THREATLOCKER

SOLUTIONS OVERVIEW

TITAN
DATA SOLUTIONS

How ThreatLocker® Protects Your Business

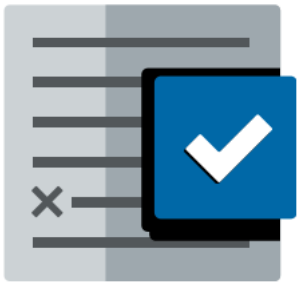
ThreatLocker® is a Zero Trust endpoint protection platform that provides enterprise-level cybersecurity to organizations globally. Instead of relying heavily on detection methods and chasing threats, the ThreatLocker® solutions block everything that is not explicitly trusted and limit actions to only what is needed.

“Zero Trust security is much more effective than detection tools,. The ThreatLocker® Zero Trust philosophy extends beyond Allowlisting to incorporate controlling what permitted applications can do, what storage areas can be accessed and how, and what network connections can be made. Denies and allows are recorded in real time in a Unified Audit to assist with compliance and ThreatLocker® Detect utilizes this real-time data to alert you of any blocked malicious action.

The ThreatLocker® endpoint protection platform is designed to be easy to use and integrate seamlessly into existing IT environments. Our innovative Learning Mode and rapid response time of the 24/7/365 Cyber Hero Support Team makes onboarding and implementing ThreatLocker® a streamlined process.

Application Allowlisting

Application Allowlisting denies all applications from running except those that are explicitly allowed. This means untrusted software, including ransomware and other malware; will be denied by default.

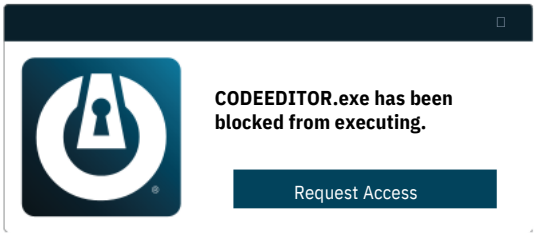


HOW DOES IT WORK?

When the agent is first installed, it operates in Learning Mode. During this period, all applications and their dependencies found on the computer are cataloged and polices are created to permit them. After the learning period, the IT administrator can review the list of applications, remove those that are not required, and secure the computer. Once the computer is secured, any untrusted applications, script or library that try to execute will be denied. The user can request new software from the IT administrator and it can be approved in 60 seconds.

WHY ALLOWLISTING?

Application Allowlisting has long been considered the gold standard in protecting businesses from known and unknown malware. Unlike antivirus, Application Allowlisting put you in control of what software, scripts, executables, and libraries can run on your endpoints and servers. This approach not only stops malicious software, but also stops other unpermitted applications from running. This process greatly minimizes cyber threats and other rogue applications running on your network.



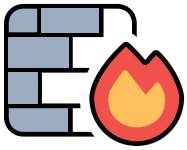
ELIMINATE THE RISK AND GUESSWORK

In addition to Allowlisting, ThreatLocker's Testing Environment is a powerful tool that allows for risk-assessed approvals that eliminate the guesswork. The Testing Environment enables administrators to quickly verify an application, providing the critical and timely information needed to make the best decision for their organization.

FEATURES

Allowlisting

Using the ThreatLocker® solution, you can deny any application from running on your device that is not a part of the allowlist. This helps to mitigate and stop cyberattacks from happening on your devices or across your network.



Firewall-like Policies

A powerful firewall-like policy engine that allows you to permit, deny or restrict application access at a granular level.

Time-Based Policies

Permit access to applications for a specified amount of time. Automatically block the application after the policy has expired.

Built-In Applications

ThreatLocker® automatically adds new hashes when application and system updates are released, allowing your applications to update without interference while preventing updates from being blocked.

Testing Environment

ThreatLocker® Testing Environment utilizes a Virtual Desktop Infrastructure (VDI) to provide administrators with a clean, isolated, cloud-based environment to evaluate unknown or untrusted application requests. Without risking potential harm to their environment, administrators can safely execute unknown files and observe their behavior before actioning an approval request.

WHY IS THIS IMPORTANT?

When users request new applications, IT admins need to know what dependencies the application requires and validate the application to ensure it's not doing anything it shouldn't be. ThreatLocker® Testing Environment gives IT admins visibility of a file's behavior before they decide whether to permit the requested application without putting their organization at risk. It also catalogs all dependencies within the installer, so the IT admin does not need to use Installation or Learning Mode on the user's computer.

HOW DOES IT WORK?

Directly from an Approval Request, IT admins can catalog files using the Testing Environment instead of placing one of their computers into Installation Mode, keeping their environment secure. ThreatLocker® will spin up a clean, temporary VDI to install the requested file. ThreatLocker® Testing Environment will evaluate the file's safety based on industry knowledge and observed file behavior. It will provide the information admins need to decide the best course of action for their specific organization.

Fig. 1

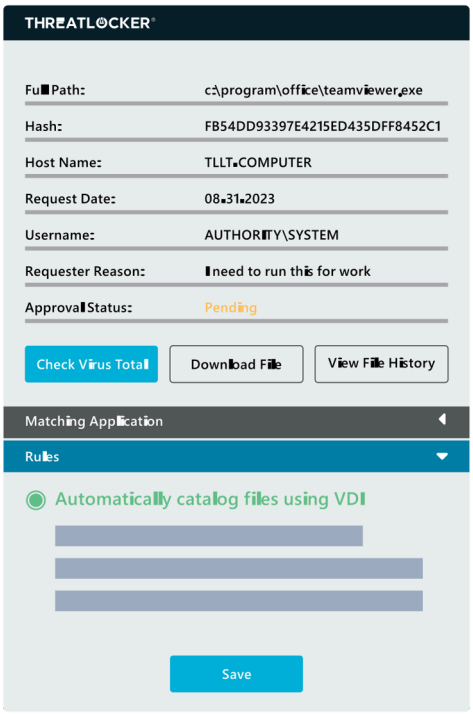
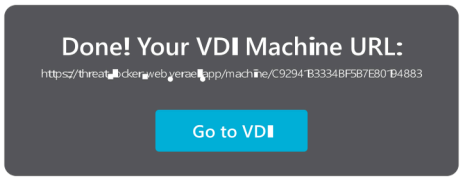


Figure 1: Shows an Approval Request with "Automatically cataloged files using VDI" selected.



FEATURES

File Evaluation

ThreatLocker® Testing Environment automatically evaluates the requested file and all its dependencies. Each file is checked using VirusTotal to leverage the knowledge of the antivirus community. Any flagged files, along with their threat classification, will be displayed.

File Behavior

Along with evaluating potential known malicious behavior, the files will be observed in real-time, revealing any unexpected behavior. The Testing Environment will show if the files are attempting to interact with the registry, make system changes, or reach out to the internet.

Real-time Audit

ThreatLocker® Testing Environment provides an on-screen real-time audit of file activity on the VDI, including any new files being created.

Canaries

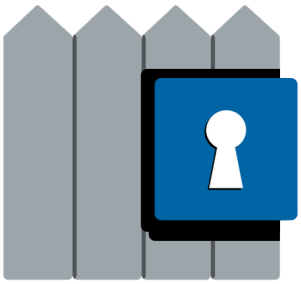
The ThreatLocker® Testing Environment contains simulated confidential data and automatically monitors access to that data. Malicious applications often look at these canary files, and the Testing Environment provides visibility of this behavior.

Permit or Discard Based on Observation

Given the information uncovered by the Testing Environment, IT admins can be confident in making a well-educated decision to permit or discard the requested application.

Ringfencing™

Ringfencing™ controls what applications are able to do once they are running. By limiting what software can do, ThreatLocker® can reduce the likelihood of an exploit being successful or an attacker weaponizing legitimate tools such as PowerShell.



Ringfencing™ allows you to control how applications can interact with other applications. For example, while both Microsoft Word and PowerShell may be permitted, Ringfencing™ will prevent Microsoft Word from being able to call PowerShell, thus preventing an attempted exploit of a vulnerability such as the Follina vulnerability from being successful.

WHY IS THIS IMPORTANT?

Under normal operations, all applications permitted on an endpoint have the same access as the operating user: data, applications, the network, and the registry. If compromised, an attacker can use the application to steal or encrypt files, abuse legitimate tools, communicate with malicious IPs, and make changes to the registry. Ringfencing™ allows you to create boundaries to permit applications access to only what they need.

HOW DOES IT WORK?

When you first deploy Ringfencing™, your device will automatically be aligned with the default ThreatLocker® policies. These policies are then automatically applied to a list of known applications such as Microsoft Office, PowerShell, or Zoom. The default policies aim to provide a baseline level of protection for all endpoints. Policies can be created and changed to fit any environment. Our dedicated Cyber Hero Team is always on hand to support any requests, 24/7/365.

Fig. 2

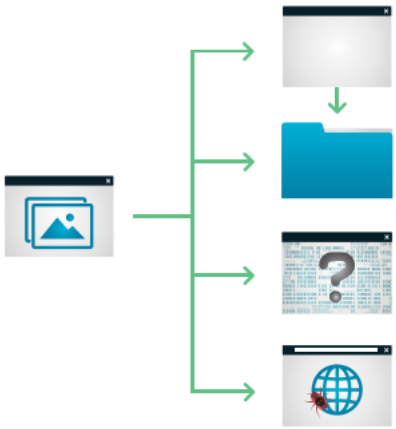


Fig. 3

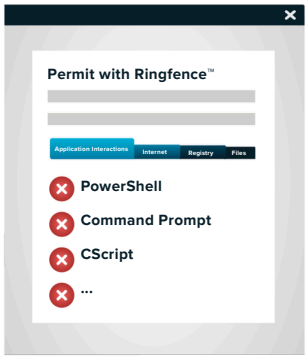


Figure 2: Demonstrates the Application Control Policies page, containing a list of Application policies. Figure 3: Demonstrates a partial policy list. The yellow fence icons appear beside Permit with Ringfence™ policies.

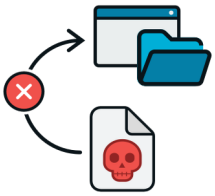
FEATURES

Mitigate Against Fileless Malware

Stop fileless malware by limiting what applications are allowed to do.

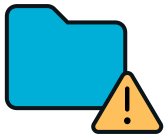
Granular Application Policies

Stop applications from interacting with other applications, network resources, registry keys, files, and more.



Limit Application Attacks

Limit application attacks like application hopping by limiting what applications can access.



Limit Access To Your Files

The average computer has over 500 applications, and only a handful of those need to access your files. With Ringfencing™, you can choose which applications need to see which files.

Storage Control

Storage Control provides policy-driven control over storage devices, whether the storage device is a local folder, a network share, or external storage. ThreatLocker® Storage Control allows granular policies to be set, which could be as simple as blocking USB drives, or as detailed as blocking access to your backup share, except when accessed by your backup application.

DIGITAL TRAIL WITH UNIFIED AUDIT

Unified Audit provides a central log of all storage access by users on the network and those working remotely, right down to the files that were copied and the device's serial number.

Fig. 4

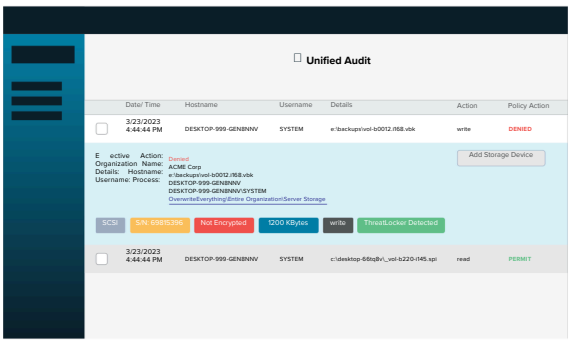


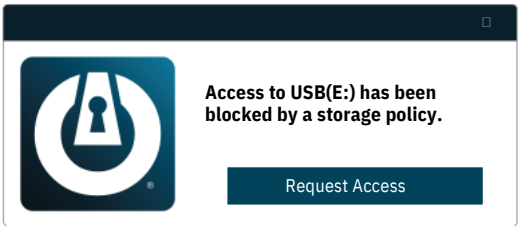
Figure 4: Demonstrates the Unified Audit page with a Storage Control Entry expanded, showing that the write access was denied.

HOW DOES IT WORK?

Policies can be created to permit or deny access to storage locations based on the user, window of time, type of file, and the application in use. When a storage device or location is blocked, a user will be presented with a pop-up where they can request access to the device or location. The administrator can then permit the storage device in as little as 60 seconds.

WHY IS THIS IMPORTANT?

As a high-value target for threat actors, protecting data from unwanted access is important. ThreatLocker® Storage Control enables the creation of granular policies to permit and deny access to network shares, local folders, and external storage by specific users or applications, and to enforce encryption on external storage devices.



FEATURES

Audit Access to Files

A full detailed audit of all file access on USB, Network, and Local Hard Drives is centrally accessible within minutes of a file being opened.

Granular Storage Policies

These policies allow or deny access to storage based on user, time, applications, and more.

Simple Requests for Access

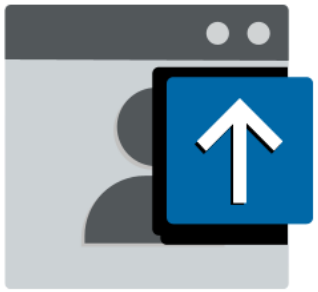
Upon denial due to policy, a pop-up appears to provide the user an option to request access to the storage device.

Simple USB Blocking

USB Policies allow access based on device serial number, vendor, and/ or file type.

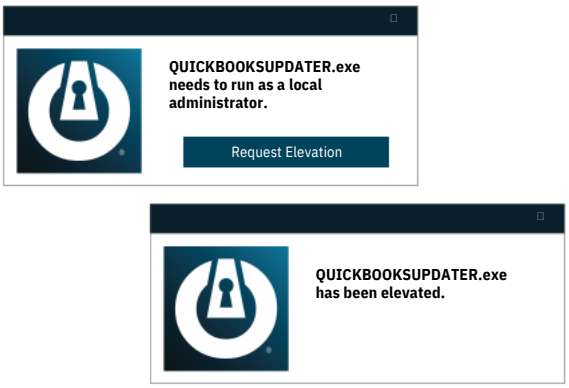
Elevation Control

Elevation Control enables users to run specific applications as a local administrator, even when they do not have local admin privileges. Elevation Control puts IT administrators in the driving seat, enabling them to control exactly what applications can run as a local admin without giving users local admin rights.



HOW DOES IT WORK?

When ThreatLocker® is first deployed, all existing applications are learned. Administrators can review the applications and select which can be run as a local administrator. Once enabled, a user can run the software as a local administrator without entering any credentials.



WHY IS THIS IMPORTANT?

Local administrator credentials are a sought-after target for cybercriminals. An attacker who has gained access to a user's endpoint with local admin rights can impersonate other logged-on users or exploit tools locally, potentially pivoting into the entire network. Elevation Control enables IT administrators to eliminate the possibility of these credentials being hijacked and used against them without hampering productivity.

FEATURES

Complete Visibility of Administrative Rights

Gives you the ability to approve specific applications to run as an administrator, even if the user is not a local administrator.

Streamlined Permission Requests

Users can request permission to elevate applications and attach files and notes to support their requests.

Varied Levels of Elevation

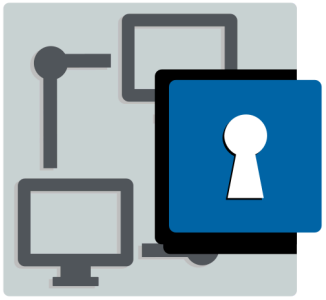
Enables you to set durations for how long users are allowed access to specific applications by granting either temporary or permanent access.

Secure Application Integration

Ringfencing™ ensures that users cannot jump to infiltrate connected applications within the network once applications are elevated.

Network Control

ThreatLocker® Network Control is an endpoint and server firewall that enables you to have total control over network traffic, which ultimately helps you to protect your devices. Using custom-built policies, you can allow granular access based on IP address, specific keywords, or even agent authentication or dynamic ACLs.



WHY IS THIS IMPORTANT?

The corporate firewall is no more. Users are not only working from the office but also remotely, meaning that the network we all utilize has quickly become the internet. This dissolution of the perimeter leaves devices and data vulnerable and exposed to cyber threats. This is why you need controls on network traffic in place to protect your device and, by extension, your data. You can achieve this by implementing a Network Control solution.

HOW DOES IT WORK?

Network Control enables you to set firewall policies for all endpoints from a single location. Control network traffic using on-demand port control. Once a connection request is received, ThreatLocker® checks to see if the requesting endpoint is permitted to make that connection. If permission is verified, ThreatLocker® will open the requested port on the device. Unapproved devices will not have visibility of the open port. Once an authorized device is no longer using the open port, it will automatically close within 5 minutes.

Fig. 5

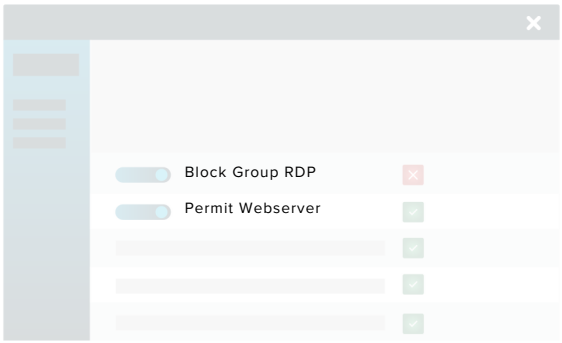


Figure 5: Depicts a partial Network Control policy list.
Figure 6: Depicts a partial Network Control policy.

Fig. 6

FEATURES

Configurable

Using global and granular policies, Network Control allows users to configure network access to endpoints.

Cloud - B ased

The cloud-managed solution provides customers with a centralized view of endpoint policies and network traffic across your organization.

Dynamic

Network Control enables users to deny all traffic to published servers while only allowing a single computer by IP address or dynamically using a keyword. This is great for a user who is often traveling.

Enhanced Network Security

Ensure rogue devices on your network cannot access your servers or endpoints with Dynamic ACLs.

ThreatLocker® Detect

ThreatLocker® Detect identifies and detects anomalies within an environment. Unknown vulnerabilities in an environment could leave the environment susceptible to a cyberattack.

ThreatLocker® Detect uses the telemetry data collected across all the ThreatLocker® modules to identify and respond to potential indicators of compromise or weakness in the environment. For example, if a business uses a vulnerable version of Microsoft Exchange, ThreatLocker® will warn the admin that they are running a known vulnerable version of MS Exchange. Whereas if an attempted breach occurs based on this vulnerability, Detect can take automatic remediations to respond and harden the environment. At the same time, ThreatLocker® Application Control will block the execution of malicious payloads.

WHY IS THIS IMPORTANT?

Building upon the ThreatLocker® zero trust deny first approach, ThreatLocker® Detect provides additional functionality to combat and mitigate the exploitation of known and unknown vulnerabilities. While zero trust effectively reduces the likelihood of a successful cyberattack, ThreatLocker® Detect further hardens an environment by notifying and automatically responding to identifiers of attempted compromise in the event of an attack. Suppose a cybercriminal gains access to a server through remote access software used by a business and then tries to connect to IP addresses associated with Royal ransomware; using IOCs, ThreatLocker® Detect alerts the admin that their server is trying to communicate with known malicious IPs while isolating the offending server from the network.

HOW DOES IT WORK?

ThreatLocker® Detect uses telemetry data and personalized policies to communicate with admins and respond to potential threats. The ThreatLocker® team has created and maintains ThreatLocker® Detect policies for many known indicators of compromise. When the IOCs change, the policy will be automatically updated to reflect those changes. New policies will be added as ThreatLocker® observes and responds to real-world malware events. IT admins can share and adopt ThreatLocker® Detect policies using the ThreatLocker® Community.

NEW ADD-ON

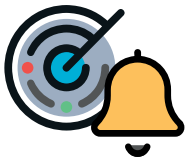
Cyber Hero Managed Detection & Response

The CHMDR is an add-on to ThreatLocker® Detect (previously known as Ops) that enables organizations to opt for ThreatLocker® Cyber Heroes to monitor and respond to Indicators of Compromise (IoC).

In the event an attacker is on your device, the Cyber Hero will follow the customer's runbook to either isolate or lock down the device and notify the customer. They will be able to identify additional information for the customer, including:

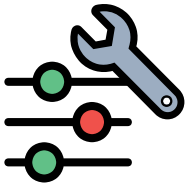
- **What the threat was**
- **How initial access was gained**
- **Where the threat originated**
- **What the threat attempted to do**
- **How the threat was blocked & mitigated**

FEATURES



Alert and Detect

ThreatLocker® Detect will detect and notify admins of suspicious behavior based on customizable thresholds and notification methods. Using industry- known indicators of compromise, ThreatLocker® Detect can detect and alert IT professionals that their organization may be under an attempted attack.



Set Custom Thresholds

Based on an organization's risk appetite, ThreatLocker® Detect policies can be tailored to alert and respond differently based on the threat level to reduce alert fatigue. Seeing an IP scanner trying to run may not be considered a threat but combine the behavior with multiple attempts to RDP to other servers, and the threat level increases. Once the threat level reaches the specified threshold, action can be taken as directed by the policy creator.

Respond

ThreatLocker® Detect policies can be set to act when specific behaviors are observed, or thresholds are reached. IT admins can set ThreatLocker® Detect policies to enable, disable, or create Application Control, Storage Control, or Network Control policies in response to specified observations, like shutting down the RDP port in response to failed login attempts from unauthorized IP addresses.

Leverage Community Knowledge

IT admins can easily share their own ThreatLocker® Detect policies or "shop" for policies shared by their industry peers and the ThreatLocker® team.

Configuration Manager

ThreatLocker® Configuration Manager enables IT professionals to set best practice configuration policies across their environment from a single central console.

WHY IS THIS IMPORTANT?

Traditionally, companies require components of group policy from Active Directory to set Windows configurations, requiring users to be on the network or using an Active Directory domain. Today's business network is not always isolated to a single Active Directory domain, making setting and enforcing configurations difficult. ThreatLocker® Configuration Manager allows IT admins to set standardized Windows configurations, such as automatic lock policies, disabling Universal Plug and Play, and disabling autoplay, or blocking SMB v1 from one central location, whether or not the computers are connected to an Active Directory domain.

Fig. 7

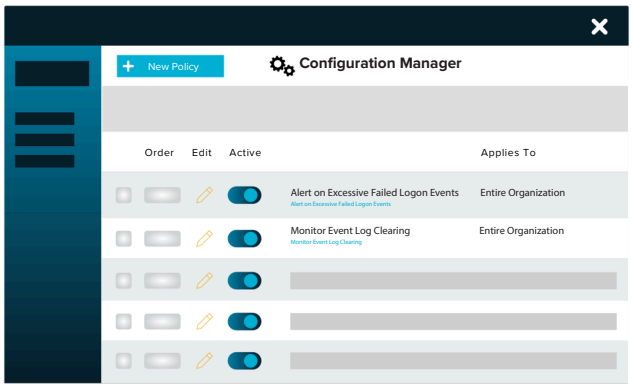


Figure 7: Demonstrates the Configuration Manager page containing a list of configuration policies.

HOW DOES IT WORK?

ThreatLocker® Configuration Manager provides a centralized, policy-driven portal where IT admins can set configuration policies per individual computer, computer group, organization, or across multiple organizations. Admins can quickly manage important security configurations from a single pane of glass.

Fig. 8

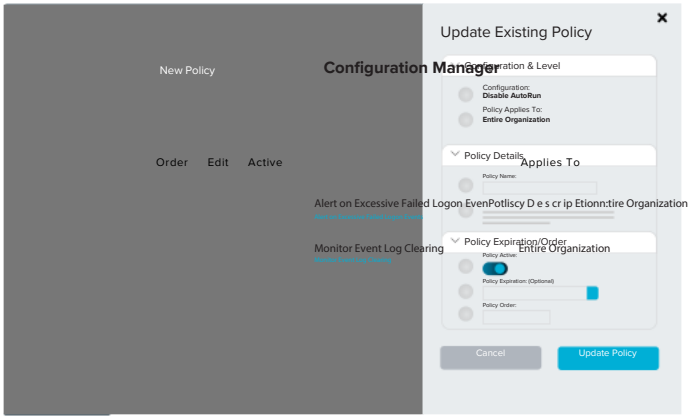
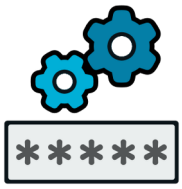


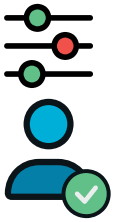
Figure 8: Demonstrates a configuration policy edit window.

FEATURES



Centralized Password Policy Configuration

Configure user password policies across an entire organization or multiple organizations from a central location. Set password requirements such as length, complexity, and change frequency from a single policy.

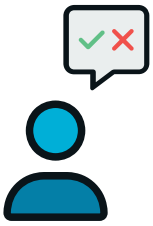


User Account Management

Disable guest and local admin accounts to harden your environment. Rename local administrator accounts and apply a unique rotating password to each computer for their local admin account, making it more challenging to compromise credentials.

Set Boundaries for MS Office

ThreatLocker® Configuration Manager provides access to disable all downloaded macros and OLE in MS Office documents. Block these common attack vectors across the entire environment quickly from within the ThreatLocker® Portal.



Control User Social Media Access

Admins can enable and disable user access to the most common social media platforms. ThreatLocker® Configuration Manager empowers IT admins to select which social media platforms are acceptable or disable all the common platforms to keep employees productive and protect their business environment.

ThreatLocker® Community

ThreatLocker® Community brings IT admins together to stay ahead of zero-day vulnerabilities and other potential threats. This feature provides a forum where admins can help each other implement a proactive strategy for protecting their endpoints through shared or suggested policies created by ThreatLocker® or approved contributors. This pooled knowledge from countless organizations and use cases will help IT admins effectively secure their environments.

WHY IS THIS IMPORTANT?

The threat landscape is ever evolving, making cooperating with other cybersecurity professionals a necessity. This newly added feature to the ThreatLocker® platform allows IT admins to adopt policies tested and used by their peers instead of creating their own, streamlining and simplifying their workflow.

HOW DOES IT WORK?

ThreatLocker® Community allows ThreatLocker® users to create and share policies for the benefit of the collective. Users can follow policy creators to see their posts and subscribe to policies they want to use in their environment. With ThreatLocker® Community, IT admins can reduce their workload by adopting policies used by fellow cybersecurity professionals.

Fig. 9

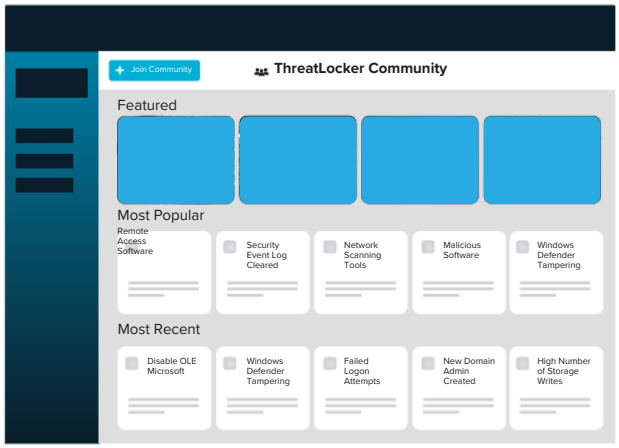


Figure 9: Demonstrates the ThreatLocker® Community page displaying policies shared by community members. Users can select from this screen to adopt policies in their own organization.

Fig. 10

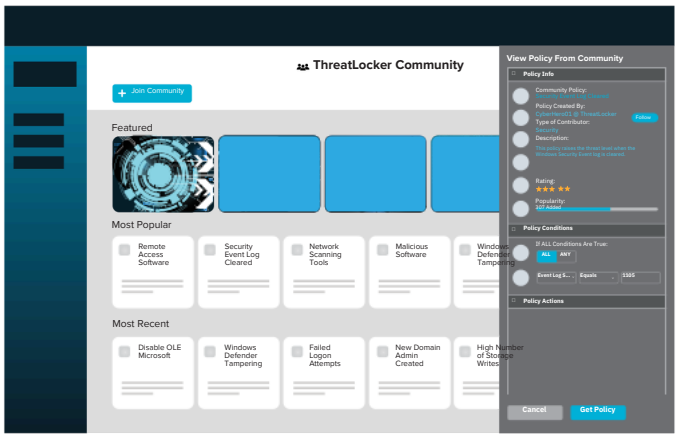


Figure 10: Demonstrates the ThreatLocker® Community page with a shared policy open.

FEATURES

ThreatLocker® Community

Harness the expertise of ThreatLocker® users around the globe to share policies for various use cases, like Ringfencing™ accounting software to only access a single folder, to prevent known and unknown exploits.

Become a Contributor

Apply to become a community contributor, create dynamic policies, and share them with the ThreatLocker® Community. Contributors can publish policies that may be helpful to other IT professionals in the same vertical, like policies that only permit backup software to access backup files, Ringfence™ common business applications from interacting with one another, or permit coding software in only a development environment.

Policy Rating

Rate policies created by other ThreatLocker® contributors and have your shared policies rated. Policies that are useful and highly rated within the community are showcased, and poorly rated policies move closer to the bottom of the list.

TITAN
DATA SOLUTIONS

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 & Configuration Manager.