THREATLOCKER®
ZERO TRUST PLATFORM

MEET THE

ZERO TRUST PLATFORM

FOR ENDPOINTS, CLOUD, AND NETWORK SECURITY

See what's possible and take swift control of your organization like others did.

> When we first engaged with ThreatLocker, we were looking for a solution for application control in a highly regulated industry. The flexibility and ease of deployment were major factors that attracted us to ThreatLocker.

Rob Thackeray, End User Technical Architect
Heathrow Airport

> Within the first week of implementing ThreatLocker, we were able to look at our entire application inventory—something my team previously had to do manually. Within an hour or two, we could see every learned application on our system.

Ismael Hernandez, VP of Information Technology
TLG Peterbilt

> We had explored other options, but achieving the same level of control would have meant piecing together solutions from multiple vendors. With ThreatLocker, we were able to get everything we needed from one place.

Jeff Lutes, Executive Vice President of Technology
Orlando Magic

> Before we had ThreatLocker, we had a lot of risk that we just couldn't control. And with ThreatLocker, I think we're doing a much better job of providing a more secure environment for our patients, our doctors, and our manufacturers.

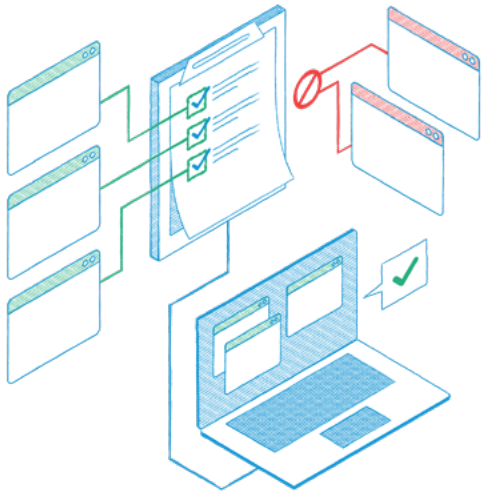
Greg Gootee, CISO / SVP of Information Security
Asembia

Stop ransomware, rogue apps, and zero-day exploits before they can run.

It's been impossible to react to every threat. So, with ThreatLocker®, you flip the script. Instead of chasing cybercriminals, you block them out instead. You allow only what you explicitly need and trust. Everything else is then blocked by default.

Deployment is straightforward, the platform scales with ease, and the experience is simpler than many expect.

Your environment stays secure through proactive, policy-driven protection that simplifies your operations while locking things down. And when it matters most, you're backed by dedicated ThreatLocker Cyber Hero® team members who act fast to keep your business running smoothly and securely.



Take control of what runs in your environment.

Allowlisting

Get a straightforward, lightweight, yet powerful, deny-by-default solution that is scalable and deploys within a matter of hours-to-days thanks to 13,000+ pre-built applications and automatic learning. Unknown software can't slip in; silent installs don't happen in the background, and ransomware won't begin quiet encryption.

ThreatLocker® Allowlisting puts you in control. Only approved applications run across your environment. It's a simple, binary approach: You list what needs to run, and anything not on that list is unable to execute.

Stop shadow IT, enforce application control for compliance (NIST, CMMC, CIS, and more), and gain full visibility and control of every app, dependency, and update in your environment.

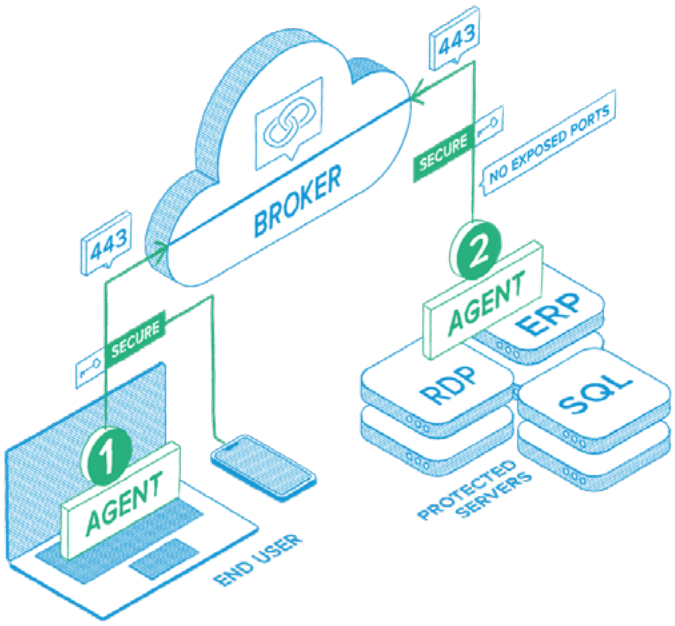
Decide exactly what every trusted application is allowed to do.

Ringfencing™

Enforce strict boundaries on your trusted applications, so, if compromised, cybercriminals can't turn your applications into attack vectors. Prevent Word, PowerShell, and other trusted tools from launching unauthorized processes or reaching the internet. Limit how applications interact so attackers can't pivot, escalate, or exfiltrate data.

With this application containment technology, you allow your trusted applications to run. Yet, you only let them interact with the specific files, registry keys, network resources, or other applications they actually need.

Deploy with strong, default protections, then customize with high granularity for another layer of powerful Zero Trust protection to reduce your attack surface and contain living-off-the-land attacks.



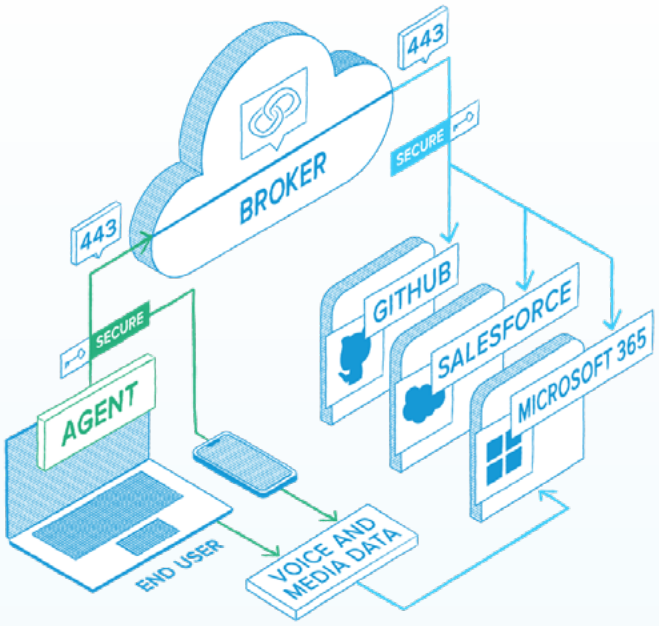
Secure every connection, even when credentials are compromised.

Zero Trust Network Access

Dramatically reduce your attack surface while simplifying secure access for users. Zero Trust Network Access (ZTNA) from ThreatLocker® allows you to provide secure connectivity for explicitly authorized user-assigned devices to access specific internal resources, without exposing your network to the internet.

By shifting control to the device level, you define exactly who can access what, based on user identity, device, and context. Whether users are in the office, traveling, or working remotely, they experience seamless access while your network remains locked down.

Inbound ports, unnecessary exposure, or complex infrastructure changes are no longer a critical worry.



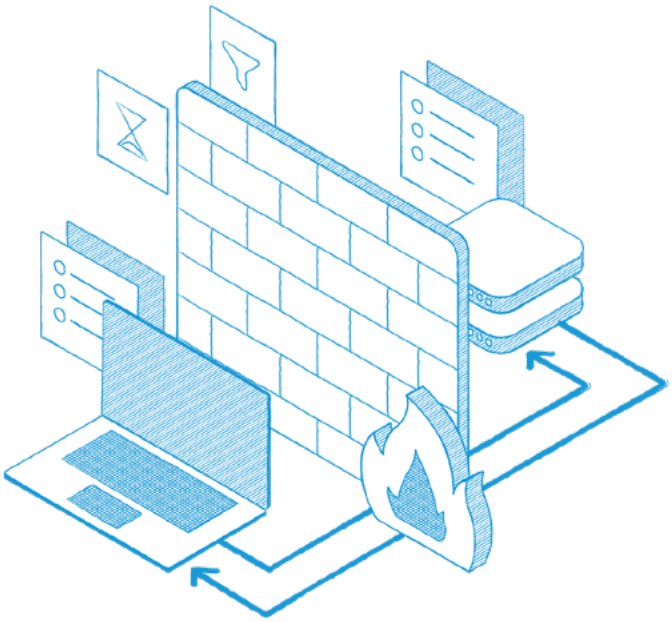
Protect your cloud and stop phishing attacks from gaining access.

Zero Trust Cloud Access

Maintain secure cloud and SaaS access across your organization with ThreatLocker Zero Trust Cloud Access. Even with MFA in place, phishing, token theft, and adversary-in-the-middle attacks can bypass traditional defenses. That's why every request is routed through a secure, ThreatLocker-managed broker that validates identity, device, and policy before granting access. Ensure credentials, and even approved MFA requests, aren't enough for attackers to get in. Only authorized devices can access Microsoft 365, Salesforce, Google Workspace, GitHub, Asana, and other critical cloud services.

Stop token replay, block unapproved devices, and contain phishing impact instantly.

The result? Controlled, device-bound access that keeps users productive, meets compliance requirements, and prevents attackers from turning valid credentials into breaches.



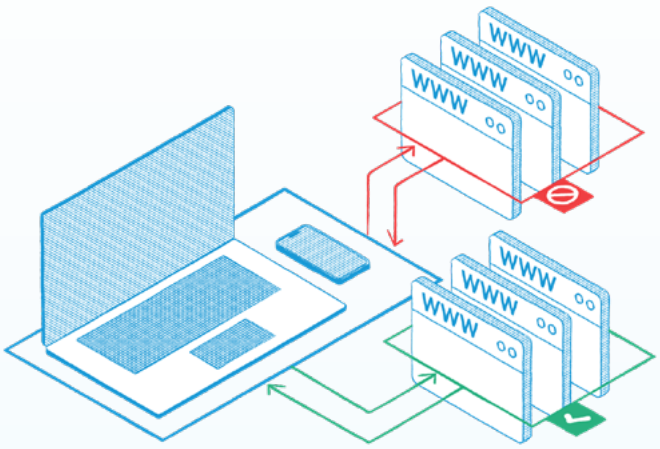
Keep your network safe with dynamic access controls at the device level.

Zero Trust Endpoint Firewall

This host-based firewall for endpoints and servers gives you complete control over network traffic by enforcing access based on device, IP, port, and policy via granular, device-level firewall policies across your entire environment.

Whether users are in the office, at home, or on the road, you maintain control over who can connect, what they can access, and when. Monitor all inbound and outbound connections across endpoints—see the source, destination, and behavior of every request and eliminate unauthorized connections while maintaining control across your entire environment.

With centralized visibility into all network activity and dynamic policy enforcement, you harden your environment against unauthorized access without adding complexity.



Stop phishing at the browser without adding another security tool.

Web Content Control

A fully integrated, agent-based web filtering capability built right into the ThreatLocker® platform, Web Content Control from ThreatLocker eliminates additional third-party tool risks, blocks phishing threats with real-time intelligence, and applies security policies to both managed and unmanaged devices, on and off your network.

Employees and guests connecting to your network are instantly blocked from prohibited sites, reducing exposure to phishing and malicious content. Plus, you deliver a seamless, low-friction user experience by avoiding DNS redirects that cause certificate errors and confusion. Instead, you provide clear, company-controlled guidance to the users and a simple way for them to request legitimate access.

Within one platform, control what websites users can access and reduce the risks of phishing attacks.

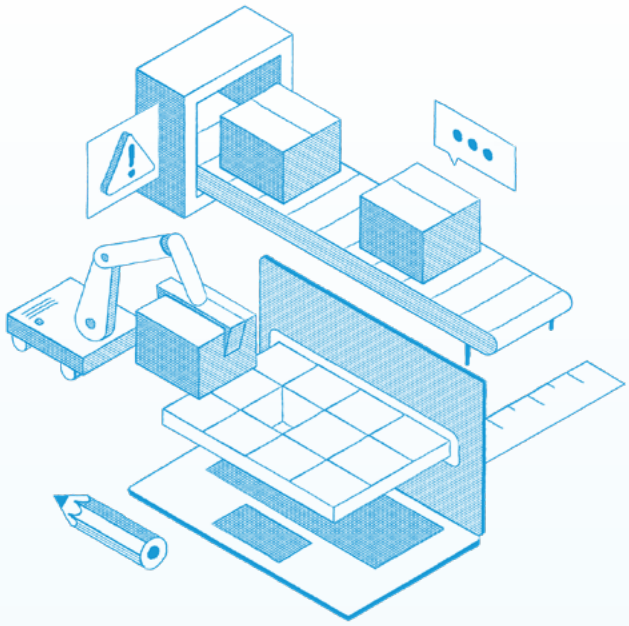
Stop admin privilege abuse with application-level access, not user-level rights.

Privileged Access Management

Grant elevated access only where it's needed at the application level, eliminate credential exposure, and prevent privilege abuse before it turns into lateral movement or ransomware.

Prevent admin credential theft by eliminating credential entry on endpoints and tightly controlling elevation events. Set time limits by user, groups of users, or applications. Plus, demonstrate enforceable least privilege controls aligned to NIST, CMMC, CIS Controls, and other frameworks.

The result? Less standing admin rights means less exposed credentials and no unnecessary privilege for attackers to exploit. Users still get the access they need while your attack surface shrinks and your control expands. Your breach risk drops immediately.



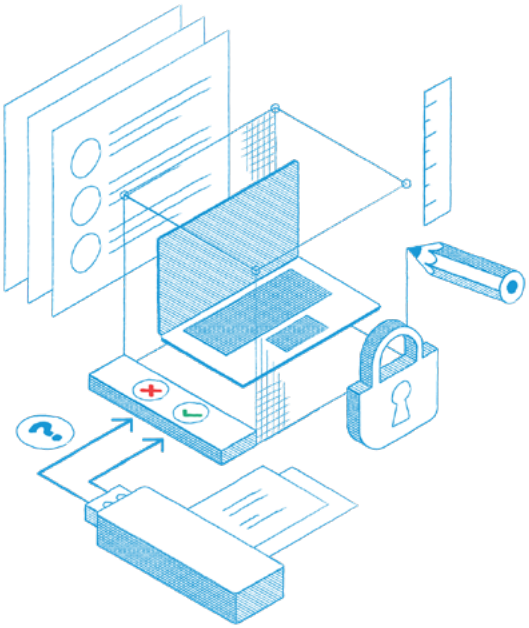
Swiftly remove the patching gaps so they don't become breaches.

Patch Management

Deploy ThreatLocker® Patch Management to simplify and strengthen your application patching process and ensure critical updates, including those for portable apps, are applied consistently.

Instead of spending hours researching which patches to apply and when, ThreatLocker does the work for you. We use hash-based detection to identify unpatched software, including portable applications that traditional tools miss. Every patch is tested by ThreatLocker in a secure environment before release. We ensure your updates are correctly applied according to your policies.

The results? Your systems stay current, and your risk stays controlled. Your patching process is now your reliable protection.



Gain total control over external storage device access.

External Storage Device Control

Eliminate one of the easiest paths for data exfiltration and malware by enforcing precise, policy-driven control over removable media. Place a granular definition over which devices can connect, who can use them, and what they're allowed to do.

External Storage Device Control ensures only approved devices can access your environment, preventing unauthorized data transfers and blocking potential threats carried in through USBs and other media. With full visibility into every connection attempt, you avoid user disruption while removing blind spots and ensuring no unapproved external devices can interact with your sensitive data.

The result? You stop silent file copying to unknown devices, control exactly who can move sensitive data and how, enforce encryption, and produce audit-ready visibility into device usage.

Prevent data exfiltration from occurring in your environment.

Data Storage Access Control

Take control of your data with precise, policy-based access across local folders, network shares, and cloud storage. Define exactly who can access sensitive files—and under what conditions—so you can prevent insider misuse, accidental exposure, and data breaches before they happen.

Ensure only approved users and applications interact with your most critical systems and repositories, while maintaining full visibility into file activity across your environment. Track who accessed, modified, moved, or deleted data at any time.

With flexible policies based on users, groups, devices, applications, file types, and timing, you can quickly detect unusual behavior, trigger alerts, and automatically contain potential exfiltration attempts before they escalate.

Automatically isolate compromised machines —before damage is done.

EDR Real-Time Threat Detection

What if your EDR could act the moment a threat appears without waiting for human or AI intervention? Detect abnormal behavior instantly and enforce policies to isolate compromised devices, shut down risky processes like PowerShell, and block attacker pathways in real time. If a user uploads sensitive files, triggers a known exploit, or shows unusual behavior, containment happens automatically to minimize impact.

Stop ransomware before it spreads by isolating machines and restricting RDP or unauthorized connections within seconds.

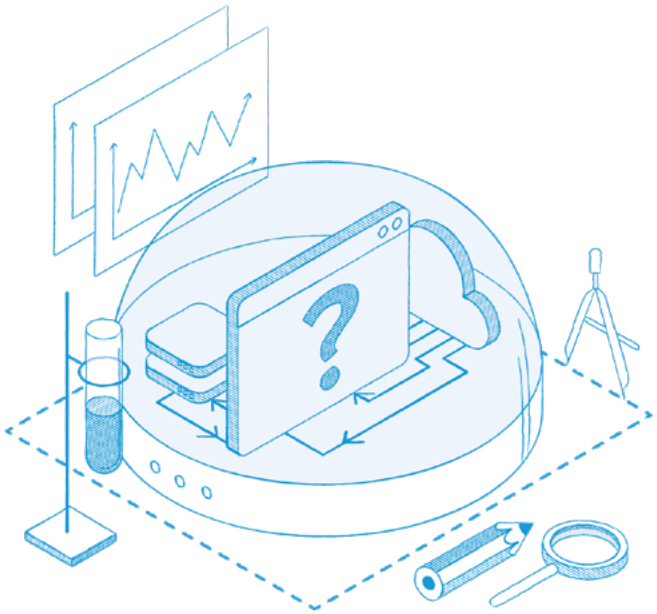
Extend protection to the cloud with identity threat detection and response for Microsoft 365—flagging impossible travel, anonymous sign-ins, and suspicious activity. Reduce dwell time and take immediate control—stopping attacks before they spread, and keeping your business running without disruption.

Stop threats faster with response in minutes, 24/7/365.

Managed Detection and Response (MDR)

Stop attacks before they spread with 24/7 Managed Detection and Response (MDR) powered by real-time threat detection and a dedicated Cyber Hero® Team. You gain full telemetry across endpoints, cloud, users, and networks without expanding your SOC. The moment suspicious activity appears, our team takes action. We isolate compromised devices and shut down malicious activity within minutes, reducing the risk of lateral movement. We validate every alert and escalate only real threats.

While others sync telemetry to the cloud, we contain threats immediately. You get fast, decisive response when it matters most. Stay protected around the clock as ThreatLocker-trained Cyber Hero experts respond in minutes—24/7/365—giving you confidence, control, and stronger security across your entire environment.



See exactly what an application will do before it touches your network.

Controlled Application Testing Environment

Run unknown or untrusted applications in a secure, isolated environment without risking your production systems. ThreatLocker® provides a cloud-based Virtual Desktop Infrastructure (VDI) where you can safely test, observe, and analyze files before approving them. Identify hidden risks, dependencies, registry changes, suspicious network activity, and embedded payloads with confidence.

Give your team a controlled space to evaluate third-party and newly requested applications while reducing software supply chain risk. By analyzing behavior before deployment, you prevent malicious or unstable software from reaching your endpoints.

The result? No blind approvals or risky installs. Your environment stays clean and your team stays in control.

Set your security standards on and off the network, Active Directory domain-joined or not.

Centralized Configuration Management

Maintain uniform security baselines across domain and non-domain systems, closing configuration gaps created by hybrid work and cloud expansion and enforce best practice security policies.

Disable risky services (SMBv1, UPnP), enforce password policies, remove guest and dormant admin accounts, and standardize Microsoft Defender settings across the enterprise. Manage configurations per device, group, or organization from one single console and reduce fragmentation to improve governance at scale.

Plus, apply and verify standardized configuration controls aligned to NIST, CIS, CMMC, ISO, and other frameworks and ensure every device meets policy requirements, whether on the network or remote.

Seal your configuration gaps and build a stronger compliance posture.

Defense Against Configurations (DAC)

See exactly how your systems are configured, identify misconfigurations immediately, and take clear, actionable steps to harden your environment and stay compliant.

Through a powerful dashboard, you can see exactly what needs to be fixed. Think of this as your ultimate resilience assessment center.

Swiftly flag potential risks. See the dormant admin rights accounts, ability to use USB drives, potential gaps in compliance and actionable steps to fix them all.

We make it easy for you: daily scans of your systems, easy-to-digest charts and security-critical lists, visibility into your frameworks, mapping to HIPAA, ISO IEC 27001, NIS2, NIST 800-171, NIST 800-53, Essential 8, FedRAMP, CMMC, GDPR, and more, plus weekly emails with the latest status updates.

Take the next step to securing your environment.

Book a demo and see ThreatLocker in action.

Visit threatlocker.com/demo

About ThreatLocker®

ThreatLocker is a global cybersecurity leader that stops cyberattacks before they happen. The company's Zero Trust Platform prevents breaches from both known and unknown threats by allowing only explicitly trusted software and activity across endpoints, networks, and cloud systems. Built to deploy quickly and scale across complex environments, the platform reduces operational overhead while keeping business running uninterrupted. Headquartered in Orlando, Florida, with offices in Dublin, Dubai, and Brisbane, ThreatLocker protects over 70,000 organizations worldwide.

sales@threatlocker.com

threatlocker.com