THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

SOLUTIONS STACK
SUMMARY

Introduction

Detection-based solutions are no longer the heavy hitters of the modern security arsenal. It's time to say "Goodbye" to traditional detection tools and "Hello" to the next big name in cybersecurity.

The early days of the internet when antivirus software was the only protection from online threats are long gone. New tools like Endpoint Detection and Response (EDR) have been developed to fill the gap as antivirus grew unable to stop newer forms of cyberattacks like malware.

But even traditional EDR has its weaknesses—most notably that it only registers threats once they have penetrated your system. Your organization needs a Zero Trust endpoint security solution that stops threats before they execute in your environment.

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

We built the ThreatLocker® Zero Trust Endpoint Protection Platform because it is impossible to stay ahead of every threat. So, with ThreatLocker, we flipped the script. Instead of chasing cybercriminals, you block them out instead. You allow what you explicitly need and trust. Everything else? Block by default.

There's nothing traditional about ThreatLocker or our 24/7/365 Cyber Hero® Team, responding in about 60 seconds. Our proactive, policy-driven security is designed to simplify your operations and securely lock down your environment. It's all backed by industry-redefining, world-class support from real humans who know how to act fast when it matters most to you.

THREATLOCKER® PROTECT

Application Allowlisting

ThreatLocker Application Allowlisting is a powerful deny-by-default solution that makes application control simple. Only trusted software runs. Everything else, including ransomware, is blocked by default. You stay in control.

- **Deploy in Learning Mode:** Automatically catalog apps and dependencies. With thousands of pre-built apps recognized, you get instant visibility, streamlined lists, and policy suggestions without manual effort.
- **Approve what you trust:** Select and approve apps with one click. Everything else, unapproved apps, scripts, or libraries, is blocked by default.
- **Easily add new apps:** Users request new app access via a popup. IT can approve, or the Cyber Hero® Team can respond in about 60 seconds.

The results? Faster Allowlisting solution deployment. Easier to scale. Lightweight and powerful.

Ringfencing™

ThreatLocker Ringfencing is your application containment strategy. It allows trusted apps to run, but only interact with the files, registry keys, network resources, or apps they actually need. It ensures apps do only what they're supposed to, nothing more.

- **Deploy with default protections:** Baseline policies apply instantly for common apps like Microsoft Office, PowerShell, and Zoom; no setup required.
- **Customize with precision:** Want PowerShell to run but stay offline? Or Word to open docs without launching other apps? You set the rules.

Bonus: The ThreatLocker 24/7 Cyber Hero Team helps fine-tune policies, fast, with about 60-sec response. The results? Less risk. Tighter control. No more application overreach.

Network Control

ThreatLocker Network Control is a host-based firewall built for endpoints and servers, giving you full command over all network traffic. Lock down access by port, source IP, or dynamically with ACLs that automatically update as IP addresses change. In short: You decide who gets in, and everyone else gets nothing. Network Control puts you in command.

- Set firewall policies for every endpoint from one console.
- When a connection request comes in, ThreatLocker checks if the device is authorized.
- If it is, the port opens automatically. If not, the door stays closed and invisible.
- Once an authorized connection ends, the port automatically closes within minutes.

The results? Safer environment and more protection from rogue network traffic.

MORE WAYS TO POWER UP YOUR ZERO TRUST STRATEGY

Explore additional tools that make your Zero Trust environment smarter, safer, and easier to manage.

Storage Control

Prevent breaches with granular storage control

ThreatLocker Storage Control puts you in the driver's seat, giving you complete control over what data can be accessed, when, and how. Set precise policies based on users, applications, devices, and context across local folders, network shares, USB devices, and cloud storage.

Nothing gets through unless it meets your security rules. The result? Stronger protection against data breaches, insider threats, and unauthorized access.

Elevation Control

Stop admin privilege abuse: Elevate apps, not users

ThreatLocker Elevation Control stops local admin privilege abuse by granting elevated rights to applications—not users. Approved apps run with elevated privileges. Users never need full local admin access. Need to elevate a new app? It's a simple one-click request, no admin credentials required. Plus, Elevation Control can remove unnecessary or unused admin accounts and eliminates the need for admins to enter credentials on standard endpoints. Fewer privileges for fewer risks and more control.

Configuration Manager

Enforce best-practice security from one powerful console

ThreatLocker Configuration Manager puts you in full control with a single, centralized console to enforce best-practice security policies on any device, whether it's connected to a single Active Directory or not. Easily set and manage configuration policies per device, group, organization, or across your entire environment. From one powerful interface, you can quickly lock down settings like disabling Universal Plug and Play, blocking SMBv1, enforcing automatic lock policies, and much more. Simplify management, strengthen security, take control.

Detect

Detect and neutralize threats instantly

ThreatLocker Detect is a powerful, policy-driven Endpoint Detection and Response (EDR) solution engineered to instantly identify, react to, and isolate threats, automatically and in real time. It relentlessly analyzes telemetry, behavioral patterns, and Indicators of Compromise (IoCs), springing into action the moment any suspicious activity is detected. Say goodbye to critical time delays and say hello to rapid threat neutralization.

Cloud Detect

Harden Microsoft 365 against threats

ThreatLocker Cloud Detect extends deep into your Microsoft 365 environment, giving you powerful visibility and control. It continuously monitors M365 logs and flags real threats, like leaked credentials, suspicious sign-ins, impossible travel, and risky behavior that often goes unnoticed.

Best of all, you set the rules. With fully customizable policies using Microsoft 365 and Graph API log fields, Cloud Detect alerts you promptly, so you can respond faster and stay ahead of evolving threats.

Cyber Hero® MDR

Elite threat response in about 60 seconds

ThreatLocker Cyber Hero MDR is a fully Managed Detection and Response (MDR) service built around ThreatLocker Detect. It gives you a direct line to our elite Cyber Hero Team, trained security pros who monitor alerts, validate threats, and act fast based on your playbook. How fast? We respond in about 60 seconds, faster than anyone else in the industry. While others are still syncing telemetry to the cloud, we're already isolating compromised devices and stopping threats before they spread.

Cloud Control

Protect Microsoft 365 from phishing and token theft

Your new powerful ally to protect your Microsoft 365 tenant against phishing attacks and token thefts. With a state-of-the-art built-in intelligence capability at its core, ThreatLocker Cloud Control automatically tracks your users' protected devices, records their IP addresses, and determines with high precision the trusted connections. It keeps you in the know. No more manual updates.

Patch Management

Simplify patching with automated, centralized management

ThreatLocker Patch Management acts as a vigilant guard, constantly scanning your devices for outdated applications and identifying those in need of patching. It takes care of the tedious work, eliminating the need to check multiple sources for different alerts by consolidating everything into one place for seamless management. Instead of spending time researching and deciding on every pending patch—what, when, and how—Patch Management handles it all for you.

Insights

Powerful endpoint intelligence for smarter security decisions

ThreatLocker Insights taps into data from millions of endpoints worldwide, giving you a clear view of application usage and adoption trends. By benchmarking real-world data and decisions from IT professionals like you, Insights empowers you to make smarter, faster security choices, helping you ensure your network stays protected without guesswork and grueling research. You save hours—possibly days—of tedious research, eliminate guesswork, and future-proof your environment by making the best decisions to strengthen your security posture.

Web Control

Block phishing and protect every device on your network

ThreatLocker Web Control makes it simple to manage web access without relying on additional third-party tools. It blocks phishing threats with real-time intelligence and enforces policies across both managed and unmanaged devices.

Extensive, auto-updating libraries and pre-organized categories let you easily block unwanted sites. Users are redirected to a company page (not a DNS redirect), avoiding certificate errors and confusion. Need an exception? Create exclusions in just a few clicks.

Web Control also applies your policies to personal and guest devices on your network, reducing risk and helping you stay compliant with GDPR, HIPAA, and PCI DSS—with less effort.

User Store

Cut support requests and stop shadow IT

The ThreatLocker User Store is a catalog of pre-approved applications that empowers users to run the apps they need without compromising your cybersecurity posture or creating unnecessary work for IT.

Once configured, the User Store acts as a centralized hub for both app approval and license key management. It actively manages access and allocates license keys, so users can easily install approved software without delays or extra support requests.

No more back-and-forth between users and IT. No more risk of shadow IT or unauthorized installs. Users get what they need to stay productive without jeopardizing security or breaking Zero Trust principles.

About ThreatLocker®

ThreatLocker is a Zero Trust Endpoint Protection Platform that improves enterprise-level server and endpoint security with Zero Trust controls, including: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker Detect, Elevation Control, and Configuration Manager.

sales@oldpueblosecuritygroup.com

+1-520 - 372-5377

Oldpueblosecuritygroup.com