admin rights required, no suspicious binaries dropped, no obvious malware signatures created.

Limitless automation

There is almost no limit to what a USB Rubber Ducky can do, as Human explained. "You just create the PowerShell script and then run it. It could be literally anything. You can use it for any repetitive task; we had 500 computers that had to get connected to the internet, and instead of having to go to each one manually, I made a script that opened PowerShell and connected them automatically and did a few other fixes."

Of course, not every use is quite as benign. “In my lab sessions, I’ve put together a script that will take screenshots of your computer every 10 seconds, or one that copies your clipboard every minute and uploads it. There is another one that will detect if you copy a Bitcoin address and then switch it with a fake one. I’ve even managed to put ransomware on a Ducky. One major endpoint detection and response (EDR) vendor initially detected it, but after I split it up and made a couple of changes, they couldn’t see it. I ran it across multiple EDRs—the big EDRs you hear about—and none of them detect it. It’s straight ransomware.”

> **“Anything you can do with a keyboard, Rubber Ducky can do. It can open PowerShell, delete files, exfiltrate data or encrypt it**

Why traditional security tools fail

This is the uncomfortable truth: Behavioral security tools are trained to detect malware, not a user typing at lightning speed. And since blocking keyboards is not generally an option, the Rubber Ducky cannot be stopped conventionally.

In the years since the product first reached the market, it has evolved significantly, making detection even more difficult. That is true post-attachment, with modern iterations of the Ducky platform able to slow typing to human speed and cadence, avoiding behavioral detection. And it is true of the physical form of the Rubber Ducky, too. Though many versions remain packaged in the familiar USB flash drive shell, some now hide in the limited space usually afforded to e-marker chips in USB cables.

The only practical defensive strategies for stopping Rubber Ducky attacks involve removing the ability of the scripts to do any damage, reducing the attack surface, and containing the blast radius through microsegmentation. “Even if you need access to PowerShell,” explained Human, “using Ringfencing™ properly means it can’t access all your files, and it can’t access the internet. If you don’t need PowerShell, block it with Application Allowlisting. The whole point is that even if the Ducky gets a command through, the application it launches shouldn’t be allowed to do anything it isn’t allowed to do.”

HOW THREATLOCKER NEUTRALIZES RUBBER DUCKY ATTACKS

Even though a Rubber Ducky masquerades as a genuine keyboard, ThreatLocker can neutralize what it attempts to do after the keystrokes land.

Application Allowlisting
Ducky payloads rely heavily on PowerShell, the command prompt, and other script interpreters. Allowlisting ensures that only approved applications can run. If an endpoint does not need PowerShell, block it entirely; if it does, restrict its use.

Ringfencing
Ringfencing isolates applications from one another and from sensitive data. A Rubber Ducky script may successfully launch PowerShell, but ThreatLocker prevents it from reading user documents, connecting to remote repositories, executing unapproved binaries, or exfiltrating content that is outside its permission boundary. The payload may “run,” but it becomes functionally toothless.

Many Ducky scripts rely on outside sources. Even if a Ducky attempts to download a full malicious script from an attacker’s server, which is a common tactic to evade detection, ThreatLocker can block outbound traffic from tools that should not have internet access.

Storage Control
While Rubber Duckies tend to use only minimal storage, many attackers pair HID devices with the capacity of traditional USB drives. ThreatLocker can enforce device-level restrictions to prevent data exfiltration or the execution of unwanted files.

Beyond signatures
Most Rubber Ducky payloads never drop files and are therefore invisible to traditional EDR signature-based detection. Policy-based enforcement stops the behavior, not the specific file.

THE GEEK GIFT

Trojanized open source software (OSS) projects are multiplying—and they are targeting everyone, hackers included

Few threats in the cyber underworld capture the hacker mindset as perfectly as the Trojan horse. The concept of hiding malware behind a trustworthy-presenting front has long been a source of concern. Decades after the idea was conceived, the trojan remains a favored method of attack despite roots in the very earliest days of mainstream computing, the reason is simple—they are effective.

This inherent disguise often allows hackers to outsmart anti-malware software, making trojan attacks an especially dangerous prospect—and as methods have evolved, so have the targets.

Trojan attacks now seriously threaten the open-source supply chain, the public platforms that underpin so much software development.

Trojans now seriously threaten the open-source supply chain, the public platforms that underpin so much software development

Much has been said about the vulnerability of relying upon open-source libraries and freely available code to underpin application development, with hackers able to exploit under-resourced and unmaintained packages. But now, targets are shifting away from poisoning OSS repositories such as Python's Package Index (PyPI) and Node Package Manager (npm) to less obvious targets found on GitHub and SourceForge.[‡]

Bad actors are increasingly turning their attention to exploiting people's inherent trust in OSS. They lace seemingly legitimate software with snippets of malicious code. Recent targets have ranged from end-users looking for Microsoft Office plugins on SourceForge to gamers looking for a cheat code. However, hackers are increasingly happy to target their own.

Hacker vs. hacker

The concept of hacker infighting is not that new—inter-group enmity has long been the fodder of intros and text files—but we have recently seen an increase in the frequency of such attacks. In part, this is a result of less experienced aggressors being lured into honeytraps, so-called "script kiddies" looking for an easy ride, downloading the wrong tool and becoming, themselves, victims.

Most worryingly for security professionals, however, the tools being targeted include the very OSS packages they may consider using to test their own organization's defenses, from white hat hacking tools to pen-testing utilities.

In May and June 2025, two separate hacker-targeting campaigns were detected. One originated from an established bad actor, Banana Squad, which flooded GitHub with more than 60 fake repositories containing trojanized versions of known Python hacking tools.[‡] The other involved a newly identified actor—Water Curse—that hid malware inside build scripts and project files, this time targeting Visual Studio.

Over 76 repositories have been linked to Water Curse over the past two years, revealing that while the threat is newly recognized, it is already well-established. Each new repository shows signs of evolution over previous releases, leading some researchers to term these groups a malware factory.[‡]

Attack vectors revealed

The obvious question, at least beyond the Trojan Horse metaphor, is how this malware gets onto machines and into networks in the first place. The answer is a combination of trickery and persuasion.

Both Banana Squad and Water Curse have manipulated GitHub's trust-building features—stars, forks, subscribers, and so on—to persuade visitors that their packages are genuine. They have leaned into existing, trusted OSS tools that appeal to their target audience, in most cases by forking genuine software, then adding code to the build scripts that launches the attack when the tool is compiled or run.

As a matter of course, cybersecurity professionals will vet any code before downloading and running it. But less experienced users can be caught out by a quirk in GitHub's code display: Because the site does not use word wrap, it is possible to "hide" malicious code off-screen to the right through the clever use of blank spaces. To the untrained eye, the code appears legitimate and therefore safe to download.

How infection occurs

Once the victim believes the repository is safe, they then clone or download the contents as usual before running the build or compilation script. But even here, most malicious scripts are careful not to act in plain sight. When the trojan code is triggered in the otherwise legitimate script, it simply downloads another payload, which then gets to work. This often involves a complex, multistage infection process that, at least initially, goes to great lengths to hide itself.

ThreatLocker provides granular protection designed to stop trojan-type malware before it can ever execute

In the case of Water Curse infections, which target Windows machines, the compromised script contains just one additional snippet of code, which starts the following chain reaction when executed[4]:

Download and execute two scripts:
- *a. Obfuscated Microsoft Visual Basic Scripting Edition (VBScript)*
- *b. PowerShell script*

This main attack involves the use of more PowerShell scripts to disable built-in protections like Defender and System Restore, and deleting any pre-infected shadow copies of files to make detection and removal harder.

It also bypasses Windows User Account Control (UAC) protections to attempt privilege escalation to gain the ability to perform system reconnaissance and install the data-stealing software it needs to achieve its main goal: the extraction of sensitive data from browsers, which is then exfiltrated using public file-sharing channels, in this case Gofile and Telegram.

Those already familiar with ThreatLocker® will note that the majority of this infection procedure would not make it through a well-configured set of policies.

ThreatLocker Application Allowlisting can entirely stop unauthorized scripts from running, blocking the PowerShell and VBS portions of the attack. The ThreatLocker interface also warns administration about applications like 7-Zip, a Russian-based application known to have numerous security flaws, so they can keep it blocked.

Beyond data theft

Establishing infostealers is just one use for these trojans—another is to install backdoors onto target machines through Remote Access Trojan (RAT) packages. This type of malware is designed to give attackers full control over the victim's computer, effectively creating a fox-in-the-henhouse scenario if that computer is part of a larger network, such as an organization or business.

With hackers of all persuasions now actively targeting teams, it only takes one weak link—or one good-intentioned, unwitting security tester—to compromise an entire network

It is this approach that underpinned another recent attack, albeit one that deviated from the norm by not piggybacking on a compromised but genuine tool. When Sakura RAT appeared on GitHub in April 2025, it seemed the perfect tool for hackers looking to attack other machines.

Yet, when cybersecurity researchers took a closer look, they found that not only did the RAT not function as intended, but the malicious code buried inside it actually targeted whoever downloaded and compiled it, creating a backdoor into their own system.

The repository has since been linked with over 141 other GitHub repositories, 133 of which were backdoored. The tools in these repositories targeted a variety of user—mostly gamers—but Sakura RAT was one of 24% that claimed to be malware projects, exploits, or attack tools, in a clear assault on hackers.[‡]

How to protect yourself

Becoming infected by one of these new-breed trojans requires a lot of heavy lifting on the victim's part. Crucially, the user must voluntarily download and run the code, which is not something a security professional would be inclined to do.

But can the same be said for everyone in every organization? With hackers of all persuasions now actively targeting teams, it only takes one weak link—or more likely, one good-intentioned, unwitting security tester—to compromise an entire network.

Relying solely on traditional detection techniques, whether signature- or heuristics-based, is not enough. Trojan attacks tend to do most of their damage in the early hours and days after their release.

Threat actors have mastered techniques to evade behavioral detection, including code-signing and split-stage payloads that flood the system with clean processes to hide what is really going on. Often, the result is that the file is marked "unknown" or "unrecognized," leaving the final decision to the individual who downloaded it in the first place.

The most effective form of protection against this type of behavioral threat is, of course, to take organizational control away from end-users and apply it universally.

ThreatLocker provides layered protection designed to stop trojan-type malware before it can ever execute. At the core is Application Allowlisting, which follows a simple but powerful rule: If it is not explicitly approved, it does not run. This is especially critical with trojans, which disguise themselves as trusted files or ride along with seemingly harmless downloads.

Because ThreatLocker only allows preapproved applications to execute, a trojan—no matter how convincingly it masquerades—gets blocked outright. And even in the unlikely event a malicious file were somehow granted approval, ThreatLocker has additional controls, such as Ringfencing™, which restrict what that process can access or communicate with. That means the trojan cannot spread, cannot reach sensitive data, and cannot call home.

These days, the OSS tool supply chain is too easy for bad actors to game, and it is not possible to stay ahead of it solely by relying on last-chance security solutions that detect threats and block or remove them.

Choose a suite of cybersecurity solutions that only allows what you explicitly trust, and even then, provides strong guardrails to prevent it from breaking out. Do this, and your organization is far less likely to fall victim to the very tools you thought would keep it secure.

FROM LEGACY BROADCAST TO DIGITAL DEFENSE

Modernizing a global media network by rethinking cybersecurity from the ground up

The Eternal Word Television Network (EWTN) is one of the world's largest religious media networks, broadcasting television, radio, and digital content to millions of viewers across more than 150 countries. For decades, it operated primarily as a traditional broadcaster, with limited exposure to modern cyber risk. But as the organization shifted toward a fully digital future, the need for a modern security posture became urgent. When industry veteran Greg August joined as Chief Information Officer (CIO), he found that the organization lacked strategic and tactical capacity, had no dedicated security team, operated with fragmented systems, and struggled with visibility into active distributed denial-of-service (DDoS) attacks from multiple international locations. In this interview, he explains how he rebuilt EWTN's cybersecurity strategy with the help of ThreatLocker®.

> “
> Moving toward digital meant we had increased risks and exposures in privacy, data protection, and safeguarding people’s experience with content consumption

When you arrived at EWTN, what was the cybersecurity situation like?

EWTN had operated for decades in the traditional broadcast world, where cybersecurity simply wasn’t a major concern. You wouldn’t really worry about someone hacking your transmission or hijacking a program in the same manner as websites or enterprise systems. No one knows who’s watching on the other side of a satellite feed, and there’s no personal data trail involved. But once the organization decided to move decisively into a more digital environment, the need for security increased exponentially.

When I arrived, there was an IT team, but absolutely no one dedicated to strategic understanding or the practice of risk mitigation through security implementation. I quickly discovered that we were under a continuous DDoS attack. We lacked a unified picture of what was happening inside the environment.

The beauty of the organization is that, as a faith-based organization, it has grown like a mustard seed in an organic, prolific way. The downside of organic growth is that it can create fragmentation and hyper-verticalized systems and departments, each area taking care of a few things on its own, without a holistic approach.

Moving toward digital meant we had increased risks and exposures in privacy, data protection, and safeguarding people’s experience with content consumption. My goal is to create a digital space and experience where we, as a company, walk with our users without placing demands on them. I would like to build a security model that allows consumers to view our content in privacy.

How did ThreatLocker first come onto your radar?

Right after joining the organization, I had the opportunity to attend the Gartner CIO conference. I had a generalized shopping list of the tools and products I would need to secure a global network. My background has always been steeped in security; I’ve built systems for organizations including the National Association of Securities Dealers (NASD), the Drug Enforcement Administration (DEA), the State Department, General Electric, Walmart, and banks in Africa. I was not window shopping, but rather on a hunt for the right products, ready to move from acquisition to deployment in weeks, not months or years.

When I walked up to the ThreatLocker booth, it did not take long to discover that what they were offering was a unique foundational product to add to the Zero Trust security tool chest we were building for EWTN. Their approach clicked instantly with the problems I knew we had to solve.

What stood out to you about the ThreatLocker approach?

I’ve been a CIO since before social media existed, before mobile devices were part of organizational life. In the early years of my career, the edge was a firewall connected to the internet. Everything else sat on the inside. There was no widespread exposure. Once mobile arrived, every laptop, phone, tablet, and remote

connection became the edge. Managing that explosion is perhaps the greatest security challenge of the last 20 years.

I think ThreatLocker fundamentally changes that geometry. Instead of having all those devices at the edge, we can now pull back toward the core, bringing security control back to the center. That resonated with me immediately because it felt like the kind of foundational, defensive posture we used to seek to build. It represents a genuine shift in capability—a technlogical up-armoring. In the defensive cybersecurity role, if a hacker suddenly shows up with a technological crossbow, I need better armor. It fundamentally differs, and that difference enables organizations to win when the landscape shifts.

Why did you choose the full ThreatLocker platform rather than individual components?

In my view, the unified platform is a very sensible way to adopt ThreatLocker. If you're going to commit to this kind of security model, then you commit fully. The unified platform allows you to eliminate a long list of legacy tools. Not everything, but in a Windows environment you can deploy Microsoft Defender and be far more comfortable and confident with it, as it becomes a genuinely stronger tool when layered with ThreatLocker controls.

I agree with their offering of different solutions, as it provides flexibility to deploy the needed functionality without unnecessary overlap in products within an environment. I was building from the ground up with little concern for legacy investments, so the full ThreatLocker platform was the right choice.

“
In my view, the unified platform is a very sensible way to adopt ThreatLocker. If you're going to commit to this kind of security model, then you commit fully. The unified platform allows you to eliminate a long list of legacy tools

How does ThreatLocker fit within your layered security strategy?

I think of security in depth in much the same way I think about the medieval cities found across Europe. Those old cities had moats, walls, narrow winding streets designed to slow attackers, and multiple defensive rings leading toward the keep. If one wall fell, another one still held. That structure still holds my imagination as an analogy for modern cybersecurity.

ThreatLocker is one of those rings. It isn't the whole city structure, but it's a vital part of the security ecosystem.

Inside our environment, the team jokingly calls our security posture "lighting up the Christmas tree." When something suspicious happens, our systems start lighting up one after another. They interoperate by passing signals across technologies and watching how data moves. ThreatLocker plays a core role in that chain. Danny Jenkins often talks about not relying on AI but on science, and that's exactly how the system behaves. It's a mathematical model of control. Because of that layered approach, we've been able to stop a lot of trouble before it spreads.

EWTN is a global broadcaster. What kinds of threats does that attract?

We work in a global environment and comment on global issues, and that means global actors react. If we report that a particular conflict involves killing civilians, the groups responsible often launch attacks on us. If we highlight human rights violations, the organizations or nations mentioned in our reporting respond aggressively.

At different times, we've seen activity originating from sources in China and Russia, or from what appears to be

With ThreatLocker, this global media organization can adopt a Zero Trust cybersecurity posture

sources associated with traffickers, cartels, and other nation states. Operating in the public eye brings that level of attention. Because of this, we need tools that operate across the entire spectrum, from the very broad to the extremely detailed. The threats come from everywhere, depending on what we have covered and who we may have angered. That is simply the reality of being a global media organization.

You built EWTN's first security team. How did you approach that?

When I arrived, there was no dedicated security team, so I invited my team members to consider pivoting their careers from more generalized network admin to cybersecurity roles. That is something I like to do and have done repeatedly across other organizations. I really like to invite internal people to grow.

The work begins with the invitation and the individuals who accept it. Through traditional training, product research, and gradual implementations, they start to recognize the attack surface of the organization. From there, they can't unsee the challenges, and we begin again to train, implement, and hone the skill of responding to incidents and refining processes.

The transformation wasn't just organizational; it is a personal journey for each of them. Today, we have visibility across our environment and a deeper level of control over it, which was something we did not have before we began this process. At the moment, I'm serving as both CIO and acting CISO. Eventually, the organization will bring in a dedicated CISO and, perhaps, a more narrowly focused CIO, but for now, the duality helps us maintain momentum.

CUSTOMER PROFILE

Greg August has spent 27 years as a CIO, specializing in building technology leadership from the ground up. His background spans government, public affairs, media, and global infrastructure, including serving as CIO for one of the largest lobbying and public-relations firms in Washington, D.C.

At **EWTN**, August currently serves as Global CIO and acting CISO. He is a father, a grandfather, and is deeply involved in humanitarian and community work. He has worked internationally to assist the most vulnerable communities.

What do you enjoy most about your role?

What I enjoy most is inviting people on a journey. I love the moment when someone realizes they can become who they are, perhaps who they are supposed to be. There is a deeply human responsibility in that, and it aligns with how I lead.

Every time I join a new organization, the first thing I ask people is, "What do you want to be when you grow up? How can I help you get from here to there?" I've done this with several hundred people over my career, and many of them return to work with me later in their lives. The individuals I elevate from help desk roles tend to have little visibility and perhaps less control over their careers. Helping them grow is my responsibility while I lead them.

What lesson would you pass on to a peer starting this journey?

Always see the other person. Work for the other more than for yourself. You will never have the perfect network, the perfect systems, or the perfect team. Those things don't exist. What you can have is the ability to influence the person in front of you in a truly positive way.

Over nearly four decades in IT, I've watched almost every system I've ever built disappear—99.999% of them are gone or in the trash. Machines don't matter. Ones and zeros disappear. People matter. Don't let the people around you, or those you are tasked with leading, disappear. The most important lesson is simple: See the person in front of you.

NEXT PAGE

Signal intrusion is far from theoretical. Media has power and hackers will do anything to take it, making cybersecurity a critical part of the broadcast stack

SIGNAL UNDER SIEGE

Broadcast media may be more vulnerable than it has ever been, but a strong cybersecurity posture is key to protecting the medium and the message

Whatever the show or the message, broadcast media is built on trust. Trust that the feed is authentic, that its content has not been tampered with, and that you are tuned in to what you think you are tuned in to. For most of broadcasting's history, that trust was built on physical systems—transmitters, towers, satellite uplinks, and cables—the theoretically immutable infrastructure connecting the broadcaster to the home.

But as the industry has followed the path of technology and now leans less on the airwaves and more on internet protocol (IP), the attack surface has expanded, and the opportunities for attackers have grown with it.

The risk that the world's media could be silenced, hijacked, or manipulated in real time is very real; the same digital transformation efforts that have made modern media agile and globally scalable make it a prized target for attackers.

From hijinks to hostility

The idea of hacking the airwaves has not been born from this new technology, of course. The first TV signal intrusions, beginning in the late 1970s, were more pranks than plots, in line with hacker culture of the time—frequently bizarre interruptions, often seeming comedic in retrospect, localized to individual transmitters.

But whoever controls the feed controls the message. With so many more feeds to control, and so many entities inter-

A BRIEF HISTORY OF BROADCAST BREACHES

1986: "Captain Midnight" vs. HBO
Florida satellite engineer John R. MacDougall, frustrated with rising satellite TV fees, overrode HBO's satellite uplink one April night. For four minutes, American households saw a black screen with white text: "GOOD EVENING HBO FROM CAPTAIN MIDNIGHT. USD 12.95/MONTH? NO WAY!" It was the first known satellite signal hijack.

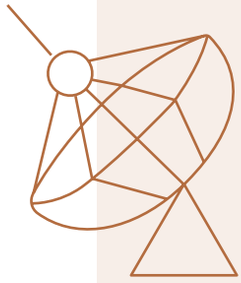
1987: The Max Headroom incident
In Chicago, a masked figure dressed as TV's dystopian icon Max Headroom interrupted two live broadcasts—first WGN's sports segment, then a "Doctor Who" episode on PBS affiliate WTTW—injecting his own bizarre monologue. Investigators never caught the perpetrator, and this remains a symbol of how even analog infrastructure could be commandeered.

2007: Czech TV "nuclear explosion" hoax
Hackers compromised a server at Czech TV channel ČT2 and, during a weather broadcast, injected fake footage of a nuclear explosion near the city of Brno. The video ran for several seconds before being cut. This was a sea change, one of the first publicly known cases where an attacker breached a digital video server rather than a transmitter.

2021: Sinclair Broadcast Group ransomware attack
Sinclair, one of America's largest broadcast groups, suffered a ransomware attack that encrypted servers and disrupted local TV operations across dozens of stations. Commercials could not run, newscasts went dark, and internal systems were locked.

2024–25: Geopolitical broadcast hacks
Recent years have seen more overtly hostile attacks. Iranian state TV was hijacked mid-broadcast to display protest imagery. Ukrainian broadcasters have faced cyber-jamming and deepfake content insertions attributed to Russian actors. The motive is now influence rather than mischief.

The risk that the world's media could be silenced, hijacked, or manipulated in real time is very real



ested in broadcasting propaganda and misinformation, the threat has grown from analog stunts to large-scale, state-backed operations with far darker intent.

Broadcast networks used to be hardware fortresses, purpose-built systems running on isolated hardware. Today, the typical broadcaster leans more on hybrid enterprise cloud tools. Content moves from the camera to the editing suite to the playout server, then over IP to transmitters, streaming encoders, content delivery networks (CDNs), and mobile applications. Each of those steps introduces software, credentials, application programming interfaces (APIs), and third-party integrations—each being a potential attack vector.

Ransomware and downtime

IT infrastructure is crucial to maintaining media continuity. When ransomware struck Sinclair Broadcasting in 2021, the group's transmitters remained untouched, but its IT backbone was crippled. Servers handling scheduling, advertising, and distribution were encrypted, and the attack cascaded from business systems into the live broadcast chain.

In an industry where airtime equals revenue, even an hour offline can cost hundreds of thousands. Sinclair's accounts suggest the attack, which affected operations for several weeks, had a much greater impact, causing at least USD 63 million in lost advertising revenue and USD 11 million in direct costs.[‡] Sinclair's is not an isolated story.

Broadcasters in Europe and Asia have experienced similar disruption. Unlike traditional engineering faults, these are not predictable outages—they are deliberate attacks that exploit the convergence of IT and broadcast control systems. Traditional redundancy offers little protection when the threat sits inside the software stack. Two transmitters will not help if the playout automation that feeds them is encrypted.

In the age of ransomware, continuity depends not on extra hardware but on isolation, containment, and verified execution—the Zero Trust model, in effect.

The broadcast stack goes wide

Zero Trust is especially important considering that modern media networks tend to act more like a digital supply chain than a single company. Production, post-production, advertising, captioning, streaming, and analytics are often handled by separate vendors across different time zones. A single live bulletin might rely on half a dozen cloud services before it ever hits a transmitter.

Each dependency introduces its own risk, new credentials, and APIs that could be subject to compromise. When one link fails, the consequences can cascade across every connected system. Attackers understand this better than most broadcasters do.

In 2015, Russian hackers compromised the internal systems (IS) of French network TV5Monde, interrupting the signal of 12 channels—one key staging point of the bespoke attack was a Dutch company, the supplier of TV5Monde's remote-controlled cameras.

It was later learned that the company's Instagram and YouTube accounts, also part of the attack, were breached through less complex means: Their passwords had been broadcast for all to see, pinned to a board in the background during an interview conducted at a staffer's desk.

Verifying content veracity

The days of disruption for disruption's sake may be behind us. Attackers are no longer content to shut down broadcasts—they are looking to control the narrative.

We have seen this repeatedly in new media. YouTube channels, including large entities like Linus Tech Tips, have had their feed taken over by scammers broadcasting footage of a deepfake Elon Musk, encouraging viewers to buy certain cryptocurrencies. More insidiously, state-backed hackers in Iran recently targeted a streaming platform based in the UAE, inserting an AI-generated newsreader delivering fabricated political messages as news.

We have come a long way from the supposed hysteria which followed Orson Welles' 1938 broadcast of the slightly tongue-in-cheek "War of the Worlds;" this is messaging with serious intent.

Sophisticated digital fakes like Iran's propaganda bot now seriously threaten legitimate pipelines. AI-generated footage is cheap and easy to create thanks to services like OpenAI's Sora, meaning realistic synthetic audio, video, and images can enter the newsroom through freelancers, unvetted third-party feeds, or simply unwitting inclusion.

Once inside a production workflow, the difference between genuine and fake becomes difficult to spot—especially under the immense pressure of producing live news.

That makes cybersecurity an editorial issue, too. Protecting the feed now involves ensuring the authenticity of the information itself through both strict verification techniques and a network architecture that prevents untrusted or modified content from entering production systems unseen.

The need for Zero Trust

The industry's path of digital transformation has not been uniform. Many broadcasters still run decades-old transmitter control systems alongside IP-enabled automation. That mix of operational technology (OT) and information technology (IT) creates blind spots.

Broadcast media, like virtually every other industry, must deal with outdated firmware, unpatched systems, and staff who see security as an engineering problem, not a cyber one.

What, then, does resilience look like in this environment? Broadcasters must assume breach and design around containment. The Zero Trust model proves

The days of disruption for disruption's sake may be behind us. Attackers are no longer satisfied to shut down broadcasts—they are looking to control the narrative

highly practical here, encouraging continuous identity verification, workload isolation, and strict control over which systems each process can access. Distrusting unverified footage goes without saying; controlling access to critical systems might not be quite as obvious.

Implementing such controls means reassessing the broadcast process from the top down. Playback automation software should be able to read from a content library, but does not need to access scheduling databases, for example. The editing suite needs storage access, but there is no reason for it to execute unknown scripts or connect to external systems. Even if a system is compromised, it should be prevented from pivoting deeper into the network.

A promising future

Broadcast media have spent decades mastering the art of keeping the signal alive through storms, strikes, and power cuts. Cyberattacks are now a firm part of that equation. Every open connection is a potential vector. The future of secure broadcasting lies in creating narrow environments—each process, application, and user confined to exactly the space it needs, no more.

Zero Trust fits the broadcast mindset because it is a tool built for control and continuity, principles engineers already readily understand. By locking down what should never change, and clearly defining what can, broadcasters can embrace digital transformation without fear of going dark.

The 2021 Sinclair attack led to **USD 63 million** in lost ad revenue and **USD 11 million** in direct costs

HOW THREATLOCKER® HELPS PROTECT THE BROADCAST CHAIN

Broadcast infrastructures are complex mosaics of systems that use everything from proprietary automation software to everyday Windows and Linux servers. ThreatLocker provides layered control across that diverse landscape without the friction that slows production.

1. Application Allowlisting: Stop the unknown before it starts
In broadcasting, many systems run 24/7. Application Allowlisting lets operators define exactly which applications, scripts, and executables are allowed, which means ransomware, rogue macros, or unauthorized utilities never get a chance to execute, even if they reach a machine.

2. Ringfencing™: Keep systems doing only what they need
Broadcast workflows involve sensitive interconnections—automation talking to storage, encoders talking to cloud CDNs, editors accessing libraries. Ringfencing ensures that each application can communicate only with approved resources. The playout system cannot suddenly connect to the finance database; the editing tool cannot spawn PowerShell. A compromised system alone does not provide an attacker with a useful staging point.

3. Storage Control: Protect your content vaults
Every broadcaster has critical media storage: decades of footage, commercials, and news archives. Storage Control provides granular permissions over who and what applications can access, modify, or delete files. Even if an endpoint is compromised, attackers cannot encrypt or exfiltrate terabytes of irreplaceable content.

4. Network Control: Stop attackers from moving sideways
Legacy broadcast devices often hide on flat networks. Network Control allows dynamic policies that limit which endpoints can communicate with which servers, preventing lateral movement. It is an elegant way to retrofit Zero Trust principles onto networks that were not designed for them.

5. Unified Audit: Watch the content stream
In a live environment, accountability matters. ThreatLocker logs every executable launch, file modification, and policy event—creating a forensic record that security teams can review without interrupting on-air operations.

UNSECURE COMMUNICATIONS: **WHY ZERO TRUST COMES FIRST**

To truly enforce an effective Zero Trust framework, teams should look beyond locking down devices and users. Granular control over conversations, links, and data paths is equally crucial

Cybersecurity is broken only when trust ends too soon. The goal of Zero Trust was never to wall off the network; it was to eliminate blind faith in any system or link. To secure the future of communication, that principle must be taken literally—verify everything, including the path the message takes to reach its destination.

This is a cultural challenge: Until organizations apply the same scrutiny to how data moves as they do to who moves it, they will be protecting only half of the attack surface.

The weakest link in the chain

Recent academic research into commercial satellite communications revealed just how fragile communication paths can be. Researchers found that roughly half of the geostationary satellite signals they analyzed contained data transmitted without encryption.[‡] The intercepted traffic included corporate backhaul data, maritime communications, and in some cases, government and military transmissions.

The finding revealed a gap between how customers perceive data security and how it is handled. Signals carrying phone calls, text messages, or military logistical data were sent in plaintext, which anyone with relatively inexpensive ground equipment could intercept. The vulnerability was simply an absence of encryption on the communications channel itself.

The same pattern repeats across countless enterprise environments. Information security teams may enforce multi-factor authentication (MFA), device posture checks, and segmented networks, but once data leaves the verified endpoint, it often passes through unmonitored channels. The endpoint is trusted, the user is verified, but the path remains invisible.

Invisible leaks in everyday communication

Inside corporate networks, the most common leaks occur through routine tools rather than advanced attacks. Employees forward confidential documents to their personal email accounts to work from home or paste internal information into AI chatbots to speed up drafting and analysis. A 2024 analysis found that more than a quarter of employees had pasted sensitive corporate data into AI tools, including confidential information shared by customers.[‡]

Cloud collaboration platforms present similar risks. Shared folders left open to "anyone with the link," unsecured third-party integrations, and personal devices syncing corporate drives all bypass central controls. Studies of cloud misconfigurations have repeatedly shown that large numbers of storage buckets and repositories are left exposed, many containing sensitive customer or employee data.

Messaging applications compound the problem. Even when encrypted, they still generate metadata, which can reveal sensitive patterns of behavior. Push notification platforms and cloud backup services sometimes store that metadata unencrypted, and smart assistants add another layer of risk by capturing background audio that may contain private or sensitive conversations.

None of these issues are particularly new, but together they show that some interpretations of the Zero Trust perimeter—verifying users and devices—leaves out a critical dimension: the route that data takes after it is sent.

Extending Zero Trust to the data path

If Zero Trust means never assuming safety, then communication channels must be treated with the same skepticism as endpoints. Every hop between devices, networks, satellites, or application programming interfaces (APIs) should be assumed hostile until proven otherwise. That requires visibility, encryption, and verification, not just at the moment of access, but throughout transmission.

In satellite networks, that might mean mandating link-level encryption as a baseline rather than an optional feature. In enterprise collaboration, it means enforcing encryption between internal and external tenants and validating that data-loss-prevention and monitoring tools extend into third-party applications. For emerging AI workflows, it means treating model prompts and outputs as data in motion—subject to the same classification and protection policies as any other sensitive document.

Operationalizing Zero Trust at the communication layer requires enforceable control. ThreatLocker® Network Control and Web Control address this gap by applying least privilege to how endpoints communicate beyond themselves. Network Control provides total control over inbound and outbound network traffic, ensuring that only explicitly authorized devices, systems, and services are permitted to communicate with one another. Each network connection is logged in ThreatLocker Unified Audit, giving security teams continuous visibility into where data is flowing and the ability to analyze or investigate activity after the fact.

Web Control makes controlling web traffic easy by categorizing websites and enforcing access policies that block unsanctioned destinations, such as high-risk cloud services and AI platforms where accidental data exposure is most common. Together, these controls make the data path visible, restricted, and auditable, preventing verified users and trusted endpoints from silently leaking sensitive information through unmonitored channels.

Communications-layer security also depends on understanding metadata and side channels. Encryption requires companion safeguards; identifiers, timestamps, and routing details must also be protected. The principle of least privilege applies here as well: Minimize the amount of metadata retained and restrict access to it as tightly as possible, in line with the underlying content.

Cultural habits that outpace policy

Technology alone cannot eliminate these risks. The real vulnerability often stems from everyday human behavior shaped by convenience. Sending a document to a personal email may seem harmless, and pasting code into a chatbot might look like a quick fix, but each of these small actions can expose data beyond an organization's control.

Training and awareness programs often focus on phishing and password hygiene, while ignoring data-handling norms. The result is a disconnect between what security teams believe is protected and what employees do. Zero Trust in communications requires encryption, monitoring, and cultural reinforcement: clear rules about what data can leave sanctioned systems—and why those rules matter.

From isolated protection to end-to-end assurance

To fully secure communications, organizations need to bring every channel—wired, wireless, satellite, cloud, API, and voice—under one unified visibility framework. Ongoing monitoring of data flows should make it clear where information is moving, who is accessing it, and whether it is leaving the boundaries it was intended to stay within. Independent audits

> In the context of communication, verification must include how data is transmitted, stored temporarily, and received

of external service providers, including satellite operators and cloud vendors, should confirm that encryption, key management, and access controls are properly implemented.

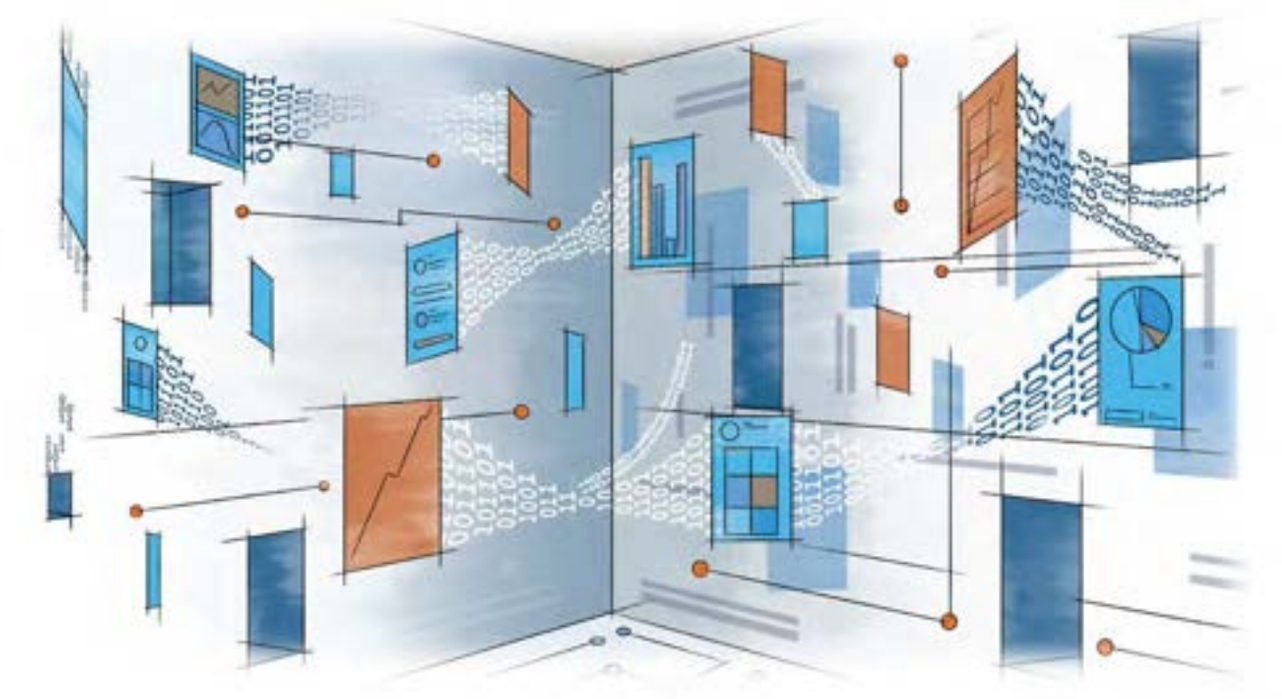
These steps extend Zero Trust from the endpoint to the transmission layer. Instead of verifying access only at the start of a session, the system verifies each transaction, ensuring that the communication itself meets the same standards as the device and user that initiated it.

That approach aligns with the fundamental principle of Zero Trust: assume breach. If a channel is compromised, segmentation and encryption limit the damage. Each connection must be isolated to prevent environment-wide exposure.

The role of automation and AI

Today's networks produce more data than any team can reasonably monitor manually. Automated analytics and AI-powered monitoring can identify unusual patterns, such as files being sent to unexpected locations or transfers that are larger than usual. However, these tools also require strong oversight to ensure they are used responsibly and within clear governance limits. Automated inspection of encrypted traffic, for instance, should comply with privacy laws and limit decryption to only what is necessary.

As machine-learning systems become an integral part of everyday business processes, companies must remember that every interaction with a model constitutes a form of data sharing. The text entered, the responses returned, and even the prompts themselves can include sensitive details that current data-classification rules may not cover. Integrating AI systems into Zero Trust governance frameworks ensures that these exchanges are logged, encrypted, and auditable.



Information security teams may enforce MFA and device checks, but data often travels through unmonitored channels after leaving the verified endpoint

Once data leaves the verified endpoint, it often passes through channels no one monitors

What Zero Trust really means for communication

Zero Trust was never intended to stop at device management. Its real purpose is to verify every interaction across the digital ecosystem. In the context of communication, verification must include how data is transmitted, stored temporarily, and received.

Applying Zero Trust to communication requires three practical shifts. First, organizations must view every communication as a transaction, not a conversation—an event that can be authenticated, encrypted, and logged. Second, all communication channels, both internal and external, should be treated as untrusted until verified. Third, encryption and authentication must be embedded into day-to-day operations, not applied simply to satisfy compliance obligations.

Extending Zero Trust in this way does not diminish the model; it confirms it. No single lapse, whether a misconfigured cloud share, an overlooked API, or an unsanctioned chatbot session, should be allowed to expose the wider environment.

Why the message still matters

As enterprise environments become more interconnected, communications increasingly span internal systems, cloud services, partners, and automated platforms. These pathways represent the same attack surface as endpoints and identities and must be governed with the same rigor. Applying Zero Trust consistently across these channels closes the gaps that attackers most often exploit, reinforcing the model rather than redefining it.

The road ahead

The growth of communications security will take time. Regulations are beginning to recognize the need: Satellite operators are drafting encryption mandates, and data protection agencies are emphasizing secure transmission in compliance audits. But technology adoption alone will not solve the problem.

Organizations must establish habits for continually verifying channels, vendors, and data flows, just as they do for users and devices. Encryption must be assumed mandatory, not optional. Auditing and reporting must extend to every interface that moves information beyond the enterprise boundary. And employees must understand that every message, file, or prompt can become a liability if sent through the wrong channel.

INTERVIEW

LEARNING ON THE LINE

Repeated ransomware attacks, complex system requirements, and a perception of high value pushed Georgia Military College's IT leaders toward a Zero Trust model built on strict execution control

Georgia Military College (GMC) is unlike most academic institutions. It brings together a traditional college, a K–12 preparatory school and a military cadet program, all within one organization. This diversity creates a complex technology environment, with distinct user population, evolving risk, and a persistent need to protect student data at scale.

In this interview, Robert Johnson and Matthew Keyes explain how GMC approaches security and operational resilience in a world where threats are persistent, phishing is convincing, and the cost of disruption is high. They share how their team assessed risk, sharpened their approach, and what changed once they committed to a Zero Trust model.

Before ThreatLocker®, what was the core security problem you were trying to solve?

MATTHEW KEYES: We had already lived through ransomware, and once that happens, it permanently changes how you think. We were hit back in 2017 or 2018, right around Thanksgiving, and while we were able to recover without paying—we had backups—it was still incredibly disruptive. We strenghthened our defenses, identified how the attackers gained access, patched what we could, and moved forward.

But then in 2022, we experienced another ransomware incident. Smaller, but significant enough to force a hard stop. That was when we said, "This cannot keep happening." Even when no data is lost, the impact is real. It keeps you up at night. You start questionning constantly about what you might have missed. That is when we really started looking inward and asking what we could do differently to prevent this, not just recover from it.

ROBERT JOHNSON: My biggest concern was always what happens after something gets inside the network. We had strong perimeter security, firewalls, and endpoint tools, but perimeter defenses only get you so far. Once an attacker gets past that layer, you need a final control point and last line of defense.

What worried us most was unauthorized execution: malware, ransomware, or even a user installing software they should not. In such a complex environment, we needed something that controlled what could run.

What makes GMC's environment more complex than a typical college?

MATTHEW: We're not just a college—we also serve K–12. A student can start here in kindergarten and stay through a bachelor's degree. That's rare, and it makes technology policy far more complex. Most software and security tools are designed for either K–12 or higher education, not both. That forces us to constantly adapt policies to support very different age groups and compliance needs.

On top of that, we have a junior college cadet corps. They're a smaller subset of students, but they operate under different expectations and structures. In practice, we're managing traditional students, K–12 students, and cadets all in the same environment.

← Since 1879, Georgia Military College has shaped students into servant leaders and engaged citizens

→ The "Military" in GMC's name increase vulnerability, as attackers assume sensitive data is present

"

What worried us most was unauthorized execution: malware, ransomware, or even a user installing something they should not. In such a complex environment, we needed something that controlled what could run

ROBERT: The "Military" in the name matters more than people think. Although the cadet corps represents a small subset of about 250 students out of roughly 16,000 across all our campuses, attackers don't see that nuance. They see "Military College" and assume we have sensitive data or direct ties to the military. We don't, but the perception alone makes us a more attractive target.

How did those realities shape your view of cyber risk?

ROBERT: Because we are targeted more, we can't rely solely on traditional security layers. We must assume that someone will eventually get past the perimeter, which isn't pessimism; it's realism. Once something gets inside, the question becomes: What can it actually do?

Before ThreatLocker, we were worried that even with solid tools, something could still run, encrypt data, or move laterally. In previous ransomware incidents, local and mapped network drives were impacted, and that's the nightmare scenario. So, our focus shifted to controlling execution itself, not just detecting bad things after the fact.

> Our response has completely changed, from panic mode to considered investigation and cleanup

MATTHEW: You also have to factor in human behavior. Even well-trained users occasionally click the wrong thing, especially now. Phishing emails are more convincing than ever, and AI has made things worse. I have seen phishing emails in my personal inbox that looked almost completely legitimate. Training helps, but it doesn't eliminate mistakes. Your controls have to assume that someone will click.

What was your security stack like before ThreatLocker, and why was it not enough?

ROBERT: We were doing what most organizations do. We had a fairly standard enterprise stack: antivirus and XDR, custom Group Policy Objects, least-privilege access, and a product that allowed users to install software without us having to remote into their machines every time. Nobody had local admin rights, which is good, but it created friction.

The larger issue was that everything was all very reactive. There were too many alerts and exceptions, and not enough certainty about what was allowed to run in the environment. We were also paying about USD 15,000 a year for that one privilege-elevation product, even though it only handled one small piece of what ThreatLocker ultimately provides.

MATTHEW: We could see threats and respond to them, but we could not guarantee that only approved applications were running. That gap is what kept us worried.

How did you move from hearing about Zero Trust to choosing ThreatLocker?

ROBERT: At first, Zero Trust felt like a buzzword. Then we started going to conferences like the Atlanta Cybersecurity Summit and realized it wasn't just marketing. It became clear that it was a real architectural model.

MATTHEW: The ransomware incidents really pushed us in that direction. We didn't want just to add more detection tools. We wanted a model where, by default, nothing could run unless we explicitly allowed it. When Robert found ThreatLocker, and we started talking to them, it made sense. We ran a proof of concept after beginning the relationship around October 2024, and once we saw it in action, we were sold.

Why did ThreatLocker fit GMC's needs better than other options?

ROBERT: For us, it was that last line of defense. ThreatLocker enforces Zero Trust at the endpoint by only allowing what we explicitly trust. Everything else is blocked. That is the definition of Zero Trust in practice. If ransomware lands on a system today, it simply will not execute. That changes everything.

MEET THE TEAM

Robert Johnson

Johnson is Associate Vice President of Enterprise Networks & Systems at GMC. A long-serving IT leader at GMC for nearly 15 years, he progressed from Senior Network Engineer to Director of IT, and now oversees the institution's information technology systems.

Matthew Keyes

Keyes is Director of GMC's Network Operations Center and has been with the college for 12 years, starting as a technician and working up through operational roles. He works closely with Johnson and a team of system administrators to keep services running across the institution's diverse environment, supporting day-to-day delivery while strengthening resilience against cyber disruption.

Serving kindergarten through bachelor's students, GMC requires adaptable security across all age groups

> We know what is running, why it's running, and who approved it. That's incredibly powerful. We're not constantly reacting anymore—we're operating from a position of control

Previously, ransomware could encrypt local files and mapped network drives. Now, even if the payload somehow lands on the endpoint, it cannot run. Our response has completely changed, from panic mode to considered investigation and cleanup.

MATTHEW: It also aligns with how modern attacks work now. Even if you miss a phishing email or someone clicks a link, the attacker still has to run something. ThreatLocker stops that.

Did you encounter any challenges deploying ThreatLocker in a complex environment?

ROBERT: We did, because our environment is not typical. We run VMware with 100% virtual servers on a shared Nimble SAN. When we made specific ThreatLocker configuration changes, all those servers would check in at once and cause massive storage latency. It got so bad that Active Directory authentication would time out, and people could not log in.

MATTHEW: We worked directly with ThreatLocker developers and helped design a delay option so those updates don't all happen at once. It staggers them—a few at a time, then a pause, then more—which prevents the storm. They turned it around in about three to four weeks, which is incredibly fast for development work like that.

How has life changed since ThreatLocker, and what does the future look like?

MATTHEW: The biggest difference is our peace of mind. We sleep better. Our security posture is much stronger, and day-to-day operations are calmer. Software requests are easier because their Managed Detection and Response (MDR) and Cyber Hero® Team handles approvals for applications we already use, while we keep control over anything new. That reduces workload without compromising security.

ROBERT: For me, it is predictability. We know what's running, why it's running, and who approved it. That's incredibly powerful. We're not constantly reacting anymore—we're operating from a position of control.

Looking ahead, we will keep optimizing. We have not even fully used every ThreatLocker solution yet, but we're already in a much better place. We have gone from hoping our tools will catch attacks to knowing that even if something slips through, it will not be able to run.

NEXT PAGE

While GMC falls outside direct military requirements, FedRAMP pressure means federal-grade security is a necessity for more and more businesses

THE QUIET SIGNAL OF SECURITY MATURITY

Why FedRAMP matters to organizations that need Zero Trust enforcement, not just compliance claims

ThreatLocker® is now on the FedRAMP Marketplace. For customers, that matters far beyond federal contracting.

Being on the FedRAMP Marketplace signals that a platform has reached a level of technical maturity and security rigor capable of withstanding one of the most demanding audit and validation programs in the world. It is evidence that the system, the processes behind it, and the organization operating it are built to meet sustained, enforceable security expectations.

For customers operating in regulated environments, defense supply chains, or industries where compliance requirements are tightening quickly, FedRAMP status is a meaningful indicator of long-term viability.

WHAT BEING ON THE FEDRAMP MARKETPLACE MEANS IN PRACTICE

FedRAMP examines how security is designed, enforced, monitored, documented, and sustained over time.

A FedRAMP-aligned platform must demonstrate:

- Enforced least-privilege access rather than permissive defaults
- Continuous monitoring instead of point-in-time compliance
- Disciplined change control and configuration management
- Mature incident response, vulnerability management, and audit processes
- Evidence that controls are effective, repeatable, and resistant to drift

Being on the FedRAMP Marketplace confirms that the ThreatLocker platform architecture and operating model have been aligned to these expectations and validated through rigorous assessment by a Certified Third-Party Assessor Organization (C3PAO).

The company's deny-by-default Zero Trust approach places it among a small subset of tools on the FedRAMP Marketplace that emphasize prevention and enforcement, not post-incident detection.

This means customers are inheriting a security foundation that is already designed to operate at federal standards rather than using a tool that needs to be fundamentally reworked as requirements increase.

WHY THIS MATTERS TO COMMERCIAL AND MID-MARKET ORGANIZATIONS

Federal security expectations are not just stopping at federal agencies anymore, but flowing outward through prime contractors, subcontractors, managed service providers (MSPs), and technology providers—becoming implicit requirements in procurement and vendor risk assessments.

Organizations that previously viewed FedRAMP as irrelevant now face questions such as:

- Can your tools support continuous enforcement?
- Can they produce reliable audit evidence over time?
- Can they scale into regulated environments without replacement?

Being on the FedRAMP Marketplace answers those questions early.

It signals that the platform has already been hardened, tested, remediated, and validated under conditions far stricter than most commercial frameworks demand.

THE FEDRAMP–CMMC CONNECTION

FedRAMP and the Cybersecurity Maturity Model Certification (CMMC) are distinct programs, but they share foundational principles rooted in NIST standards: least privilege, continuous control enforcement, and proof of effectiveness.

While no product can certify an organization for CMMC, tools designed to meet FedRAMP expectations often:

- Map cleanly to CMMC-relevant NIST requirements
- Reduce the need for compensating controls and narrative justifications
- Provide enforceable controls rather than policy-only assurances

ThreatLocker FedRAMP-aligned controls help organizations pursuing CMMC by delivering inherently strong systems that support assessment readiness. Customers inherit mature access control, application control, and enforcement mechanisms that make it easier to demonstrate compliance rather than explain gaps.

COMPLIANCE IS NO LONGER A SNAPSHOT

Modern compliance programs are moving away from "secure on audit day" toward continuous validation. Drift, undocumented changes, and exception-heavy environments increasingly fail scrutiny.

Organizations that delay adopting compliance-grade security often pay later through:

- Weak audit trails
- Operational workarounds
- Costly rip-and-replace projects under deadline pressure

Platforms on FedRAMP reduce that risk. They are built to help establish and maintain enforcement.

FEDRAMP SECURITY IS PRACTICAL SECURITY

The value of FedRAMP-aligned security shows up in three tangible ways:

Stronger security by design
Taking deny-by-default actions supports Zero Trust principles like least privilege to significantly reduce the number of incidents that can occur. ThreatLocker enforces this through Application Allowlisting, Elevation Control, and controlled administrative access, preventing unauthorized activity rather than reacting to it.

Faster alignment with common frameworks
FedRAMP, CMMC, and NIST frameworks have a heavy overlap in their intent. When foundational controls are already enforced, organizations spend less time inventing controls and more time proving what is already in place.

Less future rework
Regulatory exposure often changes suddenly: a new contract, a new customer, or a new supply-chain requirement. A ThreatLocker Zero Trust foundation helps ensure customers do not need to rebuild their security stack when expectations rise.

WHAT CUSTOMERS INHERIT WITH A PLATFORM ON THE FEDRAMP MARKETPLACE

Being on FedRAMP reflects a platform built to operate where security expectations are highest and least forgiving.

For organizations whose regulatory exposure may expand, and for those already navigating CMMC or defense-adjacent requirements, ThreatLocker provides a security foundation designed to scale forward.

When customers adopt a platform like ThreatLocker, they inherit a proven security discipline.

This includes:

- **Inherently strong system design**
  Security controls built around deny-by-default, least privilege, and enforced access, not permissive assumptions or after-the-fact detection.
- **Mature operational processes**
  Documented, tested procedures for change management, incident response, vulnerability handling, and access control that are designed to withstand audit scrutiny.
- **Continuously enforced controls**
  Security that operates every day, reducing configuration drift and audit risk.
- **Audit-ready evidence and telemetry**
  Consistent, repeatable evidence that controls are in place and effective, simplifying audits and assessments.
- **Cleaner alignment to CMMC and NIST requirements**
  Foundational controls that map naturally to CMMC and NIST objectives, reducing the need for compensating controls and narrative explanations.
- **Lower compliance friction as requirements evolve**
  A security foundation designed to scale into regulated environments without disruptive rip-and-replace projects.

For customers, this means less time proving intent, fewer gaps to explain, and more confidence that their security posture can support future regulatory demands.

AUSTRALIA'S ESSENTIAL EIGHT DECODED

The straightforward framework supporting the Southern Hemisphere's rapid growth

1. Patch applications

Application vulnerabilities must be scanned every two weeks at minimum, with critical patches applied within 48 hours at the highest maturity level

2. Patch operating systems

The framework allows more time for OS updates than applications, requiring monthly patches at level one and 48-hour deployment at level three

3. Multi-factor authentication (MFA)

Organizations must deploy MFA across end-users, administrators, and customer access points, with activity logs maintained for security analysis

4. Restrict administrative privileges

Administrative privileges should be automatically retired when inactive, with dedicated workstations and detailed logging for admin tasks

5. Application control

Controlling what runs, from email attachments to server files, requires defined access policies, annual updates, and incident reporting protocols

6. Restrict Microsoft Office macros

Downloaded documents must be blocked from running macros at minimum, with digital signature inspection required at the highest maturity level

7. User application hardening

Detailed guidance covers general hardening practices and third-party (such as ThreatLocker®) compliance tools, with specific instructions for common applications like PowerShell

8. Regular backups

Maintaining business continuity plans forms the baseline, with advanced maturity requiring strict access controls and integrity verification for all backups

In the last quarter of 2025 alone, personal details of five million Qantas customers were leaked to the dark web following a ransomware attack

Australia plays a leading role in regional cybersecurity and global intelligence partnerships

Fairly or not, Australians have a reputation for plain speaking and getting to the point, along with a creativity of expression that favors brevity over formality. So, it should not be a surprise that one of the most straightforward and easy-to-understand frameworks for cybersecurity design and implementation was developed there. The Essential Eight maturity model is now a vital part of the lexicon for local specialists, government organizations, and enterprise operations, and an extremely useful framework for their peers across the globe.

As the name suggests, the framework is designed around eight principles (or pillars) that can be used to understand an organization's security position. On top of the pillars are three levels of maturity, which cover everything from the basics—such as how frequently to check for application updates—to regular scans of endpoint logs for abnormal behavior.

Security professionals will recognize the pillars of the Australian Cyber Security Centre's Essential Eight. They closely mirror the principles of Zero Trust security, focusing on restricting the capabilities of users and devices by default to reduce the potential impact of malicious actors who breach a network.

Like every major security framework, compliance can be tracked policy by policy within the ThreatLocker interface. Ringfencing™, in particular, helps address many of the Essential Eight's advisories by containing applications and preventing them from accessing data that they do not need, and specifically addressing the interactions between Microsoft applications, such as Microsoft Office and PowerShell, that are flagged in several of the pillars.

WHY THE ESSENTIAL EIGHT?

The Essential Eight was developed and published by the Australian Signals Directorate (ASD) in 2017 and has been revised regularly since. ASD's role is an important one, globally speaking. Along with the U.S., U.K., Canada, and New Zealand, Australia is a member of the "Five Eyes" intelligence-sharing network. With the U.S. and U.K., it is part of the tripartite security partnership, AUKUS, which covers military hardware such as nuclear submarines and development of AI platforms for defense.

It is, in other words, a prominent power in the geopolitics of the Asia-Pacific region, with a need to protect itself and its strategic partners against the most significant threats—from common criminal activity to highly targeted state-sponsored attacks. And the focus on the region for such attacks is only growing.

In the last quarter of 2025 alone, personal details of five million Qantas customers were leaked to the dark web following a ransomware attack[‡], while another attack was reportedly underway targeting telecoms hardware in the country.[‡] The

former involved criminals who managed to convince call center workers that they were IT engineers using social engineering and impersonation techniques. The latter employed an exploit known to be used by the hacking group Salt Typhoon, which is in turn linked to Chinese espionage agencies. In recent history, some of Australia's best-known brands—including the graphic design tool Canva and its third-largest telecommunications company, Optus—have also been subject to significant data breaches with global implications.

The Essential Eight is part of a coordinated response to these threats at the highest level. It serves three functions simultaneously: It is a policy document, a set of compliance requirements, and an advisory note detailing best practices for local businesses.

The primary purpose of the documentation is compliance. All government departments, state-owned entities (or Commonwealth-owned corporations, as they are known locally), and non-governmental organizations that require access to critical data must perform regular security audits to ensure compliance with at least Level Two of the maturity model.

The ASD also produces plain-language documentation to help small businesses and enterprises that want to use the model, as it points out that "implementing the Essential Eight proactively can be more cost-effective in terms of time, money, and effort than having to respond to a large-scale cybersecurity incident." The ASD also provides detailed guides outlining how to carry out a security assessment using the framework.

CLEAR COMMUNICATION

The biggest appeal of the Essential Eight, outside of the Australian government, is its clarity of language and purpose. The history of cybersecurity failures and their impact on ordinary businesses and individuals is as much of a problem with communication as it is a problem with technology. For obvious reasons, software vendors and application developers

ACTIONING THE ESSENTIAL EIGHT WITH THREATLOCKER

ThreatLocker is the perfect way to operationalize Australia's Essential Eight without adding unnecessary complexity. The framework provides a guideline; the ThreatLocker suite makes its tenets easy to uphold. All controls and tools live in one place, with the visibility and control that allows organizations to move beyond baseline compliance to higher levels of resilience.

Application Allowlisting supports the Essential Eight's emphasis on deny-by-default application control. Only explicitly trusted applications are permitted to run across Windows, macOS, and Linux endpoints, blocking ransomware, zero-day threats, and unauthorized software before it can be executed. This approach underpins multiple maturity requirements, including application control on workstations and servers, and implementation of Microsoft's vulnerable driver blocklist.

For restricting administrative privileges, ThreatLocker uses **Elevation Control** to remove standing local admin rights and grant access only when required, enforcing the principle of least privilege. This is strengthened by **Ringfencing**, which limits what even approved or elevated applications can do, preventing lateral movement, unauthorized process injection, or access to sensitive resources. Centralized logging through **Unified Audit** supports higher maturity levels by ensuring privileged actions are visible and traceable.

ThreatLocker also addresses user application hardening and Microsoft Office macro restrictions through a combination of **Configuration Manager**, **Ringfencing**, and **Storage Control**. With these tools, streamline the blocking of risky behaviors such as running macros from internet-sourced documents, PowerShell usage, and applications that might spawn unauthorized child processes or access the internet unnecessarily.

Additionally, ThreatLocker offers a **Patch Management** solution that keeps vigilant watch over devices in your organization to ensure applications receive software updates as required, with a testing environment used before being pushed onto managed devices. The process of patching applications and operating systems is also supported by ThreatLocker Software Health Report, where unsupported or discontinued software is identified, whilst administrators are also alerted to operating system update requirements.

ThreatLocker Defense Against Configurations (DAC) helps ensure alignment with the Essential Eight by continuously checking an organization's environment and highlighting where gaps may exist. DAC highlights the misconfigurations and offers clear guidance on how to remediate each finding. Where an issue relates to a ThreatLocker policy, remediation is intentionally simple, often requiring just a single click to apply the correct control.

Finally, **Storage Control** plays a key role in restricting who can access backup locations and ensuring only authorized backup applications can write to them. Combined with optional 24/7 monitoring through **Cyber Hero® MDR**, ThreatLocker helps organizations meet higher Essential Eight maturity levels with consistent, auditable enforcement.

Scan to learn how ThreatLocker helps you master the Essential Eight

do not build marketing strategies around the risks inherent in using their products. Communicating the benefits of a product in plain language makes commercial sense, but who wants to highlight the complex, risky stuff rather than bury it in the small print? As a result, the language of cybersecurity is jargon-heavy and impenetrable for non-specialists.

While the C-suite is undoubtedly better at taking shared responsibility for cybersecurity than it used to be, the temptation to leave it all to IT—as the experts who understand and will take care of it—remains. To make matters worse, the current climate of investment in and hype around new tech is unprecedented. Many fear that it is putting executives under pressure to move fast and not miss out on the next tech-powered boom. Well-known venture capitalist Kevin Rose worries firms may be making the same product development mistakes they did in the past by not considering emerging risks and leaving IT to solve the problems after the fact.[‡]

It should not be surprising. As a species, we instinctively trust the experts to take care of complex things. They enable the computers to work and safeguard our servers against ransomware attacks. All too often, we only learn about best practices and Zero Trust environments after a catastrophic event has occurred.

Making cybersecurity as simple as possible is fundamental to the ethos of ThreatLocker and other organizations that aim to help end-users and decision makers rather than baffle them. The principles of the Essential Eight are universal, and the core language makes them easy to understand.

> “
>
> Implementing the Essential Eight proactively can be more cost-effective in terms of time, money, and effort than having to respond to a large-scale cybersecurity incident

THE CRITICAL VIEW

The Essential Eight does have its critics. Some complain that the model is overly simplistic and is mostly common sense for experienced IT professionals. The Essential Eight is by no means as broad and detailed a tool for governance as, for instance, the FedRAMP regulations and marketplace in the U.S. This is fair, but it also serves to highlight the Essential Eight's true usefulness for the non-professional audience. After all, if most breaches are still caused by human error and poor communication, as an industry, we still need to close the knowledge gap between experts, decision makers, and users.

Other critiques may be more pressing to address. The sections on locking down Microsoft software, for example, could be easily generalized and applied to products from other vendors, including emerging providers in the large language model (LLM) space. Microsoft remains dominant in many sectors, but it is not without competitors. Many governments—particularly those in the European Union—are developing local solutions to counter monopoly behaviors by U.S. giants. All solutions, no matter their origin, should be introduced in a Zero Trust environment where internet-facing macros and scripts are disabled by default.

Perhaps most important, though, are the outright omissions in the Essential Eight. The document, for example, does not touch on cybersecurity within organizational culture or mention employee training. This is perhaps understandable given its primary purpose, but it is a reminder that no framework is comprehensive enough to be considered in a vacuum.

The Essential Eight is constantly being revised and may address some of these concerns in the future, but the lesson is that no single tool or framework can do everything or promise total security. Layering defense and ensuring the application of best practice through a tool like ThreatLocker is vital to mitigate current threats and those that are rapidly emerging.

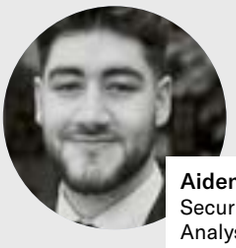
The industry has seen exponential growth in the number of attacks, driven by the combination of novel AI tools and traditional phishing techniques. Keeping the Essential Eight in your toolbox as a baseline guide for locking down applications and access can be a great starting point for keeping your organization secure and having the right conversations with the C-suite.

FINANCIAL **RESPONSIBILITY**

netwealth

Australia's Netwealth transformed its security function and built regulatory compliance the ThreatLocker® way

MEET THE TEAM



Aiden Bitic
Security Operations Analyst

Bitic joined Netwealth over four years ago, starting his career on the Helpdesk straight out of university before transitioning into cybersecurity. He now works as a Security Operations Analyst, handling day-to-day security tasks, including reviewing alerts, email security, and maintaining Netwealth's security posture. He learned the foundations of Zero Trust and least privilege during his Helpdesk years and later developed a deeper interest in security that led him into the internal security team.

Dylan Lohr
Security Engineer

Lohr has been with Netwealth for around six years. Like Bitic, he began on the Helpdesk, but from the start, he made it clear he intended to work in cybersecurity. When Netwealth formally created its security function, he moved into the newly established internal team and now works as a Security Engineer. He handles the same day-to-day operations as the analysts but also leads hands-on projects and plays a key role in selecting and rolling out ThreatLocker.

Netwealth is one of Australia's leading financial services and wealth management technology companies, with hundreds of employees across development, operations, and client-facing teams.

As the organization expanded and remote work reshaped its operating environment, the security team faced increasing pressure to modernize its approach to endpoint control and tighten its security posture without slowing down productivity.

With a significant developer population and stringent industry regulations to meet, Netwealth needed a practical way to standardize software usage, protect sensitive data, and align with best-practice frameworks such as the Essential Eight—all while maintaining a streamlined user experience.

The search for a modern, flexible, and highly granular application control solution ultimately led the team to ThreatLocker. In the following interview, two members of Netwealth's internal security team share how their Zero Trust journey evolved, why application control became essential, and how ThreatLocker now underpins some of the organization's core security operations.

What made Zero Trust a priority for Netwealth, and how did your approach evolve?

DYLAN LOHR: COVID was a major turning point. Before that, everyone worked on-prem behind corporate firewalls, using office desktops. When we suddenly shifted to remote work, people were logging in from different locations and sometimes from personal devices. We had to start asking: How do we gain visibility? What access do users really need? That pushed us toward a Zero Trust mindset.

AIDEN BITIC: When I joined Helpdesk, a lot of the security-first foundations were already in place—least privilege, limited access. That helped me learn the Zero Trust approach early on, and it made sense to strengthen it when remote work became normal.

Why did you begin looking for an application control solution, and why ThreatLocker specifically?

DYLAN: The initial requirement came from a major client who needed application control. Combined with the Essential Eight expectations, we knew it was time. We evaluated multiple vendors at CyberCon, and ThreatLocker was the clear standout. The UI was modern,

RISING TO THE SECURITY CHALLENGE

Building a modern internal security function at scale is a challenge for any organization, especially one supporting a large base of users and developers. Netwealth's security team aims for efficiency, applying multi-skilled personnel to react to issues fast. The team's philosophy revolves around being tightly aligned, agile, and highly responsive.

"We move at speed," Lohr explained. "A ticket comes in, then whoever grabs it first does the job." This flexible model keeps responsibilities fluid and avoids bottlenecks. Bitic added that the pair's day-to-day work is "almost identical," which means anyone can step in to handle an emerging threat, incident, or investigation. That practical background—shared across the whole team—creates a culture grounded in understanding real user behavior, not just policy.

The team also benefits from the way it was built—not inherited. "There was no security team," Lohr said. "I made it very clear in my interview that I was destined for security, whether they wanted me to or not." When Netwealth's leadership later formalized the function, he was pulled in to help shape it.

For CISOs, the takeaway is clear: teams are most effective when workflows are streamlined, responsibilities overlap intentionally, and the culture values curiosity, adaptability, and hands-on experience.

but more importantly, the capabilities were stronger—especially Ringfencing™. Some competitors felt like products from 2006. ThreatLocker had everything we needed and more.

AIDEN: Application control fits well with our industry. Developers have different privilege requirements, and without strong controls things can get messy fast. ThreatLocker addressed that gap.

How does ThreatLocker support your Zero Trust strategy day to day?

DYLAN: ThreatLocker lets us define exactly what an application can and can't do. Ringfencing stops misuse of living-off-the-land (LOTL) binaries—things built into the operating system (OS) that attackers commonly abuse. Elevation Control is huge: Developers no longer need full local admin. Only approved applications get elevated, not the whole user account. That's real least privilege in action.

AIDEN: And we get visibility into everything users run. If something odd happens, it stands out immediately.

What was the rollout process like?

DYLAN: Very smooth. We piloted with a number of our developers—they have the most complex workflows. We used Learning Mode so ThreatLocker could observe their normal patterns and prebuild rules. Once that was stable, we rolled out to a few hundred more users with barely any issues. ThreatLocker has been an outstanding partner. With most other vendors, support can take at least a day, whereas the ThreatLocker Cyber Hero® Team has an average response time of 60 seconds or less.

AIDEN: We don't contact them often, but when we do, especially with niche questions, they're fast and accurate. In terms of the software itself, it really helped us standardize which applications people use and where they use them. That alone was a major improvement.

What changed most in your day-to-day operations once ThreatLocker was in place?

AIDEN: The big change is control and consistency. Before, developers could download anything they liked—it felt like the Wild West. That leads to issues like missing patches or unpredictable software. Now, we can deny-by-default: Let in what we want and block what we don't. ThreatLocker helps ensure users only run what's approved and safe.

DYLAN: We get only about four or five requests a day, and each takes seconds to review. It also lets us safely remove local admin from developers without upsetting their workflows, and it's perfect for the financial sector because it supports frameworks we work under—such as ISO 27001, CPS 234, GS 007, and Essential Eight. The logs and controls demonstrate real oversight.

Why do you think Zero Trust and application control are more crucial now than ever?

AIDEN: Cybersecurity keeps expanding, and attackers increasingly use tools already built into systems. Application control adds a necessary layer of protection.

DYLAN: Nation-state actors like North Korea and Russia are growing more capable and cyberwarfare is real. Controls like ThreatLocker make attackers' lives harder and give us the visibility needed to detect and stop unauthorized activity.

NEXT PAGE

Protecting trillions in assets means protecting critical systems. The finance sector must make an investment in Zero Trust to meet the new cybersecurity landscape

THE TRUST DIVIDEND

With multimillion-dollar attacks escalating and trust eroding, Zero Trust is rapidly becoming the financial industry's most strategic defense

As cyberattacks become more frequent, costly, and reputationally damaging, trust has become one of the financial sector's most valuable assets. From ransomware and supply-chain compromises to tightening regulatory scrutiny, investment firms now face risks that extend far beyond IT. Zero Trust has emerged as a strategic response, reshaping how organizations protect data, meet compliance requirements, and reassure clients and investors. The close connection between cybersecurity, valuation, and growth is increasingly evident, particularly as recent breaches reveal the limitations of traditional perimeter defenses. Firms embracing Zero Trust principles are gaining measurable advantages in resilience, reputation, and long-term confidence, illustrating the critical intersection of cybersecurity and financial success.

By 2028, wealth managers, asset managers, and financial advisors are expected to oversee a predicted

USD 171 trillion

in global assets

Roughly 65% of financial organizations dealt with ransomware issues in 2024, according to the Financial Services Information Sharing and Analysis Center (FS-ISAC). Recovery costs have climbed to an average of USD 2.58 million per incident, with attackers targeting the sector's high-value data and critical infrastructure.

This sustained pressure has driven financial firms to make serious investments in novel cybersecurity solutions, with Zero Trust principles increasingly at the center of their defense strategy.

For wealth managers, asset managers, and financial advisors—set to be responsible for a predicted USD 171 trillion in global assets by 2028‡—cybersecurity is now a fundamental business imperative. With 71% of asset managers‡ fielding investor cybersecurity questions during fundraising and 88% of financial executives fearing client withdrawal after attacks‡, security posture now directly impacts fundraising, client retention, and valuation.

Ransomware groups have recognized this vulnerability. The MOVEit supply chain attack alone compromised over 2,700 organizations and 93 million individuals‡, impacting major institutions including TD Ameritrade, Charles Schwab, Fidelity Investments, and TIAA.

RansomHub emerged as 2024's most prolific threat actor, claiming responsibility for over 500 attacks‡ targeting the financial sector, using advanced techniques to bypass traditional defenses. Compounding the threat, third-party risk appears to have become far more volatile.

SecurityScorecard data reveals that 97% of the top 100 U.S. banks experienced a third-party breach in 2024. Financial services accounted for 16% of all third-party breaches globally, with 81% of those breaches involving system intrusion and credential reuse in third-party environments.

High cost of an attack

A 2024 ransomware attack against Insight Partners, a prominent venture capital firm, underscores the escalating risk to the investment sector. The attack began with a methodical social engineering campaign designed to gain initial access, followed by months of covert data encryption.

Notably, Insight Partners' portfolio includes multiple cybersecurity companies, yet it still fell victim to the attack because traditional perimeter-based security failed once attackers gained internal access. Systems that should have been isolated were implicitly trusted.

Following the breach, Insight Partners filed mandatory data breach notifications with multiple state attorney generals and began notifying over 12,600 affected individuals. The compromised data included details on limited partners, fund information, and portfolio companies, highlighting the power of such incidents to create reputational challenges for investment firms.

STRATEGIC ROADMAP TO ZERO TRUST

CISOs at investment firms can adopt a phased approach to Zero Trust implementation, balancing immediate security improvements with long-term strategic goals. The following timeline provides a sample framework for systematic deployment that allows business operations to remain active.

Year one priorities

- Begin with a comprehensive security assessment using the NIST Cybersecurity Framework 2.0 to establish a baseline security posture
- Join FS-ISAC for threat intelligence access, including CAPS exercises and industry-specific threat feeds
- Implement ThreatLocker® Application Allowlisting to establish deny-by-default protection
- Use Ringfencing™ to establish application-level boundaries around trading systems and client data
- Deploy ThreatLocker Detect for immediate identification and remediation of cyberthreats
- Conduct incident response tabletop exercises to test the current capabilities and identify contingency gaps
- Participate in FS-ISAC CAPS exercises to validate resilience

Long-term investments

- Deploy XDR platforms integrating endpoint, network, cloud, and email telemetry
- Establish monitoring 24/7 via SOC or Managed Detection and Response (MDR)
- Implement ThreatLocker Network Control for dynamic firewall and access control lists (ACLs) management
- Integrate security tools with trading platforms through secure application programming interfaces (APIs)

The aspirational endgame

- Achieve NIST CSF Tier 3–4 maturity
- Automate Tier-1 SOC functions to improve response speed and reduce overhead
- Deploy ThreatLocker Detect for continuous threat detection
- Build board-level cybersecurity dashboards demonstrating risk reduction and ROI

Zero Trust: The critical investment

Zero Trust architecture represents a fundamental shift in cybersecurity thinking for investment companies. Treating every user, device, and application as potentially compromised allows for the creation of a hardened interior beneath the traditional perimeter defense, placing security at the heart of every process.

Zero Trust implementation requires continuous authentication and authorization for every access request, along with explicit access controls. ThreatLocker exemplifies these principles for financial institutions.

Application Allowlisting prevents unauthorized software, such as unapproved trading tools or shadow IT applications, from executing on endpoints, supporting regulatory expectations like secure change control and software integrity.

Ringfencing enforces granular access boundaries so applications, including core banking platforms, SWIFT clients, or market-data terminals can only interact with the data and processes explicitly allowed, limiting lateral movement and reducing the blast radius of a compromised account or system.

The necessity of such controls is demonstrated by the 2024 Fidelity Management & Research breach, in which attackers created two fraudulent customer accounts and used them to access other customers' sensitive data through a broken access control flaw. This allowed them to view Social Security numbers (SSNs), driver's license information, and financial account details.

Perimeter defenses cannot prevent access-based exploits like this, but Zero Trust measures such as least-privilege access, microsegmentation, and real-time access monitoring would have cut off the attack before it could even begin.

USD 400 million

in regulatory penalties have been faced by U.S. financial services firms since 2021 due to cybersecurity breaches and inadequate security controls

Meeting regulatory requirements

In the face of increased threats, the regulatory landscape has intensified dramatically. New Securities and Exchange Commission (SEC) cybersecurity rules, effective December 2023, require material incident disclosure within four business days, along with annual cybersecurity risk management reporting. The SEC settled charges against four companies in October 2024 for disclosure failures, signaling aggressive enforcement ahead.

Since 2021, U.S. financial services firms have faced approximately USD 400 million in regulatory penalties over cybersecurity breaches and inadequate security controls.[‡] Capital One incurred USD 80 million in penalties from the Office of the Comptroller of the Currency (OCC), plus a USD 190 million class-action settlement for its 2019 cloud breach affecting 100 million customers. The SEC fined Intercontinental Exchange USD 10 million for failing to disclose a hack and imposed USD 2.1 million on RR Donnelley for insufficient cybersecurity controls during a ransomware attack.[‡]

Beyond the SEC, firms must navigate Financial Industry Regulatory Authority (FINRA) requirements, state mandates such as New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act and California's privacy laws, and various worldwide regulations, including the EU General Protection Regulation (GDPR), The EU Markets in Financial Instruments Directive II (MiFID II), and System and Organization Controls (SOC) 2 Type II.

Adding to the complexity, breach notification laws differ across the 50 states, while Payment Card Industry Data Security Standard (PCI DSS) compliance is mandatory for firms that process payments. This fragmented landscape makes unified security frameworks essential.

Gaining the International Standards Organization/International Electrotechnical Commission (ISO/IEC) 27001 certification has become increasingly critical for investment firms seeking to attract European clients and gain a competitive advantage in U.S. markets.

The ThreatLocker Defense Against Configurations (DAC) dashboard can help you to ensure ISO/IEC 27001 compliance through comprehensive access controls, continuous monitoring, and detailed audit trails that demonstrate security governance.

Building trust through defense

Delaying Zero Trust adoption exposes firms to escalating risk—financial, operational, and reputational.

Those implementing strong cybersecurity programs, on the other hand, achieve measurable returns: Organizations with strong incident response plans reduce breach-related costs by an average of USD 1.49 million, while security AI and automation prevent breaches that would cost an average of USD 2.22 million.[‡]

The evidence overwhelmingly demonstrates that cybersecurity has evolved from an IT concern to a strategic business imperative. Companies with SOC 2 compliance create trust advantages, while cybersecurity excellence differentiates firms in competitive wealth management markets.

Strong cyber defenses now function as powerful differentiators, and clients now routinely ask about security protocols in the same breath as investment performance.

Success requires executive-level commitment, adequate resource allocation, and continuous improvement. Just as in investment, there is no such thing as an immediate, instant return. But in this high-stakes environment, robust cybersecurity forms the foundation for sustained growth and ongoing client trust—it is money well spent.

THREATLOCKER TIP

If you are a financial institution operating in the EU, access the ThreatLocker whitepaper on how we can help you become compliant with DORA. This paper breaks down DORA's five key pillars and how ThreatLocker enables you to meet them head-on

THE WORLD'S **SMARTEST CITY**

Singapore, a shining gem in Southeast Asia, is celebrated globally for its blend of innovation, culture, and natural beauty

Singapore's skyline is a gleaming testament to its transformation from a trading hub to a global leader in technology and innovation. But beyond the towering skyscrapers and bustling streets lies a city that seamlessly integrates cutting-edge technology into everyday life, creating a unique lifestyle that appeals to forward-thinking leaders across industries. Here, progress is matched by the city-state's commitment to maintaining high living standards for its citizens through the implementation of strict entry requirements, ensuring safety, order, and public well-being.

Recently crowned the world's smartest city, Singapore has technology embedded into its DNA. The metropolis boasts an extensive, tech-enabled public transport system where real-time data powers apps that provide commuters with accurate schedules, crowd updates, and alternative routes. Additionally, the city is testing and implementing autonomous vehicles, electric buses, and shared mobility platforms to reduce congestion and lower carbon emissions.

Through its "Smart Nation" initiative, Singapore leverages data-driven decision-making by utilizing technologies such as sensors, big data, and AI to enhance public services, including healthcare, transportation, and utilities. Integrated technology also extends to urban planning, encompassing smart building designs, energy-efficient infrastructure, and initiatives such as water recycling and urban farming, which contribute to a greener city.

Recently crowned the world's smartest city, Singapore has technology embedded into its DNA

For those who understand the importance of digital resilience, Singapore offers a compelling glimpse into the future of tech-driven living, showcasing how innovation and lifestyle are intertwined in one of the world's most dynamic cities.

URBAN LIVING AND CULTURAL ICONS

Singapore's urban infrastructure and iconic landmarks exemplify how technology and innovation shape the city's lifestyle. The lotus-shaped ArtScience Museum is a striking example of this fusion. Designed by Moshe Safdie, its form resembles a welcoming hand and cleverly captures rainwater to support eco-conscious initiatives. Inside, visitors embark on sensory journeys through permanent and rotating exhibitions.

"Future World," created in collaboration with teamLab, is a highlight—its interactive displays respond to touch and movement, allowing guests to co-create digital artwork and wander through immersive virtual ecosystems. Exhibits exploring sustainability, AI, and the relationship between art and science—along with past showcases on da Vinci, Star Wars, and the human genome—demonstrate the museum's ability to make complex ideas accessible and visually compelling.

Nearby, the Supertree Grove at Gardens by the Bay feels like stepping into a parallel world. These towering structures, ranging from 80 to 160 feet in height, are vertical gardens that host more than 160,000 plant species. Beyond their beauty, they incorporate photovoltaic cells to harness solar energy and act as environmental engines for the surrounding conservatories. By day, the grove invites slow exploration; by night, the Garden Rhapsody transforms the Supertrees into a dazzling display of color and music. The OCBC Skyway and Supertree

Singapore's urban infrastructure and iconic landmarks exemplify how technology and innovation shape the city's lifestyle

Observatory offer elevated views across the gardens and Marina Bay's skyline. Anchoring the district is Marina Bay Sands, one of Singapore's most recognizable icons. Its three towers and SkyPark form a destination in their own right, with panoramic city views from the observation deck and an infinity pool known worldwide. Through an augmented reality experience, visitors can explore historical sites, future developments, and sustainability concepts layered over the skyline. With celebrity chef dining, the nightly Spectra light and water show, and easy access to the ArtScience Museum, Marina Bay Sands embodies Singapore's bold and innovative spirit.

HOW TECHNOLOGY ENHANCES DAILY LIVING

Singapore bolsters its reputation as a global smart city by leveraging technology to shape how residents move, work, and connect across various sectors, including transportation, healthcare, urban planning, and retail.

The city's extensive MRT transport network and autonomous buses are supported by real-time tracking, digital ticketing, and AI-driven scheduling, ensuring commuters can navigate the city efficiently. Ride-hailing apps, integrated with public transit options, make last-mile travel seamless, while smart traffic systems adjust signals dynamically to reduce congestion, saving time and energy.

Through its "Smart Nation" initiative, Singapore leverages data-driven decision-making by utilizing technologies such as sensors, big data, and AI

Daily conveniences extend to homes and workplaces. At Marina One Residences, a LEED Platinum pre-certified project, smart building technologies monitor energy consumption, control lighting and climate, and even harvest rainwater, creating more sustainable and comfortable environments. Likewise, urban planning leverages data-driven insights to develop efficient and livable spaces. Smart lampposts assess real-time data to monitor air quality and traffic flow, helping to detect crime and assist with crowd control needs across neighborhoods.

For a frictionless consumer experience, retailers are adopting a range of digital solutions to enhance their operational efficiency. Through augmented reality (AR) and virtual reality (VR) technologies, consumers can virtually try on products and visualize items in their homes, driving higher engagement and increasing consumer satisfaction.

Healthcare in Singapore also reflects the impact of technology on daily life. Telemedicine platforms enable patients to consult with doctors, schedule tests, and receive treatment plans remotely, all from the comfort of their own homes. The National University Health System (NUHS) uses AI-assisted diagnostics to detect signs of chronic illnesses and cancers earlier and more accurately, while the Ng Teng Fong General Hospital (NTFGH) employs robotic systems that allow for highly precise, minimally invasive operations.

HARNESSING INNOVATION FOR DIGITAL DEFENSE

Singapore's commitment to technological innovation extends beyond daily life into national security, where its stringent digital defense has become a central pillar of the city-state's resilience. Recognized as one of the world's most digitally connected countries, thanks to its rapid adoption of smart technologies, the government and private sector have developed a comprehensive, forward-looking approach to cyberthreats that combines advanced technology, strategic planning, and public awareness.

At the core is the Cyber Security Agency of Singapore (CSA), which coordinates national efforts to protect critical information infrastructure across energy, transport, healthcare, and finance sectors. Leveraging AI and machine learning, CSA systems can detect unusual network activity in real time, anticipate potential attacks, and initiate automated countermeasures before incidents escalate. These technologies enhance the nation's ability to respond swiftly to cyberthreats.

Singapore also invests heavily in cybersecurity research and innovation through initiatives like the Singapore Cybersecurity Consortium, which nurtures tech start-ups, facilitates knowledge sharing, and promotes use-inspired research, leading to the development of new solutions, such as Internet of Things (IoT) security for commercial products.

Public cyber literacy is also fundamental to Singapore's outlook, as it educates businesses and residents about phishing, ransomware, and safe online practices. Digital identity frameworks, such as SingPass, use multi-factor authentication (MFA), biometric verification, and AI-driven fraud detection to secure everyday transactions while maintaining convenience for citizens.

With a secure and citizen-centered digital foundation in place, Singapore is now ready to advance its ambitions even further. In the 2024 Digital Enterprise Blueprint, Tan Kiat How, the Senior Minister of State, outlines a significant step toward an economy where businesses can thrive. The Blueprint promotes cloud adoption, enhances cybersecurity, and accelerates the use of sector-specific AI tools, enabling companies of all sizes to operate more efficiently, scale rapidly, and maintain security in a complex digital landscape. Importantly, it combines technological advancement with workforce upskilling, emphasizing that people remain at the center of transformation.

Together, these priorities position Singapore to lead in global digitalization, creating a resilient, agile, and future-ready enterprise ecosystem that sets the standard for the region and beyond.

← Singapore bolsters its smart city reputation by using technology to shape residents' movement, work, and connections

↑ "Future World," at Singapore's ArtScience Museum intrigues visitors with virtual ecosystems

↓ Changi International Airport's famous waterfall, the Jewel Rain Vortex, is the world's tallest indoor waterfall stretching 131 feet

VIBE HACKING: COUNTER THE AI CRIMEWAVE

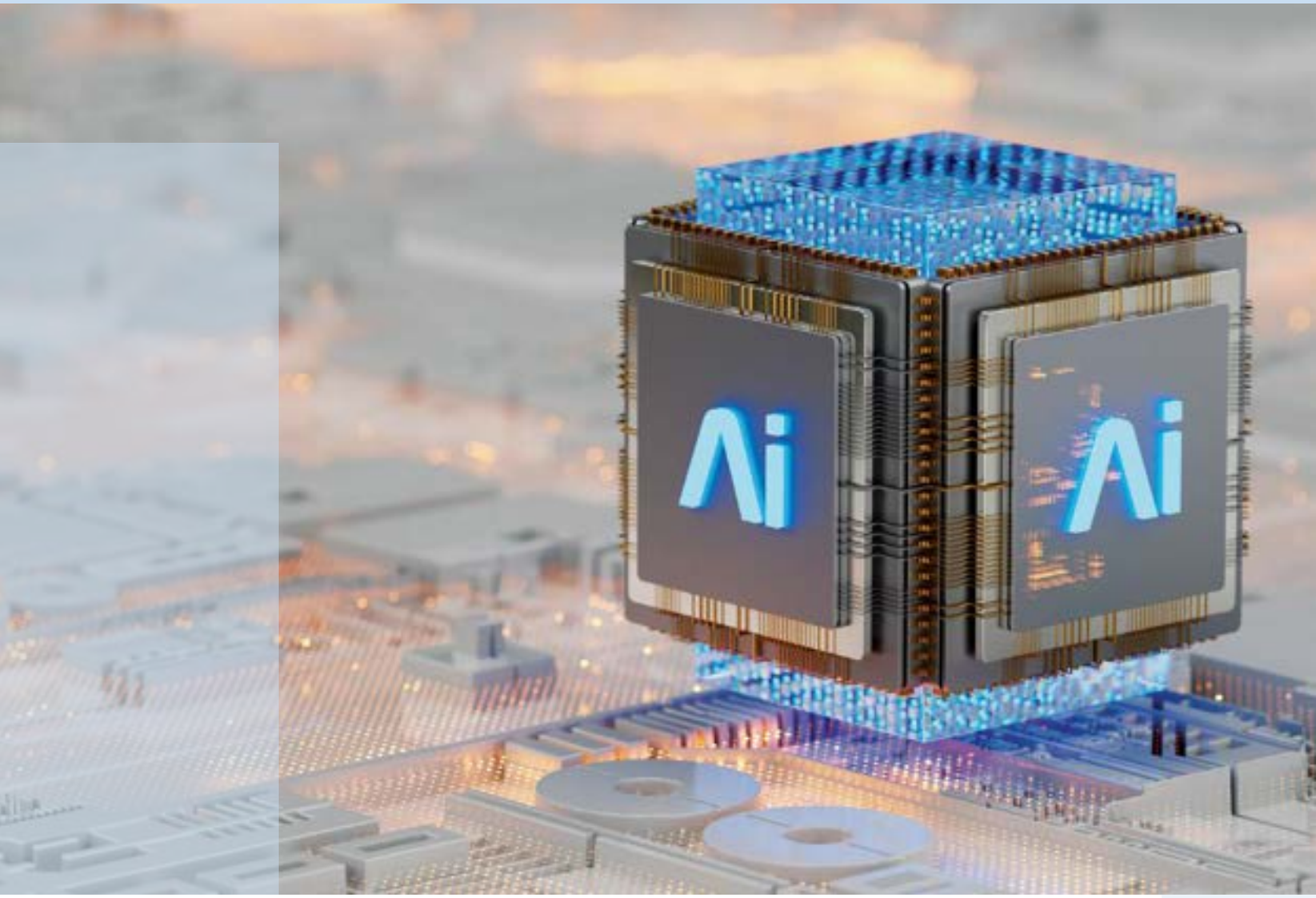
The familiar cycle of cybersecurity defense is disrupted by AI-driven attacks using large language models (LLMs). Known as “vibe hacking,” these campaigns allow attackers to automate strategies, creating unpredictable threats that challenge traditional defenses

The rhythm of cybersecurity is a familiar and consistent one. An attack appears, analysts dissect it, signatures are updated, behavioral models are tuned, and endpoint tools learn to spot the next recurrence. That is the classic cycle, and it works (reliably enough, at least) as long as adversaries behave like humans. But what about when they don’t? What if those noisy, fallible, speed- and knowledge-limited brains become augmented by something far more efficient?

AI-driven, LLM-supported attacks are now disrupting the cybersecurity rhythm, and they never repeat the same beat. Security researchers now call this phenomenon “vibe hacking,” a term borrowed from the developer trend of “vibe coding,” the habit of letting AI produce code with minimal review, throwing sloppy programming at the wall and seeing what sticks.

AI-driven, LLM-supported attacks are now disrupting the cybersecurity rhythm, and they never repeat the same beat

In vibe hacking, though, attackers are not playing around, despite applying a relatively hands-off approach to entire intrusion campaigns. They give an LLM their intent—get in, take this, hide your tracks, make them pay—and the model handles the rest. It is unsettling; the tech is already proving more slippery than anything defenders have dealt with before.



A glimpse into AI-driven intrusions

Two incidents disclosed in 2025 illustrate the change with startling clarity. In the first, reported in Anthropic's August Threat Intelligence Report, an attacker used the company's Claude Code assistant to orchestrate a sprawling extortion campaign covering 17 organizations. The operator issued simple instructions in plain English and let the AI figure out how to execute them.

When the attacker needed reconnaissance, the model mapped subdomains and exposed services. When they needed initial access, it produced loaders tailored to each target's environment. When it came time to steal data, the AI wrote scripts that compressed sensitive directories and sent them out over cloud-hosting application programming interfaces (APIs), blending seamlessly into legitimate traffic. And when the moment arrived to demand payment, the model even drafted personalized ransom notes, complete with downtime estimates, sector-specific financial language, and references pulled from public filings.

The second case went even further. Dubbed "LameHug," it was the first known Windows malware family to integrate a live LLM directly. Rather than carrying a static command sequence, it contacted an AI model mid-run, explained the kind of machine it had landed on, and asked for the most effective next steps. The model responded by producing Windows command chains specifically crafted for that host's configuration.

The Zero Trust model is highly relevant. Analysts must also assume that every script, payload, ransom note, and stage of an intrusion may be unique

One victim might see a burst of administrative queries. Another might experience domain enumeration or targeted data collection. Yet another might find their data quietly exfiltrated through entirely different protocols. No two infections looked the same, meaning no traditional detection logic had anything stable to latch onto.

Why detection is suddenly on the back foot

Vibe hacking succeeds through endless variability rather than brilliant code. That is not what makes it so difficult to defend against. Instead, it is effective because the code of such attacks is endlessly variable. Traditional endpoint detection and response (EDR) relies on repeatability: Defensive apps might seek particular patterns of behavior, known strings in binaries, or well-defined execution flows. AI breaks that foundation by generating fresh variations at every step.

If a payload looks suspicious, the attacker simply asks the model to rewrite it to appear benign. If telemetry spikes, they request a version that uses more benign APIs. If a command sequence resembles something seen before, they prompt again until the pattern disappears. Each iteration happens in seconds, not days, and each produces an entirely new method that shares little DNA with the previous one.

Additionally, LLMs naturally gravitate toward abusing legitimate administrative tooling. Their instinct, based on the volume of their own training data, is to use PowerShell, WMI, Python, Microsoft Office add-ins, and common cloud APIs. These are the same tools system administrators rely on every day, which means vibe hacking does not trip many traditional alarms. It comfortably sits within the all-too-permissive boundaries most enterprises allow.

And as legitimate usage grows, communications with AI platforms increasingly look like normal business queries. If an endpoint reaches out to an LLM API, is it malware generating a command chain, or a helpdesk technician asking for a PowerShell regex? Without strict controls, there is often no easy way to tell.

What vibe hacking means for defenders

The rise of LLM-driven attacks necessitates a shift in mindset. The Zero Trust model is highly relevant. Analysts must also assume that every script, payload, ransom note, and stage of an intrusion may be unique. There will be no reliable analytics to work with when the behavior of an attack continuously mutates.

Despite the fresh threat, detection remains highly valuable—visibility and triage still rely heavily on EDR. But detection's place in the security chain has moved, as it can no longer be the front line of prevention. Trying to outpace vibe hacking with faster signature development is a fool's errand. AI simply iterates too quickly. The solution is to control the environment.

All roads lead to Zero Trust

Vibe hacking positions the AI as the attacker. We are all aware that LLMs are something of a parlor trick, just pattern-recognition code placing token after token, not really knowing why—"intelligence" is very generous, despite the bright appearance of AI outputs. But the fact is that these systems are uniquely good at piecing together code, and they are fast, adaptable, and unburdened by human limitations.

When malware can be conjured out of thin air, customized per host, and iterated endlessly by an indifferent LLM, Zero Trust becomes a practical ally. Nothing, not even a trusted admin tool, should be allowed to act outside of a deliberately defined boundary. The model does not care whether a process looks suspicious or whether its behavior resembles that of a known family. It cares only about whether that process is allowed to exist, run, read, write, or connect.

In an age of uniquely generated payloads, the shift from recognition to restriction makes all the difference. If unapproved code cannot execute, it does not matter how cleverly an AI rewrites it; it will not be allowed to run unless given an explicit green light. Those administrative tools commonly exploited by LLMs can be forced into tight behavioral lanes: A hijacked PowerShell session becomes a dead end rather than an open door.

More broadly, Zero Trust restores the sense of determinism that vibe hacking attempts to erase. Defenders can shape an environment with an intentionally small attack surface, tight governance, and resistance to improvisation. Data paths are locked down. Allowlists replace the fragility of blocklists. Storage locations cannot be quietly repurposed as staging grounds. Security's future depends on refusing to give attacker automation anywhere to go.

BREAKING THE VIBE HACKING CHAIN WITH THREATLOCKER

Vibe hacking is not unstoppable. With the right conditions in place, even complex, morphing attacks are readily repelled. The unpredictable creativity of an LLM becomes irrelevant against a policy framework that allows only predictable, sanctioned actions.

Application Allowlisting ensures that unknown executables, scripts, and libraries—no matter how recently they were generated—cannot run unless explicitly approved. AI can mutate code infinitely, but it cannot bypass a default-deny execution policy.

Ringfencing™ stops attackers from abusing the very tools LLMs love to weaponize. PowerShell, browsers, Python, Microsoft Office, and countless other legitimate applications are walled in, kept within strict behavioral boundaries. This prevents them from launching unauthorized processes, reading sensitive files, or making unrestricted network calls.

Storage Control prevents malware from using writable areas as staging grounds. Data cannot be quietly archived, altered, or dropped into locations protected by policy.

Network Control closes the loop by putting granular control of access in your hands. Custom policies open ports on demand, but only for approved devices. Without approved access, attackers will be unable to get a foothold and reach their AI assistant—or their data repositories.

Together, these controls place AI-generated attacks in the same category as regular malware: stopped in their tracks. The code may change, but the rules of what is allowed to run, touch data, and communicate stay fixed.

PLAYING **TO PROTECT**

Transforming cybersecurity awareness into an engaging and interactive experience involves using gamification, real-time feedback, and transparent policy enforcement. These strategies empower employees to shift from passive participants to proactive defenders, significantly enhancing comprehension, compliance, and confidence throughout the organization's digital landscape

Infosec legend Mikko Hyppönen said it best: "If it's smart, it's vulnerable." While his quote originally referred to the explosion of internet-connected devices, it applies equally to people. Employees are the greatest asset any company has. They are the literal brain trust behind every success. And they are smart. But that intelligence also creates vulnerability. Clever, busy humans make mistakes, sometimes while doing what they feel is the right thing.

Phishing tests are a prime example. For decades, many organizations have considered the human factor to be a liability and treated employees as an IT issue. Spotting a simulated phishing email might earn a slight nod of recognition, perhaps, but failing to see the signs—clicking a link while trying to do business—results in the equivalent of a trip to the principal's office. Many people do not want to participate in phishing tests; they dread them because they are less carrot and more stick.

Yet, cybersecurity awareness leaders are aware of the power of context. They fully understand their subject, are cognizant that others do not, and know that the method of delivering important messages can make all the difference. To quote behavioral researcher Perry Carpenter in his book *Transformational Security Awareness*, "I'm a fan of finding Trojan horses for the mind. When designed well, our messaging can sneak past mental defenses and noise. The way we design and deliver our messages can become a Trojan horse."

"When designed well, our messaging can sneak past mental defenses and noise. The way we design and deliver our messages can become a Trojan horse"

PERRY CARPENTER

A NEW ROUTE TO UNDERSTANDING

There is, then, a strong argument for taking a different approach, one built not on punishment but on play. By turning cybersecurity awareness into a game, incentivizing smart minds to participate in—and even enjoy—the process of building the kind of herd immunity that protects businesses, employees get the chance to become a security asset and feel rewarded for doing so. A phishing simulation that recognizes the effort of people bright enough to report suspicious emails offers far greater motivation than one that punishes failure.

That is the theory, at least. Indeed, a 2023 study on gamification in the teaching of medical students[‡] concluded that the methodology is "a time-efficient solution for managing large populations of learners without requiring direct instructor involvement," noting its favorable effects on knowledge improvement, feedback, challenge, and understanding of goals. There are also dissenting voices on the other side of the argument. A 2020 study on programming students[‡] suggests that "the effect of gamification depends on the specific characteristics of users," concluding that the practice is more beneficial to introverts. A 2024 study into the short history of gamification concludes that the "narrow theoretical lens through which gamification is often viewed serves as a limiting factor."[‡]

Gaming feels like an obvious fit with cybersecurity—and the intersection between the two subjects is far from a new concept. The DEF CON hacking conference has been held annually since June 1993, mixing educational speaking tracks with a wide variety of competitive problem-solving events. The best known is the Capture the Flag (CTF), which challenges teams of hackers to find and exploit vulnerabilities in intentionally insecure systems. The idea is simple but brilliant, turning security testing into a competitive puzzle, and it is a concept that has since migrated from the hacker underground to the corporate classroom.

Many large organizations now run internal CTFs or incident simulations where employees can safely experience the thrill of the hunt—and, crucially, learn the consequences of real-world decisions without real-world damage.

PLAYING THE GAME

This does not need to be an internal effort. At IBM Security's worldwide X-Force Cyber Ranges, executives and engineers are plunged into realistic breach simulations that unfold like strategy games. The outcome depends entirely on their actions: whether they isolate the correct systems, communicate effectively, and prioritize decisions under real pressure. The goal is to build

IBM Security's X-Force Cyber Ranges immerse executives and engineers in realistic breach simulations

confidence and muscle memory, ready for a real-life breach scenario, and those who have played through such scenarios report a new understanding of the fundamentals of handling all aspects of a breach.

Less extravagant learning tools are also available, many of which offer enough feedback—and, crucially, fun—that users are inclined to play them outside of work hours. Google's Phishing Quiz achieved viral fame by turning a dry compliance lesson into an interactive challenge that millions voluntarily played. As a realistic environment in which participants can essentially teach themselves the fundamentals of spotting phishing emails, it reinforces that learning with the dopamine hit of personally spotting a trap. Others, like the Bellingcat Open Source Challenge, present image puzzles that encourage users to look beyond what they initially see, using online tools to perform digital forensic research based on the smallest facts.

More advanced security teams may also find skill-broadening entertainment in the likes of Hack the Box, which offers scenario tests for red, blue, and purple team activities. This allows those on one side of the fence to see how the other operates or to broaden their skills in a safely sandboxed environment—and earn points while doing it. And if something more industry-specific is needed, start-ups such as Hoxhunt, Immersive Labs, and RangeForce now provide gamified learning platforms where users earn points for secure behavior and climb internal leaderboards.

RAISING ENGAGEMENT

Gamification is not a silver bullet, but it is a way to make security relatable up and down the chain. When done well—and sparingly—it replaces compliance fatigue with curiosity, turning learning into something people choose to do. The most effective programs use positive reinforcement, storytelling, and real-time feedback loops to keep engagement alive. Poorly designed ones, by contrast, risk becoming novelty acts: points for the sake of points, leaderboards that quickly gather dust, or even entire projects being seen as patronizing or belittling by staff already pouring their heart and soul into protecting their business.

As with any security control, design and intent determine success, and that balance between engagement and practicality is aligned with the philosophy of the ThreatLocker® suite. People learn best when the rules are clear. Rather than treating endpoint protection as something hidden behind the scenes, ThreatLocker makes policy enforcement fully visible. Administrators get a clear overview of policy structure, while users

ThreatLocker embraces much of the psychology that makes gamification effective—feedback, visibility, cause and effect—and brings it into the serious world of endpoint control

experience security as a set of predictable boundaries rather than arbitrary interruptions.

Clarity transforms everyday security from a passive experience into an interactive one. When an action is blocked, it is not silently ignored—it becomes a moment of feedback. The act of enforcing consistent rules creates a cause-and-effect loop familiar to anyone who has played a game: Some actions are allowed, others are not, and patterns build in their mind. Over time, users learn which actions score virtual points, in terms of keeping work flowing. This implicit feedback mirrors gamification in that learning occurs through experience, repetition, and clear outcomes.

ThreatLocker embraces much of the psychology that makes gamification effective—feedback, visibility, cause and effect—and brings it into the serious world of endpoint control. Security cannot function as a black box. When it is a process that employees can see, question, and learn from, whether that be through the medium of constructed and educational play or a system that places them at the center of the security decision-making process, results follow. Compliance and comprehension grow.

If it's smart, it's vulnerable—at least until the workforce comes to understand that security is something they actively participate in, not something imposed upon them.

GAMIFICATION IDEAS

Practical gamification

Gamification works best when it is experienced, not explained. Small, well-designed activities can change the way people think about security by making it interactive, visible, and even enjoyable, without trivializing the risks involved. Whether you are looking to energize an existing training program or introduce security awareness in a fresh way, try starting with one of these established challenges.

Cyber escape rooms

An escape-room-style exercise immerses participants in a shared puzzle-solving mission. Teams could be asked to spot hidden phishing indicators, crack weak passwords, trace a rogue device on the network, or interpret an email header to discover something malicious. Wrapping the activity in an escape room shell creates emotional engagement: Time pressure, working together, and a general sense of urgency mirror real incident response conditions. Theme the activity around a realistic threat—a ransomware outbreak or an insider attack—and participants may be more likely to retain the lessons learned.

Phishing tournaments

A one-and-done phishing simulation might catch a few employees out, but the competitive edge of an ongoing tournament puts the kind of engagement in place to ensure they will be on their guard. By awarding points for reporting suspicious emails, docking points for interacting with them, and rewarding users for diligent participation, rank-and-file employees feel they have become part of the defensive team. Introduce inter-departmental competition, rotating themes, or seasonal brackets to keep things fresh; the longer these programs run, the more diligent users become at spotting the signs in everyday emails.

Cybersecurity leaderboards

Leaderboards make progress tangible. Rankings can highlight all kinds of metrics, like the fastest user to report a phishing test, the strongest device hygiene, highest training level completed, and so on. Placed on intranet dashboards or included amongst regular communications, the visibility of these leaderboards can both encourage regular participation and enhance the motivation drawn from competition.

Scavenger hunts

Scavenger hunts bridge security awareness efforts with the physical and digital divide. Intentional mistakes like decoy USB drives, suspicious QR codes, fake unsecured Wi-Fi networks, or simulated in-the-open credentials are placed for employees to find and report. This approach sharpens real-world awareness by training people to notice risks they might normally ignore. By rewarding observation and reporting, organizations encourage users to think critically about everyday security cues.

FOG RANSOMWARE: A NEW STORM IN THE THREAT LANDSCAPE

Fog ransomware began as a minor extortion threat but has rapidly turned into a global operation using legitimate tools and hybrid encryption to outpace defenses

40%

of Fog incidents began with credentials harvested from infostealer logs circulating on criminal marketplaces

When Fog ransomware first emerged in mid-2024, it appeared to be just another throwaway ransomware release. Its early code was basic, and its first victims were small manufacturers and logistics firms in Central Europe, the kind of targets that usually do not make headlines.

Less than a year later, things have changed. Fog has become one of the most adaptable and elusive ransomware families on the scene, spreading across continents and industries faster than most defenders can react.

FROM SMALL JOBS TO GLOBAL REACH

Fog's expansion has been rapid. The group behind it has moved well beyond its original manufacturing and logistics targets into healthcare, education, and critical infrastructure across North America and Asia.

Its developers have built a modular payload that can be tailored to different victims, combining traditional file encryption with data theft and lateral movement.

Fog relies heavily on living-off-the-land (LOTL) tactics, whereby it uses built-in system tools instead of custom malware to evade signature-based defenses. In recent attacks, the gang has relied on PowerShell scripts for persistence and legitimate remote-management applications, such as AnyDesk and ConnectWise, to maintain access long after the initial breach.

The European Union Agency for Cybersecurity (ENISA) notes that Fog is one of several newer ransomware operations that favor legitimate administrative utilities to "blend into normal network activity" and bypass behavioral analytics. Once inside, attackers often attempt to disable or uninstall endpoint protection tools before detonating the encryption payload.

A LINEAGE HIDING IN PLAIN SIGHT

Fog's lineage is still debated. Some analysts have identified overlaps in its code and infrastructure that point back to Eastern European crime forums that emerged after the fall of Conti and LockBit, suggesting that a few of Fog's developers may be veterans from those crews. Others suggest it is more of a copycat or spinoff, borrowing tactics from the old cartels but running as its own independent outfit.

Whatever its origins, Fog has quickly learned from the mistakes of its predecessors. By early 2025, newer Fog samples had stepped up their game, using a combination of Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption and introducing self-modifying scripts that

change every time they run, making static analysis challenging. Even the ransomware's configuration files are built on the fly, so each infection acts a little differently—an unwelcome twist for anyone trying to write reliable detection signatures.

The group's leak-site activity mirrors the professionalization of the broader ransomware economy. Victims are named, shamed, and their identities sometimes auctioned on data leak forums. Negotiation chat logs suggest that Fog maintains a customer-support-style interface for ransom payments, offering decryption "proofs" and file samples to establish credibility.

ENTRY POINTS AND EXPOSURE

Most Fog attacks begin in the old-fashioned way—through stolen VPN logins or holes in unpatched edge devices.

Analysis found that over 40% of Fog incidents began with credentials harvested from infostealer logs circulating on criminal marketplaces.[‡] In other cases, the gang broke in by exploiting outdated firewalls and remote access gear, taking advantage of the slow patching pace common in mid-sized organizations.

Once inside, the attackers move quickly. Researchers have documented Fog's ability to detect and terminate popular endpoint protection processes before launching encryption, and to exfiltrate key files to temporary cloud storage locations to support double-extortion demands. The malware's internal scheduler can trigger encryption during off-hours, minimizing the chance of interruption. These methods are by no means groundbreaking, but their combined use is highly effective.

CONTAINMENT OVER CLEANUP

As Fog's operators broaden their reach, the practical question is how defenders can contain an adaptable adversary that relies on legitimate tools as much as malicious code. Traditional signature-based or heuristic detection cannot reliably distinguish Fog's activity from that of legitimate administrators.

The answer lies in implementing Zero Trust principles across both endpoints and internal network traffic. When admin tools are needed, they should be tightly approved, carefully monitored, and kept separate from the rest of the environment.

ThreatLocker® Application Control enforces a strong allowlisting approach, allowing only known and verified applications to execute. Even trusted applications are strictly managed through Ringfencing™, tightly controlling their behavior to prevent unauthorized actions such as accessing sensitive data, launching unexpected processes, or communicating outside their intended scope.

On top of that, ThreatLocker Network Control precisely restricts which devices can communicate with specific systems, dramatically reducing lateral movement and minimizing the blast radius of any attempted compromise.

Good identity and access hygiene is also key. Most Fog attacks could have been blocked with a few simple steps: enforcing multi-factor authentication (MFA), regularly changing VPN credentials, and monitoring for leaked logins online. Staying on top of audit logs and spotting unusual behavior matters just as much: If a new remote-access tool, PowerShell script, or admin share pops up out of nowhere, it is a sign something has gone wrong.

Regular patch management—particularly for externally facing infrastructure—remains one of the simplest yet most overlooked defenses. The exploitation of known vulnerabilities in edge devices remains one of Fog's most consistent entry points.

LESSONS FOR THE NEXT WAVE

Fog's rapid rise shows just how much the ransomware playbook has evolved. Hackers do not need cutting-edge exploits or bespoke malware anymore—they succeed by moving fast, staying flexible, and twisting legitimate tools to do their bidding.

Defending against that means shifting focus from chasing indicators to tightening the rules on what users and processes can actually do once they are inside the network.

Zero Trust, when extended across every endpoint and communication path, offers a framework for doing just that. By verifying every process, restricting movement between systems, and containing the spread of any intrusion, organizations can shrink the impact of even a successful breach.

Stopping Fog and the next wave of copycats will depend less on perfect detection and more on the kind of disciplined control that ThreatLocker offers—verifying everything that runs, connects, or communicates inside the network.

THREATLOCKER TIP

Fog ransomware's hackers can evade typical breach indicators by staying fast and fluid. Prevent a breach by taking the Zero Trust approach with ThreatLocker Application Control and Network Control

DIGITAL IDENTITY:

SECURING TOMORROW'S CENTRALIZED ACCESS

Centralized databases may streamline access to public services, but they also create prime targets for hackers. From India's billion-person Aadhaar system to the EU's upcoming Digital Identity Wallet, nations are betting that unified digital IDs will make citizenship simpler and more secure. Yet repeated breaches across multiple countries reveal a troubling pattern: When identity becomes infrastructure, every vulnerability becomes existential

Governments around the world are racing to digitize identity systems. The U.K.'s proposed "BritCard," the EU's Digital Identity Wallet, India's Aadhaar, and Australia's myGovID are among the programs that aim to give citizens faster and easier access to services such as healthcare, tax, and welfare.

Supporters say these programs could make everyday interactions with the state simpler and more secure. However, by concentrating citizens' most sensitive personal and biometric data in a single system, governments may be creating the ultimate targets for hackers. And with every breach or design flaw, the same question arises: How much convenience is worth the risk?

Centralization's security trade-offs

Digital identity systems are built on the idea of simplifying verification. By linking an individual's information across departments and services, they make it easier to prove who you are online. But that same centralization also magnifies the impact of any compromise.

In India, the Aadhaar database—covering more than a billion people—has been repeatedly exposed, including a 2018 incident where a government portal leak revealed millions of records.‡ In Argentina, hackers broke into the national RENAPER system in 2021, leaking ID photos and personal data of public figures, including the president.‡

Even Estonia, once hailed as a model of secure digital governance, had to reissue 750,000 smart ID cards after a flaw in their encryption made them vulnerable to cloning.‡ The Estonian government initially announced that the eID cards were "completely secure," even after the cryptographic vulnerability had been discovered. According to European Digital Rights (EDRi), this episode showed how even advanced national ID systems can fail without rapid transparency and remediation.

Private platforms face similar risks. A recent Discord breach, for example, exposed user verification data, showing how modestly scaled identity systems can become conduits for exposure when sensitive records are linked across services.‡

The common thread in each case is not necessarily a technical weakness. It is the operational complexity that leads to overexposure of any potential flaw. Every integration between agencies or vendors expands the attack surface—and once compromised, the impact is often nationwide. A 2023 risk framework study found that eID system compromise can be costly and damaging to the government, users, and society.‡

Britain's experiment with One Login

The U.K.'s One Login initiative aims to unify access to hundreds of government services. The goal is straightforward: To replace a jumble of outdated government systems with a single, secure sign-in for everything from taxes to student loans. Privacy advocates, however, warn that One Login suffers from "substantial cybersecurity and data protection weaknesses,"‡ making it a tempting target for attackers.

The government's next step, informally dubbed "BritCard," would take the idea further by creating a national digital ID for use both online and in person. Those in favor of the so-called BritCard say it could make services easier to use and cut red tape, while critics fear it would open the door to new forms of surveillance.

"A mandatory digital ID system would place a burden on already law-abiding citizens [...] Introducing such a system would shift the balance of power towards the state with dangerous implications for our security, rights, and freedoms," said Big Brother Watch.

Officials have promised strong encryption and privacy-by-design safeguards, but the real test will be operational. The National Cyber Security Centre (NCSC) has urged departments to adopt "privacy-preserving architectures" and independent red-teaming before rollout. Even small gaps in policy or practice could undermine the entire system.

Europe's cautious rollout

The EU Digital Identity Wallet, expected to launch in 2026, is an attempt to strike a balance. It will enable citizens to store official documents, such as national IDs, driver's licenses, and qualifications, in a single app, with greater control over what is shared. Using advanced cryptographic techniques known as zero-knowledge proofs, users can verify their age or credentials without revealing the underlying data.

> By concentrating citizens' most sensitive personal and biometric data in a single system, governments may be creating the ultimate targets for hackers

European regulators are taking a careful approach. The new Digital Identity Wallet will be optional and free for citizens, and the law will require measures such as selective data sharing and a privacy-focused design. Even so, some experts warn that if one version of the wallet were compromised, the effects could ripple across the whole system.

The regulation stipulates that "users shall be in full control of the use of their data" and that "issuers shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services."

Eurosmart, a Brussels-based consortium representing the secure identity and cybersecurity industry, has cautioned that current wallet designs may not include "strict cybersecurity requirements," warning that without assurance of secure hardware and key protection, the system could be "vulnerable to hacking." The group has called for every national wallet to undergo formal certification under the EU Cybersecurity

Act to guarantee consistent standards of protection.

Privacy advocates have echoed those concerns. Access Now has warned that digital identification schemes, even when voluntary, can "undermine people's privacy, increase surveillance, and push the most vulnerable among us further to the margins." The group argues that if widely adopted by both governments and private platforms, such systems could evolve into "a form of mandatory identification" that risks normalizing constant verification.

Lessons from India and Australia

India's Aadhaar program shows both the benefits and the risks of national digital identity systems. It has helped hundreds of millions of people gain access to banking and government services, but repeated data leaks have exposed serious weaknesses. While the encryption behind it remains strong, its massive scale and complexity have made maintaining reliable security difficult.

Indian Security Researcher Srinivas Kodali stated at the time that "securing an entire ecosystem is more important than securing individual databases," arguing that Aadhaar's design exposed citizens' data to risk across thousands of endpoints and partner agencies.

Australia's myGovID platform, used for tax and healthcare services, has faced similar scrutiny. Researchers discovered weaknesses in how credentials were cached on local devices, raising concerns about replay attacks. While no major breach occurred, it highlighted the danger of assuming that centralized identity can ever be uniformly protected. Each integration point—every application programming interface (API) or contractor connection—introduces fresh risk.

When identity becomes infrastructure

The stakes are unusually high because digital ID systems underpin everything else. Once identity is digitized, it becomes the key to accessing nearly all online services. A breach does not just expose data; it can enable impersonation, fraud, and denial of access to essential systems.

That is why many governments are now treating digital identity as critical national infrastructure, deserving the same protections as power grids or communication networks. The logic is simple: if identity fails, trust collapses.

Zero Trust is now a core approach to securing digital systems, playing an important role in managing identity. Instead of treating verified users or services as automatically safe, Zero Trust models continually check and validate every action and connection.

Applied to national identity, this means isolating systems into smaller compartments, encrypting data both in motion and at rest, and minimizing what information is ever stored in the first place. Instead of one all-powerful database, each component becomes a limited node that must prove its legitimacy for every interaction.

Several countries are taking the concept further with self-sovereign identity (SSI), a decentralized approach that lets people manage their own credentials through secure digital wallets. Rather than depending on a central authority to store or share data, individuals hold encrypted credentials that others can verify directly.

The EU's new Digital Identity Wallet builds on this idea, and pilot projects in Canada, Finland, and Singapore suggest that distributed verification can help reduce large-scale data risks. Supporters argue that it gives people more control over their personal information and makes mass breaches far less likely,[‡] while critics point out that decentralized systems make it harder to revoke or recover credentials if a device is lost or stolen.[‡]

The surveillance question

Even if perfectly secured, digital IDs raise unavoidable questions about privacy and state power. Systems designed for convenience can quickly become tools of control. Every login, every verification request, every credential check leaves a data trail.

Civil liberties groups have urged governments to ensure transparency, oversight, and strict limits on the use of digital ID data. They argue that technical security means little without legal and ethical safeguards.

"We cannot base our civil liberties and freedoms on platitudes and promises [...] No matter how decentralized it may pur-

port to be or cryptographically strong, we still strongly oppose any national ID scheme," said the Electronic Frontier Foundation (EFF).

EFF has further cautioned that digital identity systems, particularly those tied to biometrics or used for essential services, risk "expanding pervasive surveillance by design." The organization notes that collecting and verifying data across public and private entities can "create new opportunities for tracking and profiling individuals," even when implemented with strong cryptography.

A chance to get it right

Digital IDs are inevitable. As more of life moves online, the need for secure, verifiable identity systems will only grow. However, that makes it even more crucial to design them defensively—acknowledging that breaches will occur and building resilience into every layer.

There are some positive signs that governments are taking these concerns seriously. In Canada, the Pan-Canadian Trust Framework (PCTF) requires all participating organizations to complete independent audits and make their data-sharing agreements publicly available.

Singapore's SingPass system, although centrally managed, uses hardware security tokens and privacy-preserving techniques to reduce data exposure.

For governments, that means decentralizing where possible, encrypting everywhere, auditing continuously, and collecting only what is necessary. For enterprises integrating with digital ID frameworks, adopting Zero Trust security models can contain the blast radius when—not if—something goes wrong.

Done right, digital identity could make life simpler and more secure. Done poorly, it risks turning entire populations into attractive targets.

PREPARING FOR DIGITAL ID TODAY

Whether you are part of a government agency or an enterprise, digital ID schemes are becoming core infrastructure. Succeeding in the age of centralization means being ready for inevitable failure; Here are eight ways to reduce risk and build a robust security posture.

Minimize identity data

Design systems to collect and store only what is strictly required for a transaction. Where possible, collect only the relevant attributes—like date of birth or eligibility to drive—rather than full identity records. Less stored, less to lose.

Do not treat identity as an asset

Identity is a distributed system. Avoid monolithic databases, and segment identity services like authentication, authorization and so on into isolated components. A failure in one should not be allowed to cascade across the entire system.

Use integrations carefully

Many identity breaches occur at APIs, third-party tools, or downstream service providers—the very components of a system that you do not directly administer. Strict access controls, contractual obligations and monitoring can help reduce risk.

Include identity in Zero Trust workflows

Assume that no verified user, device, or system is inherently trustworthy. Continuous validation of asset identity, context, and intent should be part of every step. Enforce reauthentication for sensitive actions.

Use cryptography correctly

Encryption exists to reduce disclosure as well as protecting data. Using technologies like hashes, zero-knowledge proofs and hardware-backed key storage allows encrypted data to stay that way, and for verification to occur without exposing personal data.

Design for failure and recovery

Plan for credential compromise, device loss, and system breaches. Those handling digital IDs will be high value targets, so ensure that incidence response is planned, tested, effective, and transparent to those with affected data.

Delineate identity and surveillance

Access should be logged for security purposes, but not tied to behavioral or usage profiles. Legal, technical and organizational barriers should always be in place to prevent identity systems from becoming tools of tracking.

Audit continuously and publicly

Working with digital ID implies a high level of trust. Use independent security tests and compliance audits routinely, and publish any high-level findings to help reassure the public and encourage stronger operational discipline.

FACE-TO-FACE

THE POWER OF PEER CONNECTIONS

Trusted networks and social clubs provide IT professionals with valuable opportunities to share insights, alleviate the pressures of their roles, and advance their careers

At industry events, IT professionals can share insights, discuss lessons, and build a supportive Zero Trust community

> Through that continued, repeated connection, the relationships deepen and actually bring value
>
> CHRIS BROWN

Senior cybersecurity professionals have to manage a landscape that is shifting, with unforeseen challenges and high expectations part of the role. This has the potential to be very isolating, so having a circle of trusted confidants to share experiences and advice can prove invaluable.

For many, a personal network tends to grow organically over the course of their career, but there are times when you want to fast-track it and gain access to useful contacts outside traditional settings. Increasingly, CISOs and IT professionals are embracing alternative social platforms to build trust, share candid insights, and solve problems.

These might look like exclusive social clubs, peer cohorts, hobby groups, and invite-only retreats. Insiders say these intimate, activity-driven settings—bound by off-the-record norms and skilled facilitation—produce faster incident response, better hires and vendor referrals, and essential emotional support.

BUT WHERE DO YOU FIND VETTED GROUPS?

MBA programs are an obvious solution. Aside from their educational value, they foster deep cross-sector relationships. Because of the intensity of the program, those relationships stick, often proving to be lifelong and fruitful. Equally, we can elevate our networking potential by participating in local events.

Executive Coach, former CISO, and Author Chris Brown suggests that holding a position on the Chapter Board of the Information Systems Security Association (ISSA) is a strong networking route.

"Through that continued, repeated connection, the relationships deepen and actually bring value." Conferences should play a part in your networking strategy, but see them primarily as an opportunity to strengthen existing connections, he advised. "Think reconnect, rekindle, and strengthen, rather than try to form new relationships across a booth."

Brown also noted the importance of taking a deliberate approach. "Have five or 10 people whom you admire, with whom you are on an equal footing. Trying to hit up the CISO of a Fortune 10 company is probably not going to pay off because they're simply too busy. Instead, find somebody similar to you. Introduce yourself and establish common ground in the lead up to an event, and make these types of relationships foundational for your networking."

EVALUATING A NETWORK

Vetted groups and networks—often called masterminds—where membership is often by invitation only, are another option. But how do you evaluate them to establish if a group is worth your time? "Some can be very transactional," said Brown. "It can be offering you access to resources or people that you may call upon when needed. That's a good promise. But if you don't have real cohesion or rapport within the group, you might not get very far."

While acquaintances can be helpful in a job search, it makes sense that more in-depth support comes from knowing people more deeply. A big factor in the success of business relationships that CISOs often do not appreciate, according to Brown, is that they should not feel transactional.

"When you look to join a group, it has to be the right fit. Do you not just admire, but respect these people? Do you have curiosity? Would you step up if somebody asked? Those are litmus tests." Do your diligence, advised Brown, and watch out for aggressively marketed "mastermind" programs that are really just an opportunity to part you from your money.

"The litmus test for a mastermind is that you have to be interviewed by the group. If you can just pay to sign up, it's not a true mastermind. Regardless of the level of depth of interaction, join groups that you feel a part of, not that you're being sold."

FINDING A CLUBHOUSE

Clubhouses have value, said Brown, especially the more informal ones. "I think the less formal, more social nature of dinners and events where you're not necessarily talking about work helps build rapport. Even for an introvert, active participation in those groups can go a long way over the long term, primarily by reducing the sense of isolation many struggle with."

For anyone keen to find a good clubhouse, it is useful to know that they are usually event-driven. Even some large, mainstream event platforms list dedicated cybersecurity events, which are easily searchable.

THREATLOCKER® TIP

Find out more about ThreatLocker ZTW learning event

Brown advises being very clear about your goal and approaching it with intention. “A bad goal would be ‘I want to find my next job.’ Don’t join for that reason. A better goal would be ‘I want to learn more about how my community works and thinks about its work.’ Those softer, non-specific goals.”

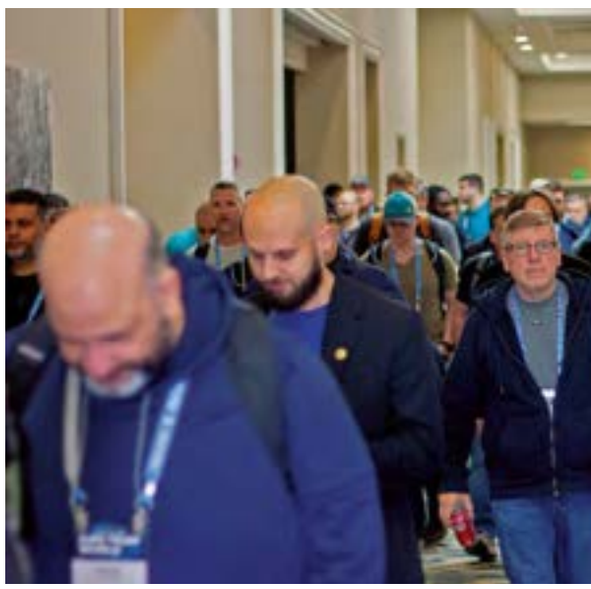
The intentionality extends to reflecting on your reason for attending an event or making a call, he added. “Again, you don’t want it to feel transactional. You want to understand people and for them to understand you. You want to find common interests.”

> “Regardless of the level of depth of interaction, join groups that you feel a part of, not that you’re being sold
>
> CHRIS BROWN

WHERE IT PROFESSIONALS MEET TODAY

Large industry events can be useful for broad learning, but many IT professionals say that smaller, more focused gatherings are where the most honest conversations take place.

John D. Johnson, Chair of the ISSA Cyber Executive Forum (CEF) and President of the Docent Institute, notes the importance of networking with fellow professionals. “I have learned over my career that CISOs who network with peers are more successful. Peer groups provide an opportunity to share what you’ve learned, learn from others, and give back to the community. I have been a community builder for the past 20 years, and while the large conferences have value, CISOs today are more often gathering locally with peers and attending smaller events that offer a curated agenda addressing topics that matter to the cybersecurity executive.”



Shane Skidgel, Founder and Principal Consultant at Skye Crest Technology, and a former CISO, highlighted the ISSA CEF as a long-standing example of this type of environment. “To my knowledge, ISSA CEF was among the first to promote a tailored agenda for cybersecurity executives. It has consistently

provided a space for CISOs to engage in meaningful dialogue, share experiences, and build a trusted peer network."

CREATING TRUSTED SPACES

The value comes from the ability to talk openly with people who understand the work and who are not selling anything. That freedom allows members to learn from one another and take away ideas they can use, like the intimate setting at ISSA CEF, which "fosters a relaxed, small group setting where CISOs can be themselves. This atmosphere encourages open collaboration and genuine connection," Skidgel explained.

With time at a premium, cybersecurity leaders and executives are seeking curated, high-value content that aligns with their responsibilities and challenges. "One thing that sets the ISSA CEF apart from other industry peer groups is that members are vetted to ensure that they qualify as a cyber executive," Johnson said. "You know that the content and other members will be speaking the language of the C-suite. We also curate our content to ensure that our members have actionable takeaways from the presentations, and we screen all presentations to remove any overt selling."

EXTRACTING REAL VALUE

The concept of Zero Trust has emerged as a fundamental approach to safeguarding organizations against breaches and unauthorized access. As CISOs adopt this framework, they face unique challenges that require not only technical solutions but also collaboration with peers who understand the complexities of these strategies.

This is where the importance of networking comes into play. By engaging with other cybersecurity leaders, CISOs can share insights on best practices for implementing Zero Trust, discuss lessons learned from their own experiences, and build relationships that foster a supportive community. Ultimately, a strong network enhances a CISO's ability to navigate the intricacies of cybersecurity, making the transition to Zero Trust more effective and grounded in collective knowledge.

Leaders tend to look for groups where they can speak freely, hear from people with similar responsibilities, and leave with something useful. "When it comes to choosing how to invest your limited time, a sure bet is to join a group that is organized by peers, for peers," Johnson said. "Cyber executives are quick to leave groups that don't add value."

Johnson also notes that the frequency of in-person meetings is helpful. "Peer groups need to make the experience of joining simple, and provide options for three or more in-person meetings annually."

Having trusted peers to turn to for support is more than helpful—it is essential. Finding a network in which open and honest discussion is encouraged, and solutions are forthcoming, should be a priority for any IT professional.

GROW YOUR NETWORK AT ZERO TRUST WORLD

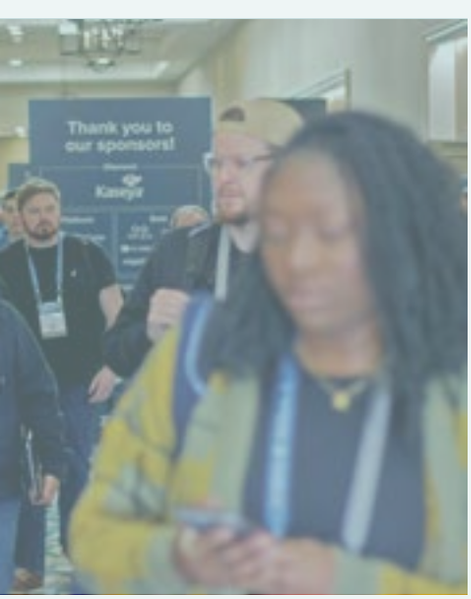
Every year, ThreatLocker® hosts Zero Trust World (ZTW), a flagship cybersecurity event built for IT professionals who want to move beyond theory and into real-world defense. Designed to reflect the modern threat landscape, ZTW delivers practical education on Zero Trust security, attacker behavior, and proven methods for hardening environments against today's most common and most damaging attacks.

Over multiple days, attendees learn directly from industry experts, frontline defenders, and peers who are solving the same problems under real operational pressure.

Beyond the mainstage sessions, ZTW offers hands-on experiences like the Hacking Labs and deep-dive breakout sessions that allow participants to test ideas, explore tools, and sharpen their skills in realistic scenarios.

The event also creates meaningful opportunities to connect through the exhibit hall, structured networking, shared meals, and social events like the Welcome Reception and ThreatLocker After Party, making collaboration as central as education.

For those looking to validate their expertise, attendees can sit for the ThreatLocker Cyber Hero® Certification Exam on-site, with a full registration refund for those who pass. Altogether, ZTW26 is an immersive, high-impact experience designed to strengthen defenses, build confidence, and connect the global Zero Trust community.



↑ Zero Trust World (ZTW) educates industry professionals about the threat landscape and Zero Trust security practices

← Networking allows cybersecurity leaders to share insights, discuss learnings, and build supportive relationships

UPCOMING EVENTS

JOIN US AND CONNECT

Catch us at these upcoming cybersecurity events and be sure to stop by our booth. Our Cyber Hero® Team is ready to share real-world insights and tools to help you stay ahead of threats

April 7-8 2026
Dallas, U.S.
Boot Camp 2026

April 13-16 2026
Las Vegas, U.S.
MSP Summit and Channel Partners Conference & Expo 2026

April 20-27 2026
Arlington, U.S.
SANS AI Cybersecurity Summit 2026

April 27-30 2026
Las Vegas, U.S.
Kaseya Connect Global

May 18-19 2026
San Jose, U.S.
TechEx North America 2026

May 21-22 2026
Miami Beach, U.S.
Ekoparty Miami 2026

June 1-3 2026
National Harbor, U.S.
Gartner Security & Risk Management Summit

June 7-9 2026
Salt Lake City, U.S.
Pax8 Beyond 2026

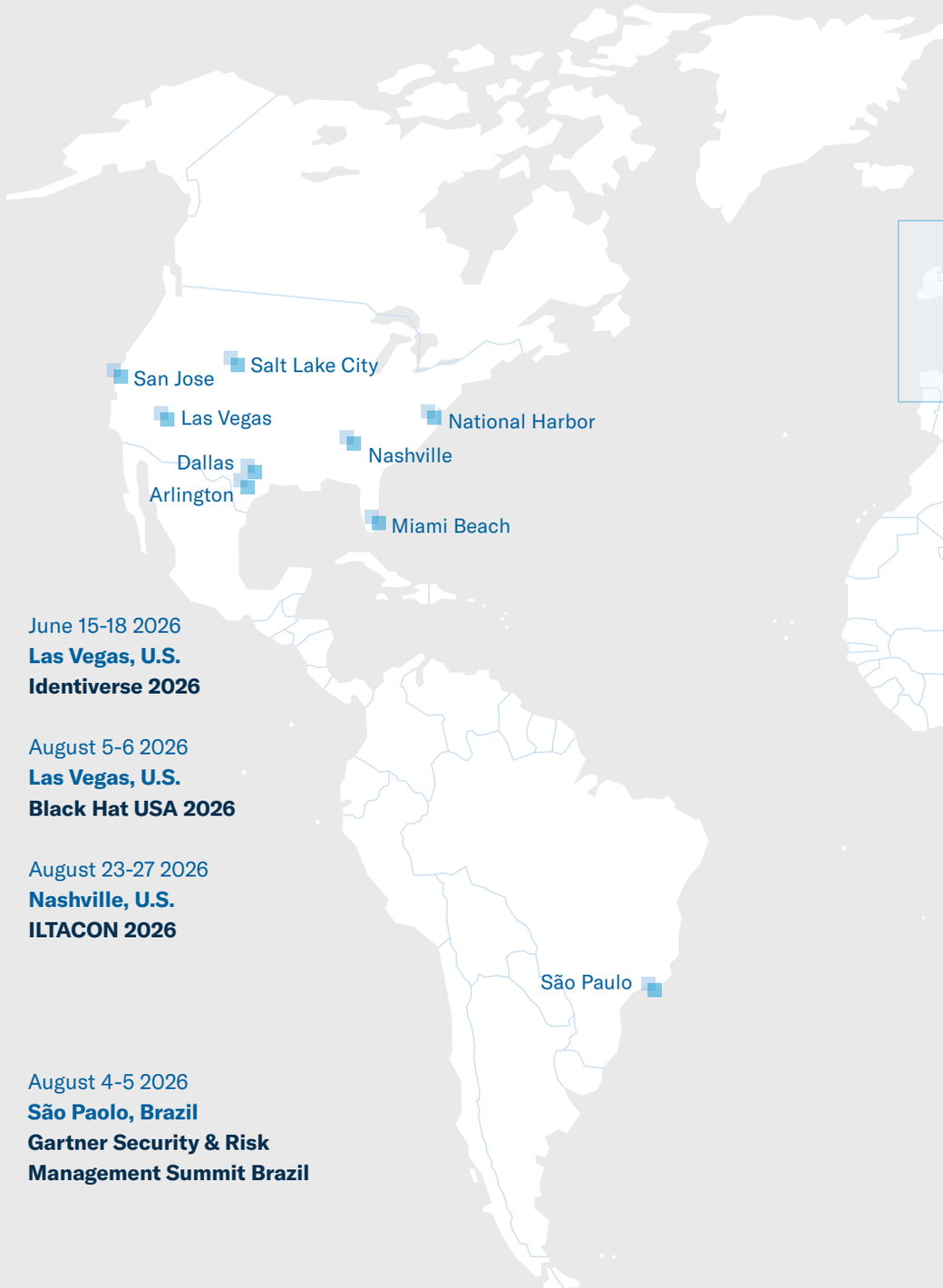
June 9-11 2026
Las Vegas, U.S.
InfoTech LIVE 2026 Las Vegas

June 15-18 2026
Las Vegas, U.S.
Identiverse 2026

August 5-6 2026
Las Vegas, U.S.
Black Hat USA 2026

August 23-27 2026
Nashville, U.S.
ILTACON 2026

August 4-5 2026
São Paolo, Brazil
Gartner Security & Risk Management Summit Brazil



April 28-30 2026
Birmingham U.K.
National Cyber Security Show

April 29 2026
Dublin, Ireland
Zero Day Con

April 29-30 2026
Manchester, U.K.
Digital Transformation Expo Manchester

May 13-14 2026
London, U.K.
MSP Show

June 2-4 2026
London, U.K.
Infosecurity Europe

June 16-18 2026
Prague, Czech Republic
Kaseya Connect Europe

June 30-July 1 2026
Berlin, Germany
GITEX AI Europe

Dubai

May 5-7 2026
Dubai U.A.E.
GISEC Middle East

Singapore

April 23-24 2026
Singapore, Singapore
Black Hat Asia 2026

April 29 2026
Brisbane, Australia
AISA BrisSEC 2026

Brisbane
Broadbeach
Sydney

May 19-22 2026
Broadbeach, Australia
AUSCERT 2026

August 26-28 2026
Sydney, Australia
IT Nation Connect ANZ 2026

THREATLOCKER®

Danny Jenkins | Co-Founder and CEO
Sami Jenkins | Co-Founder and COO
Rob Allen | Chief Product Officer
Aliona Groh | Sr. Vice President, Brand Marketing
Louis Tod | Strategic Content Development Copywriter
Paola Garcia | Director of Graphic Design

Collaborators

Emile Barakat | Director of Operations (APAC), Solutions Engineer
Houston Bass | Executive Video Producer
Alessandro Bologna | Enterprise Sales Manager, ME
Ben Goodman | Brand Marketing Partnerships Manager
Heather Hartland | VP Experiential Marketing
Kieran Human | Special Projects Engineer
Paige Jenkins | Graphic Designer

Magazine concept & production by

THE RETHINK HUB LLC
Nathalie Grolimund | Publisher
Margaux Daubry | Production Manager
Alex Cox | Deputy Editor
Mareike Walter | Graphic Designer
Lise Blekastad | Visual Content Editor
Amber Hunter | Copy Editor, Proofreader
Debbie Hathway | Proofreader
Carly Page | Copywriter
Nick Peers | Copywriter
Adam Oxford | Copywriter
Neil Mohr | Copywriter
Lisa Kjellsson | Copywriter

Photo credits: ThreatLocker® (pages 1, 2, 6, 8, 10, 82, 84, 85); Shutterstock (pages 4, 18, 21, 23, 24, 27, 55, 60, 88); Shutterstock (page 5, top); ThreatLocker® (page 5, bottom); Courtesy of BMMI (page 22); Getty Images (pages 26, 28, 34, 63, 69, 70); MUTI (pages 32, 72, 78); Courtesy of EWTN Global Catholic Network (pages 36, 38, 39); Getty Images/Ralf Hettler (page 40); Getty Images/Batuhan Toker (page 43); Freepik (page 44); Courtesy of Georgia Military College (pages 48, 49, 50, 51); Courtesy of Netwealth (page 58); Courtesy of Marina Bay Sands (pages 64, 66); Sergio Sala (page 65); Courtesy of Marina Bay Sands (page 67, top); Shutterstock (page 67, bottom); Courtesy of IBM (page 74); Rawpixel Ltd. (page 79).

‡ Data Sources: (page 25) World Economic Forum: “Why transport and supply chain ecosystems need to be cyber secured”; BBC: “Suez blockage is holding up USD 9.6bn of goods a day”; Bloomberg: “Maersk Says June Cyberattack Will Cost It up to $300 Million”; Memphis Business Journal: “FedEx ‘significantly affected’ by virus, trading briefly halted”; ZDNET: “Petya ransomware: Companies are still dealing with aftermath of global cyberattack”; Riviera Maritime: “Protect and survive: how Maersk learned from the NotPetya cyber attack”; Nagoya Port Authority; Financial Times: “Cyber attacks on shipping rise amid geopolitical tensions”; (page 27) World Economic Forum: “Why transport and supply chain ecosystems need to be cyber secured”; (page 33) Reversing Labs: “Less malware, more risk: The changing face of open-source security”; Hack Read: “Malware Security Banana Squad Hides Data-Stealing Malware in Fake GitHub Repositories”; Malicious Life by Cybereason: “Who’s Hacking the Hackers: No Honor Among Thieves”; (page 34) Trend Micro: “Clone, Compile, Compromise: Water Curse’s Open-Source Malware Trap on GitHub”; (page 35) Cybersecurity Asia: “Sakura RAT: Cybercriminals Sabotaged by Their Own Malware Campaign, Sophos Finds”; (page 41) TV Tech: “2021 Cyberattack Cost Sinclair $63M in Lost Ad Revenue”; (page 45) WIRED: “Satellites Are Leaking the World’s Secrets: Calls, Texts, Military and Corporate Data”; Cyberhaven Labs (Q2 2024): “AI Adoption and Risk Report”; (page 55) The Guardian: “Five million Qantas customers have had personal information leaked on the dark web”; Australian Signals Directorate: “Don’t take BADCANDY from strangers – How your devices could be implanted and what to do about it”; (pages 57) TechCrunch: “Kevin Rose’s simple test for AI hardware — would you want to punch someone in the face who’s wearing it?”; (page 61) PwC 2024 Asset & Wealth Management Report; Institutional Asset Manager: “Survey reveals 71% of asset managers dealt with institutional investor concerns around cybersecurity in 2022”; Omega Systems report: “The Visual State of Cybersecurity in Financial Services”; Medium: “Zero-Day Vulnerabilities in Third-Party Software: The Supply Chain Time Bomb”; The Hacker News: “RansomHub Becomes 2024’s Top Ransomware Group, Hitting 600+ Organizations Globally”; (page 63) SC Media: “The high cost of mishandling data breaches, security reporting for financial services”; Compliance Corylated: “U.S. regulators fine security companies for cyber, data and privacy breaches”; IBM: “Cost of a Data Breach Report 2025”; (page 73) PubMed Central - NIH: “Effectiveness of Gamification in Enhancing Learning and Attitudes: A Study of Statistics Education for Health School Students”; Springer Nature Link: “The impact of gamification on students’ learning, engagement and behavior based on their personality traits”; Sage Journals: “Gamification is not Working: Why?”; (page 77) Rapid7: “Q2 2025 Ransomware Trends Analysis: Boom and Bust”; (page 79) BBC: “Aadhaar: ‘Leak’ in world’s biggest database worries Indians”; The Record: “Hacker steals government ID database for Argentina’s entire population”; European Digital Rights (EDRi): “Estonian eID cryptography mess – 750000 cards compromised”; arXiv: “An Impact and Risk Assessment Framework for National Electronic Identity (eID) Systems”; Big Brother Watch: “Checkpoint Britain: The dangers of digital ID and why privacy must be protected”; (page 80) Truvera by Dock Labs: “Self-Sovereign Identity: The Ultimate Guide 2025”; arXiv: “Distributed Attestation Revocation in Self-Sovereign Identity.”

READ ABOUT UNWINDING
UNDERWATER IN THE NEXT ISSUE
OF THREATLOCKER CYBER HERO
FRONTLINE MAGAZINE

Time to rethink how you block ransomware.

Is your detection solution faster than the hacker? Spoiler—it won't always be. Make sure your organization runs smoothly by keeping bad actors out.

Remove implicit trust. Block all untrusted software.

THREATLOCKER®
ZERO TRUST PLATFORM

See how we can help you take a default-deny approach to cybersecurity to keep you ahead of the game.