CYBER HERO
FRONTLINE

magazine by THREATLOCKER®

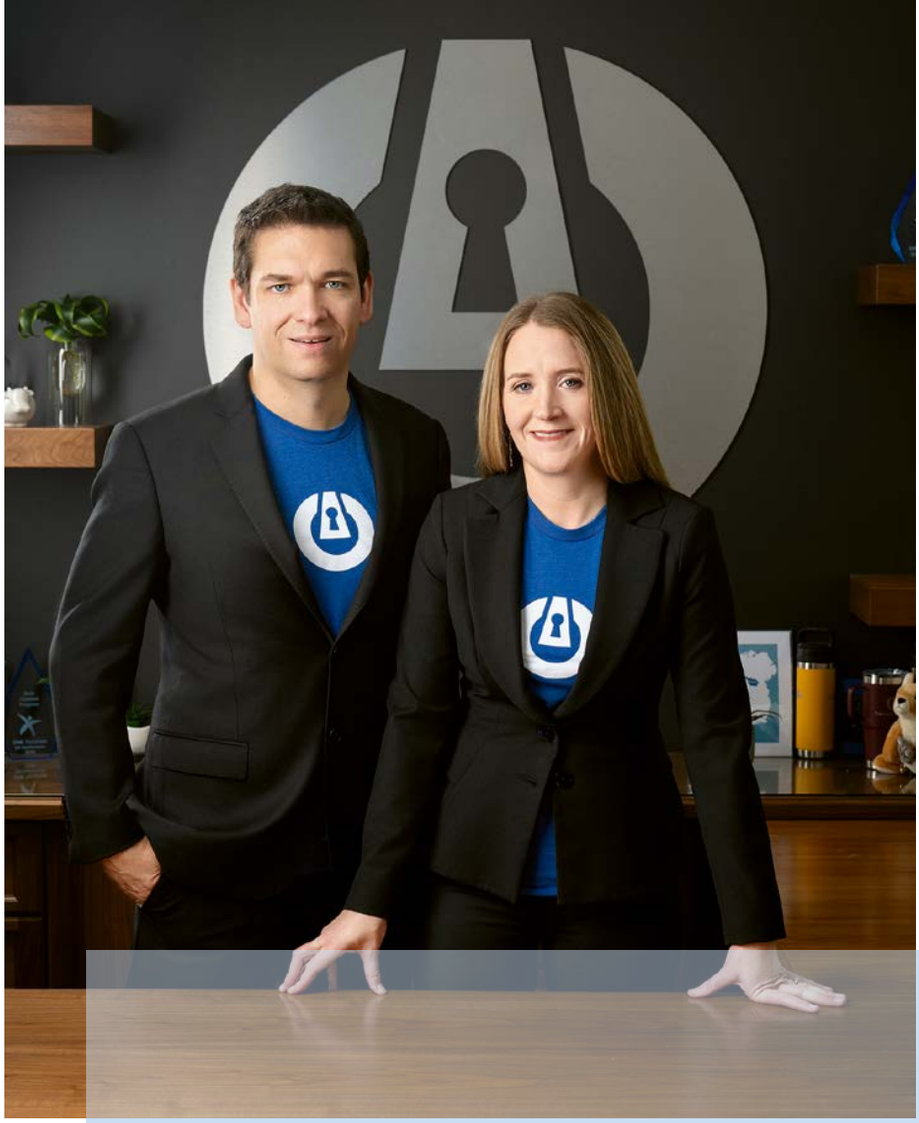
Clearing the lane
Taking control of connected traffic in the new network era

The RTO status quo
Avoiding security assumptions in the return-to-office rush

Playing defense
Why cybersecurity is a priority for connected sports teams

Control your AI tools.

Get all the emerging advantages, without all the emerging risks.



INSIDE THREATLOCKER®

A word from Co-founders
Sami Jenkins and Danny Jenkins

Hello and welcome to issue 4 of Cyber Hero® Frontline. We continue to bring this publication to you each quarter in the firm belief that education and awareness are paramount to securing your environment. The noise around continuous advancements and threat capabilities will carry on hitting security circles, and knowledge is key.

In that spirit, we were delighted to host Zero Trust World 2026 (ZTW26). It's always an absolute thrill to connect with cybersecurity and IT professionals from all over the world, with over 40 countries represented at the event. We are always energized by the significant interest in implementing a Zero Trust cybersecurity framework.

It is thanks to our distinguished guests and the dedication of our fantastic team that ThreatLocker continues to deliver an event that blends education, networking, and even some fun (we like to mix things up with the after-party). The goal is to empower cybersecurity professionals with practical and immediately actionable Zero Trust strategies.

During the event, ThreatLocker was also immensely proud to announce a donation of over USD 122,000 to Ronald McDonald House Charities. It is a charity close to our hearts, and we appreciate everyone who helped make this achievement a reality by purchasing ThreatLocker branded merchandise from the ThreatLocker Cyber Hero Swag store.

Talking about ZTW26, it was during the event that we announced innovative new capabilities on the platform. **Zero Trust Network Access (ZTNA)** and **Zero Trust Cloud Access** are designed to securely broker connection through ThreatLocker, ensuring only trusted users and devices are accessing both your internal and cloud-based resources.

The development team worked around the clock to tackle emerging vulnerabilities around identity-based access and cloud services. Risks around open ports and phishing have long been a hot-button issue and we are delighted to provide you with what we are very confident is the best solution to that problem.

These new capabilities are another signal of our commitment to lead the way in bringing you the most comprehensive suite of Zero Trust solutions available and to stay ahead of threats that continue to evolve amid emerging technologies.

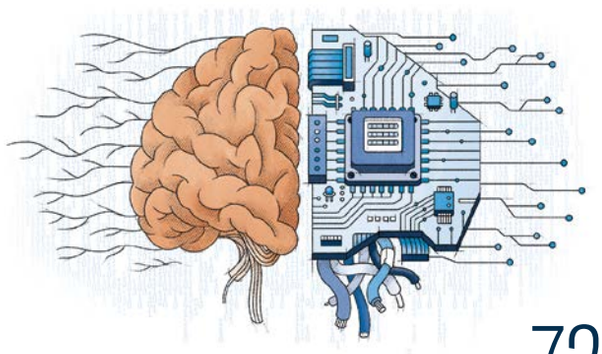
Thank you for taking the time to pick this magazine up as we bring forward topics we believe will help you secure your environment better. We hope you get immense value through its pages.

Yours,

Sami Jenkins,
ThreatLocker Co-founder
and Chief Operating Officer

Danny Jenkins,
ThreatLocker Co-founder
and Chief Executive Officer

TABLE OF **CONTENTS**



72

48

SECURITY INSIGHTS

TRENDING

52

GLOBAL POLICY

EXPERT INTERVIEW

CYBER TOOLS

PEACE OF MIND

ON MY **MIND**

BY DANNY JENKINS

Emerging technology has enhanced the scale and speed of both defensive and attacking capabilities. What concerns me most is the growing reliance on additional tools and escalating internal complexity within many defensive frameworks. I believe that while there are more options for defenders, these layers are beginning to produce gaps that favor attackers.

That is why we should not lose sight of something that works. The fact remains that setting proactive controls across your environment is incredibly effective and doesn't need to cause disruption across your organization.

We champion Zero Trust from the firm belief that it is both the strongest and most straightforward route to safety. Nothing is guaranteed, but prevention remains paramount.

As we continue building solutions that simplify and strengthen defenses, there are a few key topics that have been standing out for me recently, shaping the cybersecurity landscape.

1 THE ANSWER IS MORE ABOUT HOW TO CONTROL YOUR ENVIRONMENT

Over time, organizations have built security stacks that are anything but straightforward. Incorporating tool after tool, with each assigned towards solving a specific problem or perceived vulnerability, it can end up making things more complicated and cause unnecessary gaps in your framework.

Complexity will eventually work against you. Attackers are now able to win out through sheer volume. The more tools you introduce, the harder it becomes to manage, configure, and monitor them effectively. Misconfigurations, alert fatigue, and integration failures all create opportunities for attackers.

So, the answer becomes less about how many tools you need to solve specific problems, and more about how you can control your environment.

Think consolidation when building your approach. Place focus on foundational Zero Trust principles like deny-by-default and least privilege to dramatically reduce risk without tacking on cumbersome overhead.

When you simplify your stack and take control of what's allowed to run, what can interact, and what has access, you are executing on a sustainable and proactive approach. Attacking speed and scale might continue to grow, but as long as you're emphasizing control, you will significantly reduce the impact of emerging risks.

2 AI IS TURNING ATTACK AND DEFENSE INTO A RELENTLESS GAME OF ONE-UPMANSHIP

Recent reporting on Anthropic's leaked "Mythos" model describes a "watershed event in the history of cybersecurity," with AI agents now able to autonomously discover and exploit vulnerabilities at unprecedented speed. As these more advanced, agentic systems reshape both offense and defense, organizations are being forced to rethink how they approach control, trust, and risk in an AI-driven landscape.

AI is not going anywhere. It will continue to change the way businesses approach numerous key activities and cybersecurity is no different. This is a technology that has actively bolstered both defensive and attacking capabilities.

On the defensive side, detection, fixes, and product development is occurring at a speed that's entirely unparalleled.

This is all great, but it's important we are not losing sight of another crucial variable here; these rapid developments apply to attackers as well.

Cybercriminals are using AI to overwhelm defenses, automating reconnaissance, generating more convincing phishing campaigns, and developing adaptive malware at scale. This creates a new challenge: How do we apply something that is constantly evolving, learning, and in many cases, operating outside traditional control boundaries, without it turning security into an endless game of one-upmanship?

You limit your attack surface.

Deny-by-default functions just the same against AI-powered capabilities as it would against any other. Similar to any other application or system, when attempting to enter an environment governed by strict controls, AI tools will have a very limited, even nonexistent, pathway. That includes limiting what data they can access, defining how they can be used, and ensuring they operate within clearly defined boundaries.

> "From a Zero Trust perspective, AI should be treated like any other untrusted entity

From a Zero Trust perspective, AI should be treated like any other untrusted entity. Verify everything, enforce least privilege, and monitor interactions closely. If we don't apply the same discipline to AI that we do to other technologies, it will quickly become one of the largest attack vectors in modern environments.

3 SUPPLY CHAIN & THIRD-PARTY RISK EXPLOSION

Organizations today rely on more third-party vendors, integrations, and services than ever before. While this accelerates innovation and efficiency, it also dramatically expands the attack surface.

A single compromised vendor can become a potential entry point into thousands of organizations. We've seen time and time again that attackers are targeting the weakest link in the chain, not necessarily the primary target.

The challenge is that you don't control these third parties. What you can control is how your organization interacts with them.

This means limiting access, enforcing strict permissions, and continuously validating trust. Just because a vendor is "trusted" doesn't mean they should have unrestricted access. It's unrealistic to expect that you can remove third-party vendors from your environment nowadays, but what you can do is limit what they are allowed to do once inside.

4 THE VISIBILITY CRISIS

Cloud adoption has fundamentally changed both how organizations operate and how they're attacked. With infrastructure, applications, and data spread across multiple environments, visibility has become one of the biggest challenges in cybersecurity.

Shadow IT, unmanaged assets, and misconfigured cloud services all contribute to an ever-expanding attack surface. And in many cases, organizations don't even realize what's exposed until it is too late.

However, gaining visibility is not where the solution ends. Once you understand your environment, you need to enforce control. That means limiting access, reducing permissions, and applying Zero Trust principles across every user, device, application, and data location. Enforce device-validated access to your cloud and software as a service (SaaS) platforms, so credentials alone are never enough to breach your systems.

The cloud isn't inherently insecure but, without visibility and control, it becomes one of the easiest places for attackers to operate undetected.

Cybersecurity is evolving rapidly, but the fundamentals of Zero Trust will always remain the same. Reduce complexity. Eliminate unnecessary trust. Control what can run and how it behaves. And, for your cloud's sake, only let trusted devices access your cloud and SaaS applications.

If we stay focused on these principles, we can keep ahead of attackers by making their job significantly harder from the start. I believe you will have a great deal of applicable value within these pages to achieve that goal.

IDENTITY CRISIS

Emboldened by emerging technologies, attackers have learned that breaking through multi-factor authentication (MFA) is only one option, and increasingly, they are not bothering to try

It is a common narrative in cybersecurity: Implement MFA, train users to spot phishing, and you have secured the front door. However, the reality around developing cybercriminal capabilities has rendered this tactic less viable than ever.

Organizations are being breached despite robust MFA deployments. Users follow the prescribed protocol perfectly, logging in through familiar sites, approving authentication prompts, entering the verification codes they are sent, yet attackers still find a way through. MFA remains valuable, but it works best as one layer among many. Identity as security must be reexamined and treated differently.

The playbook has changed

Over the past year, Microsoft 365 has become one of the most targeted platforms for credential theft, in large part because of how deeply it is embedded in daily business operations. The structure of recent Microsoft 365 campaigns demonstrates the way some adversaries now operate.

This is the age of adversary-in-the-middle (AitM) attacks; rather than striking at MFA directly, attackers construct convincing phishing pages positioned between legitimate login servers and users. When a user enters credentials and passes MFA, they see what appears to be a normal sign-in flow. Behind the scenes, the attacker relays traffic directly to Microsoft, intercepting the authenticated session.

Once a session token is captured, the attacker no longer needs the password or one-time code. They are, for all intents and purposes, the logged-in user. They can access email inboxes, read sensitive conversations, and orchestrate business email compromise attacks.

Breaches at Okta reveal that attackers sent phishing emails directing users to fake login pages, harvesting both credentials and MFA codes simultaneously. Armed with these, attackers pierced the identity layer and, in some cases, gained access to the entire ecosystem of applications connected to it.

The danger here extends far beyond one compromised account. Identity systems act as trust anchors. If placed as the sole guard between users and email, collaboration tools, development platforms, admin consoles, and cloud infrastructure, a breach ripples across the entire organization.

Developers face a separate risk through OAuth phishing. Attackers trick users into authorizing malicious applications, requests that seem routine in environments where third-party integrations are normal and time and attention are stretched. Once permission

DEFENSE INSIDE THE NETWORK WITH THREATLOCKER

Zero Trust assumes breach and encourages behaving in a way that minimizes its impact. Control what executes on compromised devices, what it is allowed to touch, and where it can go next.

Allowlisting blocks the follow-on attacks that make identity breaches so damaging. Attackers typically rely on scripts, helper utilities, remote access tools, or malicious payloads—tools that should never run on properly managed devices. Block those tools from executing, and the attacker's options narrow dramatically.

Ringfencing™ provides a second layer by controlling which legitimate applications are allowed to do what. A browser might need access to Microsoft 365 or GitHub, but that does not mean it should launch PowerShell, access sensitive local files, or communicate freely with other running processes. Severing unnecessary connections blocks attackers from using trusted applications as springboards for further exploration, persistence, or lateral movement.

Privileged Access Management forms the third layer. If a compromised account attempts to install software, change system settings, or escalate to administrator privileges, those actions get blocked or routed through strict approval workflows. Privileged Access Management creates friction for attackers, slowing them down and creating visible indicators of compromise where many organizations would otherwise see nothing.

is granted, the attacker gains all privileges attached to that token: The ability to manipulate repositories, access workflows, and potentially reach secrets or automation logic without triggering the suspicious login alerts defenders are trained to catch.

Trust beyond the login

In practice, trust goes beyond strong authentication upon entry. If an attacker makes it through initial authentication, this raises serious questions: How long does the session persist? What can a browser reach from that session? Which tokens can be created, reused, or refreshed? Who has permission to grant access, and from where?

These details determine whether MFA acts as a barrier or simply a checkpoint the adversary has already factored into their strategy. If questions need to be asked at all, the latter of these is true. Device-level control is what turns MFA from a checkpoint into a genuine barrier. A resilient identity strategy has genuine value, and the two work best together.

Identity beyond authority

MFA has not failed as a concept; organizations have simply given it too much credit. Passing an MFA prompt does not mean a session is trustworthy for its entire lifespan. It does not guarantee that an OAuth grant is safe, nor prevent a browser from becoming a bridge between a legitimate login and a compromised machine.

The response must be pragmatic. Lock down the login, absolutely. But also lock down the endpoint. Constrain what applications can do. Limit what a hijacked session can accomplish. Assume compromise, so that when essential layers like MFA are bypassed, that compromise is already accounted for.

Attackers know that authentication is only one checkpoint in a longer chain. A robust identity strategy must be built the same way. The next step is continuous verification, ensuring any sign of compromise can be met with an appropriate and immediate response.

NEXT PAGE

MFA is one layer of perimeter protection, and the VPN another—but is the network perimeter as we know it dead?

VPN BLIND SPOT

When the perimeter becomes the problem, a practical approach is needed to protect it

The moment an attacker gains valid VPN credentials or compromises a device, they are effectively inside and largely invisible

As workforces have grown more mobile and remote, the traditional VPN has revealed a fundamental limitation—it was built for an era when the network perimeter meant something, when it was a true perimeter. Times have changed, and that era is over.

Once connected to a VPN, users can access any resource they are authorized to use without having to navigate multiple security layers. The moment an attacker gains valid VPN credentials or compromises a device, they are effectively inside and largely invisible. While the VPN was designed to delineate inside and outside, it was never built to ask whether a connection is authorized to access specific resources at specific times.

Perimeter devices as staging points

Compromising SSL-VPN appliances gives an attacker a base of operations as a trusted internal user with broad visibility and granted authority. VPN compromise removes the perimeter boundary; attackers with the right credentials enter with authorization and inherit the same implicit trust granted to legitimate remote users.

Recent incidents illustrate how quickly this escalates. In October 2025, SonicWall's cloud backup infrastructure leaked encrypted credentials and configuration data, exposing customers to widespread compromise. Simultaneously, threat actors exploited Fortinet and FortiGate firewalls as initial access vectors. Ransomware operators, including Akira, specifically targeted these SSL-VPN relationships to deploy ransomware at scale.

Once inside via compromised VPN credentials, attackers conducted rapid internal reconnaissance, harvested credentials, escalated privileges, and pivoted to domain controllers. The common thread in such incidents was the abuse of trusted remote-access infrastructure to bypass traditional security.

RETHINK NETWORK ACCESS FROM THE OUTSIDE IN WITH THREATLOCKER®

VPN-based access assumes that once a user is inside the network they can be trusted. They cannot. ThreatLocker removes the dependency on network location and replaces it with controlled, policy-driven access at every layer:

- **Zero Trust Network Access (ZTNA):** Grants access only to specific applications or systems, never the wider network
- **Zero Trust Endpoint Firewall:** Enforces network rules based on device identity and context, not static IP addresses
- **Allowlisting:** Blocks unauthorized tools from executing, even on compromised devices
- **Ringfencing™:** Restricts what legitimate applications can interact with, limiting misuse
- **Privileged Access Management:** Prevents unauthorized privilege escalation and locks down administrative actions

Access stays tied to the device, continuously verified, and limited to exactly what is required. It is Zero Trust in action.

Attackers may exploit unpatched vulnerabilities, abuse weak configurations, or leverage exposed cloud backups. They frequently bypass authentication controls or use legitimate-looking accounts to stage persistent access. From this trusted foothold, they escalate privileges, suppress security logging, and make firewall and VPN configuration changes. Once domain-level control is achieved, ransomware deployment becomes significantly easier.

Why traditional defenses fall short

Network segmentation can reduce the blast radius of a VPN compromise by limiting access between internal systems. But segmentation is complex, and it offers limited protection against compromised VPN credentials. Robust logging and behavioral monitoring can identify suspicious activity, but these controls typically detect activity after compromise. VPN abuse blends in. Organizations with layered controls still have options—but the window to act is narrow.

Multi-factor authentication (MFA) provides meaningful protection, but is not a guaranteed safeguard. Attackers can bypass it if they gain control of the VPN appliance itself or enroll their own MFA tokens after a compromise. An attacker inside the perimeter can modify the authentication workflow or configure additional accounts with their own MFA factors.

Prompt patching reduces exposure to known vulnerabilities, but zero-day exploitation occurs before patches are available. Operational delays and missed patches often leave exposure intact. The case of the SonicWall breach cloud backup leaks exposed credentials without any vulnerability at all—just operational mishandling.

Static rules vs. the moving workforce

Compounding this is a separate but related problem. Traditional network access controls rely on IP-based allowlists and firewall rules built on assumptions that do not match modern work patterns. Administrators created these rules expecting devices to remain within trusted ranges and for IP addresses to change only rarely.

In reality, an engineer or executive might connect to the corporate network via a home Wi-Fi connection one day, a hotel network the next, and a mobile hotspot the day after that.

Over time, rules accumulate. Temporary access remains in place long after it was required. Administrators broaden rules to cover entire internet service provider (ISP) ranges simply to reduce the administrative workload; firewall allowlists grow larger than intended, and access restrictions inevitably loosen. Administrators lose confidence that their ruleset fulfills its original purpose. In this drifting, over-permissive environment, a compromised VPN device can do real damage.

NEXT PAGE

Building secure networks requires a change of attitude—not a complete overhaul

CLEARING
THE LANE FOR ACCESS

The time has come to rethink the network boundary and take back control over connected traffic

As we have seen, identity can be taken over without breaking authentication. Once a VPN connection is established, the network often gives away far more than it should. Strengthening either layer helps, but neither is enough to make the network truly secure. The key is to define access as its own layer, and control that. Control the way access is granted, enforced, and how it changes over time.

Access matters

Network design has always revolved around connection. Get the user onto the network and through its walls first and foremost, then rely on segmentation, monitoring, and endpoint controls to manage the rest. That approach, built on the old perimeter model, assumed the core of the network was a safe space. But a compromised session or device does not announce itself; it arrives looking legitimate, and if it lands on a network segment that has been granted broad reach, it inherits that reach immediately.

Applying a Zero Trust approach to the network means treating each interaction as a separate decision. Access to a server, management interface, or service is granted with context, on its own terms. There is no general state of being “on the network” that carries any implicit privilege. A Zero Trust framework limits what a session can do, even when that session appears valid.

There is no general state of being “on the network” that carries any implicit privilege. Zero Trust limits what a session can do, even when that session appears valid

Identity, not location

Traditional network access control leans heavily on IP addresses. Firewalls and allowlists are configured with the expectation that devices remain within known ranges. But a mobile workforce is no longer that uncommon, appearing from different networks daily. Over time, rules surrounding network access tend to drift. Temporary access persists, ranges widen, and the ruleset loses its original intent.

The principle of dynamic network access takes a different approach, in which the decision to allow access is tied to the device itself. A host-based agent already knows which device it is running on, which user is active, and what its current network context looks like. When that device attempts to connect to the network, the endpoint agent reports its current IP address to the control plane.

If the device is authorized to reach a specific service, Remote Desktop Protocol (RDP) to a management server, for example, the platform automatically updates the access rule to match that address. When the address changes, the rule changes with it. There is no ticket to deal with, no need to broaden the rule to cover uncertainty, and crucially, little to no delay—nowhere near the friction of classic VPN connectivity because the permission follows the device.

Nothing feels different on the user end. They attempt to connect from wherever they are, and the connection succeeds if they are authorized to do so. From the network's side, the rules associated with that connection remain narrow and precise. And if the endpoint agent is not present, not authenticated, or not authorized to connect, the machine is simply not granted access to the network. The location is irrelevant.

Rules reflecting reality

One of the quiet failures in traditional firewall management is how quickly rules lose their original meaning. A rule created for a specific purpose tends to outlive that purpose. The environment changes, yet the rule inadvertently stays. Over time, the rule-set becomes a complex, difficult-to-manage record of past exceptions rather than a reflection of current network policy.

Dynamic updates remove much of that drift because rules are derived from policy and tied to device identity, thereby remaining aligned with the intended design. There is no need to expand a single IP entry into a broader range just to avoid repeated change requests. The rule exists for the device, and only for that device.

That has two effects. First, the rule set stays smaller and easier to understand. Second, it behaves predictably. This is deny-by-default in action: When a connection is allowed, there is a clear reason.

Speed without compromise

Access delays are often treated as a necessary part of access control. A user requests access, a team reviews it, a rule is applied, and only then does the connection proceed. That delay is manageable for planned work, but it becomes a persistent problem in day-to-day operations, where access needs shift quickly and frequently.

Under a dynamic access control structure, the decision is made at the point of connection. If the device and user are verified to meet the current policy requirements, access is granted immediately. If they do not meet policy requirements, the connection fails immediately. There is no waiting period during which a legitimate user is blocked. With tight enough policy management, there can be no window in which an unauthorized connection slips through because a rule was left too broad.

Using dynamic access control lists (ACLs) means control remains tight without adding friction to normal activity, so users are less frustrated and less tempted to seek dangerous workarounds.

Breach conditions

In previous articles, we have described how attackers operate after gaining access—moving laterally, discovering new systems, escalating privileges, and establishing permanent, under-the-radar access. Those steps depend on the network giving them room to move. Creating a tight, unified access scope through Zero Trust endpoint controls keeps attackers contained.

A Zero Trust model does not assume a perfect environment; it is built around the inevitability that things will go wrong. Even if an attacker compromises a device, they can only use the access it was legitimately granted—and nothing beyond that. Attempts to reach other systems fail at the first step. Endpoint detection and response (EDR) solutions stay relatively quiet because there is little to detect if malicious activity cannot begin.

A Zero Trust model does not assume a perfect environment; it is built around the inevitability that things will go wrong

HOW THREATLOCKER® CHANGES NETWORK ACCESS CONTROL

Traditional network security assumes that once a user is inside the network, they can be trusted. ThreatLocker replaces this philosophy with continuous verification at every point of access.

Together, the ThreatLocker network solutions remove implicit trust from the network. Access decisions are no longer tied to static IP addresses or manually maintained rules. A compromised credential or device no longer exposes the wider environment, because access is tightly scoped, continuously verified, and quickly revocable.

Zero Trust Network Access (ZTNA) removes the need for broad VPN connectivity. Users are never placed "on the network." Instead, they are granted access only to the specific applications or systems they are authorized to use. Every session is validated in real time, and access can be withdrawn immediately if conditions change.

Zero Trust Endpoint Firewall applies the same principle at the network layer. Policies follow the device, using identity, context, and posture to determine what is allowed. As devices move between locations or networks, access controls move with them automatically.

Find out how ThreatLocker protects the network on page 16.

This changes the way incidents play out. Instead of spreading across the environment, activity remains confined to the already permitted paths, which benefits the investigation process by making it more focused and the recovery process more straightforward.

Continuous verification in practice

The “always verify” component of Zero Trust is fully relevant in the context of network access. No decision is ever static, because a device can fall out of compliance, a user’s restrictions can change, and risk can increase during a session.

Traditional models handle this poorly because granted access tends to persist until the session ends or there is a need for manual intervention. With a deny-by-default approach, the system maintains ongoing, step-by-step visibility into device state and can adjust access as conditions change. If a device no longer meets policy, the connection can be revoked in real time without waiting for the current token to expire, which keeps access aligned with current conditions.

Removing the VPN dependency

One practical outcome of this model is that the role of the VPN lessens, in many cases becoming almost redundant in the face of more effective connection methods. Perhaps only its role as an encrypted traffic tunnel really persists because when users are not given broad access to the network to reach what they need, they can be managed differently.

With dynamic ACLs, users connect directly to the specific services they are authorized to use at that time. Each connection is governed by policy, validated continuously, and limited in scope.

The operational view

From an operational standpoint, the benefits of the change can be quite immediate. Once a policy base is built, the management overhead significantly decreases, with less time and effort required to maintain IP allowlists, fewer repetitive access requests, and so on. Because policies are enforced automatically, they can remain specific, and there is no pressure to generalize them to reduce workload. That improves both security and clarity, letting administrators know what the system is supposed to do and ensuring it behaves accordingly.

The network still carries the traffic. Its performance still matters for speed, availability, and segmentation where appropriate. But when access is tied to the endpoint and enforced through policy, the network is abstracted from identity and authorization. The network becomes what it should be: a transport layer for authorized connections rather than a boundary that decides who or what is allowed in.

If identity can be misused and perimeter access can be abused, then neither should be treated as a sufficient condition for trust. Access should be treated as its own layer, not in theory but in practice. It replaces a set of assumptions with a model that reflects the way systems are used.

Each connection is granted for a reason. Each device carries its own access with it, wherever it connects. This principle applies equally to internal infrastructure and cloud applications, and it makes the difference in both day-to-day operations and when things go wrong.

NEXT PAGE

Gaining complete control over network security depends on a platform that knows Zero Trust inside out. Discover the ThreatLocker difference

THE THREATLOCKER® NETWORK

When the network can no longer be trusted as a boundary, access itself becomes the control point—and ThreatLocker builds enforcement around it

If there is anything we have learned during this journey through the topology of common connectivity frameworks, it is that the traditional network still exists physically, but it has lost its meaning as a security concept. Users no longer sit inside a pre-defined boundary, and neither do applications. Connections, behaviors, and service consumption can all be points of failure.

ThreatLocker offers numerous network capabilities, a suite of functions that act together as a single model ready to be applied consistently across the network environment. There is much to be gained by using them in unison: Access itself must be treated as the control point and reinforced at every step. What matters is what a user can do, and whether that is true from minute to minute.

Access is granted to resources, not to networks. Even when credentials are valid, there is nothing else to reach

Individually, each ThreatLocker network component addresses a specific problem. Together, they represent a robust access model: A user connects via **Zero Trust Network Access (ZTNA)** to a defined resource. **Zero Trust Endpoint Firewall** hardens a network through its access policies, such as restricting outbound network connections for servers. Plus, **ThreatLocker Zero Trust Cloud Access** policies determine whether software as a service (SaaS) services are reachable, and detection and enforcement operate continuously across all three.

This leaves all access scoped, contextual, continuous, and, most importantly, enforceable: a package built for the variable, moving target of modern connectivity, a practical shift that acknowledges that the network is not something that must be trusted, just a tool to carry authorized traffic.

ThreatLocker: The complete defense solution

Inside the network and outside of it, ThreatLocker protects users, data, and endpoints from exposure and compromise. Rigid policy enforcement, access control, and reporting help maintain Zero Trust principles and minimize the impact of breaches. Power up your network with these three ThreatLocker capabilities:

THREATLOCKER ZERO TRUST NETWORK ACCESS (ZTNA)

Direct-to-resource connectivity, without network exposure

ZTNA removes the concept of broad network access entirely. Users are never placed onto a network in the traditional sense. Instead, connections are brokered directly between a verified device and a specific resource. This structure has several practical consequences:

- **Application-level access only**
  Users connect to individual systems (RDP, SSH, internal apps, web services) without visibility of anything else. There is no scanning, no discovery, no lateral movement path.

- **No inbound ports or exposed services**
  Internal resources do not need to be publicly reachable. ZTNA creates outbound, brokered connections, significantly reducing the attack surface.

- **Policy-driven access control**
  Access is defined centrally and enforced consistently. Permissions can be scoped to user, device, role, time, or environment without relying on network location.

- **Instant revocation**
  Access can be withdrawn in real time. There is no dependency on session expiry or reauthentication cycles.

- **Seamless user experience**
  Users connect directly to what they need, without routing through a VPN or manually switching contexts.

The result is simple but reflects a new philosophy: Access is granted to resources, not to networks. Even when credentials are valid, there is nothing else to reach.

THREATLOCKER ZERO TRUST ENDPOINT FIREWALL

Device-led network control, without static rules

Where ZTNA controls what can be accessed, Zero Trust Endpoint Firewall controls how connections are made—replacing traditional, IP-based firewall logic with identity-driven enforcement at the device level.

- **Dynamic rule creation and enforcement**
  Firewall rules are not manually built and maintained; they can be generated from policy and applied automatically based on device identity and behavior.

- **IP-agnostic access control**
  Policies follow the device. Whether a user is on office Wi-Fi, home broadband, or mobile data, enforcement remains consistent.

- **Granular connection control**
  Define exactly which processes can communicate, over which ports, to which destinations. This applies equally to inbound and outbound traffic.

- **Real-time adaptation**
  As a device's IP address or context changes, rules update automatically. There is no lag, no ticketing, and no rule sprawl.

- **Deny-by-default enforcement**
  Block unauthorized connections unless explicitly permitted. This reduces unintended exposure and keeps rule sets tight and readable.

Operationally, this removes rule drift, one of the most persistent challenges in network security. Policies remain aligned with intent because they are enforced continuously, not edited reactively.

THREATLOCKER ZERO TRUST CLOUD ACCESS

Conditional, context-aware control over SaaS environments

Cloud platforms introduce a different kind of exposure. ThreatLocker extends Zero Trust principles into this layer through conditional, policy-driven cloud access.

- **Context-aware access policies**
  Decisions are based on multiple factors simultaneously: user identity, device status, time of access, and behavioral patterns.

- **Device-based enforcement for cloud apps**
  Access can be restricted to managed endpoints only, preventing logins from unmanaged or unknown devices even with valid credentials.

- **Dynamic IP validation**
  ThreatLocker reports real-time IP and location data, allowing policies to adapt as users move between networks.

- **Granular SaaS control**
  Policies can apply across Microsoft 365, GitHub, Slack, and other cloud services, ensuring consistent enforcement across the application estate.

- **Identity threat detection and response**
  Continuous monitoring identifies suspicious behavior such as impossible travel, anomalous logins, and token misuse.

- **Automated response and enforcement**
  When risk indicators appear, policies can immediately restrict or block access without waiting for manual intervention.

This approach avoids the traditional trade-off between usability and security. Legitimate access flows smoothly under expected conditions, while deviations trigger proportionate controls.

NEXT PAGE
Extend network control beyond the local—securing third-party and cloud services is within reach

CONDITIONAL CLOUD

As SaaS platforms become the default operating environment for most organizations, the question is no longer whether to secure the cloud, but how to enforce Zero Trust principles across applications your team does not control

For many organizations, a rolling quest for agility means the idea of working locally has been left firmly in the past. For others, the ability to keep their workplace apps contained has been taken away by the wave of software as a service (SaaS) migration across the industry, with major vendors like Microsoft pushing customers away from desktop apps and toward connected cloud software. Great for convenience, but a significant hot spot for security threats.

Cloud applications now hold the sensitive data. They are the meeting point, the collaboration hub. Even seemingly local software relies on cloud infrastructure and application programming interfaces (APIs), driving business operations with a growing reliance on what happens on someone else's servers.

The shift toward distributed, cloud-first working is all but complete. Zero Trust principles must extend to these environments with the same logic and care that protects internal resources. Identity and context matter just as much at the application layer as they do at the network layer—and it could be argued that they matter more.

Security both ways

We see the same assumptions applied to inside-out cloud access as we do to outside-in remote connectivity. If the user can authenticate and pass multi-factor authentication (MFA) or provide convincing credentials, access is broadly granted. This structure has already proven insufficient—it only takes a stolen token, a compromised browser, or a convincing phishing attempt to grant an attacker cloud access with the same rights as a legitimate user.

Considering the scale of SaaS applications and their often broad logins, a breach at one point can provide immediate lateral access to others. A compromised Microsoft 365 account can expose calendar, email, files, and contacts; GitHub might offer access to repositories and deployment secrets; a Slack session could expose internal conversations and integrations.

The obvious-seeming response may be rules that are either too broad or too restrictive. Allowing access from anywhere defeats the purpose of security;

The key with these policies is that while restrictive, they should facilitate smooth, secure access for legitimate activity. [...] They are in place to evaluate risk and adjust requirements dynamically, allowing maximum flexibility with minimum danger

locking down to specific IP ranges breaks remote work. This is the classic trade-off between security and usability, but Zero Trust offers a more refined, context-based approach.

Terms and conditions

Conditional policy-based enforcement helps put guardrails around access, evaluating not only authorization but also identity, location, device compliance, and behavior to ensure cloud access is granted only when required. A user might be allowed to connect to Microsoft 365 from the office network on a corporate device but denied access from public Wi-Fi on a personal laptop. A developer could access GitHub from home during business hours, but requires additional validation if accessing from an unexpected location at 1 a.m.

The key with these policies is that while restrictive, they should facilitate smooth, secure access for legitimate activity. They should not block legitimate work. They are in place to evaluate risk and adjust requirements dynamically, allowing maximum flexibility with minimum danger.

Enforcement action

This is where detection and enforcement come together. **ThreatLocker® Identity Threat Detection and Response (ITDR)** continuously monitors Microsoft 365 environments for the threats that often slip past traditional defenses: leaked credentials, suspicious sign-ins, impossible travel patterns, and risky behavior that indicates compromise. It flags these in real time, allowing security teams to respond faster.

ThreatLocker works alongside conditional access policies by reporting a user's IP address and location from trusted devices and integrating with Microsoft 365. This allows organizations to enforce policies that only grant access from trusted, dynamically updated IPs on approved devices. Together, these tools ensure that conditional access policies are backed by the visibility and automation needed to work.

The result is a security posture that adapts to risk as it happens. Security teams gain visibility and resilience. Users gain better protection against accidental errors and external attacks. The cloud services that today's businesses rely on gain a powerful security layer that keeps data, identity, and continuity safe.

CONDITIONAL ACCESS IN PRACTICE

The principle of conditional access is straightforward in theory, and similarly simple in practice. Say an organization wants to protect its SaaS applications, such as Microsoft 365—ensuring access to email, calendar, files, and chat can only occur from approved devices. The goal is simply to allow trusted devices to connect and block others by default.

Here is how it happens:

Step 1: Define a trusted location
Create a named location in Microsoft Entra ID that represents the IP address of their dedicated ThreatLocker broker.

Step 2: Create a policy
Build a conditional access policy that says: "For all users accessing Microsoft 365, require that they are connecting from the named location we just defined. Any other devices are blocked by default."

Step 3: Define access parameters
Define what devices automatically connect to the broker for a smooth connection experience.

Step 4: Execute the control
Any login attempt from outside the trusted location is immediately blocked.

The result: A user working from the office or anywhere else on an approved device can access their email, files, and collaboration tools normally. An attacker with stolen credentials cannot access Microsoft 365 from just any device, and if they do somehow breach the network, other controls will contain the damage.

TRUST, FRAUD & THE WELLNESS ECONOMY

The wellness economy has become a victim of its own accelerated growth, and its customers are a soft target for those looking to exploit it. Using an arsenal of online weapons stretching from fake pharmacies to glowing AI-generated endorsements, cyberfraud has established a significant foothold in a market now worth trillions.

For legitimate businesses, this means a fight to maintain trust and identity even while opportunistic opponents erode it at every turn

Much of the modern wellness industry runs on trust, and that trust is increasingly being exploited. Outside of hospitals and clinics, a huge commercial market has grown around sleep, stress, diet, and longevity, offering quick fixes and tailored advice to anyone with a smartphone and a willingness to believe. Wellness solutions are convenient, accessible, and in many cases genuinely useful, but the sector is also one of the least consistently scrutinized corners of the digital economy.

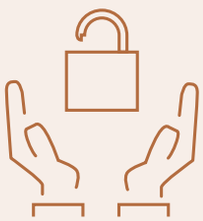
While healthcare providers invest heavily in defending themselves against ransomware and data breaches, the wellness market has expanded quickly with relatively few of the same guardrails. Entry is straightforward, oversight is uneven, and the audience is already engaged. That combination has created conditions in which misleading claims and bold forms of cyber-enabled fraud can take hold without much resistance.

The scale of the market helps explain the level of interest from bad actors. Now worth trillions globally[‡], wellness spans everything from fitness and nutrition to mental health applications and supplements, drawing in hundreds of millions of users each year. Growth has been driven largely by technology's friction removal, allowing consumers to subscribe to services, follow advice, or purchase products in seconds, often based on recommendations surfaced through algorithms or social feeds.

What has not kept pace is any consistent framework for verifying the legitimacy of what is being offered, leaving credibility to be established through branding, confidence, and visibility rather than hard evidence.

Wellness as an attack surface

The sector's fragility has not gone unnoticed. Health and wellness scams now sit comfortably within the wider cybercrime economy, which continues to grow at scale. Consumers reported USD 2.7 billion in losses from imposter scams in 2023, according to the Federal Trade Commission (FTC), while the FBI logged USD 12.5 billion in total cybercrime losses, most of which were tied to fraud. In that context, wellness stands out not for the complexity of the fraud, but for how straightforward it is to exploit.



While healthcare providers invest heavily in defending themselves against ransomware and data breaches, the wellness market has expanded quickly with relatively few of the same guardrails

The market is set up in a way that invites exploitation. Online pharmacies are among the clearest examples—estimates suggest that about 95% operate outside regulatory standards[‡], leaving plenty of room for counterfeit or nonexistent treatments to be sold online. The surge in demand for weight-loss drugs such as GLP-1 agonists has only exacerbated the issue, with fraudulent sellers quickly filling search results and social feeds, often fronted by convincing but entirely fake storefronts.

Social media has become the primary point of contact for scams, accounting for more than USD 1.4 billion in reported consumer losses in a single year[‡], and it is also the environment where wellness advice and product recommendations are most actively consumed.

Technology is accelerating these dynamics in ways that are difficult to track in real time. Europol has warned that AI is lowering the cost of deception, enabling the rapid generation of convincing testimonials, endorsements, and even entirely synthetic experts powered by large language models (LLMs). In a market built on personal recommendations and perceived authenticity, those signals can be remarkably effective.

Trust, influence, and manipulation

At the same time, health advice originates from different places than it used to. It is no longer limited to doctors or institutions; increasingly, it comes from individuals online, building large audiences around personal routines and shared experiences.

These influencers now play a central role in that ecosystem, recommending supplements, diets, and health routines to audiences of millions. The line between personal experience and paid promotion is not always obvious, and in many cases, it is deliberately blurred.

A lot of this content sits in a gray area. Claims are rarely outright false, but they are often framed in a way that suggests results that may not hold up under scrutiny. The business model behind it only pushes things further in that direction, with affiliate links, sponsorships, and brand deals driving clicks and sales, not necessarily in ways that are accurate or responsible.

For users, that makes it harder to tell who is offering genuine expertise and who is simply good at presenting information. A polished video or a large following can, for some, carry as much weight as formal qualifications, especially when the advice lines up with what someone already hopes might be true.

Consumers reported

USD 2.7 billion

in losses to imposter scams in 2023

At first glance, this does not look like a typical cyberattack, but the pattern is familiar to anyone who understands phishing. Trust is built quickly and then used to steer behavior in a way that benefits the person on the other side. Confidence tricks lure in the vulnerable and exploit their weaknesses.

Data, design, and built-in vulnerabilities

In many cases, though, the bigger issue is not what is being promised but how it is sold. Subscription models frequently rely on short trial periods that roll into recurring payments, with cancellation processes that are harder than they need to be, counting on people to give up rather than push through.

Alongside the financial risks, there is a separate issue regarding the handling of personal data. Many wellness applications collect far more than simple usage information, pulling in details about mental health, physical activity, repro-

As individuals online build large audiences around personal routines and experiences, health advice now comes from beyond doctors and institutions

ductive cycles, and day-to-day habits. In a clinical setting, that kind of data would be tightly controlled, but in the wellness market, the picture is much less clear.

Studies have found that many of these applications share user data with third parties, sometimes for advertising or analytics. Most users will have clicked through terms and conditions at some point, but that does not mean they have a clear sense of where their information ends up or how it is being used.

The issue here is not usually a breach or a system being broken into. It is the way things are set up in the first place. Data is collected, used, and passed on as part of the service's normal operation, meaning the risk is baked in rather than introduced from the outside.

More broadly, the same pattern shows up across the market. Speed and accessibility tend to come first, while verification comes later, if at all. It is easy to launch a product, reach an audience, and create something that looks credible on the surface. AI tools are making that even simpler, helping generate content, reviews, and even entire brands that can appear legitimate with relatively little effort.

Closing the gap between trust and control

The impact is not always obvious, but tends to creep in over time. People spend money on things that do not work, stay signed up to subscriptions they forgot about, or hand over personal information without thinking about where it might go. Some will even put off getting proper help while trying options that sound more convincing than they actually are.

On their own, those outcomes can seem small, but they start to chip away at trust in digital health and wellness services more broadly. Regulators and platforms have begun to respond, introducing tighter rules on advertising, disclosures, and subscriptions. Enforcement often comes after the fact, which means stronger built-in controls matter more than ever. By the time something is taken down or challenged, it may already have reached a large audience, or simply been replaced by something similar under a different name.

For anyone working in cybersecurity, the allegory here is probably rather clear. Systems that rely on trust by default tend to run into trouble sooner or later, whether that is in enterprise environments or consumer platforms. If something is allowed to operate without adequate oversight, it becomes easier to abuse.

Demand for wellness products and services is not going anywhere. If anything, it is growing as more people seek ways to manage their health outside traditional systems. Digital tools will continue to meet that demand, and stronger controls—on data handling, advertising standards, and platform accountability—are what will determine whether that growth is built on something people can actually rely on.

PROTECTING DATA **STARTS WITH PEOPLE**

The human factor defines risk—and when that risk has real human impact, it must be controlled at all costs

Security looks different when the data you protect carries emotional weight. At Aurora Mental Health & Recovery (AMHR), the stakes are very real. Patient records reflect some of the most vulnerable moments in people's lives, and any breach would cut deeper than a compliance failure or financial loss. AMHR's team, with the help of ThreatLocker®, has moved from an environment with limited visibility to one of tightly controlled systems, introducing application control, and strengthening policies.

Cyber Hero® Frontline speaks to security lead Joshua Clabo about AMHR's philosophy, exploring the way the company restored boundaries in a post-COVID workplace, recognizing where technology stops and human behavior begins, and building a security culture that holds under pressure without breaking the people propping it up.

> People come to mental health treatment because they need help. The last thing they should worry about is whether their information will leak

Why does protecting mental health records demand a different security mindset?

This is deeply personal to me. When I think about security, I ask what I would want if this were my medical records, and my answer is always that I'd want them locked in a room, in a vault, behind a cage, behind another vault, with an armed guard patrolling the hallway. That's the standard I bring here.

The golden rule applies perfectly, in that I treat others' data the way I'd want mine treated—with the highest standard and quality. People come to mental health treatment because they need help. The last thing they should worry about is whether their information will leak. I want them to sleep safely at night, and knowing it's protected keeps me sleeping soundly too.

Why has healthcare become a prime target for ransomware attacks?

I heard something at Zero Trust World last year that stuck with me. In the '90s, there was a code of honor among hackers. You didn't go after critical infrastructure, and you definitely didn't hit hospitals. But money changed everything. Ransomware changed everything. Attackers realized hospitals and healthcare organizations would pay enormous sums to restore operations. Greed transformed the landscape entirely.

Today, for a medical entity, every day is a roll of the dice. You have to wake up and consider whether today is the day you'll be hit. I take comfort in the fact that we've locked down our environment completely—firewalls, ThreatLocker, application control policies, everything is secured on the technology side. Our biggest weakness remains the human element. That's where the real risk lives.

What did you find when you started auditing your security posture?

I joined the company about three years ago, and when I started tightening controls, we had some foundational security tools in place, but they turned out to have serious gaps. Over three years, I helped raise our Microsoft Security score to 80%.

Score is one thing, but the key revelation of the audits was that we needed application control that others couldn't provide. People were downloading everything (Chrome extensions, VPN extensions, gaming extensions) circumventing admin controls. We had limited visibility into what people were installing. That's when I looked at ThreatLocker and immediately called my boss. I knew this was what we needed. ThreatLocker gave us excellent visibility.

What changed once ThreatLocker came in?

The biggest selling point was the ability to lock a machine down in 10 seconds. Previously, if HR needed to terminate someone remotely, we had 30 minutes to an hour of lag time, if the process worked at all. Now it's instant. That's massive for incident response.

Allowlisting was transformative. When I did the initial scan after 60 days of **Learning Mode**, my boss could now see all of the applications, extensions, and programs that had flown under the radar. We let ThreatLocker learn our systems, our applications, our healthcare software—everything. Once we locked everything down, we told people that new applications need business justification. Nine times out of ten, people couldn't justify why they needed it.

At Aurora Mental Health & Recovery, the team moved from limited visibility to disciplined, tightly controlled security to protect patients' most vulnerable moments

At AMHR, leadership prioritizes staff well-being—encouraging mental health days, providing wellness facilities, and keeping operations running so self-care comes first

The post-COVID landscape has made this harder. Pre-pandemic, there was a clear line between work and personal devices. After that, the line blurred. People now think a work computer is their computer. ThreatLocker helped us restore that boundary: It's not their device, it's ours, and it has to be protected.

How do you approach the human side of security?

Security always comes down to people. I don't use fear tactics. A five-minute education session can save your company USD 5 million, simply by teaching someone not to click a malicious link. We instituted phishing simulation and mandatory security training. I set up monthly training—short, precise, five- or 10-minute sessions with videos or interactive games. Our team is made up of hundreds of staff who already deal with heavy compliance training, so I keep it light and practical.

> "AMHR's greatest strength is understanding mental health, and that extends beyond our patients

The feedback has been great. This month, an employee created a ticket after training to ensure their personal phone was fully updated. I didn't mean to scare anyone, but that's exactly the outcome I hoped for. Informed people taking ownership.

How does AMHR's mission shape its approach to employee burnout?

AMHR's greatest strength is understanding mental health, and that extends beyond our patients. We're encouraged to take mental health days. If we can't take care of ourselves, we can't care for others. Leadership genuinely emphasizes this at town halls. We have facilities and support for physical wellness, too.

I'm proud that when I need to unplug and disconnect, the servers keep running. The organization gets it, and that's rare in this field. We're not a company that lectures about self-care while grinding people down. We actually mean it—self-care comes first.

Joshua Clabo is a Senior Systems Administrator and de facto Security Lead at Aurora Mental Health & Recovery (AMHR), one of Colorado's Certified Community Behavioral Health Centers. Based remotely in Florida, Clabo oversees security operations across nearly 900 endpoints as part of a small IT infrastructure team.

With prior sysadmin experience at financial, hospitality, and law institutions, Clabo has helped rebuild and manage AMHR's security function over the past three years.

As the organization states: "Aurora Mental Health & Recovery is based out of Aurora, Colorado. Deeply rooted in our diverse community, we deliver state-of-the-art care impacting emotional well-being and addiction recovery."

What do you think companies get wrong about IT burnout, and what's your advice?

Companies think two weeks of vacation fix burnout, but they don't. It requires structural change. If the underlying problem is overwork, understaffing, lack of visibility, or tool sprawl, people return to the same broken environment. Burnout comes back worse.

Leaders need to listen when their security teams recommend tools that prevent catastrophe. Spending USD 10,000 now can prevent a USD 5 million ransomware attack, yet justification often only comes after attacks occur. We're trying to prevent that entirely.

If you're stretched thin, I would start with finding a 24/7 managed detection and response (MDR) team. ThreatLocker has changed things for us, knowing experts are watching around the clock and a phone call away when a crisis hits.

> "A five-minute education session can save your company USD 5 million, simply by teaching someone not to click a malicious link

Second, automate relentlessly. Capture the small minutes eaten by manual tasks and redirect those hours toward meaningful projects. Third, build healthy work-life boundaries. Tell colleagues when you're unavailable after hours and protect that time fiercely. If you bring yesterday's problems into tomorrow, you're headed to burnout. No one thrives there.

Security professionals carry unique pressure—you're responsible for protecting everything, and the consequences of failure are very public. How do you manage that weight?

Although every day is a roll of the dice, there's a way to rig the game in your favor with the right security applications. But every now and then the inevitable does happen. We've seen it happen to major companies and small mom-and-pop operations alike. It's all about controlling and minimizing the impact.

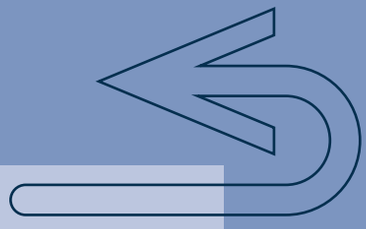
For me, the best way to manage that weight is knowing I've got the proper security buffers and measures in place to handle any scenario my team could encounter. And if something does happen, we have cyber insurance and third-party partners to get us back up and running.

ThreatLocker helps immensely with this—they have our backs 24/7. I want to commend their MDR team, especially. They're often 30 minutes to an hour ahead of other security vendors we use when they reach out about potential issues. That's what helps me: knowing people are watching, and that we're not alone in this.

THREATLOCKER TIP

Need MDR assistance?
The ThreatLocker Cyber Hero® MDR team is ready to help

BACK TO THE STATUS QUO WITH RTO



The office comeback is well underway, but assuming the corporate network is safer than remote work could leave organizations at risk

Return-to-office (RTO) mandates are spreading fast, driven by everything from culture concerns to productivity targets. Security rarely gets top billing in these announcements, yet it is often part of the calculation, given that many organizations still assume that being physically inside the corporate network automatically lowers cyber risk.

That assumption sounds logical, but it is also increasingly outdated. RTO does not automatically shrink cyber risk. In many cases, it simply reshapes it, sometimes reviving security problems organizations spent the pandemic years trying to solve.

THE LINGERING ILLUSION OF THE SAFE OFFICE NETWORK

Enterprise security used to assume the office was the safe zone. Keep attackers outside the firewall, and most problems stay outside with them. The mass shift to remote work blew holes in that thinking, leaving organizations to manage employees signing in from kitchen tables, shared Wi-Fi, and all kinds of personal devices.

That shift pushed many organizations toward identity-focused security, tighter endpoint monitoring, and Zero Trust policies designed to verify users continuously rather than trust them based on location.

RTO risks nudging companies back toward older assumptions that once employees are physically inside the building, the network itself is inherently safer. In practice, the office can create its own set of vulnerabilities—at least if trust is assumed within the physical network perimeter.

RTO does not automatically shrink cyber risk. In many cases, it simply reshapes it, sometimes reviving security problems organizations spent the pandemic years trying to solve

WHEN PHYSICAL ACCESS BECOMES THE WEAK LINK

Some of the most damaging breaches in recent years have not started with outside hackers at all. They have come from people who already had legitimate access to company systems.

In 2023, Tesla said two former employees were responsible for leaking confidential data belonging to tens of thousands of staff members. The breach did not involve hackers exploiting technical vulnerabilities, but rather relied on individuals with legitimate internal access.

Insider activity is notoriously difficult to detect because it often blends into normal workplace behavior. Employees already have credentials, understand internal workflows, and know where sensitive information lives.

Office environments can unintentionally increase exposure to these risks. Shared workspaces, unlocked devices, and casual credential sharing—all common in collaborative office settings—create opportunities that rarely exist in tightly controlled remote setups where employees operate in isolation.

THE USB PROBLEM

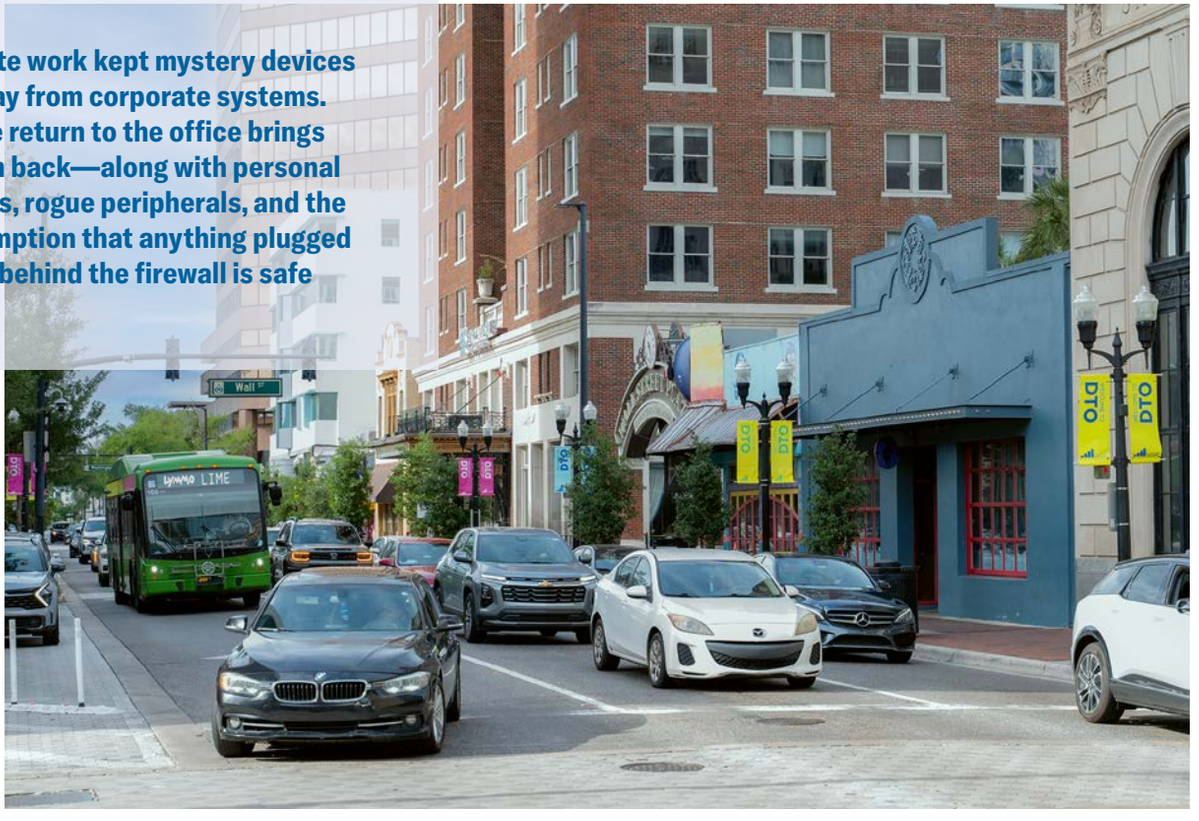
Another security issue resurfacing alongside RTO is centered around removable storage devices.

USB malware was a major problem long before remote work entered the picture. In the late 2000s and early 2010s, infected flash drives caused repeated security scares, especially in government and defense environments. The U.S. Department of Defense (DoD) eventually responded by banning removable media altogether after malicious code spread through drives plugged into internal machines.[‡]

Organizations tightened rules around removable media over the years, but remote work introduced an unexpected side effect. With fewer people sharing office equipment, there were fewer opportunities for mystery devices to get plugged into corporate systems.

Office returns change that dynamic. Suddenly, there are shared printers, docking stations, meeting room kits, and other communal tech back in the mix. Along with it comes a familiar problem: personal devices and random peripherals quietly finding their way onto company systems.

Remote work kept mystery devices away from corporate systems. The return to the office brings them back—along with personal drives, rogue peripherals, and the assumption that anything plugged in behind the firewall is safe



RANSOMWARE STILL LOVES FLAT NETWORKS

The biggest technical risk tied to office environments is often lateral movement—the ability for attackers to move between systems once they gain an initial foothold.

The 2021 ransomware attack on Ireland's Health Service Executive (HSE) is a reminder of how fast infections can spiral. An intrusion that started on a single endpoint spread through connected networks and ultimately shut down large parts of the country's healthcare IT infrastructure, forcing widespread appointment cancellations.

Although the incident did not hinge on workplace location, it showed how quickly malware can spread once it reaches shared internal systems. Office networks often connect employees to legacy platforms, shared storage, and internal services, giving attackers far more room to move than tightly controlled remote access setups.

REMOTE WORK BROUGHT RISK AND MATURITY

The shift to remote work created plenty of security problems of its own. Phishing attempts spiked, home networks became part of enterprise risk, and IT teams struggled to keep track of devices scattered far beyond office walls.

However, the distributed workforce also forced organizations to modernize security architectures at unprecedented speed. Companies invested heavily in identity verification, behavioral monitoring, application control, and device trust validation because traditional network boundaries no longer existed.

Many now worry that RTO creates pressure to loosen those controls in the name of convenience or operational simplicity.

THE INSIDER THREAT GETS MORE SUBTLE IN OFFICES

Some security vendors, including ThreatLocker®, have started paying closer attention to what happens inside networks rather than just watching traffic coming in and out. That includes tightening controls on which applications are allowed to run in the first place, rather than waiting to spot suspicious behavior after it appears.

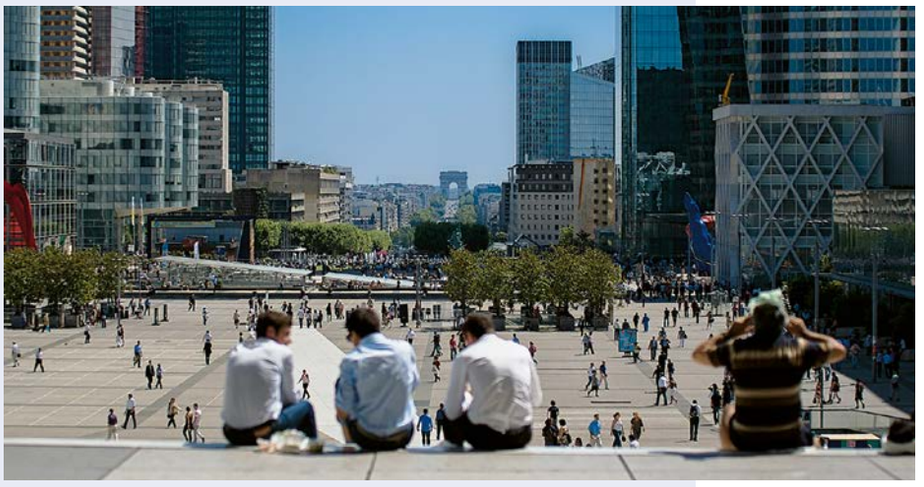
That model reflects a broader industry shift toward assuming that compromise is inevitable. Instead of trusting users because they are physically present, organizations increasingly focus on controlling what those users can actually do.

The challenge is cultural as much as technical. Office environments naturally encourage collaboration and information sharing, behaviors that can conflict with strict least-privilege security models. Employees will bypass controls in an attempt to get work done faster, particularly when returning to offices after years of remote flexibility.

HYBRID WORK: THE WORST OF BOTH WORLDS?

Many organizations are not returning to fully office-based operations. Hybrid work models have become the default in some cases, and certainly the majority: Indeed reports that 85% of U.K. job postings in 2025 mentioned a hybrid schedule of at least two days a week in-office. This adds additional complexity.

Security teams must now defend both distributed remote endpoints and internal office infrastructure simultaneously as devices move between home networks, public Wi-Fi, and corporate environments. This creates constantly shifting trust boundaries.



The use of hybrid models also makes policy enforcement harder. A device that appears compliant on a home network may behave differently when connected to internal systems, particularly if network segmentation or monitoring varies between environments.

Hybrid scheduling can also complicate oversight of physical access. When employees rotate in and out of offices on irregular schedules, it becomes harder for organizations to track who should legitimately be on-site at any given time. That uncertainty can create small but meaningful gaps in badge auditing, visitor monitoring, and access verification that attackers may exploit.

SECURITY IS ABOUT IDENTITY, NOT GEOGRAPHY

Most attackers are not particularly concerned about whether someone is working from home or sitting in an office. What they really want are valid login details, trusted tools they can hijack, and access to everyday systems that help them stay resident and unnoticed.

The belief that office networks are safer by default is colliding with how modern IT actually works. With cloud platforms and software-as-a-service (SaaS) tools handling so much corporate data, access often comes down to a matter of credentials rather than location.

That is why many organizations now treat every user and device as requiring continuous verification. RTO does not make that thinking obsolete. If anything, it highlights why it exists.

THE REAL RISK IS COMPLACENCY

One of the bigger risks tied to office returns has less to do with technology and more to do with mindset. Some leadership teams see physical oversight as a security improvement, while employees often assume systems are safer simply because they are back inside the corporate network.

Security teams must now defend both distributed remote endpoints and internal office infrastructure simultaneously as devices move between home networks, public Wi-Fi, and corporate environments, creating constantly shifting trust boundaries

Both assumptions can lead to relaxed vigilance, reduced emphasis on training, or underinvestment in endpoint and behavioral monitoring.

Cybersecurity failures rarely stem from a single vulnerability. They usually emerge from overlapping blind spots created by trust, convenience, and outdated assumptions about where threats originate.

RETHINKING SECURITY FOR THE MODERN WORKPLACE

RTO is neither inherently secure nor safe.

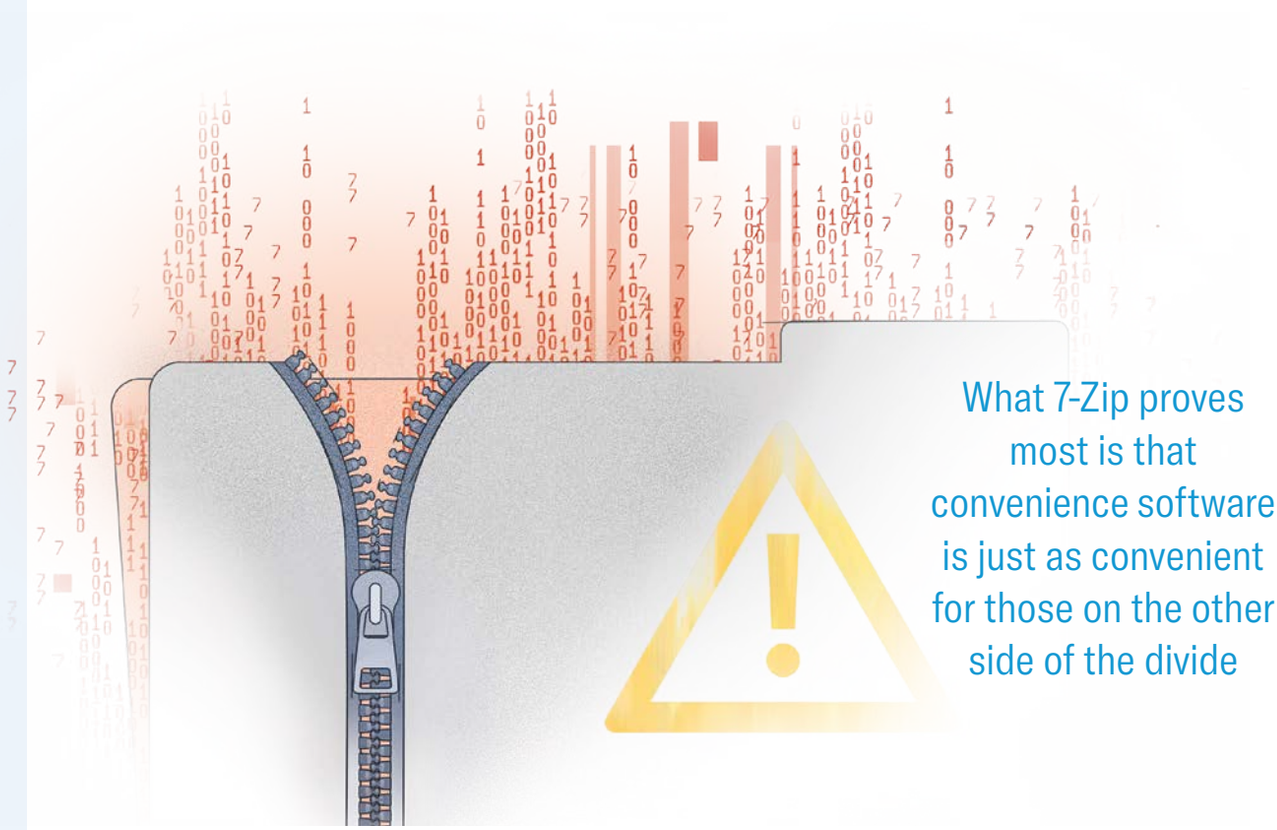
Organizations that treat office returns as a structural shift in cyber risk, rather than a security upgrade, are far more likely to maintain resilience. That means preserving identity-centric controls, enforcing least-privilege access, monitoring internal activity, and maintaining strong endpoint visibility regardless of where employees work.

Security strategies built around behavior, not location, reflect the realities of modern enterprise infrastructure.

7-ZIP:
DANGER IN PLAIN SIGHT

A string of flaws has exposed the innocent-seeming archive tool as a cybersecurity liability.

Can the genie really be put back into the bottle?



What 7-Zip proves most is that convenience software is just as convenient for those on the other side of the divide

For most of its life, 7-Zip has been regarded as relatively unassuming. It is basically a digital carpet; always there, rarely questioned, comfortable, and almost never included in discussions about cybersecurity risk. And why would it be? How dangerous can a basic file compression tool really be?

As it turns out, it is really quite dangerous. Dangerous for the Ukrainian government, which was targeted in 2024 by a group presumed to be linked with Russian cybercrime, exploiting a now-patched zero-day vulnerability in the package to sneak SmokeLoader malware past Windows' mark-of-the-web (MoTW) controls by double-archiving it.[‡] And more dangerous still, thanks to the discovery of more recent and even more insidious bugs.

How 7-Zip strips traditional defenses

7-Zip's latest vulnerabilities (CVE-2025-11001 and CVE-2025-11002) exploit the way the software processes symbolic links inside ZIP archives. When 7-Zip encounters a symlink during extraction, it fails to properly check whether that link resolves within the intended extraction directory.

In other words, the archive extraction process does not enforce a boundary check between the archive contents and the destination filesystem. A manipulated archive can redirect extracted files to any location to which the victim has permissions to write.

That means an attacker can quietly drop a malicious dynamic-link library (DLL) into a system folder, overwrite a file in a startup directory, or plant a payload where a scheduled task will dutifully pick it up. No elevated privileges are required, there is no confirmation prompt, and there is no need to execute anything directly. Open a malicious ZIP file with a vulnerable copy of 7-Zip, and that file can drop its payload somewhere it can be automatically run.

Why quiet vulnerabilities are an issue

Given the relatively quiet, low-importance stature of the application in many cyber professionals' estimations, just about every copy of 7-Zip will remain vulnerable for a long time to come. Unlike enterprise applications that follow strict lifecycle management, 7-Zip has no auto-update mechanism and is often installed packaged or in tandem with other applications. Many endpoints are running 7-Zip versions released half a decade ago.

Open a malicious ZIP file with a vulnerable copy of 7-Zip, and that file can drop its payload somewhere it can be automatically run

Threat assessment can be a great challenge, and when a package seems innocuous, it is easy to let something like this slip. Attackers know this. They rely on living-off-the-land (LOTL) techniques and abuse legitimate software to avoid triggering security alarms. 7-Zip may not be a core OS utility, but it is nonetheless a perfect candidate: Ubiquitous, unsupervised, often unpatched, performing a menial task which might not even seem worth monitoring.

It would be comforting to think that these kinds of issues could be solved by patching. But the reality of many enterprise environments is that the process of patching non-critical software is inconsistent at best. Portable versions might end up tucked into user profiles, archived automation scripts could rely on older versions, and long-forgotten server utilities often remain untouched indefinitely.

Plus, of course, even an exhaustive patching regime would not have made a difference in this case. These recent flaws were zero-day vulnerabilities. Effective patching cannot help where there is no pre-existing knowledge.

Innocent tools, dangerous intentions

While 7-Zip has taken center stage, it is far from the only everyday utility that attackers can abuse. Consider tightening control around the following:

PowerShell and Command Prompt
Extremely powerful tools that are often unnecessary for everyday users. A favorite for attackers who want to run scripts or execute payloads silently.

WinRAR and other archive tools
The same class of vulnerabilities and behaviors applies to any file manipulation tool. If staff do not need multiple compression utilities, block the extras and restrict the rest.

File transfer clients (WinSCP, FileZilla)
These are perfect tools for attackers to exfiltrate data. Ensure access is restricted to legitimate requirements only.

Remote access tools (TeamViewer, AnyDesk, RDP)
Legitimate business helpers, perhaps, but also an attacker's direct line into your network if installed without approval or available on a forgotten user account.

Unsanctioned browsers and extensions
Plugins and alternative browsers introduce risk and reduce visibility for defenders.

Developer runtimes (Python, Node.js)
Anything that can run scripts is powerful, flexible, and highly susceptible to abuse. There is no getting around their utility for developers, but access must be carefully controlled.

The archive as a weapon

The symlink flaws are not the only reason to treat 7-Zip carefully. Attackers have been using it to compress and slowly exfiltrate stolen data for some time—small transfers, spread over weeks, indistinguishable from normal traffic. By the time anything looks wrong, the data is already gone.

The more direct threat is what 7-Zip can do to files on a machine. Password-protect an archive, delete the originals, and you have functioning ransomware. No custom encryption code, no suspicious tooling—just a compression utility doing exactly what it was designed to do. Antivirus will not flag it. The user will not see it coming.

Protection through environmental control

It is much more important and effective to administer an ounce of prevention rather than a pound of the cure. Organizations cannot afford to trust every utility on every endpoint. But they can create an environment that minimizes the impact of rogue applications.

Block first, allow by exception and, if such tools must be allowed to run, restrict software like 7-Zip to run only where it is explicitly needed, within strict boundaries. With ThreatLocker®, administrators can block 7-Zip entirely across the estate with **Allowlisting** or use **Ringfencing™** to prevent it from touching sensitive file paths, accessing scripts, or executing outside of sanctioned workflows.

Discussing whether 7-Zip is "bad software" is a separate argument. The truth is that unfettered access to it is not worth the risk, and the same is true for any executable capable of manipulating files. Policy and accountability are king. What 7-Zip proves most is that convenience software is just as convenient for those on the other side of the divide. With the right controls in place, you will greatly restrict 7-Zip's adversarial potential.

Organizations cannot afford to trust every utility on every endpoint. But they can create an environment that minimizes the impact of rogue applications

HOW THREATLOCKER NEUTRALIZES TOOLS LIKE 7-ZIP

7-Zip's vulnerabilities highlight the importance of both detection and control. ThreatLocker provides several layers of protection that work together to contain, limit, or outright block risky utilities long before they can be abused.

Allowlisting

Block first, allow by exception
The most effective defense is simply not allowing 7-Zip (or any unapproved utility) to run at all. Using a deny-by-default model ensures only explicitly authorized applications can execute. If your business does not need 7-Zip, it never becomes a threat vector.

Ringfencing

Contain what you must allow
Where tools like 7-Zip are required, Ringfencing restricts what they can touch. You can allow the executable but prevent it from accessing system folders, startup paths, scripts, PowerShell, or network locations, effectively neutralizing vulnerabilities like the recent symlink bug.

Data Storage Access Control

Stop rogue file writes at the source
ThreatLocker can block applications like 7-Zip from writing to sensitive directories or types of storage. That means no DLLs quietly dropped into system folders, no persistence mechanisms planted by stealth, and no unauthorized file manipulation.

Privileged Access Management

Remove the attacker's shortcut
Sometimes users run tools with elevated rights without even realizing it. ThreatLocker can enforce strict rules about which applications can request elevation, preventing 7-Zip or similar tools from running with privileges that could enable a catastrophic exploit.

Controlled Application Testing Environment

Test tools before deployment
Administrators can monitor the behavior of any new tool in a safe, sandboxed environment before it goes live, allowing full-scale tests that could reveal unseen vulnerabilities and flaws.

Unified Visibility

Know where the risks are
ThreatLocker exposes unknowns such as portable copies of 7-Zip in user folders, outdated versions bundled inside third-party applications, or rarely seen utilities sitting on servers. Visibility transforms surprise risks into controllable ones.

ZERO TRUST NEEDS HUMAN TRUST

Many organizations are failing to achieve Zero Trust maturity across all pillars. New research is clear: Closing the gap requires deployment strategies that build human trust and embed security with people, not imposed on them

As recently as 2023, just 2% of organizations achieved Zero Trust maturity across all pillars, according to Cisco's Security Outcomes Report, which canvassed 4,700 security professionals. More recent statistics from Gartner predict that the figure could rise in 2026, but only to around 10%. Those are numbers that should keep security leaders awake at night—and digging further into the figures reveals the issues preventing adoption from reaching maturity.

Accenture's 2025 State of Cybersecurity Resilience report reveals 63% of corporations face significant implementation challenges, with 27% either strong on cyber strategy but lacking in implementation or strong on protection but lacking strategic alignment. Only the final 10% demonstrate robust security capabilities and an integrated cyber strategy.

These implementation challenges have led Gartner analyst Craig Porter to predict that 30% will abandon Zero Trust entirely by 2028. The reason behind these figures is not budgetary or technological: It is what Gartner calls "implementation fatigue."

That phrase deserves a closer look. Tools and spending can only take an organization so far; those that make Zero Trust work treat implementation as a challenge on both the human and technical level. The gap separating success from failure is measured in how well security teams bring their people along with their Zero Trust policy.

Resistance is not futile

McKinsey research suggests that 70% of all change management initiatives fail, largely because of employee resistance. Zero Trust is no exception to this trend. When tested with 320 professionals, a study published in the Information Systems Journal found that coercive authority, the use of mandates, employee penalties, and top-down enforcement consistently produce lower compliance and greater pushback than influence-based approaches.

There is a classic industry tale—almost a parable by now—around the time GoDaddy emailed 500 employees a fake offer of USD 650 holiday bonuses. Those who clicked were told they had "failed" a phishing test and were enrolled in mandatory training. The backlash was inevitable. A social media outcry forced the company to issue a public apology‡ and caused an unnecessary hit to worker morale. Research published in Computers & Security reinforces the pattern, finding that fear-based motivation reduced discretionary security behaviors.

Gartner predicts only around 10% of organizations will achieve Zero Trust maturity by 2026

With your people, not at them

There are many successes to learn from. When the U.S. Department of the Interior adopted Zero Trust, the team built a "Zero Trust community of practice," a monthly gathering that grew to roughly 1,000 participants. Acting CISO Louis Eichenbaum was candid about where the real difficulty lay, suggesting that "cultural change is the biggest challenge. It's making people understand that Zero Trust is not about implementing new technology. It's a mindset."‡

Behavioral science supports the lessons learned and demonstrated by the Interior Department. Multiple studies have shown that appeals to intrinsic motivation with clear explanations of the purpose behind security measures, connecting processes to shared goals, and treating employees as partners in the policy produce far higher compliance than fear-based messaging.

A 2025 systematic review presented at the ACM CHI conference went further, documenting a shift in the way researchers now think about humans in security. Enabling employees to openly embrace Zero Trust technologies and practices transforms them into "valuable resources" within the security apparatus.

Consistent enforcement becomes a trust-building exercise. When security rules apply equally, with no executive or other arbitrary exceptions, people will be far more willing to accept them. Research into procedural justice shows that perceived fairness is a more powerful driver of compliance than punishment, especially when leaders do indeed lead.

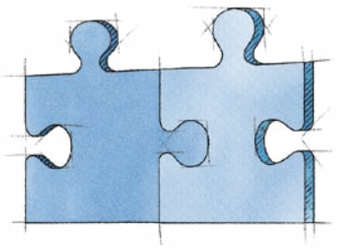
Communicating security clearly

Clichés can be rooted in deeper truths. As true as the saying "people do not like change" is, it overlooks the fact that change itself is not necessarily the problem for people. In 2025, the Proceedings of the National Academy of Sciences (PNAS) published a study from researchers at the Technical University of Munich that drew on nearly 50,000 respondents, demonstrating that psychological resistance to system-level policies peaks just before implementation and dissipates quickly afterwards.

The takeaway here for CISOs is significant: Pre-rollout complaints are not reliable indicators of long-term failure or non-compliance. They are predictable, temporary, and manageable, provided the groundwork has been done. Communicating early, clearly explaining the positive reasoning behind changes, and starting with controls that visibly improve the employee experience makes all the difference.

GitLab, for example, launched its Zero Trust program for a fully remote workforce by introducing single sign-on first, an improvement people widely welcomed. This was followed by multi-factor authentication (MFA), running an open beta that let employees choose which factors worked best for their roles before making it mandatory. Automated provisioning came next, cutting the new-hire access setup from three weeks to near-instant. By the time more restrictive device-trust controls arrived, the workforce had already seen security make their daily experience easier and understood the goal of strengthening company security.

The gap separating success from failure is measured in how well security teams bring their people along with their Zero Trust policy

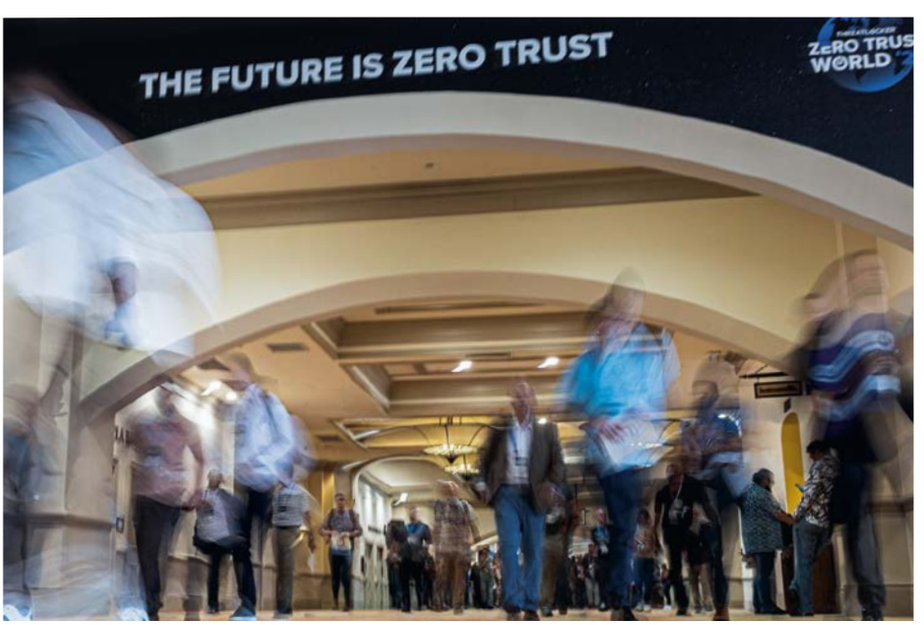


The non-negotiable

Of course, there are times and environments where a slow rollout is not an option. Healthcare organizations operating under the Health Insurance Portability and Accountability Act (HIPAA) or financial institutions bound by the Payment Card Industry Data Security Standard (PCI DSS) cannot wait for full cultural buy-in before enforcing access controls, but they still need to build it along the way. Regulators tend not to accept "we're still socializing the change" as a compliance posture.

With delay not an option, the human-centered approach makes an argument for sequencing. In regulated environments, the most effective teams introduce controls that solve a visible pain point first—automated audit logging to eliminate manual spreadsheets, single sign-on to reduce password fatigue—and then build outward toward more restrictive policies. This attitude makes the compliance mandate the baseline.

Staff who see security making their audits easier are far more willing to accept tighter application controls down the line. The approach still holds. Explain the "why," start with what helps, enforce consistently and fairly.



When Zero Trust moves from policy to practice, it takes more than technology—it takes people willing to lead the change together

Stay secure without disruption

The design principle is simple. Users should feel that "things just work." No fanfare, no disruption, no helpdesk surge. This aligns with what the National Institute of Standards and Technology (NIST) study on security fatigue identified as a critical barrier: When users face too many security decisions, they disengage entirely. The researchers proposed three remedies: Limit security decisions, simplify the right action, and design for consistency.

There are financial benefits to successful deployment. A 2025 Forrester Total Economic Impact study validated Zero Trust at enterprise scale, reporting 184% ROI over three years; a 50% reduction in security operations labor; a seven-month payback period; and a 99% reduction in addressable security incidents.

The distance between the near-universal Zero Trust aspiration and the 2% who have achieved maturity appears to be a trust gap. As we have seen, organizations that close the gap share common good practices: They explain the "why" behind every control, design policies around real behavior, enforce rules consistently and fairly, and start with changes that make employees' working lives easier before introducing restrictions.

> "Cultural change is the biggest challenge. It's making people understand that Zero Trust is not about implementing new technology. It's a mindset
>
> LOUIS EICHENBAUM

Accenture's 2025 research highlights that currently only 10% of organizations achieve its "Reinvention-Ready" security posture, which integrates strategy and capability. Those who do get there are 69% less likely to face advanced attacks. The 2% problem is, at its core, a leadership problem. And leadership, in security as in everything else, comes down to influence.

THREATLOCKER® CLOSES THE ASPIRATION-EXECUTION GAP

Zero Trust works when it works with your people. ThreatLocker is designed around that principle, not as a product that imposes security from above, but as a platform designed to work with people and reduce the friction that derails adoption.

ThreatLocker helps organizations adopt the mindset of Zero Trust by removing the friction that derails it.

The philosophy starts with how policies are created. **Learning Mode** observes which applications are running in an environment and builds allowlisting policies from real behavior, not theoretical assumptions. Security teams start from what people do.

For end users, the experience is designed to be seamless. **User Store** offers a catalog of pre-approved applications that employees can install themselves.

Privileged Access Management enables specific applications to run with the permissions they need without granting full admin rights. When a request does arise, deny-by-default with a 60-second approval process means nobody is left waiting.

And with the ThreatLocker Cyber Hero® Team ready to respond around the clock, even the smallest IT teams can maintain responsive security without burnout.

THE HYPERVISOR **COMPROMISE**

Bring visibility to the infrastructure blind spot your security team may not be watching

Server farms have become less prevalent over time. Even enterprise data centers have largely moved away from buying physical servers in bulk. Today's IT operations teams lean more on virtual machines (VMs), provisioning services on demand through centralized management consoles.

There is significant efficiency to be gained from this approach. VMs mean administrators can spin up hundreds of instances in hours rather than weeks. That flexibility comes courtesy of the Type 1 hypervisor, a layer that runs directly on hardware and abstracts the underlying infrastructure. The catch is that the same abstraction layer now sits at the top of every security stack, and most organizations lack meaningful visibility into it.

Understanding what is at risk

For those unfamiliar with virtualization architecture, here is the run-down: A Type 1 hypervisor sits between physical hardware and virtual machines running applications. It then decides how much compute, memory, and storage each VM gets. When a hypervisor administrator logs in to the management console to create a new server or modify network settings, they operate at a layer above any individual guest operating system.

That location is important. An attacker who compromises the hypervisor management plane basically enters the network at the penthouse. They do not need to breach individual servers because their vantage point offers them access to all virtual machines beneath as raw data stores, bypassing operating system security controls entirely. They can take snapshots of running workloads, copy sensitive data, or shut down critical systems simultaneously.

Hypervisors have understandably become attractive targets for attack, yet this critical layer remains a high-security hurdle for many organizations. The problem is that most Type 1 hypervisors do not play well with traditional security tools. Enterprise security teams typically rely on endpoint detection and response (EDR) agents, antivirus software, and host-based intrusion detection systems (HIDS) installed directly on servers, but these tools simply will not run on a bare-metal hypervisor. The architectural design does not support them.

An EDR agent cannot be dropped onto a Type 1 hypervisor such as an ESXi virtualization management console in the same way as it can on a Windows Server. Attackers, including the Akira ransomware group, are actively exploiting[‡] this visibility gap—and it is one that awareness alone will not fix.

The three layers of defense

Organizations cannot install agents on hypervisors, so instead they must build a coherent defense to protect the management plane. Three compensating controls work together to reduce exposure: identity and access, network isolation, and detection.

1. IDENTITY AND ACCESS

Hypervisor management accounts hold broad, overarching power over infrastructure. An attacker needs only to compromise one account to inherit that power.

Multi-factor authentication (MFA) is therefore non-negotiable—it is the single most effective way to prevent credential-based attacks against privileged accounts.

Organizations should also enforce the principle of least privilege, granting administrative rights only to staff who need them for their actual job functions, and only when those rights are required. Quarterly access reviews are useful to catch privilege creep before it becomes a liability.

2. NETWORK ISOLATION

Most data center networks operate with relatively flat topologies, meaning systems can reach one another freely. Hypervisor management interfaces typically sit on standard ports like 22, 80, and 443, and these can be left accessible from anywhere. The fix is network segmentation: Isolate management traffic to a dedicated virtual local area network (VLAN) and restrict access to a small set of authorized systems.

Better still, implement a dedicated administrative jump box, a hardened system that serves as the only path to the hypervisor management plane. Instead of allowing administrators to log in from their workstations or multiple access points, this ensures all management activity flows through a single machine.

Consolidation like this makes monitoring easier and creates a natural checkpoint for additional controls. Tools that enforce granular access policies can then ensure only approved systems are allowed to communicate with the jump box itself. In a healthcare environment, for example, physicians and scheduling staff have no reason to access hypervisor management consoles. Cutting access from thousands of systems down to a single administrative terminal dramatically reduces the attack surface.

3. DETECTION

Prevention and isolation cannot eliminate all risk because the management plane must remain accessible to do its job. This is where continuous monitoring becomes critical. Hypervisor management logs should flow into a centralized security information and event management (SIEM) platform with detection rules built around privileged activity. The sophistication comes from monitoring behavioral deviations rather than relying solely on known attack signatures.

If your organization has a formal process for creating administrative accounts, any account creation outside that process should trigger an alert. If administrators do not typically shut down multiple VMs simultaneously, threshold-based rules can flag mass power-downs. These behavioral baselines catch credential misuse and insider threats earlier in the attack chain. Detection will not prevent hypervisor compromise, but it will catch it before damage becomes irreversible.

Making the case

Infrastructure and security teams speak different languages and sometimes work at cross purposes. Virtualization specialists value flexibility and operational ease. Security teams want restrictions and visibility. These three controls bridge that gap; they are operational, minimize overhead, and meaningfully reduce risk.

For organizations operating at scale, there is nothing optional about this. Hypervisors are the crown jewel of the infrastructure hierarchy, and defenders need to act accordingly.

HOW THREATLOCKER® PROTECTS THE HYPERVISOR PLANE

ThreatLocker reinforces the three compensating controls organizations depend on to protect hypervisors.

Zero Trust Endpoint Firewall enforces segmentation by dynamically opening and closing ports only when required, restricting which systems can communicate with administrative access systems.

Privileged Access Management ensures that only approved accounts can connect to hardened jump boxes, and even then, only when required, preventing unauthorized administrative endpoints from reaching hypervisor management consoles.

ThreatLocker EDR monitors endpoint activity across the infrastructure to identify compromised administrative accounts or anomalous behavior that precedes hypervisor attacks. And if a workstation is compromised, **Ringfencing™** limits how applications interact, preventing administrative tools from being weaponized.

Together, these capabilities fill gaps in hypervisor security by controlling access, limiting lateral movement, and providing the visibility required to detect threats before they reach the management plane.

PLAYING DEFENSE

Cybersecurity has moved from a back-office concern to an operational priority for sports organizations at every scale

Like cybersecurity, professional sport runs on information. Performance analytics guide tactical decision-making. Medical data informs selection and field time. Commercial platforms keep fans connected long after the final whistle. Though inherently human-driven, the modern sports team is as much a digital enterprise as a sporting one. Yet cybersecurity maturity in sports often lags behind the scale of exposure, despite numerous high-profile incidents that have offered a glimpse of what is at stake.

In 2021, the Houston Rockets confirmed a ransomware attack that disrupted internal systems and exposed over 500GB of sensitive business information, including player contracts and financial data.[‡] In the previous year, Manchester United experienced a cyber incident that affected club operations and reportedly forced the shutdown of critical IT systems.

Teams are not the only target; large sporting events like the FIFA World Cup

and the Olympic Games can trigger a rise in cyberattacks. It is estimated that the 2026 World Cup will lead to upwards of 55 million attempted cyberattacks in Mexico alone.[‡] The larger the event's scale, the more reliant it becomes on automation, digital access, and complex networked systems, presenting hackers with a large playing field, and a watching crowd for whom any disruption will be highly visible.

The competitive value of information

In sports, cybersecurity can be directly linked to team reputation and performance. Teams generate and collect large volumes of data that influence game outcomes. Tactical playbooks, scouting intelligence, contract negotiations, and draft strategies are all commercially and competitively sensitive. Performance departments increasingly rely on wearable and biomechanical technology to guide training loads and injury prevention. Video analysis platforms house detailed breakdowns of player and team tendencies.

Even partial exposure of this material can create uncertainty or, if leaked, confer a significant advantage to opposing teams, but the stakes extend beyond competitive secrecy. Medical and rehabilitation data carry privacy implications. Sports organizations operating across jurisdictions (especially European clubs) face General Data Protection Regulation (GDPR) obligations around athletes' medical data, biometrics, and fan data, adding further pressure.

Leaked travel schedules or personal details can create security risks for high-profile athletes and staff. In a sector where emotional tension can run high and where individuals are among the most recognizable public figures in the world, breaches can quickly shift from an operational inconvenience to a personal concern.

It is estimated that the 2026 World Cup will lead to upwards of

55 million

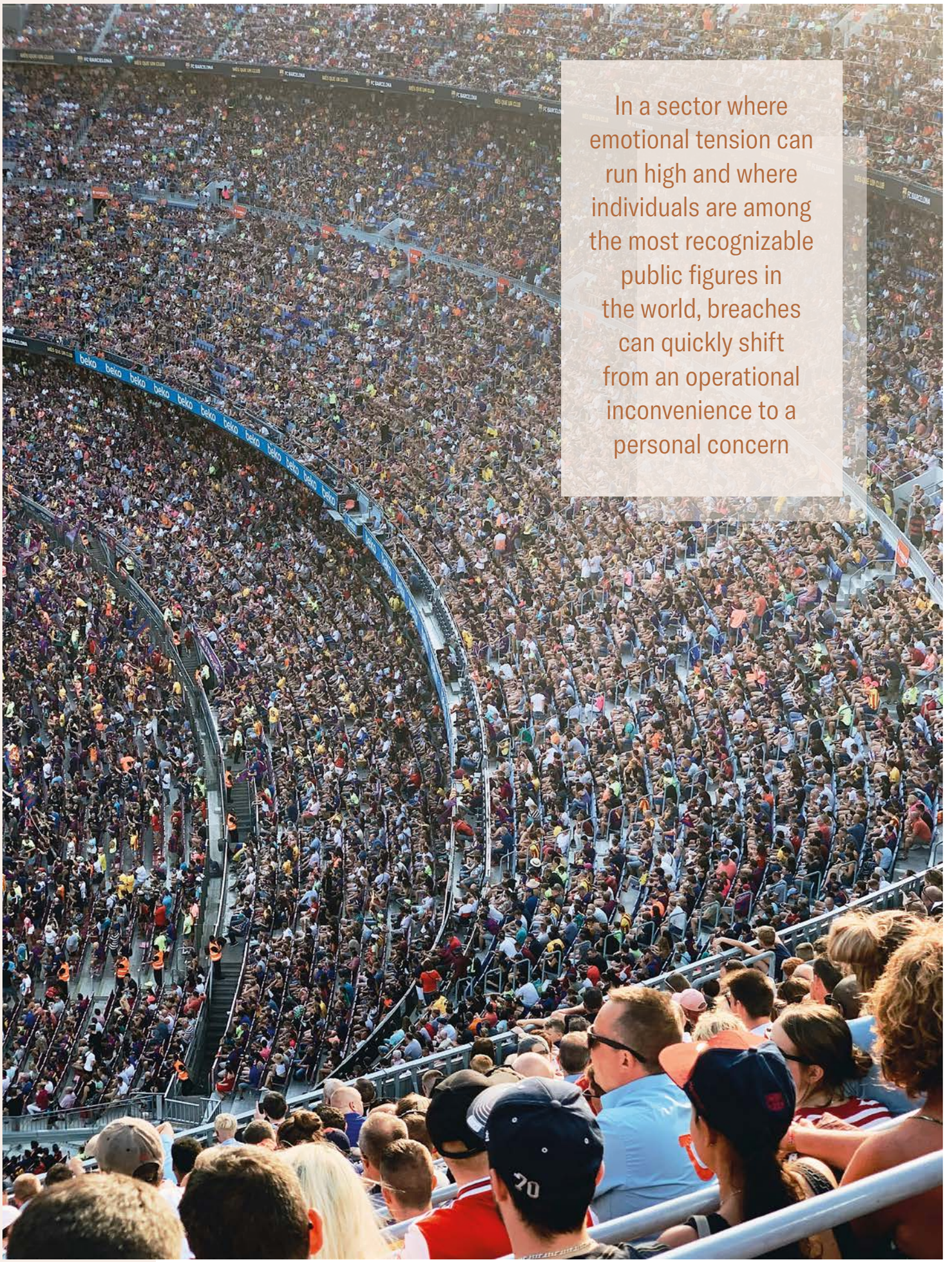
attempted cyberattacks in Mexico alone

A broad digital ecosystem

A team is not an island. Like most enterprises, sports teams rely on a web of partners: League infrastructure, analytics providers, player agents, ticketing vendors, broadcast partners, and stadium operators all interact with team systems. Each connection introduces new dependencies. Each new dependency complicates security governance and adds the possibility for a third-party breach to spread.

It is a familiar story, but the results of a breach reach far beyond regulatory repercussions for sports organizations. A compromise in a system such as ticketing could immediately affect thousands of supporters—it is the kind of negative event that creates immediate and long-lasting reputational impact. Problems at broadcast and media partners could send games dark, threatening critical rights agreements and causing cascading issues down the line.

Teams realistically have little control over what happens outside of their direct jurisdiction, other than following their obligation to select partners based on demonstrable trustworthiness. They do, though, have the ability to control their own perimeter, and everything that goes on inside it.



In a sector where emotional tension can run high and where individuals are among the most recognizable public figures in the world, breaches can quickly shift from an operational inconvenience to a personal concern

The connected stadium

In many leagues, scaling follows team performance. A sudden hot season, a promotion to a higher division, and the complexity ramps fast. It is vital to implement scalable cybersecurity that can maintain its rock-solid floor no matter how much is piled upon it.

When a team's roster of temporary contractors, seasonal staff, and specialist consultants grows, access requirements shift week by week. Identity management is incredibly challenging without the right toolset. Teams must also consider the stadium itself, a complex, connected environment. The operational environment of a stadium—its access control, surveillance, digital signage and other systems that keep operations running—supports fan experience and venue efficiency, yet it also creates additional entry points.

In this context, cybersecurity is equal to physical resilience. A system breach leading to a turnstile failure could cascade into a crush of spectators. A payment outage could derail food vendors, ticket sales, and even toilet facilities—fans unhappy about a game result is one thing, but spectators unhappy about their treatment is quite another, and may have very different results. Such incidents do not always stem from malicious activity, to be clear, but the fact that they could, should be enough to trigger decisive action.

The National Football League averages

18.7 million

viewers per game

Game day pressure

Stadium technology increasingly resembles critical infrastructure, even when framed as entertainment, and like most critical infrastructure, sports teams face periods of fluctuating demand and risk. Transfer windows, drafts, and contract negotiations concentrate sensitive data within short periods. Playoffs and major tournaments amplify public attention, raising the stakes of operational disruption. A ransomware incident during an off-season period presents one set of challenges, but the same incident on a game day can create immediate operational and reputational strain.

Live events introduce additional complexity for incident response. The National Football League (NFL), for example, averages 18.7 million viewers per game[‡], so broadcast schedules, fan expectations, and logistical constraints limit the scope for prolonged system outages. Teams like the Green Bay Packers attract nearly 78,000 fans every time they play at home[‡], meaning security teams must balance containment with continuity, often under intense time pressure.

THREATLOCKER® TIP

OUTPLAYING CYBERCRIME WITH THREATLOCKER

Sports organizations rely on a constantly shifting mix of staff, partners, and specialist technologies, making strong control over applications and access essential. The granular controls of **Allowlisting** help teams prevent ransomware and unauthorized tools from executing, even as new performance analytics or wearable platforms are introduced during a season.

Alongside this, **Privileged Access Management** supports clear, easy management of least-privilege access for athletes, coaches, contractors, and operational staff, ensuring individuals can perform their roles without creating unnecessary risk. This is particularly valuable when access requirements change rapidly around transfers, tournaments, or game-day operations.

Finally, **Zero Trust Endpoint Firewall** enables segmentation across stadium infrastructure, corporate systems, and performance environments. By limiting lateral movement and providing visibility into device communications, teams can reduce the likelihood that disruption in one area cascades across game-day systems, helping protect competitive data, fan services, and broadcast continuity.

Cultural realities inside sports organizations

Cybersecurity within sports teams must be molded to fit around evolving organizational needs. Performance environments prioritize speed, collaboration, and flexibility. Coaching staff may adopt new analytics tools quickly. Athletes and agents expect seamless digital access. Prioritize a frictionless, adaptive security posture, and these challenges become straightforward to manage; do not, and they could lead to shadow IT or informal data-sharing practices that sit outside formal governance.

Sporting teams tend to host high-profile individuals, and these can also influence expectations around access. Athletes, senior coaches, and commercial stakeholders frequently require mobility and remote connectivity. Security controls perceived as obstructive will inevitably encounter resistance, particularly in competitive environments where marginal gains are closely pursued. Effective cybersecurity means taking an approach that understands the way the team and its stars work, rather than one that puts blockers in their way.

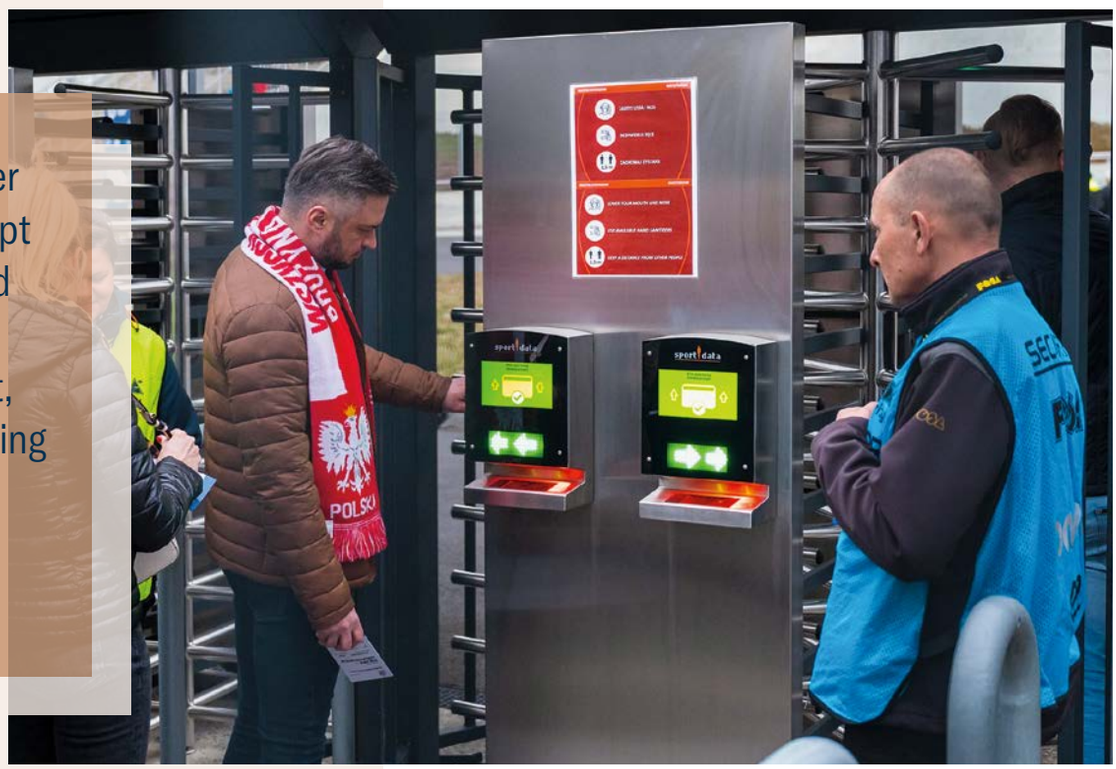
Threat actors and motivations

Sports teams share many characteristics with conventional enterprises, but their diversity gives them potentially the widest attack surface of any business. Financially motivated ransomware groups view teams as attractive targets due to brand visibility and perceived ability to pay. Hacktivists may target organizations connected to political or social controversies. Insiders, whether malicious or negligent, remain a persistent concern given the fluid workforce and high contractor turnover.

Consider also the rise of sports betting, particularly in the U.S., given the rapid growth of new prediction markets like Kalshi and Polymarket. Access to injury reports, lineup decisions, or internal performance data essentially gives bettors a zero-day advantage over the sports book. While the pursuit of such data may not always attract highly coordinated attacks, it does highlight the sensitivity of seemingly routine information.

Sports teams share many characteristics with conventional enterprises, but their diversity gives them potentially the widest attack surface of any business

A significant cyber incident can prompt questions around governance and risk management, potentially influencing partnerships or insurance considerations



For supporters, the action on the field remains the focus—but behind the scenes, digital resilience has become part of the broader infrastructure that allows sport to operate smoothly

Fan trust and commercial impact

In the end, the playbook for sports teams must focus on maintaining trust through a Zero Trust approach: Keeping supporters happy and sponsors sweet, creating secure relationships with key personnel, and building a confident foundation on the bedrock of cybersecurity. A significant cyber incident can prompt questions around governance and risk management, potentially influencing partnerships or insurance considerations.

For teams operating in a competitive commercial landscape, maintaining confidence across stakeholders is as important as protecting internal data. Cybersecurity is a key component of data protection, meeting privacy frameworks, complying with gambling integrity regulations, and, increasingly, meeting security expectations issued by leagues and governing bodies.

Sports teams are accustomed to preparing for varied opponents and adapting tactics over a season. Cybersecurity requires a similar mindset: Awareness of evolving threats, investment in defensive capabilities, and readiness to respond under pressure. The organizations that approach resilience as an ongoing discipline rather than a periodic project are likely to be better positioned when challenges arise.

For supporters, the action on the field remains the focus. Behind the scenes, digital resilience has become part of the broader infrastructure that allows sport to operate smoothly. Strong cybersecurity rarely attracts headlines when it works well, yet it protects athletes, fans, and partners alike. In that sense, it resembles a well-organized defense: often unnoticed, occasionally tested, and vital over the course of a long season.

FULL-COURT PRESS

For the Orlando Magic, Zero Trust is the ultimate lockdown defender, controlling every play behind the scenes so nothing slips through on NBA game day

When the game clock is ticking, downtime is not an option. At the Orlando Magic, technology underpins everything from fan experience to broadcast operations, and it all happens in real time. The Magic face a cybersecurity challenge quite unlike that of a typical environment.

Jeff Lutes, Executive Vice President of Technology, has spent more than a decade shaping the team's complex security stack. He speaks to Cyber Hero® Frontline about the Magic's adoption of Zero Trust, the role of ThreatLocker® in that journey, and what it takes to shift from enterprise security to the pace and pressure of game day.

Can you describe the technology environment you're responsible for at the Orlando Magic?

When people think about technology in sports, they tend to focus on what happens on the court, but it's much broader than that. On any given day, we support three distinct environments: a live arena with thousands of fans, a training facility focused on player performance, and a corporate operation spread across multiple locations.

We run a hybrid environment built around Microsoft 365, Azure, and Nutanix, which gives us the flexibility to support a mobile workforce while keeping things secure and stable. Cybersecurity is built into everything we do, and it has to be, especially given league expectations and the visibility that comes with being part of the NBA.

It all comes together on game day: Wi-Fi, ticketing, digital signage, IPTV, broadcast systems—they all have to work, and there's no margin for error. Technology doesn't just support the experience. It is the experience.

What threats concern you most in that kind of environment?

We're a high-value target. We're protecting player information, financial data, fan transactions, and more. The threats that stay front of mind are the ones that target people first. Phishing continues to evolve, and attackers only need one successful click to do damage. Ransomware is another major concern, particularly given our live-event model.

We also pay close attention to data exposure. When you're using cloud platforms and collaboration tools, access has to be tightly controlled—and because we rely on a range of partners, third-party risk is a constant concern. In our world, maintaining trust and continuity is just as important as preventing incidents. On game day, downtime isn't an option.

What led you to adopt a Zero Trust approach?

It wasn't a single moment. It was more a recognition that the environment had changed. With more cloud services, remote access, and reliance on third parties, the traditional perimeter didn't really hold up anymore. Identity became the front line.

At the same time, given our need for uptime and the league's expectations around security, it was clear we needed a more structured approach. Zero Trust gave us that framework: strong identity controls, least privilege, and continuous validation. But it had to be done in a practical way. The goal was to reduce risk while still enabling the organization to move.

How does game day change your threat model?

Game day changes everything. You move from a relatively controlled environment to one where thousands of devices connect at once, including fans, media, vendors, and internal teams. The attack surface expands very quickly—and so does the pressure. This is a live production environment. Ticketing, concessions, retail, broadcast, connectivity, it all has to function in real time, with very little tolerance for disruption.

That means we have to take a very deliberate approach. We segment aggressively, isolate critical systems, and rely heavily on identity and continuous monitoring. We also plan for rapid response, because response time matters.

What problem were you trying to solve when you brought in ThreatLocker?

We were trying to answer a simple question: How do we get control over what's running in our environment? We had strong visibility and detection in place, including **Managed Detection and Response (MDR)**. But those tools are, by nature, reactive. They tell you after something has happened. We wanted to move upstream and prevent execution in the first place.

The ThreatLocker allowlisting model aligned with that. It lets us define what "normal" looks like and block everything else by default. That's a fundamental shift. Working with ThreatLocker wasn't about adding another tool. It was about closing a gap and moving from reacting to controlling.

> "Game day changes everything. You move from a relatively controlled environment to one where thousands of devices connect at once, including fans, media, vendors, and internal teams. The attack surface expands very quickly, and so does the pressure

How did the implementation go in practice?

It was more straightforward than you might expect, largely because we didn't rush into enforcement. We used the ThreatLocker **Learning Mode** to build a clear picture of what normal activity looked like across the environment. That gave us a clean baseline and avoided disruption when we enforced policies. The rollout followed the same principle as the broader Zero Trust approach: phase it, test it, and align it with how the business operates.

ThreatLocker application control functions were a big step forward for us. Previously, we didn't have a consistent way to manage and contain applications across platforms. And direct engagement really helped: the ThreatLocker team spent time understanding the specifics of our environment, especially around game-day operations. That made a real difference.

What has changed day to day since deployment?

The biggest change is control. Before, as in most environments, we had good detection, but there was always a window during which something could execute before being flagged. Now, if it's not approved, it doesn't run.

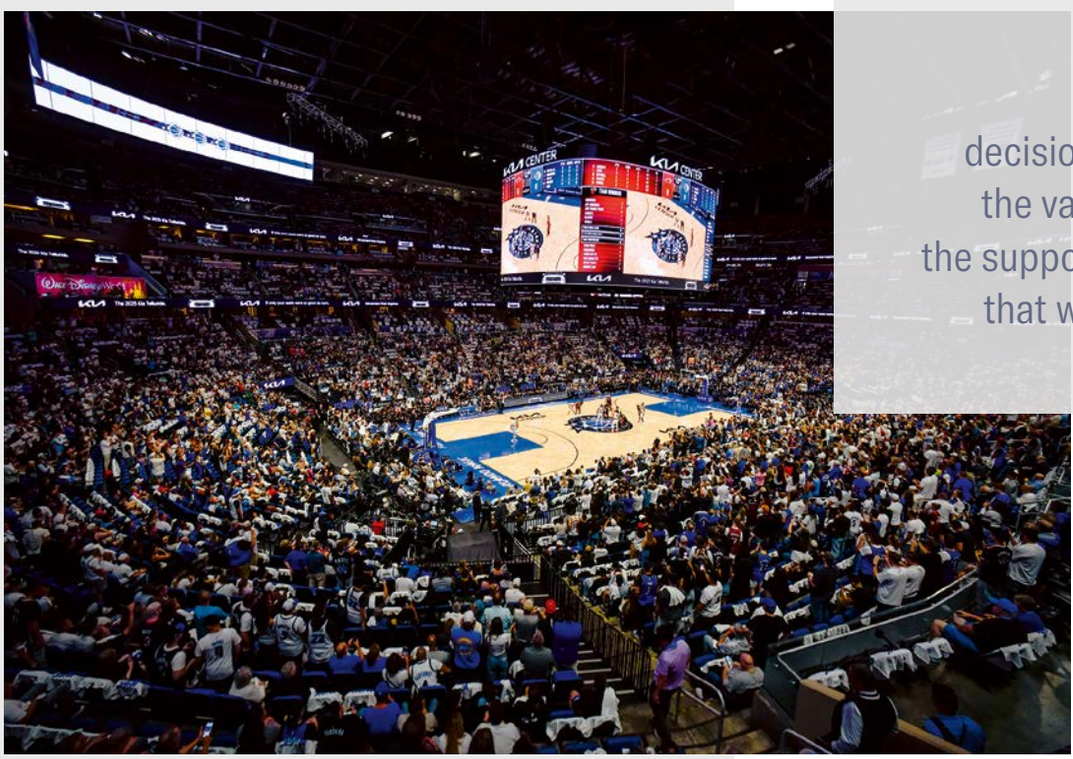
A simple example is scripts. A lot of attacks start with something attempting to run quietly in the background. Previously, that might have been detected after the fact. Now, we've seen unknown scripts or executables stopped—with no impact—multiple times. We're not chasing alerts; we're controlling what can happen.

Which ThreatLocker capabilities have made the biggest difference?

Deny-by-default is the foundation. If something isn't approved, **Allowlisting** means it simply doesn't execute. That changes the risk profile straight away. **Ringfencing™** has also been important. Even approved applications are restricted in what they can do. If something goes wrong, it's contained.

We've also removed standing admin rights. That's a common attack path, and eliminating it without slowing users down is a big step forward. Just as important, it works operationally. If something legitimate is blocked—especially on a game day—we can review and approve it quickly. It's that balance of control and

> "We can make decisions in real time; the value lies in both the support and the fact that we don't need it



Recently renovated by ANC, the Kia Center's state-of-the-art scoreboard treats fans to a 360-degree view of the action

The 875,000 square foot Kia Center, in downtown Orlando, features one of the most advanced broadcast control rooms in professional sports

flexibility that makes the difference. Because the process of applying rules through ThreatLocker is predictable and quick, it hasn't created friction. It's just introduced a level of discipline.

Our support experience has also been strong. When we need the Cyber Hero® Team, they're there, but more importantly, the platform gives us the control to handle most situations ourselves. That's critical on a game day. We can make decisions in real time; the value lies in both the support and the fact that we don't need it.

Looking ahead, how do you see cybersecurity evolving in professional sports?

The industry is becoming more connected. Venues, mobile platforms, fan engagement, and partnerships are all linked together, which naturally expands the attack surface. The focus will continue to shift away from perimeter security toward identity, device control, and execution control.

Automation and AI will play a bigger role as well. There's simply too much activity to manage manually, and at the same time, expectations are rising. Whether it's the league, partners, or fans, there's an assumption that systems are secure and always available. We need to ensure that the assumption holds true so cybersecurity becomes more integrated. It's part of how the business runs.

Finally, what's your focus for the future at the Orlando Magic?

Technology will continue to play a bigger role across the organization, both on the business side and in basketball operations. We'll see greater reliance on data and a growing need for low-latency systems to support real-time decision-making.

At the same time, the attack surface will keep expanding as the NBA grows globally. For us, it's about staying ahead of that, continuing to reduce risk while supporting the organization's goals. The mission is to deliver at a high level, both on and off the court. Technology and security are a big part of that.

Jeff Lutes
Executive Vice President
of Technology, Orlando Magic

Jeff Lutes brings more than 35 years of leadership experience in technology organizations to the Orlando Magic, spanning financial services, real estate, manufacturing, and professional sports. He has spent nearly 14 years with the Magic, overseeing both IT and broadcast technologies.

Lutes' remit spans cybersecurity, enterprise IT strategy, and the delivery of game-day production across the 20,000-seat Kia Center, the team's training facilities, and its affiliated organizations. He leads the development of hybrid cloud and on-premises environments designed to support a highly visible, real-time operation, where performance and reliability are non-negotiable.

Lutes and Orlando Magic's Director of Technology, Victor Porras sat down to discuss their experience with ThreatLocker Zero Trust capabilities. Check out the video interviews at *threatlocker.com* or scan QR code.

EMERGING DIGITAL MARKETS

AND THE EVOLUTION OF CYBERSECURITY

Growth economies are driving digital development—
while businesses learn how to expand securely alongside them

If you ask most technology leaders where their next growth markets are, the answers increasingly point far beyond Silicon Valley or Western Europe. India, Nigeria, Colombia, Brazil, and a growing list of digital economies are not just joining the global tech ecosystem; they are building some of its most important moving parts.

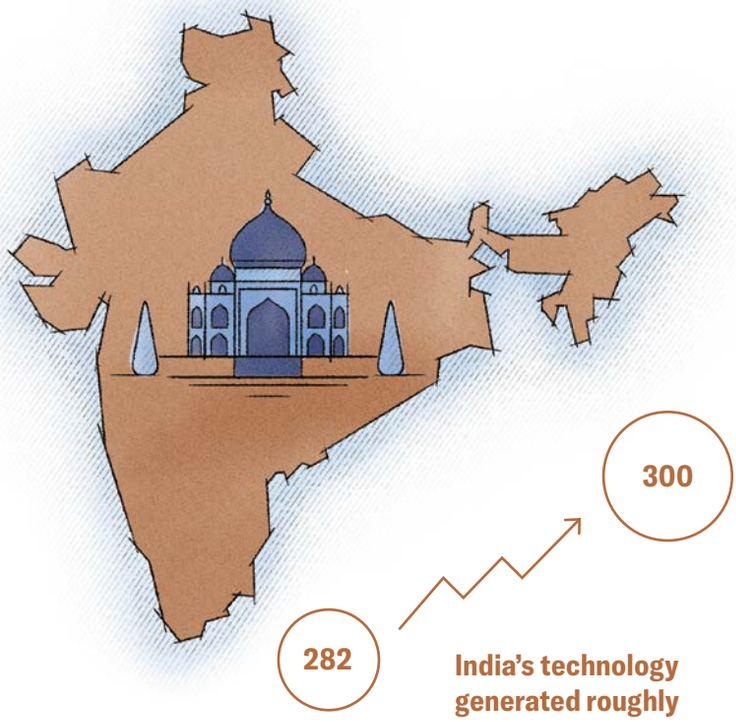
That global integration has created huge opportunities for companies looking to scale faster or operate around the clock, but it has also sparked a quieter conversation that is only just beginning to get attention. As digital partnerships expand across borders, cybersecurity is being reshaped in ways many organizations still struggle to grasp.

The question is no longer whether emerging markets are safe places to do business. In many cases the opportunities are too important to pass up. Global companies must, though, adapt their security strategies quickly enough to keep pace with the internationalization of their operations.

India's rise from an outsourcing hub to a cybersecurity stakeholder

People still tend to associate India with outsourced support work, but that description has fallen behind reality. In many organizations, teams in India are now working on engineering projects, operating infrastructure, and managing systems that customers interact with every day.

Government figures show that India's digital economy accounted for just under 12% of national output in the 2022 to 2023 fiscal year, with projections indicating it will continue to grow.[‡] Industry group NASSCOM states that the country's technology sector generated roughly USD 282 billion in revenue in the 2025 fiscal year, with expectations that it will soon surpass the USD 300 billion mark.



India's technology generated roughly USD 282 billion in revenue in the 2025 fiscal year, with expectations that it will soon surpass USD 300 billion

Those numbers explain why companies increasingly rely on India-based teams to run critical infrastructure. Global Capability Centers (GCCs) across cities such as Bengaluru and Hyderabad now handle everything from software development and cloud engineering to security monitoring and threat response.

None of that is inherently risky, but it does change a fundamental aspect about cybersecurity. When teams on the other side of the world can reset production servers, deploy code, or access customer environments, trust relationships become far more complex than traditional outsourcing models ever required.

India has been steadily building out privacy and cybersecurity oversight to match its growing digital footprint. The country introduced the Digital Personal Data Protection (DPDP) Act in 2023, establishing national rules around consent, data processing, and breach reporting. The legislation reflects a broader recognition that digital growth depends heavily on trust, particularly when international companies are moving large volumes of customer data across borders.

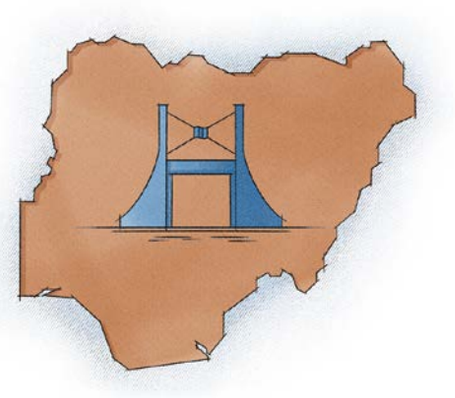
↑ In Bengaluru, Global Capability Centers now handle everything from software development and cloud engineering to security monitoring and threat response

Nigeria's digital finance surge

In Nigeria, digital growth has been closely tied to mobile phones and fintech services rather than outsourcing. Payment applications, mobile wallets, and peer-to-peer transfers have made financial services accessible to millions of users who previously had little interaction with conventional banking.

According to GSMA, mobile technology contributed approximately NGN 33 trillion (approx. USD 52 billion at 2023 exchange rates) to Nigeria's economy in 2023. That figure captures just how quickly digital services have become woven into everyday commerce, from sending money to paying utility bills.

With that growth has come a parallel push to strengthen cyber governance. Nigeria introduced a National Cybersecurity Policy and Strategy (NCPS) in 2021. It followed that up with the Nigeria Data Protection Act (NDPA) in 2023, which created the Nigeria Data Protection Commission (NDPC) as the country's privacy watchdog. Enforcement is already beginning to take shape, too: In 2024, the regulator fined Fidelity Bank over failures linked to how customer data was handled during account creation[‡], signaling that privacy rules in the country are starting to carry real consequences.



Still, the most common cybersecurity challenges linked to emerging digital economies rarely appear at the national policy level—they surface within vendor ecosystems. A large fintech platform is likely to have spent years building its security program, while a smaller contractor working on onboarding or infrastructure may not have had the same resources. When attackers go looking, they usually start with whoever looks least prepared.

Cybersecurity policy in Nigeria has also had to contend with political reality. A proposed levy to fund cyber initiatives was paused in 2024 after it sparked public opposition tied to the cost-of-living crisis.[‡] It showed how hard it can be to move security programs forward when economic pressures are already high.

According to GSMA, mobile technology contributed approximately

NGN 33 trillion

(approx. USD 52 billion at 2023 exchange rates) to Nigeria's economy in 2023

Nigeria's mobile fintech boom drove stronger cyber governance, leading to the establishment of the Nigeria Data Protection Commission as the country's privacy watchdog

Latin America's digital footprint

Latin America has quietly become a more attractive option for companies trying to balance global outsourcing with closer collaboration. Colombia has been one of the countries benefiting from that shift, building a nearshore tech services sector supported by local talent and overlapping work schedules with North America.

The U.S. International Trade Administration (ITA) reports that internet use in Colombia rose from about 38% of the population in 2014 to roughly 63% by 2023. That expansion has supported growth in software development, customer support operations, and cloud management services aimed at international clients.

Guadalajara has been coined Mexico's Silicon Valley, with the city attracting a high concentration of major multinational tech firms and contributing to Mexico's 130,000 yearly software engineering graduates

Colombia has also developed robust privacy legislation compared with some regional peers. Law 1581, introduced in 2012, established national data protection requirements enforced by the Superintendence of Industry and Commerce (SIC). The government later expanded its cybersecurity strategy through initiatives such as its CONPES 3995 digital security policy, which focuses on improving cybersecurity awareness and strengthening institutional response capacity.

The region's cyberthreat landscape is expanding alongside its digital economy. Research from the World Bank suggests Latin America and the Caribbean have experienced one of the fastest increases in reported cyber incidents globally, with disclosures growing significantly over the past decade. Countries such as Brazil and Mexico are seeing similar patterns, as digital banking, cloud adoption, and international outsourcing continue to expand.

Brazil now operates under the LGPD privacy law, while Mexico has pushed ahead with digital modernization and closer cyber cooperation between the public and private sectors. The approaches vary, but across Latin America, the same tension keeps coming up: Technology is moving faster than the systems designed to secure it.

In Nigeria, mobile fintech has brought payment apps, wallets, and peer-to-peer transfers to millions outside traditional banking

Security maturity rarely grows evenly

One of the biggest misconceptions about emerging markets is that cybersecurity strength can be assessed on a country-by-country basis. In reality, cyber maturity often varies far more between individual companies than between national borders.

The International Telecommunication Union's Global Cybersecurity Index (GCI) groups countries into tiers based on cybersecurity commitment. India has been placed in the highest tier, reflecting strong national investment in cybersecurity programs. Other fast-growing economies, including Nigeria, fall into lower tiers, suggesting security frameworks are still developing or unevenly implemented across sectors.

For multinational organizations, those rankings offer useful context but rarely tell the full story. A contractor with strong security practices in a lower-ranked country may present less risk than a poorly managed vendor operating in a mature regulatory environment. Cybersecurity in global supply chains has shifted from geography to governance.

Collaboration is expanding faster than security assumptions

Companies are running global operations by default, and development, support, and infrastructure management are often handled by teams scattered across the globe. That level of interconnection has made organizations more flexible, but it has also influenced how security incidents unfold once attackers get access.

Many of today's major breaches begin with stolen credentials, social engineering, or compromised third-party vendors rather than direct attacks on corporate infrastructure. Supply chain compromise has become one of the most common entry points in large cyber incidents.

For companies operating across borders, the challenge is finding a workable middle ground between pulling back entirely and assuming everything will be fine

Organizations are responding by shifting away from security models built on network location or implicit trust. Instead, many are adopting Zero Trust approaches that continuously verify access, limit administrative privileges, and closely monitor software behavior regardless of where users are located.

One response companies are leaning toward is tightening control over what software can run and when administrative access is granted. Tools built around those ideas are becoming more common as organizations try to limit what attackers can do if they get inside a system. Companies such as ThreatLocker® offer capabilities that focus on application allowlisting and controlled privilege access, helping organizations contain damage from compromised devices or stolen credentials.

A collective responsibility in a shared digital economy

It is getting harder to talk about the global tech industry as something centered in just a handful of countries. India underpins much of the world's software and IT services industry. Nigeria's fintech sector is changing how people access financial services at scale. And across Latin America, companies are spreading development and operations work more widely than before. Together, those shifts are reshaping how global tech actually functions.

Cybersecurity is evolving alongside that transformation, though not always at the same pace. For companies operating across borders, the challenge is finding a workable middle ground between pulling back entirely and assuming everything will be fine. The organizations seeing the most success are the ones designing partnerships around strong security controls from the start, assuming compromise is possible and planning accordingly.

The expansion of emerging digital markets is one of the defining business stories of the decade. It is also quietly reshaping how cybersecurity works across industries, continents, and supply chains. Companies that understand both sides of that shift are likely to find that opportunity and security need not compete.

↓ In Brazil, rapid digital expansion in banking and cloud adoption has coincided with rising cyber incidents, prompting enforcement under the LGPD

↗ India's 2023 DPDP Act set national standards for consent, data processing, and breach reporting to strengthen trust as its digital economy grows

THE SIX-PILLAR **STRATEGIC ADVANTAGE**

The White House's latest Cyber Strategy for America positions the federal government in an active fight against cyberthreats—and its goals bring security teams across the world along for the ride

The six pillars of the White House's 2026 Cyber Strategy reinforce principles that security professionals have advocated for years: Be proactive, adopt least-privilege and Zero Trust models, manage the supply chain, invest in people, and ensure that security is built in from the ground up.

1 PILLAR ONE: SHAPE ADVERSARY BEHAVIOR

The first pillar hinges on disrupting threats before they cause damage, using both offensive and defensive operations to raise the cost for bad actors to attack in the first place. It is equal parts provocative and proactive, calling for an erosion of adversary capabilities, a dismantling of criminal infrastructure, and consequences for those who attack American networks.

The obvious take for security professionals is that there is no sense in waiting for a breach to happen. Security cannot be managed reactively; by that point, teams are more realistically dealing with the fallout. Using tools such as threat intelligence feeds, dark web monitoring, and vulnerability assessments, security teams can build the foresight to act before an attacker does. And by building Zero Trust–driven defenses, they can be proactively prepared for breaches and minimize their impact.

2 PILLAR TWO: PROMOTE COMMON SENSE REGULATION

Here, the White House pushes back against bloated compliance frameworks which it suggests slow down the speed of defense without making businesses meaningfully safer. This pillar posits that regulations should be streamlined and that privacy protections for individuals and their data should be emphasized.

On the ground, this is a nudge to review compliance obligations critically to determine whether controls are reducing risk or simply satisfying an audit requirement. Security teams need to look for value in their tools outside of the checkbox being ticked. It could be argued that prioritizing the implementation of methods like application allowlisting and least-privilege access provides a far greater short-term return on time investment than spending energy on more paperwork.

3 PILLAR THREE: MODERNIZE AND SECURE FEDERAL GOVERNMENT NETWORKS

This strategy calls for accelerated adoption of modernized cybersecurity tools and attitudes across federal systems—everything from Zero Trust architecture to post-quantum cryptography. It also pushes for cyber leadership to be elevated within government frameworks.

Realistically, this pillar mirrors what is already happening across the forward-thinking corners of the private-sector IT world. Those who have acknowledged the importance of cybersecurity, given IT leaders their due, pushed for the implementation of the Zero Trust model, and implemented advanced endpoint detection and response (EDR) tools are those setting the baseline for cybersecurity expectations. If this does not reflect your team's outlook, it is time to become aligned.

4 PILLAR FOUR: SECURE CRITICAL INFRASTRUCTURE

Our understanding of what constitutes critical infrastructure has grown, and this pillar urges that essential systems across the sector—from energy grids to water utilities, to financial networks and data centers—be hardened against attack. It also highlights the dual importance and vulnerability of the supply chain, calling for a move away from adversary-controlled vendors and products.

Even if your organization is not what the federal government would deem "critical," this is a philosophy that should not be ignored. Supply chain risk applies to every organization, not just government. Every third-party application, managed service provider (MSP), and software-as-a-service (SaaS) tool could act as an entry point for attackers, so all vendor relationships and access rules should be regularly audited to weed out potential compromise.

5 PILLAR FIVE: SUSTAIN SUPERIORITY IN CRITICAL AND EMERGING TECHNOLOGIES

Here, the White House addresses the ongoing technology race and the security concerns that come along with the growing worldwide competition to lead in fields such as AI, quantum computing, and blockchain. The key here is the recommendation that all new technologies be built with security in mind, rather than treating security as a separate layer to be bolted on afterwards.

This is a reminder that the threat landscape is evolving, often faster than some security tools and techniques. With attackers employing AI to speed up reconnaissance, craft increasingly targeted phishing attacks, and identify vulnerabilities, defenses need to keep pace for businesses of every size. Security is not a trend, it is the core of every advancement. Without it, systems can crumble.

6 PILLAR SIX: BUILD TALENT AND CAPACITY

The final pillar acknowledges the importance of the cyber workforce as a strategic national asset. It emphasizes the need for training and talent pipelines that stretch across academia, vocational training, and industry. It also calls for removing barriers that might prevent skilled professionals from entering the profession.

The IT sector has certainly felt the sting of the talent shortage, but IT leaders should also be investing all they can in training existing staff at all levels. Certifications and simulations to bring IT staff up to speed, and cross-functional awareness programs to cement the need for security in the rank and file are essentials for uniting the entire business as a security team.

THREATLOCKER® TIP

If you represent a government entity or are a government contractor in the U.S., access this page to learn more about how ThreatLocker helps you align with the 2026 Cyber Strategy for America

BUILDING TRUST IN A DIGITAL FUTURE

Estonian Ambassador-at-Large for Cyber Diplomacy Helen Popp talks about Estonia's cybersecurity leadership and the vital steps required to build trust and citizen buy-in

Estonia has become the benchmark for digital governance—a small European nation that deliberately transformed itself into one of the world's most advanced digital societies. During the 2023 Estonian parliamentary election, when 51.1% of voters cast their ballots online[‡], the shift was unmistakable: Digital voting had crossed into the mainstream of democratic practice. This milestone was no accident, but the result of years of careful sequencing—building digital services step by step until they became both trusted and routine.

Helen Popp, Estonia's Ambassador-at-Large for Cyber Diplomacy, explains the foundation, "The key was to provide citizens with services that met their real needs." She points to e-tax filing, launched in 2002, which enabled taxpayers to submit income tax returns online for the first time.

Then followed digital prescriptions, "Doctors issue prescriptions electronically, allowing patients to collect their medication from any pharmacy in the country simply by identifying themselves with their ID card."

Before asking citizens to engage in something as politically sensitive as online voting, the government had to prove it could deliver secure digital services at scale. "By the time online voting was introduced, there had already been hundreds of millions of secure online banking transactions, with no losses due to system failure. This helped build public trust," Popp said.

"Internet voting initially attracted about 10% of voters," she explained, suggesting it reached 51.1% by 2023 because the government demonstrated transparency and auditability at each stage. "The government first led with services that were transparent and auditable. Once trust was established in these systems, it became easier for citizens to accept that online voting would also be secure and auditable."

Popp says public-private cooperation proved equally essential to Estonia's digital journey. She notes: "From the beginning, digital development has not been solely a government initiative. Public–private partnership has been a national priority and continues to evolve alongside technological progress." For Estonia, digital development was never purely a government effort. Banks, healthcare providers, and software companies worked alongside public agencies to build secure services in tandem.

When crisis forced strategy

Cyberattacks rarely occur in isolation; they are often the digital expression of broader geopolitical tensions. A 2007 series of cyberattacks[‡] on Estonia's critical infrastructure shifted how the government understood cyberthreats. "While those 2007 attacks were not the feared 'cyber–Pearl Harbor' by any stretch, it could no longer be argued that cyberwarfare was not a foreign policy issue and didn't need a strategy," Popp reflected.

Preparedness was not improvised in the wake of crisis—it had already been built into the system. "Prior to the 2007 attacks, Estonian intelligence had alerted the government to the risk of cyber operations in the context of online voting," explained Popp, emphasizing the strategic advantage this foresight created. "This early warning cultivated both mental and institutional readiness, sparing critical time that might otherwise have been lost challenging entrenched assumptions about cyberwarfare."

Popp frames the attacks not as purely damaging events, but as catalysts for institutional reform. "Estonia released its first Cyber Security Strategy (May 2008) that became the guiding document for the state's comprehensive cyber policy, including creating the Cyber Security Council under the government."

That same year, NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) opened in Tallinn. "In 2003, even before Estonia joined NATO, Estonia recommended the creation of a new center of excellence for telecommunications security within the NATO framework. Despite general support from NATO leadership, the idea did not gain momentum until after the 2007 attacks, when it received significant support."

Estonia expanded its expertise network with the creation of the Cyber Defense League in 2010. "The league is made up of IT specialists who volunteer to assist the Estonian military during a time of crisis." Popp suggests that the attacks ultimately brought alignment to Estonia's cyber strategy. "Out of the 2007 attacks emerged a sense of unity, a sense that all elements of the government infrastructure—working together—were necessary to combat the cyberthreat."

The democratic equation

When nearly all government services exist online, cybersecurity becomes inseparable from democratic legitimacy. "When systems are secure, democracy feels reliable and legitimate. When they are not, trust erodes quickly," Popp stated. Citizens vote online, pay taxes online, and access health records online. If those systems fail or are compromised, confidence in government institutions quickly declines.

Building that trust, says Popp, requires more than technical measures. "Resilience does not happen by chance. It is shaped by how deliberately we manage risks and sustain trust at every level, from states and organizations to individual citizens." She suggests that protection means "close cooperation between governments, intelligence agencies, and the private sector. It is critical to clarify shared priorities, strengthen attribution, and make deterrence meaningful in practice."

> "By the time online voting was introduced, there had already been hundreds of millions of secure online banking transactions, with no losses due to system failure. This helped build public trust

Building systems for failure

Estonia designed its digital state to assume disruption. "The strength of Estonia's digital state lies not only in smart services," stated Popp, "but in their quiet reliability, even when cyberspace is turbulent and technology unpredictable. This invisible continuity is a pillar of modern society. The international community must avoid repeating the mistakes made during the rapid adoption of earlier digital technologies, where security was often treated as an afterthought."

"For governments, this includes establishing strong procurement and security protocols to ensure AI systems are securely designed, developed, deployed, and used, especially when handling sensitive or classified data. By supporting research, training, and commercialization—particularly for startups and subject matter experts developing cutting-edge AI and cybersecurity solutions—governments can also use security as a lever for economic growth."

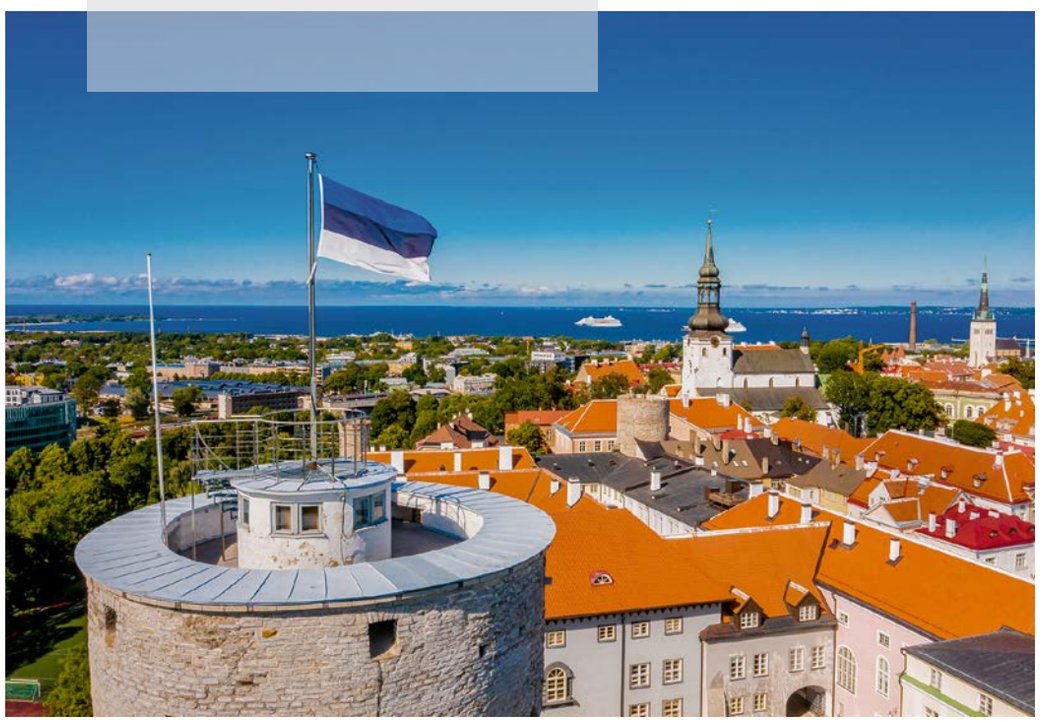
AI and blockchain

Autonomous AI systems also raise new diplomatic questions that current international frameworks do not address. Popp is direct: "Governments should set clear expectations for acceptable AI use in national security, grounded in the UN Charter, international humanitarian law, and international human rights law. Increased international coordination will be needed to enforce existing norms and develop new ones that reflect the capabilities and risks of AI, especially as autonomous, agentic systems advance."

On blockchain, Popp distinguishes between two distinct security problems that are often conflated in policy. "Blockchain plays a crucial role in strengthening data integrity, which is a foundational element of security in a digital state. While cybersecurity often focuses on preventing unauthorized access, blockchain technology primarily addresses a different but equally critical issue: preventing unauthorized alteration of data."

"In a fully digital society," continued Popp, "essential state functions such as healthcare records, property registries, legal statutes, and court decisions exist primarily in electronic form. If someone merely views sensitive data, that is a privacy breach. However, if someone alters medical information, property ownership records, or legal precedents, the consequences can be far more severe."

> "When systems are secure, democracy feels reliable and legitimate. When they are not, trust erodes quickly



Estonia moved from the 2007 crisis to 51.1% online voting by building trust methodically and testing each new service before expanding it

She explains how blockchain offers Estonia verifiability. "Blockchain, particularly in the form of a permissioned or private blockchain used by public institutions, enhances security by making data tampering evident. Records are cryptographically linked and distributed across multiple authorized nodes. Any attempt to modify data retroactively would be immediately detectable because it would break the cryptographic chain and fail integrity verification checks."

The distributed architecture increases resilience. "Because data is replicated and continuously verified, it is far more difficult for a single point of failure—whether caused by cyberattack, technical malfunction, or even physical disruption—to compromise the system. Its real value in the public sector lies in ensuring that critical state data remains accurate, verifiable, and trustworthy."

The path forward

"To build a digital future that earns and sustains citizens' trust, international cooperation should be guided by several core principles," reinforced Popp. "This starts with protection of fundamental rights and security and resilience by design, but must also include transparency, accountability, public-private partnership, inclusiveness, and digital equity."

> From the beginning, digital development has not been solely a government initiative. Public–private partnership has been a national priority and continues to evolve alongside technological progress

Estonia moved from the 2007 crisis to 51.1% online voting by building trust methodically and testing each new service before expanding it. The government demonstrated its resilience and created citizen buy-in by showing, not telling. Estonia's approach mirrors core Zero Trust principles: Assume no implicit trust, continuously validate identity, and enforce minimum access. Democratic legitimacy depends on digital infrastructure; that discipline may be the difference between systems that function and systems citizens believe in.

CYBER-CONSCIOUS ESTONIA

The Cyber-conscious Estonia strategy embeds Zero Trust-aligned principles across national electronic services by shifting security from perimeter-based trust to modern, risk-informed, and continuously validated controls.[‡]

1. Secure basic architecture and modern security principles
The strategy mandates adoption of secure architectural frameworks and "modern security principles," moving away from monolithic, legacy trust assumptions toward modular, continuously assessed controls

2. Minimum requirements for information security and IT services
By setting minimum organization and technical requirements for all digital services, Estonia enforces least-privilege and consistent verification of service components

3. Transition from vulnerable legacy systems
A clear strategic goal is to phase out highly vulnerable legacy software that implicitly trusts internal networks, replacing it with systems designed for dynamic trust evaluation

4. Risk-based national cybersecurity architecture analysis by 2027
The strategy calls for a comprehensive analysis of the national cyber architecture to prioritize risk controls and continuous monitoring across public services—a core Zero Trust tenet

COMPLIANCE **MEETS** INTERDEPENDENCE

As cyber incidents ripple across supply chains and critical services, the U.K.'s Cyber Security and Resilience (Network and Information Systems) Bill aims to strengthen oversight and accountability

The U.K. Bill tightens cybersecurity standards and regulators' powers to reduce attacks and limit breach impacts

The increase in the volume and severity of cyberattacks in both the public and private sectors in recent years is clear, and the U.K.'s latest cyber legislation reflects this.

The documentation and debates that have accompanied the Cyber Security and Resilience (Network and Information Systems) Bill during its journey through parliamentary proceedings cite recent, well-publicized attacks on household names, such as Marks & Spencer and Jaguar Land Rover. Most strikingly, they discuss the constant challenges faced by the country's National Health Service (NHS), which is a high-profile target for cybercriminals. At least one patient death was directly linked to logistics issues in the wake of a 2024 ransomware attack.[‡]

U.K. government statistics suggest that more than 40% of local businesses experienced a cyberattack in 2025, with 204 "nationally significant" incidents.[‡] Almost all of the U.K.'s critical national infrastructure organizations experienced some form of data breach in 2024, a quarter of which only found out after the attacker notified them.[‡]

The U.K. Bill, which is entering its final stages before passing into law, aims to reduce the number of successful attacks and mitigate the impact of future breaches, by updating cybersecurity standards and expanding the remit of regulators. It amends the existing Network and Information Systems (NIS) Regulations, which were published in 2018.

U.K. government statistics suggest that over

40%

of local businesses experienced a cyberattack in 2025

THE THREE PILLARS OF CHANGE

1. Expansion of scope

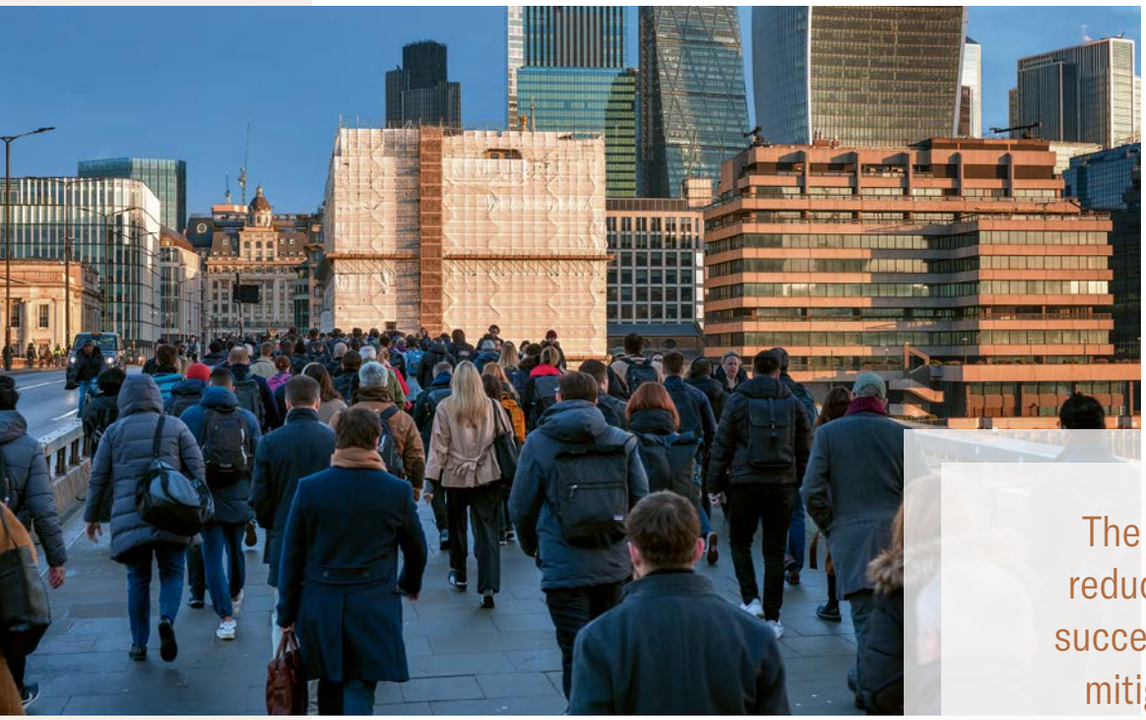
Under the revised regulations, data centers and managed service providers (MSPs) will be recognized as vital to the U.K.'s economy and national security. This move recognizes the vulnerability of critical services such as the NHS to supply chain attacks. In addition, sector regulators may designate individual businesses as critical suppliers that must comply. The U.K. Bill also extends coverage of the energy sector to include newer power management controllers for charging electric vehicles and the like.

2. Effective regulation

Recognizing that regulators face capacity challenges and relatively low compliance with incident-reporting requirements, the updated NIS provides a framework for data sharing between regulators and allows them to recover costs through fines. Requirements for incident reporting are also being changed to ensure regulators are made aware of breaches more quickly.

3. Enabling resilience

The final pillar relates to futureproofing the legislation, enabling quicker updates and allowing the government to provide direction to regulators. While this does not directly impact businesses, it does mean that choosing a partner who can keep you informed about future changes is vital.



In 2025, fewer than one in three U.K. businesses had effective breach-monitoring tools or had conducted a thorough risk assessment

The U.K. Bill aims to reduce the number of successful attacks and mitigate the impact of future breaches by updating cybersecurity standards and expanding the remit of regulators

The NIS Regulations were introduced as part of the Brexit process to bring U.K. law in line with the then-current EU directives governing security in critical infrastructure. NIS coordinates the work of 12 regulatory bodies in five operational areas, namely energy, transport, health, drinking water, and digital infrastructure, with some limited powers over other digital services as well.

Under the existing NIS, a maximum fine of USD 17 million can be imposed on organizations found to be non-compliant with their security stance or their duty to inform the relevant regulator of a reportable incident.

Time for reform

The current government's Strategic Defence Review (SDR), published last year, highlighted areas where the NIS needed to be updated to match the increasing complexity of modern cybersecurity challenges. As the SDR pointed out, the EU has since updated its own regulations with the NIS 2 directive, published in 2022, as have other countries such as Australia.

There are three key "pillars of reform" that underpin the U.K. Bill: expansion of scope, effective regulation, and enabling resilience. For most organizations, the first two will require the most attention to determine whether the new NIS applies.

The expanded scope brings thousands more businesses into the compliance regime. For a start, the updated NIS identifies data centers and managed service providers (MSPs) as essential services, with the same compliance requirements as healthcare, energy and water providers to protect data and report incidents.

The legislation does not cover MSPs with fewer than 50 employees by default, but they may be designated a critical service provider based on their role in the supply chain and be obliged to be compliant. An IT supplier working with an NHS trust, for example, would be subject to the regulations regardless of its size.

To make regulators more effective, the amended NIS will allow for larger fines for non-compliance, allow regulators to cover costs, and require companies to have improved risk management and reporting structures. It also broadens the scope of reportable incidents to include those that affect operational activities and clarifies the 24-hour window for initial reporting.

THREATLOCKER® TIP

THREATLOCKER APPROPRIATE AND PROPORTIONAL DEFENSE

The U.K. Bill deliberately avoids prescribing specific technologies, instead calling for "appropriate and proportional" controls that reduce the likelihood and impact of incidents. A Zero Trust endpoint strategy can help organizations demonstrate this in practice.

Allowlisting ensures only approved applications and scripts can execute, reducing exposure to ransomware, living-off-the-land (LOTL) activity, and unauthorized tooling often seen in supply-chain breaches.

Ringfencing™ then limits how trusted applications interact with data, backups, and system resources, helping contain attacks and prevent lateral movement if an endpoint is compromised.

ThreatLocker EDR provides real-time visibility into unusual behavior and attempted policy violations, supporting faster investigation and reporting within tightening regulatory timelines.

Together, these capabilities help organizations move beyond reactive security towards measurable resilience aligned with emerging NIS expectations.

How to get ready for the new rules

Organizations looking to parse the U.K. Bill for specific ways to be compliant and avoid fines will not find all the details they need. While the new reporting structures, staff designations, and regulatory responsibilities are made clear, the language around what constitutes a reportable incident and the adequate protections that must be in place is deliberately vague and will be left to sector regulators to define in secondary legislation. They describe "appropriate and proportional measures to prevent and minimize the impact of an incident," which must take into account state-of-the-art in security practices and risk-appropriate implementation.

For organizations looking to bring their cybersecurity operations into compliance, the National Cyber Security Centre (NCSC) already publishes a set of guidelines called "10 Steps to Cybersecurity," which should be carefully noted alongside international standards such as ISO 27001 and the EU's NIS 2 regulations. The 10 steps include sound best practices, such as implementing Zero Trust security, ensuring adequate network control, and reducing the impact of compromise by isolating applications. These are security principles that products such as **Ringfencing** are designed to implement.

The scale of the compliance challenge should not be underestimated. In its Cyber Security Breaches Survey (CSBS), published last year, the U.K. government found that fewer than one in three businesses had implemented effective tools for breach monitoring or had carried out a thorough risk assessment. The percentage of businesses with a robust internal architecture designed to mitigate the impact of attacks fell compared to the year before.[‡] The U.K. Bill is the top-down part of improving cybersecurity across the board, but it is still down to individual businesses to be responsible and take action today.

The U.K. National Cyber Security Centre provides guidance, threat intelligence, and incident response to protect Britain's digital infrastructure

SECURITY **AT EVERY SCALE**

Mass indiscriminate attacks are leaving businesses and organizations of all sizes at greater risk of being compromised

In 2025, the exploitation of vulnerabilities rose

34%

to account for 20% of all breaches

Not all cyberattacks are carefully targeted. Indiscriminate attacks on a huge scale are nothing new—just ask anyone who has been a victim of a distributed denial-of-service (DDoS) attack driven by hundreds of thousands of infected devices—they are on the rise. It has never been easier for even relatively inexperienced hackers to wreak havoc.

The increasing availability of automated tools, including semi-autonomous AI agents[‡], means that the hard work of finding and attacking vulnerable networks has never been so easy. That is bad news for any business. It could be particularly troubling for smaller organizations that can ill afford to find themselves on the wrong end of a major outage or, worse, an attack that leaves them in breach of regulatory obligations and subject to massive fines.

Anyone and everyone is effectively a target. That makes it vitally important that every business brings its cybersecurity policy up to scratch and ensures that everyone within the organization is educated in good security practices.

Identifying attack vectors

Mass-scale attacks come in all shapes and sizes, and most of the techniques are familiar to those who have been subjected to targeted attacks. They include attempts to penetrate networks using stolen credentials or session tokens captured from previous breaches. Many are scattershot, using indiscriminate phishing attacks aided by dedicated phishing-as-a-service (PhaaS) and malvertising platforms.

Widespread DDoS attacks using botnets are also carried out indiscriminately, but mass-exploitation attacks are a dangerous and growing threat. In 2025, the exploitation of vulnerabilities rose 34% to account for 20% of all breaches.[‡] Automated tools allow even relatively inexperienced hackers to scan the entire internet looking for networks with exploitable vulnerabilities, making this type of attack increasingly popular.

Vulnerability, in this case, does not simply refer to unpatched software and platforms; hackers can also scan for zero-day exploits. They have access to the same inventory tools, such as Shodan and Censys, that report newly discovered vulnerabilities to security professionals. Exposure means the possibility of attacks ranging from data theft and ransomware demands to service disruptions that can wreak havoc on a wider scale if other organizations rely on those services for their own operations.

The problem is exacerbated by the growing number of devices connecting to organizational networks. On-premises Internet of Things (IoT) and edge devices introduce potentially unknown, unmonitored vulnerabilities. Off-premises devices used in remote environments can remove the direct control of security. The number of potential entry points has exploded; in 2025, the percentage of breaches involving a third party doubled from 15% to 30%.[‡]

The fast growth of AI has made things even more complicated. Hackers are using AI to educate themselves and to gain easy access to automated tools—and they are increasingly deploying AI to execute attacks on their behalf.[‡] This expansion makes it increasingly difficult to manage cybersecurity policies manually.

Thankfully, businesses do not need to be large-scale enterprises to apply strong cybersecurity protection. Implementation of Zero Trust principles is a size-agnostic practice, and Zero Trust controls are applicable to every organization at every scale. For those who need a little more help, managed service providers (MSPs) often offer additional security support to lighten the load on smaller security teams.

Small business, big protection

Even the smallest business must ensure that its cybersecurity solution can meet these challenges head-on. The first layer of protection against mass-exploit attacks is to ensure systems are fully and promptly patched to protect them against attacks based on known vulnerabilities. A tool like **ThreatLocker® Patch Management** reports on out-of-date applications and automatically updates them, backed up by a comprehensive database of application information.

MOVEit TRANSFER BREACH

DATE: May 2023
ATTACK TYPE: mass-exploit attack
EFFECTS: Impacted over 2,500 organizations and 93 million individuals[‡], including multiple U.S. government organizations and companies worldwide.

This breach in transfer software, first reported on May 31, occurred when Progress Software published an advisory on a critical SQL injection vulnerability in its MOVEit Transfer product. This affected organizations worldwide and resulted in advisories from CISA and the U.K.'s National Cyber Security Centre (NCSC).

On June 6, a day after the first companies disclosed breaches, the Russian-affiliated Clop ransomware group posted a video claiming responsibility and outlining its demands. Multiple vulnerabilities in the software were subsequently discovered, but research indicates organizations were swift to apply patches.[‡]

SALT TYPHOON TELECOM ATTACK

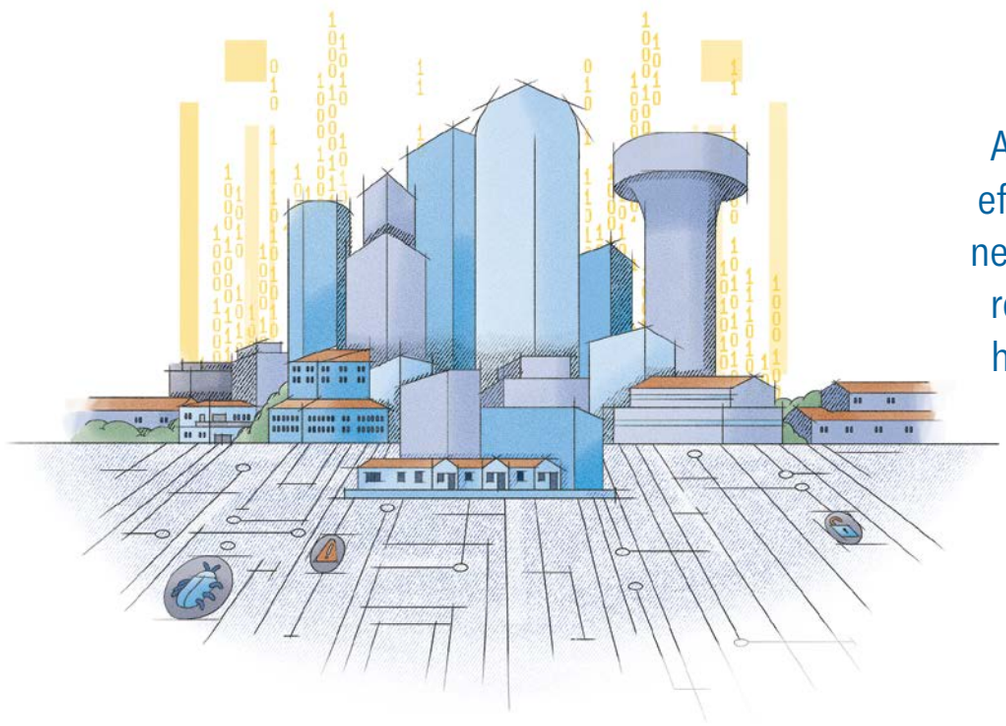
DATE: August 2024
ATTACK TYPE: Zero-day network compromise
EFFECTS: Believed to be linked with China, APT actor Salt Typhoon struck at least two major internet service provider (ISPs), nine telecommunications firms, and over a dozen countries with a widespread attack against a zero-day vulnerability in Versa Networks' Director virtualization platform.[‡]

Though much of the attack was focused on the Washington, D.C. area—allowing Salt Typhoon to obtain records of prominent politicians as well as extensive lists of U.S. wiretaps—the group's network compromise allowed it immediate access to over 100,000 routers at AT&T alone.

The attack yielded extensive metadata on calls and messages, and is understood to have extracted the phone numbers of over one million users. The U.S. Cyber Safety Review Board investigated the attack, though this was later disbanded along with other DHS advisory boards.

You should also restrict outside access to your network by closing unnecessary ports. In an ideal world, all ports would be closed except when explicitly needed, which is where tools like **Zero Trust Network Access (ZTNA)** and **Zero Trust Endpoint Firewall** come into play. They give you granular control over who or what has access to your network, and when. By keeping network ports closed except when needed, your network is far less visible to speculative internet scanning tools looking for easy entry points to target.

Robust modern security hinges on the deny-by-default methodology of Zero Trust. Instead of building a denylist of prohibited programs, a cybersecurity solution like **Allowlisting** does the opposite: It blocks everything except explicitly approved software, scripts, and libraries. This should halt most mass attacks in their tracks. If an attacker spots a vulnerability, any payload they attempt to run should be blocked by default.



Anyone and everyone is effectively a target. It has never been easier for even relatively inexperienced hackers to wreak havoc

ThreatLocker supports a deny-by-default model while minimizing disruptions to keep operations smooth and secure. If your MSP offers a tool like **Allowlisting**, which provides a smart Learning Mode to help you quickly build your list of approved applications, this can help streamline setup while minimizing impact on your business.

Your cybersecurity solution should also give you granular control over what even permitted services can do. A solution like **Ringfencing™** gives you the tools to define policies that place additional safeguards on those services you have allowed, for example, by limiting their access to your organization's data and the internet to restrict the reach of any malware that might sneak through.

Further restrictions worth seeking from your security team include some form of privilege control. **Privileged Access Management** enables you to revoke local administrator rights from your users while granting certain applications limited elevated access strictly in accordance with your organization's security policies. Doing so can help limit the effects if malware or a hacker somehow evades other defenses—for example, by physically gaining access to a device—to penetrate your network.

Take further steps

Even with the strongest cybersecurity in place, businesses should still take additional steps to defend against mass attacks. Do not overlook partnerships and the use of third-party services, such as cloud providers and contractors. The Cybersecurity and Infrastructure Security Agency (CISA) offers useful advice on how to ensure any outsourced data or services are kept secure.[‡]

Regularly audit IoT and edge devices to ensure they remain patched, plus identify those that have reached end of life and require replacement.[‡] Review how remote devices connect to your network—are they devices you control, such as work-issued phones and laptops, or are you relying on employees and contractors to supply their own equipment? Ensure their network access is tightly controlled so if they are compromised in a mass attack, they cannot be used remotely to launch a direct attack into your system.

Also, train your employees in cybersecurity essentials, from good practices to how to spot (and report) potential phishing and malvertising attacks, as well as possible signs of a breach in progress. And if you do find yourself under attack, do not forget to alert the authorities; you can report incidents to CISA at *myservices.cisa.gov/irf*.

THREATLOCKER TIP

Learn more about how ThreatLocker Zero Trust protects you against modern attack vectors:

RACCOONO365 MICROSOFT ACCOUNT ATTACK

DATE: February 2025
ATTACK TYPE: PhaaS
EFFECTS: A Nigerian service was used to steal over 5,000 Microsoft user credentials across 340 sites before it was seized in September 2025.[‡]

In February 2025, a tax-themed phishing campaign targeted over 2,300 organizations. Subsequent research revealed that a Nigerian-based service, RaccoonO365, operating through a Telegram channel, provided over 850 subscribers with the tools to impersonate trusted brands and get targets to enter Microsoft login credentials on fake web pages. Before it was taken down in September, the scam was estimated to have secured USD 100,000 in crypto payments for its users.

BADIIS GLOBAL SEO POISONING

DATE: October–November 2025
ATTACK TYPE: drive-by compromise at scale
EFFECTS: Over 1,800 Windows IIS web servers were compromised, including government, enterprise, and educational infrastructure across several countries. Their trusted domains were used to poison search results and redirect users to illicit content, including gambling and fraud websites.

A Chinese-speaking cybercrime group launched a two-phase campaign.[‡] Phase one used a malicious IIS module to serve keyword-stuffed content to search engine crawlers to manipulate rankings. The second phase saw the compromised IIS servers redirect users to unauthorized adverts and gambling sites. Infrastructure in Canada, India, and several other territories was targeted.

MAN VERSUS MACHINE

Finding a balance between human judgment and predictive analytics amidst the growing pace and volume of cyberattacks

Cybersecurity often feels like a green or red light scenario. An environment is secure, or it is not. An actor sits on one side of the fence or the other. But security is a complex field shaped by variables and nuance, and definitive lines rarely reflect reality. It is possible for more than one thing to be true at the same time.

An increasingly common argument revolves around the idea that organizations must rely either on human judgment or predictive intelligence. This stems from a lack of full context: In practice, neither approach works on its own. Security fails when people are expected to compensate for missing data, and when systems operate without human oversight.

Predictive intelligence and human decision-making must be deliberately designed to support each other, with each addressing weaknesses the other cannot avoid

Predictive intelligence must be designed to support human decision-making and vice versa, as each can address the weaknesses the other cannot avoid. Effective security will depend on it.

Why human judgment still matters

Security decisions affect people, operations, and entire businesses. Blocking an application, isolating a system, or interrupting a workflow has consequences that extend beyond the technical domain. Only humans can properly weigh those consequences.

Experienced security professionals bring real-world context that systems do not possess. They understand how their organization operates, rather than how it appears to work on paper. They know which exceptions exist and why they are in place. They understand normal behaviors for particular teams, and where rigid enforcement would create more risk than it removes.

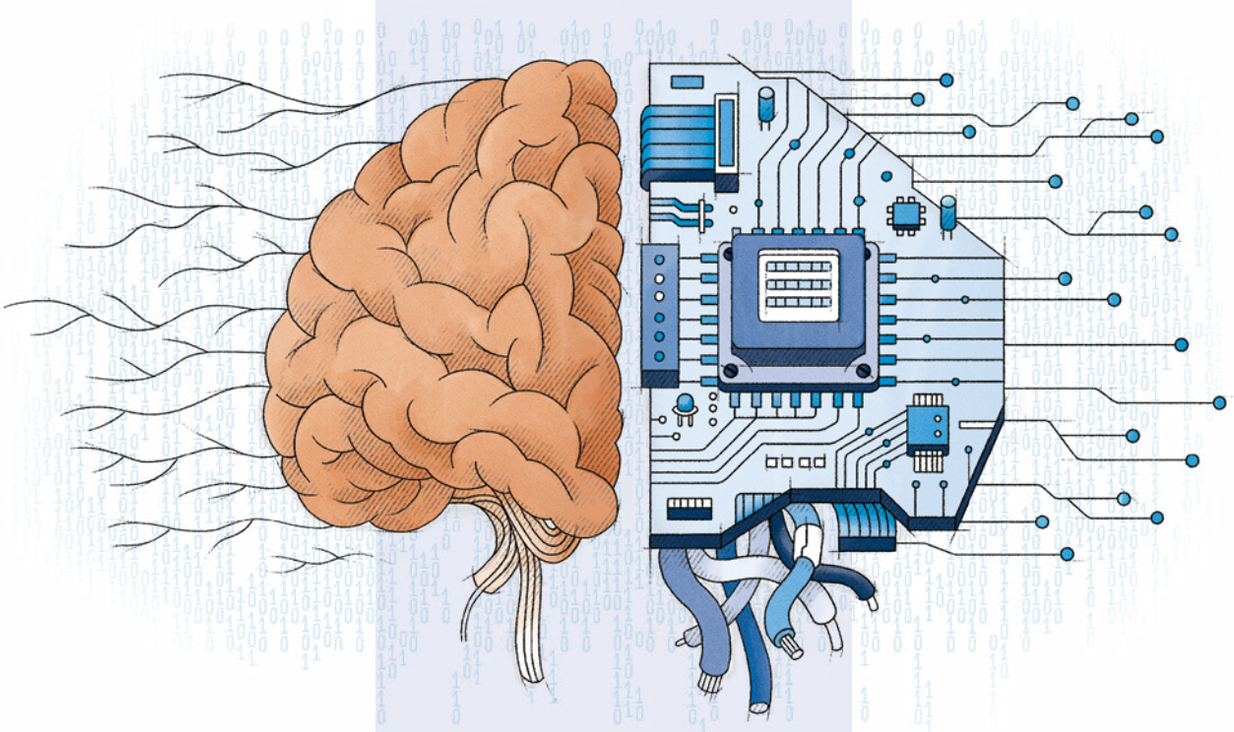
82%

are concerned they are missing real threats because of the sheer volume of alerts and data[‡]

Policy management is the bedrock of Zero Trust, but security cannot be reduced to rules alone. Governance, accountability, and trust all depend on human involvement. The problem is that judgment based solely on experience, while essential, does not scale in modern environments.

The limits of intuition in a digital environment

The pace and scale of cybersecurity have grown beyond what human intuition can handle. Some environments now produce more events in an hour than a person could reasonably assess in a week. Decision-makers are stretched, their attention fragmented across endpoints, identities, applications, and cloud services, often with limited visibility into how these pieces interact under the hood.



Security personnel face an impossible position. They are asked to detect subtle signals within constant background noise, make rapid decisions with incomplete information, and maintain consistent standards under sustained pressure. This predictably exposes weaknesses. Teams become desensitized to alerts, and unusual behavior is dismissed because it resembles past false positives. The nature of risk changes when it is judged on recent events rather than on what is structurally possible.

Attackers can use security overload to their advantage. To an adversary, an unmanageable volume of data is a resource to be exploited. In essence, they can target the weakest link in the chain. Instead of waiting for careless behavior or hoping for incompetence, they only need to take advantage of human limitations.

This problem is well-documented. The U.K.'s National Cyber Security Centre (NCSC) has noted that security teams are frequently overwhelmed by the volume of data and alerts they must handle. It suggests that the pace is very unlikely to slow: "A growing divide will emerge between organizations that can keep pace with AI-enabled threats and those that fall behind, exposing them to greater risk and intensifying the overall threat."[‡]

Why predictive intelligence matters

Many security processes are still built around reaction: something runs, connects or executes, triggering an alert, and the incident is then investigated. By the time a decision is made, the action has already occurred. This approach assumes that humans can keep pace with activity unfolding at machine speed, and that every meaningful threat announces itself clearly enough to trigger a response.

Modern attacks do not behave this way. Some are slow, quiet, and designed to blend into normal activity. They rely on legitimate tools, existing permissions, and small changes that appear harmless when viewed in isolation. Some are rapid and overwhelming, moving beyond viable levels of human care and attention, and often overcoming perimeter defenses.

72%

describe their approach to cybersecurity threats as mostly reactive[‡]

Predictive intelligence addresses this by reducing uncertainty. At its most effective, it focuses on structure rather than speculation. It defines expected behavior, permitted execution, and valid access paths, then identifies situations where those expectations are violated, regardless of whether a known threat is present. Under Zero Trust, every action is treated with the same level of concern, legitimate or not.

There are categories of risk that humans cannot track unaided: rare permission combinations that only become dangerous across multiple systems, or configuration issues that remain dormant until specific conditions are met. These problems do not resemble past incidents and do not trigger intuitive responses. They only emerge when behavior is analyzed consistently across time and scale.

Systems are well-suited to this work. They maintain focus without fatigue, understand edge cases without relying on memory, and evaluate every event against defined expectations. But predictive intelligence without human involvement creates its own problems. Automated enforcement applied without context

Security has never been truly binary—the line between safe and compromised is not a wall, but a series of decisions made on both sides of it

can interrupt critical operations. Heavy-handed automation damages confidence in security teams and encourages unsafe workarounds.

Making this work in practice

For security leaders, the question is not whether to choose humans or systems, but how to design their collaboration effectively. This requires deliberate choices about where each adds value.

Start by **mapping decision points** in security processes. Identify where judgment calls are currently made, by whom, and under what time pressure. Look for patterns: Are analysts making the same low-context decisions repeatedly? Are critical choices being rushed because data arrives too late? These are friction points where the balance between human and machine input needs adjustment.

Make human judgment matter. Employ controls that surface intelligence early; if predictive systems identify risky behavior only after it has executed, they add to cognitive load. The goal is to shift decisions upstream, where context can be applied before actions become incidents.

Make policies explicit and reviewable. When controls are opaque, trust erodes. Security teams need to understand why a system flagged something, and business stakeholders need to understand why a decision was made. This transparency is what makes human oversight possible at scale.

Create feedback loops between enforcement and outcomes. When an exception is granted or a policy adjusted, capture the reasoning and the result. This builds institutional knowledge that refines both human judgment and system logic over time. Without this, organizations repeat the same mistakes under different circumstances.

Invest in clarity. The most sophisticated predictive system is worthless if the people using it cannot interpret its output or act on it effectively. Train teams to understand what the systems are telling them and why it matters. Equally, ensure systems are designed to communicate in ways that support decision-making rather than simply generating alerts.

Do not automate everything. Automation has a place, particularly for low-risk, high-frequency decisions where speed matters and context is stable. But critical security decisions—those with operational impact or unclear risk profiles—should remain human-controlled, supported by predictive intelligence that provides clarity rather than replacing judgment.

THREATLOCKER® TIP

PREDICTIVE INTELLIGENCE WITH HUMAN CONTROL

The ThreatLocker approach to predictive intelligence is built around behavior, policy, and oversight. The aim is to surface meaningful risk early and give teams the context they need to act.

This starts with **ThreatLocker EDR**, built on deny-by-default policy controls that monitor endpoint activity and execution behavior, highlighting deviations from expected patterns and known indicators of compromise. Instead of relying on volume-based alerting, EDR focuses attention on activity that matters, reducing noise and shortening investigation time.

With **Managed Detection and Response (MDR)**, powerful predictive intelligence is mixed with experienced human intelligence. The Cyber Hero® Team reviews alerts, validates risk, and responds according to agreed runbooks, ensuring that automated detection is paired with real-world judgment and accountability.

Crucially, these detection layers operate within the guardrails created by **Allowlisting** and **Ringfencing™**. By defining what is permitted to run and the way processes may interact, ThreatLocker makes abnormal behavior easier to spot and limits the potential impact when something goes wrong. In combination, predictive insight and human oversight work together to improve clarity without removing control.

60%
report a lack of skilled threat analysts‡

A practical partnership

Cybersecurity breaks down when humans and systems are treated as substitutes rather than collaborators. People cannot monitor everything, and systems cannot understand everything. Each compensates for the other's weaknesses.

Predictive intelligence provides structure, visibility, and early warning. Human judgment provides context, accountability, and control. When these elements are aligned, security becomes more predictable and less dependent on individual heroics. Organizations that design security around this partnership are better equipped to deal with uncertainty, change, and pressure.

AKIRA

AND THE BUSINESS OF MODERN RANSOMWARE

Ransomware group Akira has built its reputation without spectacle, relying instead on stealth access, affiliate partnerships, and attacks that can spread disruption

Akira does not hit the headlines often, and that is by design. The ransomware group has built its reputation by avoiding the theatrics favored by some rivals, instead focusing on quietly breaking into corporate networks, stealing data, and applying pressure out of the spotlight.

The group's approach points to a wider change in ransomware operations. While some still try to pressure victims out in the open, many now take a quieter route, relying on access they can reuse from one intrusion to the next. That often involves compromising legitimate remote management tools or identifying vulnerabilities at the interfaces between cloud services and internal networks, where malicious activity can be easily missed.

As ransomware matures as a criminal industry, Akira offers a useful case study into how these operations function, how they gain access to corporate systems, and why organizations continue to struggle to keep them out despite years of warnings.

Meet Akira: A ransomware crew built for scale

Akira first announced itself in March 2023 with the launch of a leak site designed to list victims. Organizations from different sectors began appearing in quick succession, suggesting the group had skipped the tentative early phase that many ransomware crews undergo.

Security researchers soon identified echoes of the Russia-linked Conti group in Akira's operations. Certain infrastructure patterns and attack methods looked familiar, prompting speculation that fragments of the earlier ransomware empire may have resurfaced in a new form.

Like many modern ransomware groups, Akira appears to operate a Ransomware-as-a-Service (RaaS) model, in which core developers manage the malware and infrastructure, while external partners handle breaches. This setup allows the group to grow faster than a single team could and spreads the risk among several people.

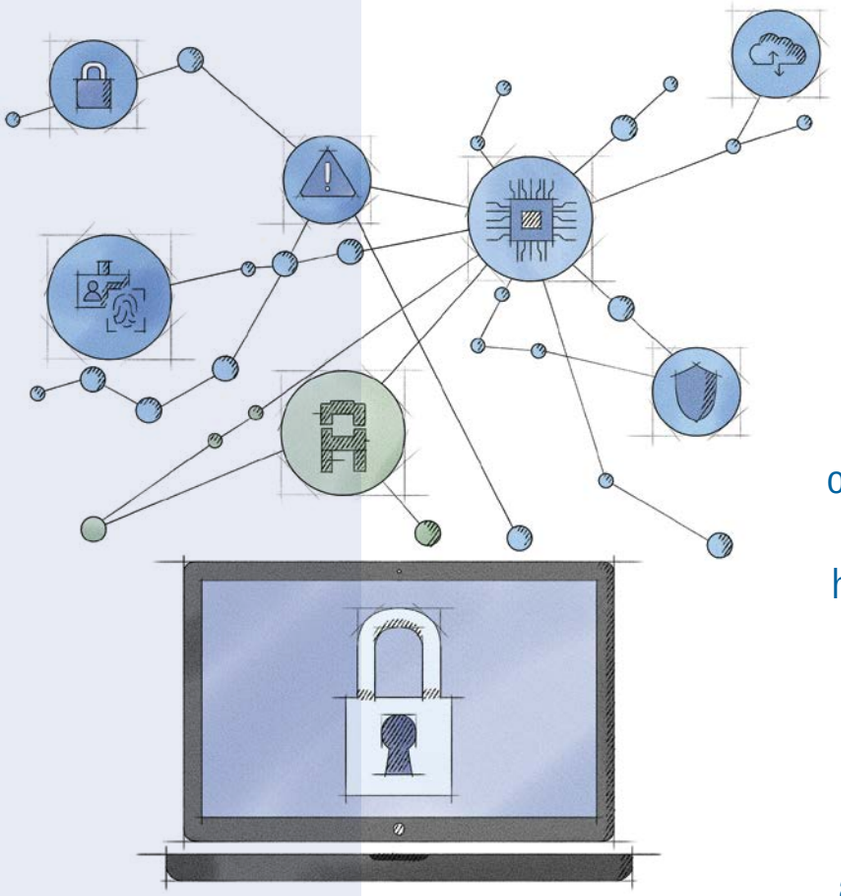
According to the U.S. government, Akira has hit manufacturing firms, hospitals, schools, and critical infrastructure operators. By mid-2024, officials estimated that the group had compromised more than 250 organizations and had received millions in ransom payments.[‡]

Tools, tactics, and operational playbook

Akira typically does not rely on cutting-edge zero-day exploits or complex intrusion chains. In many cases, initial access traces to issues organizations were already aware of, such as stolen VPN credentials, phishing messages, or internet-facing services that were left exposed.

The group also tends to lean on the same administrative tools IT teams use every day instead of dropping obvious malware straight away. Remote management software and built-in operating system features are commonly used in living-off-the-land (LOTL) attacks to move through networks and expand access. Because those tools are so widely used in legitimate environments, early warning signs can be easy to miss, especially in large or complex corporate systems.

Akira typically does not rely on cutting-edge zero-day exploits or complex intrusion chains. In many cases, initial access traces to issues organizations were already aware of



By mid-2024, officials estimated that Akira had compromised more than

250

organizations and had received millions in ransom payments

Researchers have also seen Akira deploy the Armillaria Loader.[‡] Rather than deploying ransomware immediately, tools like this give attackers time to move around inside the network and understand how systems are organized, allowing them to identify key servers, locate backups, and map out how different parts of the organization are connected before any encryption is triggered.

When the attack escalates, it happens fast. Shared drives and backup storage are often hit first, making recovery harder before defenders realize what is happening. At the same time, sensitive files are quietly stolen. If the victim does not pay, the attackers use the stolen data as leverage.

Encrypting files is no longer enough for attackers. The threat of releasing confidential data to the public, along with possible legal trouble, is now just as strong a motivator to encourage victims to pay.

The real-world impact: From stealth access to mass disruption

Akira's playbook came into sharp focus during the 2024 ransomware attack on Nordic IT services provider Tietoevry, one of the most widely reported incidents tied to the group.

The attack forced sections of the company's data center infrastructure offline, interrupting services used by customers across Finland and Sweden. Municipal systems, retail payment services, and healthcare platforms were among those affected, with some outages lasting several days while recovery work continued.

Incidents involving service providers prey on interdependency and tend to affect more than one organization at a time. Because companies such as Tietoevry operate systems for multiple customers, disruptions within their networks can spread quickly to the organizations that rely on those platforms.

Stopping Akira: Zero Trust and layered defense

Defending against groups like Akira means assuming attackers might already have a foothold. That means a Zero Trust approach—whereby no one is automatically trusted, and access is constantly verified—is now the baseline for staying secure.

The idea centers on continuously verifying users and devices rather than granting broad, indefinite access. In practice, that often means cutting back administrative privileges and separating internal systems so attackers cannot move easily if they get in.

Organizations need to look at how they can limit the software and administrative tools used inside their corporate environments. This can include application allowlisting, endpoint monitoring, and behavior-based alerting systems that look for unusual login patterns, unexpected scripting activity, or irregular access to backup infrastructure, warning signs that have been observed in several ransomware investigations.

The road ahead

Akira reflects a broader shift in ransomware operations. Organizations that only react to threats will have trouble keeping up, but those that always verify access, instead of automatically trusting it, are more likely to limit the damage from attacks.

> The threat of releasing confidential data to the public, along with possible legal trouble, is now just as strong a motivator to encourage victims to pay

THREATLOCKER® TIP

BLOCKING THE AKIRA PLAYBOOK WITH THREATLOCKER

The ThreatLocker threat intelligence team has observed Akira deploying tools such as the Armillaria Loader to execute payloads inside trusted processes, as well as endpoint detection and response (EDR)-killing components designed to disable security controls before encryption begins.

A Zero Trust endpoint approach helps break this chain early. **Allowlisting** ensures only approved applications and scripts can run, preventing loaders and LOTL tools from executing even when attackers use legitimate processes.

ThreatLocker EDR resists tampering and adds behavioral monitoring and alerting for suspicious process activity and attempts to tamper with security controls.

Together, they reduce attacker dwell time and limit ransomware operators' ability to stage, persist, and escalate privileges within compromised environments.

WIRESHARK
SEE WHAT THEY SEE

Understand your network traffic at the packet level for proactive defense

For many security professionals, Wireshark is an essential tool. It can capture, display, and track every packet on a local network card in a human-readable way, which is invaluable for understanding network behavior and helping engineers troubleshoot and understand how networks work.

It is helpful to know how Wireshark came about, as it offers insight into the depth of expertise involved in the project. Developer Gerald Combs launched the Wireshark project in 1998. At the time, hardware packet sniffers were simply too expensive, and they rarely supported Linux. So, Combs did what all good hackers do and wrote his own cross-platform, open-source, software-based example.

Wireshark gained its initial success by providing a framework for network experts to add their own low-level protocol dissectors—a feature that enabled Wireshark to grow from supporting just four base protocols at launch to over 3,000 today.[‡]

A worldwide legion of contributors ensures Wireshark supports everything from automotive protocols and telephony systems to the latest emerging standards, with modules developed by experts in their own fields.

This expandability has enabled Wireshark to progress from supporting basic Ethernet analysis through the evolution of wireless, VPN, and cloud architectures, all the way to cutting-edge HTTP/3.

SNIFFING OUT THE ADVANTAGE

For threat analysis, Wireshark enables security teams to inspect suspicious traffic patterns, identify unauthorized connections, and analyze malware communications. When an endpoint exhibits unusual behavior, packet captures reveal whether it is contacting command-and-control servers, exfiltrating data, or scanning the network for vulnerabilities.

During incident response, packet captures provide forensic evidence. Security teams can analyze traffic patterns to identify malicious connections, reconstruct attack timelines, and detect command-and-control communications. Keep in mind that beneath modern encryption, Wireshark reveals who talked to whom and when—rather than the actual content—unless you have the decryption keys.

For troubleshooting, the tool diagnoses connectivity issues, application failures, and performance bottlenecks by showing precisely where communications break down. A failed login might reveal misconfigured certificates, domain name system (DNS) problems, or firewall blocks, problems that would otherwise require hours of guesswork.

UNDERSTANDING BOTH SIDES

The crux here is that attackers also use Wireshark. The same packet-level visibility used for troubleshooting enables adversaries to map network architectures, identify unencrypted credentials, and plan attacks. When threat actors gain network access, Wireshark helps them see what you see—and that is not acceptable.

That is why adhering to Zero Trust principles is essential. Network visibility without access controls is insufficient. Wireshark has democratized network analysis, giving defenders an enterprise-grade analysis tool without the need for an enterprise budget.

Organizations must combine deep packet inspection with application control, **Ringfencing™**, and network segmentation. Techniques like MAC address allowlisting and Persistent MAC Learning (otherwise known as Sticky MAC) help ensure only specific devices—or the last connected device—are permitted to connect.

Visibility alone is not enough: With ThreatLocker®, you can actually control what is happening. Combined with Zero Trust principles and proper access controls, it empowers security teams to transition from reactive responders to proactive protectors who understand precisely what is occurring across their infrastructure—before adversaries can exploit it.

EMPIRE

THE FALL AND RED TEAM RISE

The by-the-numbers tool that gives attackers the post-exploitation power of a fully operational battle station

While it might be easy to be dismissive of the fun Star Wars ASCII graphics and the playful Darth Vader quotes, beneath Empire's light-hearted front lies some seriously dangerous code.

Beginning its life in 2015 as a legitimate open-source researcher-built penetration testing tool, Empire followed the same path to the dark side as many security tools—proving, as it did, equally effective in malicious hands.

Even after being abandoned by its original authors, a 2018 joint report from the Cybersecurity and Infrastructure Security Agency (CISA) and the Five Eyes alliance (Australia, Canada, New Zealand, the U.K., and the U.S.) listed it among the top five open-source tools used by attackers for lateral movement.

FULLY OPERATIONAL BATTLE STATION

Empire is a post-exploitation framework that uses a PowerShell 2.0-based Windows agent, with limited Linux and macOS capabilities, and supports encrypted communications and a flexible architecture. Recent updates to suit red teams have even added the option of a full graphical user interface (GUI).

Empire provides over 285 pre-built modules that automate complex attacks: privilege escalation to gain administrator rights, Mimikatz integration for credential harvesting, keyloggers for surveillance, lateral movement tools for spreading across networks, and data exfiltration methods that bypass traditional monitoring.

What makes Empire particularly insidious is its stealth. It runs PowerShell agents without requiring the executable, operates entirely in memory, and uses encrypted communications to evade network detection. When over 76% of ransomware attacks leverage PowerShell[‡], tools like Empire become a linchpin—turning single compromised endpoints into bridgeheads for network-wide attacks.

TURNING TO THE DARK SIDE

Empire's greatest danger lies in its accessibility. It remains an open-source project hosted on GitHub and includes extensive documentation, tutorials, and a graphical interface called Starkiller. It is a complete package that enables even relatively inexperienced attackers to deploy professional-grade, post-exploitation tactics.

Multiple sources describe it as "easy to use," with a modular design that requires basic technical knowledge. An attacker who gains initial access through phishing needs only rudimentary command-line skills to establish persistence, escalate privileges, and exfiltrate credentials—capabilities that once required highly specialized expertise.

Post-exploitation frameworks only succeed when applications can interact freely with each other. The deny-by-default, permit-by-exception philosophy turns Empire into a contained threat.

HOW THREATLOCKER STOPS THE EMPIRE

Breaches do happen. Perimeter defenses fail, credentials are stolen, and social engineering is successful. What separates contained incidents from catastrophic breaches is what happens next. Zero Trust architecture recognizes that post-exploitation tools are only dangerous when they can execute.

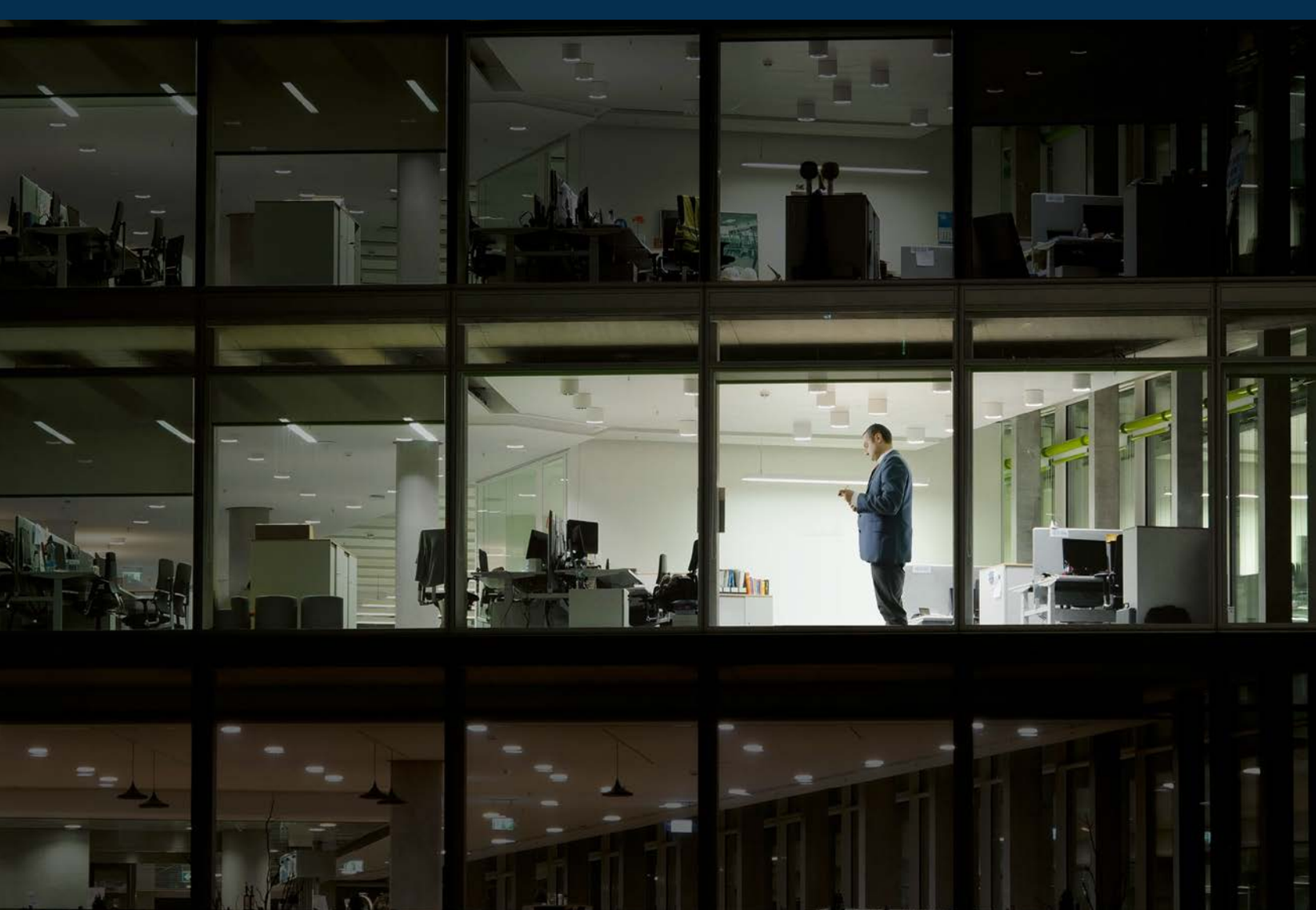
With ThreatLocker, **Allowlisting** prevents Empire agents from running in the first place—they are unlikely to feature on approved application lists, after all.

Even if an attacker somehow gains initial access, **Ringfencing** contains the damage. PowerShell rarely requires internet access, document access, or the ability to interact with other applications. Default **Ringfencing** policies block PowerShell from making these interactions, stopping Empire's modules from downloading payloads, accessing credentials, or communicating with command-and-control servers. But with a toolkit as broad as Empire, full-spectrum coverage is vital.

ThreatLocker **Zero Trust Endpoint Firewall** blocks unauthorized communications, **Data Storage Access Control** prevents data exfiltration, and **ThreatLocker EDR** identifies suspicious behavior patterns. However versatile and secretive a tool like Empire might be, it can be stopped.

THE CASE FOR SUSTAINABLE SECURITY TEAMS

High-stakes stress:
How organizations can better support their frontline cyber defenders



Professionals and IT leaders face mounting pressure from rising digital demands and an always-on work culture. Security incidents require immediate, coordinated responses from multiple parties, often with barely any time for recovery before the next crisis. Teams must also document and manage the aftermath, with little opportunity to reset. Sustained stress leads to hypervigilance, sleep disruption, and burnout, especially for security operations center (SOC) analysts, incident responders, and on-call engineers, often forcing time off for recovery in an already overstretched sector.

Organizations need to focus on creating healthier work environments, not just protecting systems. Effective policies, shift design, post-incident care, and culture change help reduce stigma and support team well-being.

Martin Astley, a public speaker on cybersecurity strategy and CISO and CEO at managed IT security provider Astley Digital Group Limited, makes the case for more tailored support for teams experiencing burnout, given that stressors in cybersecurity are distinct from those in many other industries.

"There's a constant expectation of perfection. In most roles, you can make small mistakes and recover. In cybersecurity, one missed alert or misconfiguration can lead to a major incident, creating constant background pressure," said Astley. "If we want resilient security programs, we need resilient teams."

An always-on work environment

The threat landscape creates an always-on expectation. Attackers are often most active outside standard hours, increasing pressure on security teams to remain vigilant around the clock. Security roles carry significant responsibility for company assets, often without full control.

"Security leaders are accountable for risk, but they often don't control budgets, development decisions or legacy systems," said Astley. "Fixing risks depends on broader business decisions, which can be frustrating. There's also incident fatigue: Teams work long hours under pressure, knowing the organization, its reputation, and jobs are on the line."

Over time, these factors can cause exhaustion and burnout if organizations do not actively support their teams. A May 2025 State of Cybersecurity ISACA report found that 73% of European IT professionals suffer burnout amid rising workloads and skill shortages. Sixty-one percent attribute work stress to heavy workloads, 44% to tight deadlines, and 43% to lack of resources. Almost half (47%) of respondents cited unsupportive management as a factor affecting well-being. The IT skills gap increases pressure by overloading staff, and 30% named the need for specialized skills as a top challenge.

> "As the U.K. ranks among the top countries for burnout
>
> **4 in 5**
>
> workers believe it would be easy to offload simpler tasks to AI

The skills gap

The World Economic Forum's 2025 Global Cybersecurity Outlook found that only 14% of organizations have enough talent to meet cybersecurity goals, with the gap widening by 8% annually.

"With skilled employees in such high demand, it is in companies' best interests and simply the right thing to do to make sure the tech workforce feels supported, motivated, and invested in," said Chris Dimitriadis, Chief Global Strategy Officer at ISACA. "Younger IT professionals are switching jobs at a much higher rate, highlighting the need for better retention strategies, including clear career growth pathways and a focus on work-life balance. At the same time, experienced professionals must have access to the support they need to stay engaged and continue contributing their expertise. A balanced, well-supported workforce is key to sustaining the industry's growth and innovation."

John Young, CISSP, Fractional CISO at Security Postures, highlighted that while the skills shortage is real, it is "no longer the whole story."[‡]

"The larger issue is that the CISO mandate itself has expanded beyond what a human-only operating model can reliably absorb," said Young. "Even exceptional CISOs, backed by strong teams, are being asked to perform a job that is continuous, cross-domain, high-consequence, and increasingly machine-paced."

Effective support strategies

So long as the cyber skills gap continues to affect employee well-being, mentorship, effective talent development, and suitable career growth opportunities are essential to sustain progress.

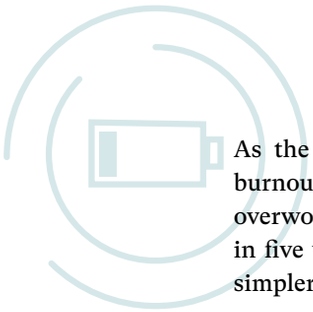
Sarah Orton, U.K. and Europe lead for ISACA's SheLeadsTech initiative, said: "There are practical steps businesses can take. By creating mentorship programs, investing in training and certifications, and establishing more accessible entry-level programs, they will relieve common pain points and improve areas of employee fulfillment and satisfaction. With this kind of support, businesses can build a more motivated, productive, inclusive, and equitable workforce, in turn building cyber resilience."
Organizations can bolster support through protected recovery time after incidents, mandatory off-ramps, blameless postmortems, incident-rotation policies, and proactive mental health support.

Other measures include using metrics that connect operational efficiency, such as mean time to repair (MTTR) and alert noise, to workforce well-being. High MTTR, poor alert-noise ratios, or high employee assistance program (EAP) use can signal burnout risk early.

Can AI help with burnout?

Many organizations are looking to automation for respite. The 2026 U.K. Mental Health Burnout report found that one in five U.K. workers needed time off last year due to stress. Employers who successfully supported staff returning from burnout cited planning and open communication as critical, along with phased returns, flexible working, and regular well-being check-ins focused on support rather than performance.

> Security teams cannot operate in permanent crisis mode. Sustainable security comes from good processes, proper resourcing, and realistic expectations, not from heroic burnout
>
> MARTIN ASTLEY



As the U.K. ranks among the top countries for burnout, many are turning to AI tools to address overwork and skills gaps. A GoTo study found four in five workers believe it would be easy to offload simpler tasks to AI.

"My focus on mental health came from seeing the human side of cybersecurity that often gets ignored," said Astley. "Cybersecurity is usually discussed in terms of technology and threats, but behind every operations center and risk decision, people carry huge responsibility. I've seen talented professionals struggle with pressure and exhaustion. In some environments, asking for help can feel like weakness, pushing people to suffer in silence."

The human story

Cybersecurity professionals face constant pressure to protect assets. Even advanced tools cannot compensate if people are exhausted or fearful. When that happens, security weakens.

"Leadership modeling is important because culture starts at the top. If leaders openly talk about workload, boundaries, and mental health, it gives everyone else permission to do the same," said Astley. "Recognizing human limits is also critical. Security teams cannot operate in permanent crisis mode. Sustainable security comes from good processes, proper resourcing, and realistic expectations, not from heroic burnout."

Cybersecurity requires both technical skill and human resilience, yet workforce well-being receives far less investment than protection. "The future of cybersecurity leadership will still require human judgment," said Young.

Building sustainable security teams is a strategic priority. Organizations that invest in recovery time, mental health support, and realistic workloads are better positioned to retain talent, respond effectively, and maintain the kind of consistent vigilance that cybersecurity demands.

THREATLOCKER® TIP

REDUCING THE LOAD

The ThreatLocker prevention-first approach is a practical way to reduce operational strain on security teams.

Allowlisting combined with strict policy enforcement helps cut alert noise, lower triage work, and reduce the scope of incidents before they escalate.

Ringfencing™ limits lateral movement, keeping incidents contained and manageable. Knowing that malicious activity on a compromised endpoint cannot spread freely across the environment gives teams room to respond in a calm manner.

Data Storage Access Control, whether covering network shares or USB devices, helps reduce insider threat exposure and the complex forensic work that follows.

Zero Trust Network Access (ZTNA) and **Zero Trust Endpoint Firewall** reduce suspicious traffic alerts, lowering the volume of day-to-day administration noise.

Fewer false positives, smaller blast radii, and tighter access controls mean security teams spend less time firefighting and more time doing the work that matters.

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

August 1–6 2026
Las Vegas, U.S.
Black Hat USA 2026

August 3–5 2026
San Diego, U.S.
ChannelCon 2026

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

September 8–10 2026
Washington DC, U.S.
Billington CyberSecurity Summit

September 29–October 2 2026
Denver, U.S.
EDUCAUSE Annual Conference

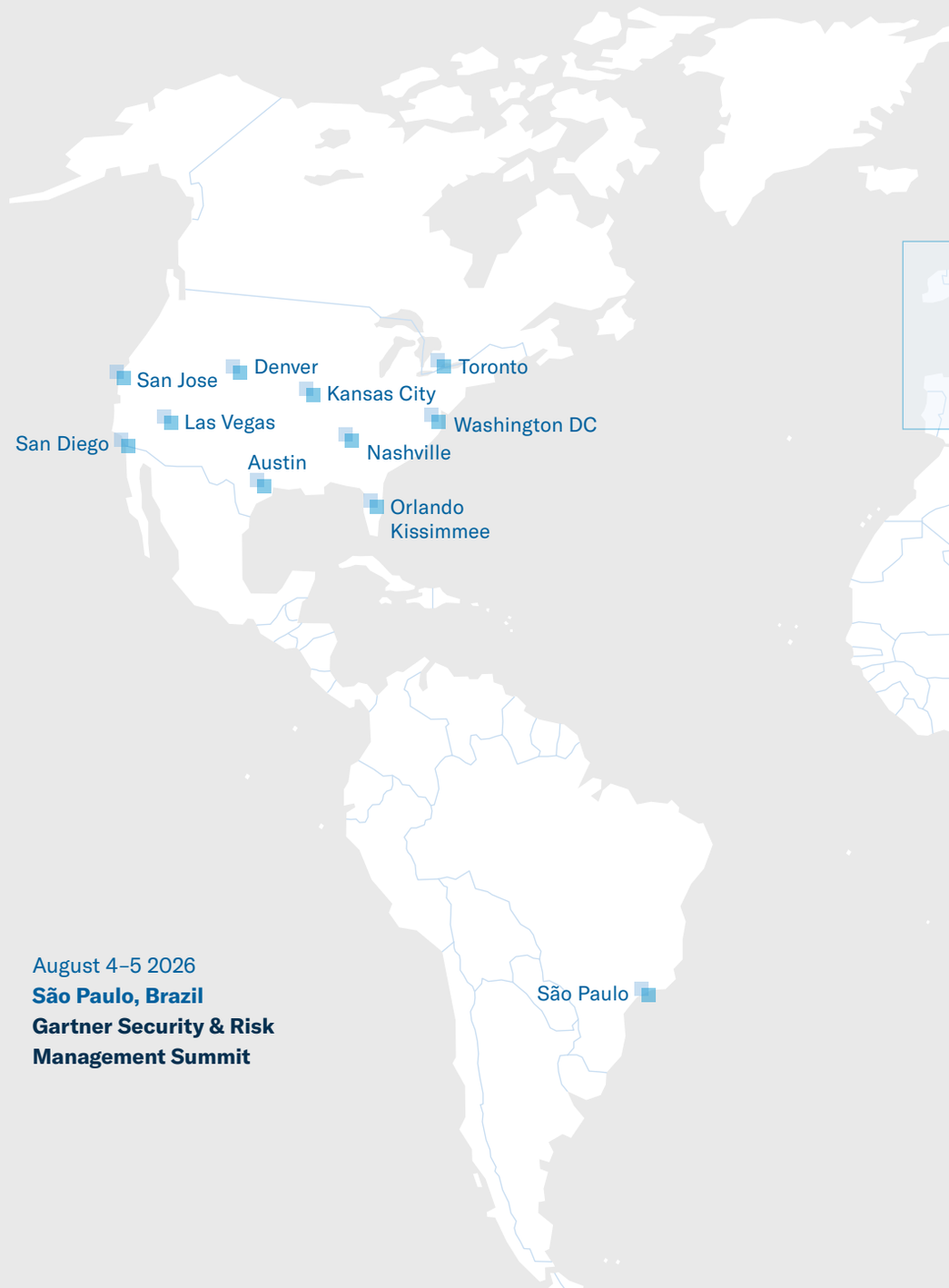
October 6–8 2026
Toronto, Canada
SecTor 2026

October 12–14 2026
Kissimmee, U.S.
InfoSec World 2026

October 19–22 2026
Orlando, U.S.
Gartner IT Symposium/Xpo™

October 19–21 2026
Kansas City, U.S.
Jack Henry™ Connect 2026

October 26–29 2026
Austin, U.S.
FS-ISAC Americas Fall Summit 2026



August 4–5 2026
São Paulo, Brazil
Gartner Security & Risk Management Summit

September 22–24 2026
London, U.K.
Gartner Security Risk & Management Summit

September 22–23 2026
Barcelona, Spain
Info-Tech Live Barcelona

September 29–30 2026
London, U.K.
International Cyber Expo

October 6–8 2026
Barcelona, Spain
Canalys Forum EMEA

October 13–15 2026
Lisbon, Portugal
World Aviation Festival

October 14–15 2026
London, U.K.
DTX London

October 18–20 2026
Copenhagen, Denmark
Pax8 Beyond EMEA Copenhagen

October 20–21 2026
Amsterdam, Netherlands
TechEx Europe

October 27–29 2026
Nuremberg, Germany
it-sa Expo&Congress

Dubai

September 16–18 2026
Dubai, U.A.E.
GISEC Global

October 5–7 2026
Dubai, U.A.E.
Gartner CIO & IT Executive Conference

August 4–5 2026
Canberra, Australia
Tech in Gov

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

September 14–16 2026
Broadbeach, Australia
Gartner IT Symposium/Xpo™

October 15–17 2026
Melbourne, Australia
2026 AISA Melbourne CyberCon

Broadbeach
Sydney
Canberra
Melbourne

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
Heather Hartland | VP Experiential Marketing
Kieran Human | Security Enablement Lead
Paige Jenkins | Graphic Designer
Izzy Martinez | 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
Adam Oxford | Copywriter
Carly Page | Copywriter
Lauren Hurrell | Copywriter
Neil Mohr | Copywriter
Nick Peers | Copywriter

Photo credits: ThreatLocker® (pages 2, 3, 4, 6, 38) © ThreatLocker; (pages 5, 30, 32, 36, 38, 53, 54, 55, 70, 73, 78) ILLUSTRATIONS © MUTI; (page 5/top) © Sergio Rojo/Shutterstock; (page 5/bottom) © Neelakshi Singh/Unsplash; (page 10) © Blvdone/Shutterstock; (page 13) © Viola Dolas/Shutterstock; (pages 18, 29, 68) © REMAINPHOTOGRAPHY LLC; (page 20) © Manjaaa/Shutterstock; (page 22) © Chay_Tee/Shutterstock; (pages 24, 25, 26, 27) Courtesy of Aurora Mental Health & Recovery (AMHR); (page 31) © EiZivile/Shutterstock; (page 35) © TinoFotografie/Shutterstock; (page 42) © Ringo Chiu/Shutterstock; (page 43 from top) Fitria Ramli/Shutterstock, Steve Dimatteo/Unsplash; (page 44) Anna Sullivan/Unsplash; (page 46) © Dziurek/Shutterstock; (page 47) © Paolo Bona/Shutterstock; (pages 48, 50/top) © Fernando Medina/Getty Images; (page 50/bottom) © Gary Bassing/Orlando Magic; (page 51) © courtesy of the Orlando Magic; (page 52) Ravi_Sharma1030/Shutterstock; (page 53) © Noppasin Wongchum/Shutterstock; (page 54) © Ariyo Olasunkanmi/Shutterstock; (page 56) © I_am_zews/Shutterstock; (page 57 from top) © Neelakshi Singh/Unsplash, © Tarcisio Schnaider/Shutterstock; (page 59) © Ramaz Bluashvili/Pexels; (page 60) © Evelin Elmest Photography; (page 62) © Pandora Pictures/Shutterstock; (page 64) © Alexey Fedorenko/Shutterstock; (page 65) © Sergio Rojo/Shutterstock; (page 66) © Sven Hansche/Shutterstock; (page 67) © GCHQ; (page 74) © KenSoftTH/Shutterstock; (page 77) © Gorodenkoff/Shutterstock; (page 82) © MEDIAIMAG/Shutterstock; (page 84) © King Ajyad/Shutterstock; (page 88) © Gorodenkoff/Shutterstock.

‡ Data Sources: (page 21) Global Wellness Institute: “Wellness Economy Statistics & Facts”; CDC: “Potential public health risk among individuals ordering counterfeit prescription medications from online pharmacies”; FTC: “Think you know what the top scam of 2023 was? Take a guess”; (page 29) Wired: “Under Worm Assault, Military Bans Disks, USB Drives”; (page 33) NVD: “CVE-2025-0411 Detail”; (page 37) CBS News: “GoDaddy apologizes for “insensitive” phishing email offering bonuses to employees”; InformationWeek: “Forrester Panel: Government Cybersecurity Leaders Discuss Next Steps for Zero Trust”; (page 40) CISA: “StopRansomware: Akira Ransomware”; (page 42) Forbes: “Ransomware Gang Strikes The Houston Rockets”; (page 43) Mexico Business News: “World Cup 2026 Could Trigger 55 Million Cyberattacks in Mexico”; (page 45) ESPN: “NFL viewership up 10% this season at 18.7M per game”; ESPN: NFL Attendance - 2025; (page 53) Government of India: “Future Ready: India’s Digital Economy to Contribute One-Fifth of National Income by 2029-30”; (page 54) Reuters: “Nigerian data agency fines Fidelity Bank for breaches”; Reuters: “Nigeria suspends cybersecurity levy amid cost of living crisis”; (page 60) e-Estonia: “How did Estonia carry out the world’s first mostly online national elections”; (page 61) NATO Strategic Communications Center of Excellence: “2007 cyber attacks on Estonia”; (page 63) ENISA: “Cybersecurity strategy 2024–2030 Cyber-conscious Estonia”; (page 65) BBC News: “Ransomware attack contributed to patient’s death”; GOV.UK: “Summary of the Bill”; Bridewell: “Cyber Security in Critical National Infrastructure Organisations: 2025”; (page 67) GOV.UK: “Cyber security breaches survey 2025”; (page 69) GOV.UK: “AI Insights: Agentic AI (HTML)”; Verizon: “Stack your cybersecurity knowledge—and watch attacks topple”; Anthropic: “Disrupting the first reported AI-orchestrated cyber espionage campaign”; (page 70) The Wall Street Journal; [MOVEIT TRANSFER BREACH] EMSISOFT: “Unpacking the MOVEit Breach: Statistics and Analysis”; BITSIGHT: “New research reveals rapid remediation of MOVEit Transfer vulnerabilities”; (page 71) CISA: “Securing the Software Supply Chain: Recommended Practices Guide for Suppliers and accompanying Fact Sheet”; CISA: “Reducing the Attack Surface for End-of-Support Edge Devices”; [RACCOONO365 MICROSOFT ACCOUNT ATTACK] Reuters: “Microsoft seizes 340 websites linked to growing phishing subscription service”; [BADIIS GLOBAL SEO POISONING] Cisco Talos: “UAT-8099: Chinese-speaking cybercrime group targets high-value IIS for SEO fraud”; (page 73, 74, 75/statistics) Forrester:“Threat Intelligence Benchmark: Stop Reacting; Start Anticipating”; (page 74) National Cyber Security Centre: “UK critical systems at increased risk from ‘digital divide’ created by AI threats”; (page 77) Internet Crime Complaint Center (IC3): “StopRansomware: Akira Ransomware”; (page 78) ThreatLocker: “From Armillaria loader to EDR killer”; (page 80) Wireshark: “Display Filter Reference”; (page 81) The Stack: “PowerShell use for ransomware is rife, seen in 76% of all incidents”; (page 84) LinkedIn: “The CISO skills shortage is real” (March 2026).

↗ READ ABOUT THE CYBERSECURITY THREAT FACING OPERATIONAL TECHNOLOGY IN THE NEXT ISSUE OF THREATLOCKER CYBER HERO® FRONTLINE MAGAZINE

Even your best employees make mistakes.

ThreatLocker® ensures those mistakes don't cost you.

Human error is a major cybersecurity risk. Intentional or unintentional threats pose the same danger. So, stop trusting and start controlling. Decide exactly what runs, when, where, and how. Deploy in hours to days and stop threats before they start

How do you prevent data breaches?

Choose the path of least privilege.

Hackers take the path of least resistance.
So, block them with the path of least privilege.
Let us surprise you with how straightforward this actually is.

Minimize breach risks. Limit access to what's essential while enabling smooth business functions. Deny by default, allow by exception, and stop ransomware in its tracks.