THREATLOCKER®
ZERO TRUST PLATFORM

SOLUTIONS OVERVIEW

The Zero Trust Platform
that prevents ransomware

threatlocker.com

Transform your business security with powerful protection

ThreatLocker® is a Zero Trust Platform that provides enterprise-grade cybersecurity to organizations globally. Unlike traditional detection-based approaches, ThreatLocker proactively blocks all untrusted actions, limiting it to only what is needed.

The ThreatLocker Zero Trust philosophy extends beyond Allowlisting by controlling the actions of permitted applications, regulating access to storage areas, and managing network connections. All denies and allows are recorded in real-time within the Unified Audit to support compliance efforts. Additionally, ThreatLocker Detect utilizes this real-time data to alert you to any blocked malicious activities.

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

Available On:

Coming Soon:

ThreatLocker® Protect

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 policies 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, scripts, or libraries that try to execute will be denied. The user can request new software from the IT administrator, which 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 - including ransomware. Unlike antivirus, Application Allowlisting puts you in control of what can run on your endpoints and servers. This approach not only stops malicious software, but also stops other unpermitted applications from running. This process minimizes cyber threats and other rogue applications from running in your network.

WHAT IS THE USER EXPERIENCE?

When a user wishes to add new software to your environment, they will receive a pop-up notifying them that the software was blocked. The user will be able to see information about the program, including where it was developed and what data access it is requesting.

Fig. 1

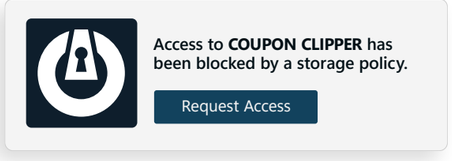


Figure 1: Pop-up shows the request was blocked by Storage Control.

Figure 2: Pop-up shows a request for a program to run.

BENEFITS

Firewall-like Policies

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

Built-in Application Definitions

Predefined lists of applications that include all dependencies and updates tracked by ThreatLocker®.

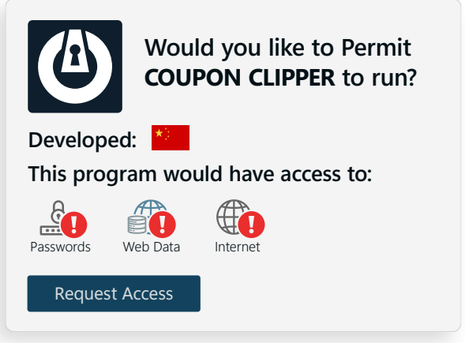
Time-based Policies

Temporarily permit software and automatically block after the policy expires.

Malware Blocking

Unlike antivirus, Allowlisting blocks both known and unknown malware from running.

Fig. 2

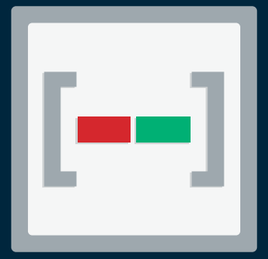


Available On:

ThreatLocker® Protect

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 administrators 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 administrators 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 administrators 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 run 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 administrators need to decide the best course of action for their specific organization.

Fig. 3

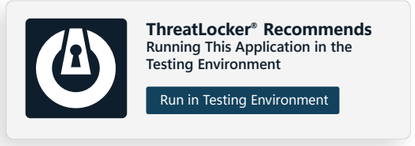
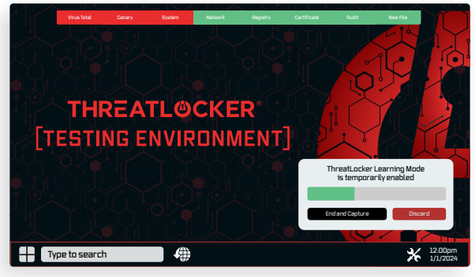


Fig. 4



BENEFITS

Canaries

Bait files that include simulations of real data. The testing environment will monitor for access or changes to those files.

Real-time Audit

Provides an on-screen real-time audit of file activity within the testing environment, including any new files being created.

Application Behavior

Applications will be monitored in real-time for unexpected behavior, such as registry interactions, system changes, or internet access, while also evaluating known malicious behavior.

Application Evaluation

Each file created within the testing environment is evaluated against multiple virus databases, and the results are displayed.

Figure 3: Shows an Approval Request with a ThreatLocker® pop-up.

Figure 4: Testing Environment Interface.

Available On:

ThreatLocker® Protect

Ringfencing™

Ringfencing™ allows you to control what applications can do. 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 to other applications, files, the network, and the registry that the operating user has. 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 system. 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. 5

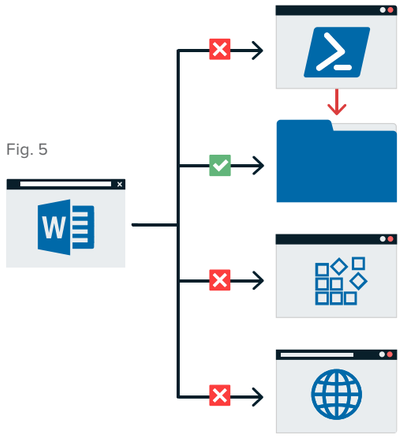


Figure 5: Ringfencing™ blocks applications from accessing other applications such as PowerShell, your data, the registry, and the internet.

Fig. 6

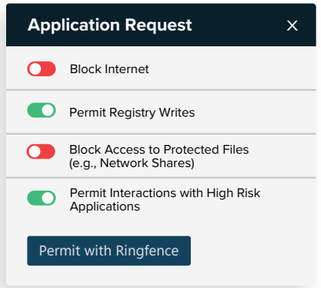


Figure 6: Excerpt from an Application Approval showing Ringfence options.

BENEFITS

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.

Available On: Coming Soon:

ThreatLocker® Protect

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 built-in policies, you can grant access based on port, source IP address, or even create dynamic ACLs that automatically update when a device changes it's IP address.

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 and 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.

DYNAMIC GEOFENCING FOR USERS

New functionality in the ThreatLocker® Mobile App and the ThreatLocker® Access App can restrict network access and other functionalities based on geolocation. The app will be a location-tracking app, allowing users to access their work Microsoft 365 account. The app's location will be used to apply conditional access to Microsoft 365 accounts*.

The ThreatLocker® Access and ThreatLocker® Mobile applications gather device IP addresses and geolocation. Administrators can use the information to create conditional access policies to allow or prevent users from accessing company Microsoft 365 resources and network locations.

*Requires Microsoft Entra ID P1 License.

Fig. 7

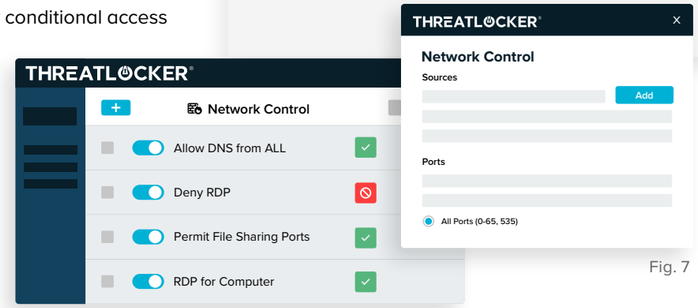


Figure 7: Depicts a partial Network Control policy list.

BENEFITS

Configurable

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

Dynamic ACLs

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.

Cloud-Based

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

Enhanced Network Security

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

Available On:

ThreatLocker® Enhancements

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 driver's seat, enabling them to control 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 credentials.

WHY IS THIS IMPORTANT?

Local administrator credentials are a sought-after target for cybercriminals. An attacker who has gained access to an endpoint with local admin rights can impersonate other logged-on users or exploit tools locally, potentially pivoting into the entire network. Elevation Control eliminates these credentials from being hijacked without hampering productivity.

Fig. 8

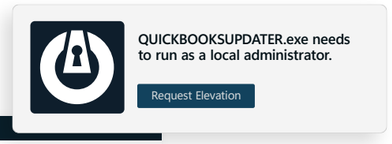


Fig. 9

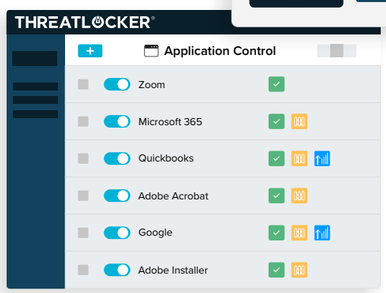


Figure 8: End user notification and request window when an application needs to run with elevated permissions.

Figure 9: Partial list of Applications with icons showing if they are permitted, with or without Ringfencing™ and Elevation.

BENEFITS

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 temporary or permanent access.

Stops Application Hopping

Ringfencing™ ensures that users cannot hop between elevated applications.

Remove Local Administrator Accounts

Automatically remove local administrator accounts not listed as exceptions.

Available On: Coming Soon:

ThreatLocker® Enhancements

Storage Control

Storage Control provides policy-driven control over storage devices, whether 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.

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 can 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, as well as to enforce encryption on external storage devices.

PROTECTING CRUCIAL DATA AND FILES

ThreatLocker® Storage Control will now include read, write, and delete actions from SharePoint and OneDrive locations. Monitoring of these actions will also be available in the ThreatLocker® Unified Audit. Additionally, ThreatLocker® administrators will be able to specify the cloud locations to monitor.

Fig. 10

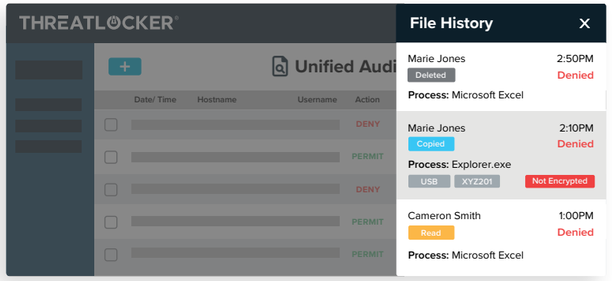


Figure 10: Shows the Unified Audit page with an entry showing that access was denied.

BENEFITS

Audit Access to Files

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

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 with an option to request access to the storage device.

Simple USB Blocking

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

Automatically Alert or Block When Thresholds are Exceeded

When used with ThreatLocker® Detect, you can automatically alert or block access if a user reads or changes too many files within a period of time. This can prevent data exfiltration or mass encryption.

ThreatLocker® Enhancements

ThreatLocker® Detect EDR

ThreatLocker® Detect is a policy-based Endpoint Detection and Response (EDR) solution. This EDR addition watches for unusual events or Indicators of Compromise (IoCs), sends alerts, and takes automated actions if an anomaly is detected.

ThreatLocker® Detect uses the telemetry data collected from the operating system and across all the ThreatLocker® modules to identify and respond to potential indicators of compromise or weakness in the environment. For example, if an attacker tries to compromise Microsoft Exchange, ThreatLocker® will notify the business of the potential exploit. Whereas if an attempted breach occurs, Detect can take automatic remedial actions 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 goes further by notifying and automatically responding to indicators of an attack. If a cybercriminal gains access to a server through remote access software used by a business and attempts to connect to IP addresses associated with Royal ransomware, ThreatLocker® Detect will alert the admin that the server is trying to communicate with known malicious IPs and will isolate the offending server from the network using IoCs.

HOW DOES IT WORK?

ThreatLocker® Detect uses telemetry data and personalized policies to communicate with administrators 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 administrators can share and adopt ThreatLocker® Detect policies using the ThreatLocker® Community.

BENEFITS

Alert and Detect

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

Leverage Community Knowledge

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

Set Custom Thresholds

Policies can be tailored to alert and respond differently based on the threat level to reduce alert fatigue.

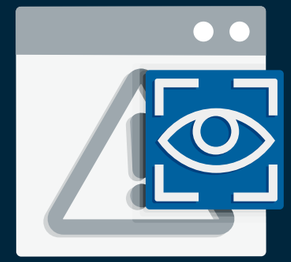
Respond

Set policies to enable, disable, or create Application Control, Storage Control, or Network Control policies in response to specified observations.

ThreatLocker® Enhancements

Managed Support for ThreatLocker® Detect EDR

Unleash the full potential of the ThreatLocker® Detect Endpoint Detection and Response (EDR) solution with managed services from the 24/7/365 ThreatLocker® Cyber Hero® Team.



Clients can opt-in for the ThreatLocker® Cyber Hero® Team to monitor and respond to Indicators of Compromise (IoC). When ThreatLocker® Detect identifies suspicious activity in your environment, the Cyber Hero® Team will review the alert to determine if there is a true IoC or a false positive. In the event of a cyber incident, 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, 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 and mitigated

Prompt Notifications 24/7/365

The 24/7/365 availability of the ThreatLocker® Cyber Hero® Team offers around-the-clock Managed Detection and Response (MDR) services to keep organizations secure and alert even outside of standard hours of operation.

The Cyber Hero® Team has an average response time of less than 60 seconds.

This metric is unique to ThreatLocker® and provides a significant advantage when responding to threats. By augmenting the ThreatLocker® Zero Trust Endpoint Protection Platform with managed detection and response services, customers can reduce agent fatigue while hardening their environment to the highest standards, ensuring the mitigation and notification of attempted attacks.

Detect Anomalies in Microsoft 365

ThreatLocker® Detect will identify unexpected and unwanted behavior in your Microsoft 365 cloud environment, which could indicate a cyberattack. ThreatLocker® Detect cloud policies will use Microsoft 365 Logs and Detect policies to communicate with ThreatLocker® administrators about any potential indicators of compromise discovered.

Policies can be customized to meet your specific requirements using any fields from the Microsoft 365 or Microsoft Graph API logs.

ThreatLocker® Detect can work with Microsoft Entra P2 to signal alerts, including, but not limited to:

Users with leaked credentials

- If a user's credentials have been compromised (e.g., due to a data breach), it raises a risk flag.

Sign-Ins from Anonymous IP Addresses

- It's considered risky when a user signs in from an IP address without proper identification.

Impossible Travel to Atypical Locations

- If a user's sign-in location is geographically implausible (e.g., sudden travel across continents), it's flagged.

Sign-Ins from Infected Devices

- If a user signs in from a device known to be infected with malware, it's considered risky.

Available On:

ThreatLocker® Enhancements

ThreatLocker® Community

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

WHY IS THIS IMPORTANT?

The threat landscape is ever-evolving, making cooperating with other cybersecurity professionals a necessity. ThreatLocker Community allows adoption of policies tested and used by peers instead of creating policies from scratch, streamlining and simplifying 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, workload is reduced by adopting policies used by fellow cybersecurity professionals.

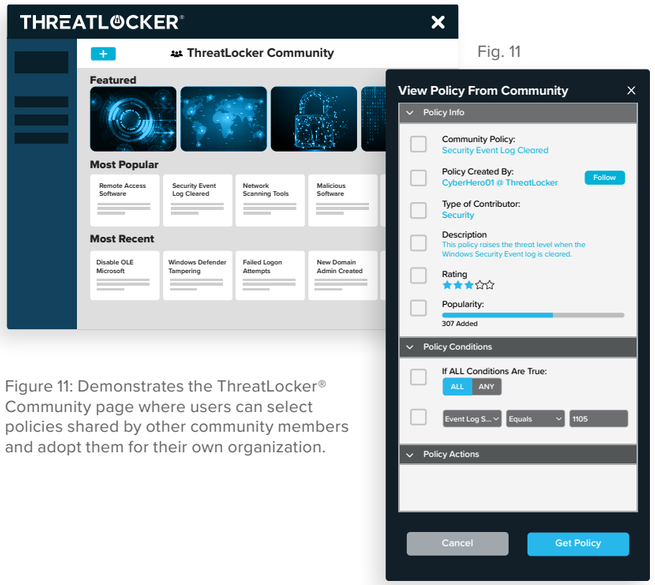


Fig. 11

Figure 11: Demonstrates the ThreatLocker® Community page where users can select policies shared by other community members and adopt them for their own organization.

BENEFITS

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.

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.

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.

Available On: Coming Soon:

ThreatLocker® Enhancements

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 administrators to set standardized Windows configurations, such as automatic lock policies, disabling Universal Plug and Play, disabling autoplay, or blocking SMB v1 from one central location, whether or not the computers are connected to an Active Directory domain.

HOW DOES IT WORK?

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

CONFIGURE MICROSOFT DEFENDER

Configure Microsoft Defender Settings in a single location for your entire organization. With Configuration Manager, you can create granular centralized policies for Microsoft Defender configuration. The configurations include all Defender settings, including Real-time Protection, Cloud Protection, and Exclusions.

Fig. 12

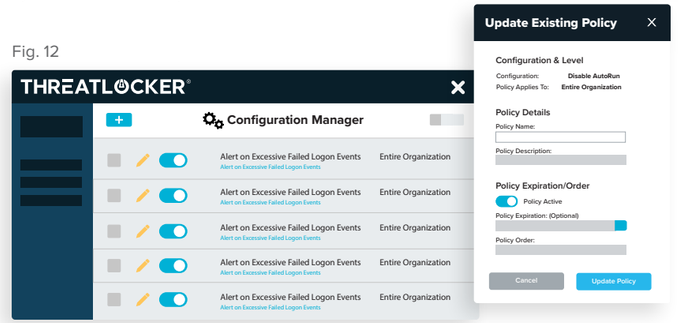


Figure 12: Demonstrates the Configuration Manager page containing a list of configuration policies.

BENEFITS

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.

Configure Microsoft Office

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

THREATLOCKER®

ThreatLocker® is a Zero Trust 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.