THREATLOCKER

ZERO TRUST ENDPOINT SECURITY

SOLUTIONS OVERVIEW

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.

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 application, script, or library that tries to execute will be denied. The user can request new software from the IT administrator, and it can be approved in 60 seconds.

Application Allowlisting has long been considered the gold standard in protecting businesses from known and unknown malware. Unlike antivirus, Application Allowlisting puts 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.

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 Application Policies

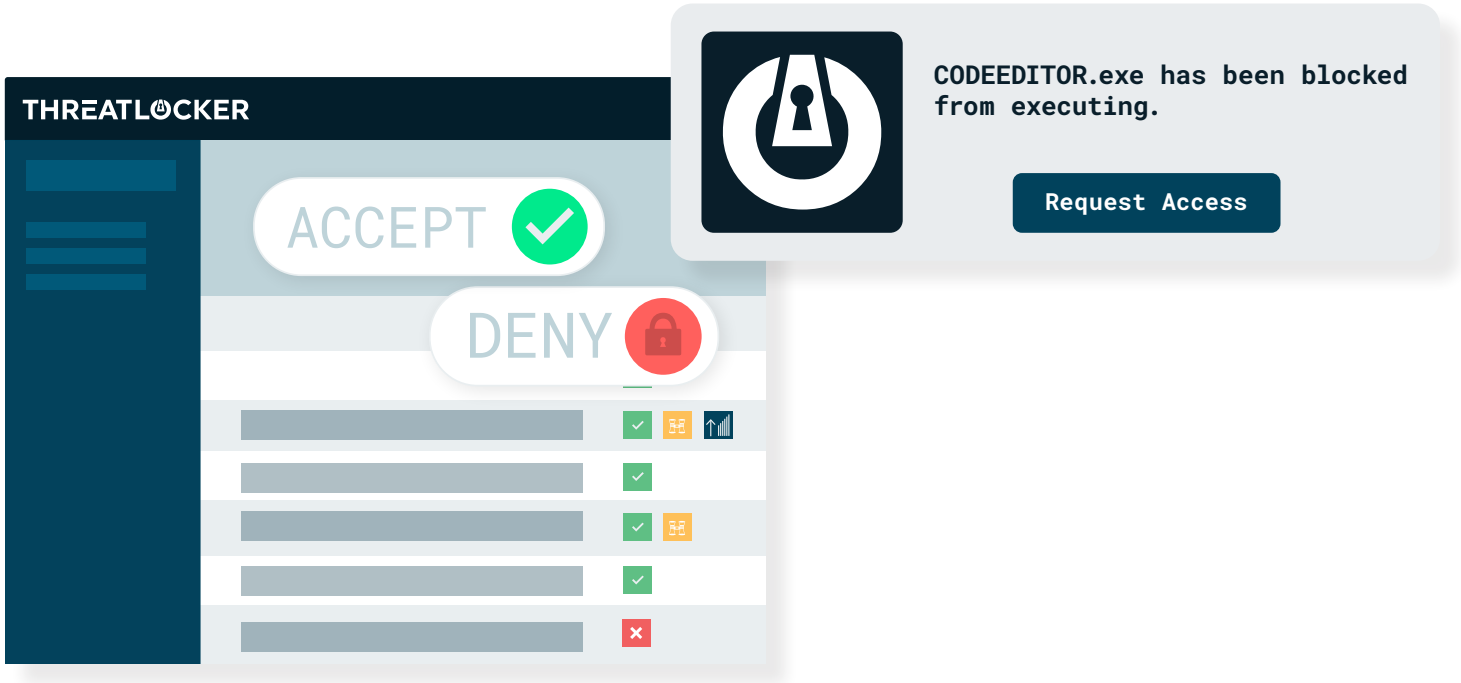
A powerful firewall-like policy engine that allows you to permit, deny or restrict application access at a granular level.

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.



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 stop Microsoft Word from being able to call PowerShell, thus preventing exploits of vulnerabilities, such as Follina, from being successful.

Under normal operations, all applications permitted on an endpoint or server are able to access all data that the operating user can access. This means if the application is compromised, the attacker can use the application to steal or encrypt files. Ringfencing™ allows you to remove file access permissions for applications that do not need access and even remove network or registry permissions.

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 aim of the default policies is to provide a baseline level of protection for all endpoints. Each of these policies can easily be manipulated to fit any environment at any time. Our team of dedicated Cyber Heroes are always on hand to support any requests, 24/7/365.

Mitigate Against Fileless Malware

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

Granular Application Policies

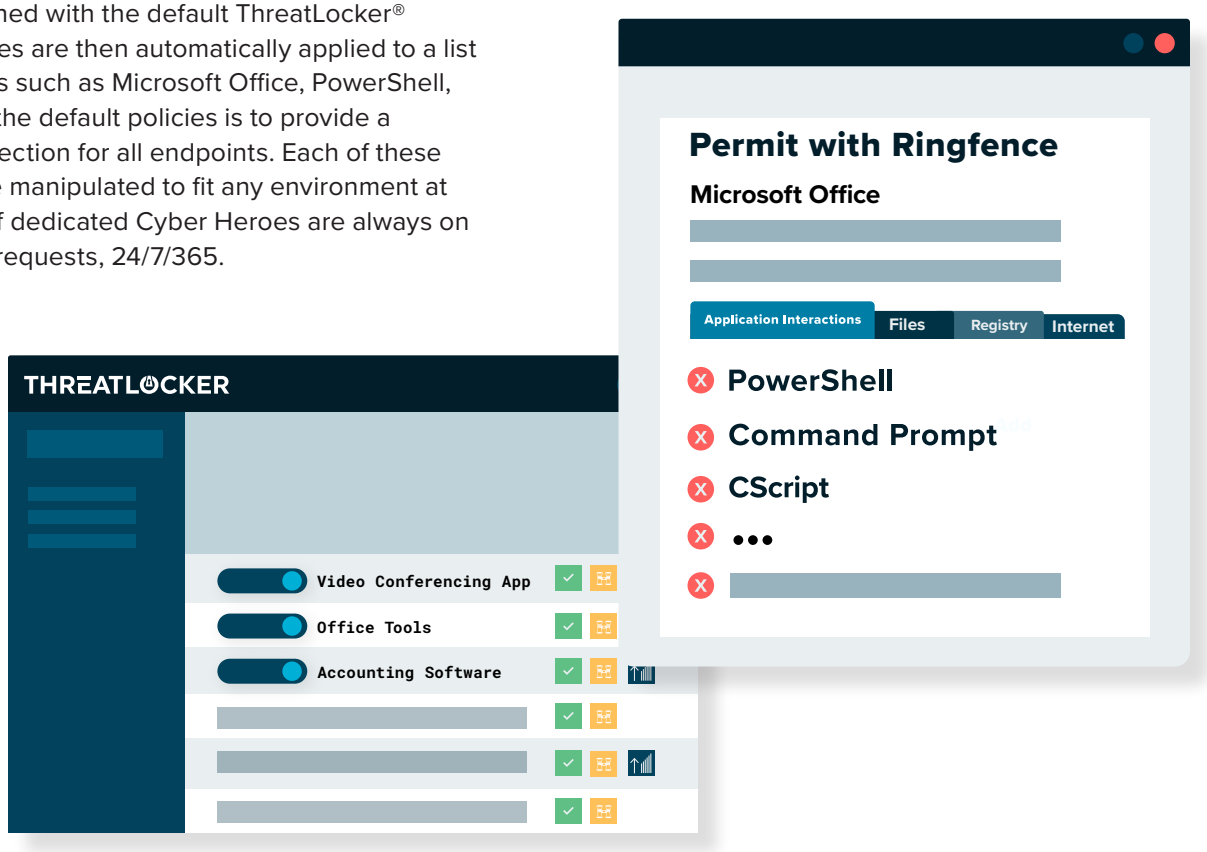
Stop applications from interacting with other applications, network resources, registry keys, files, and more.

Limit Application Attacks

Limit application attacks, such as application hopping, by controlling what applications have access to.

Limit Application 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 decide which applications need to see which files.



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.

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.

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

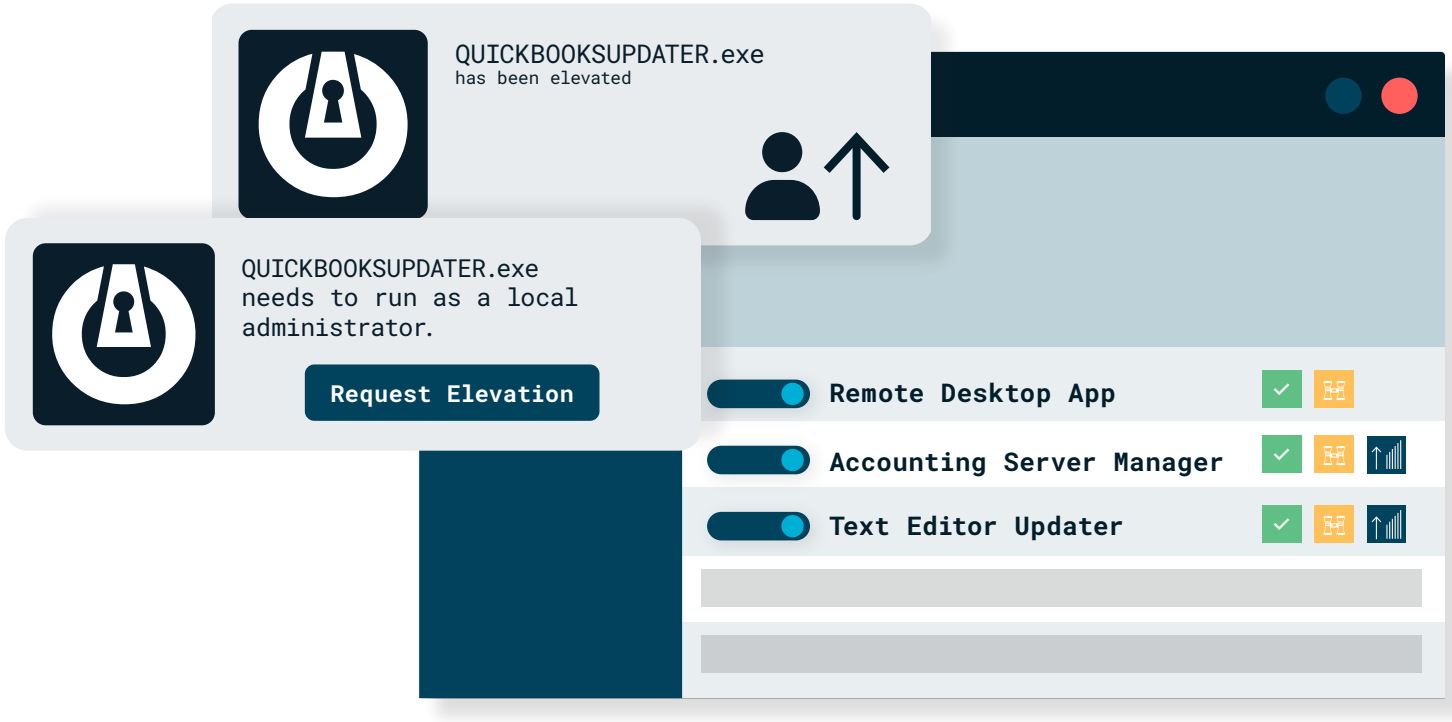
Users can request permission to elevate applications and attach files and notes to support their requests.

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 once applications are elevated, users cannot jump to infiltrate connected applications within the network.



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 such as a USB drive. 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.

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 serial number of the device.

When a storage device is blocked, a user is presented with a pop-up where they can request access to a storage device. The administrator can choose to permit the storage device in as a little as 60 seconds.

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

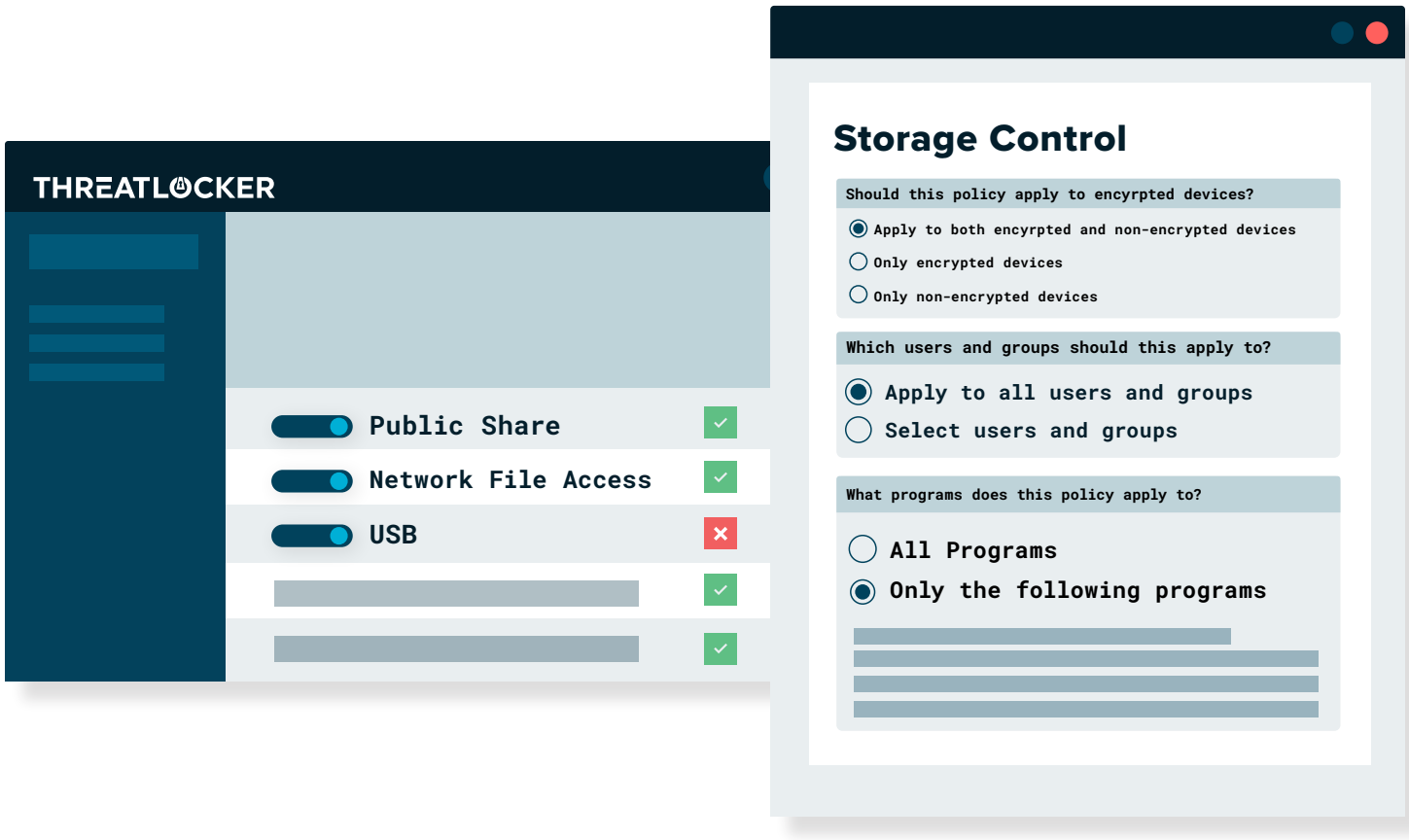
These policies allow or deny access to storage based on user, time, applications, and more.

Simple Requests for Access

The user is presented with a pop-up with the 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.



Network Access Control

ThreatLocker® NAC 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, agent authentication, or dynamic ACLs.

The local network 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 network traffic controls in place to protect your device and, by extension, your data. You can achieve this by implementing a Network Access Control solution (NAC).

Dynamic ACLs allow you to automatically open ports based on a computer's or group of computers' location at a point in time. With dynamic ACLs, the connection between server and client is direct, unlike a VPN that needs to connect through a central point.

Configurable

NAC gives users the ability to configure network access to endpoints using global and granular policies.

Cloud-Based

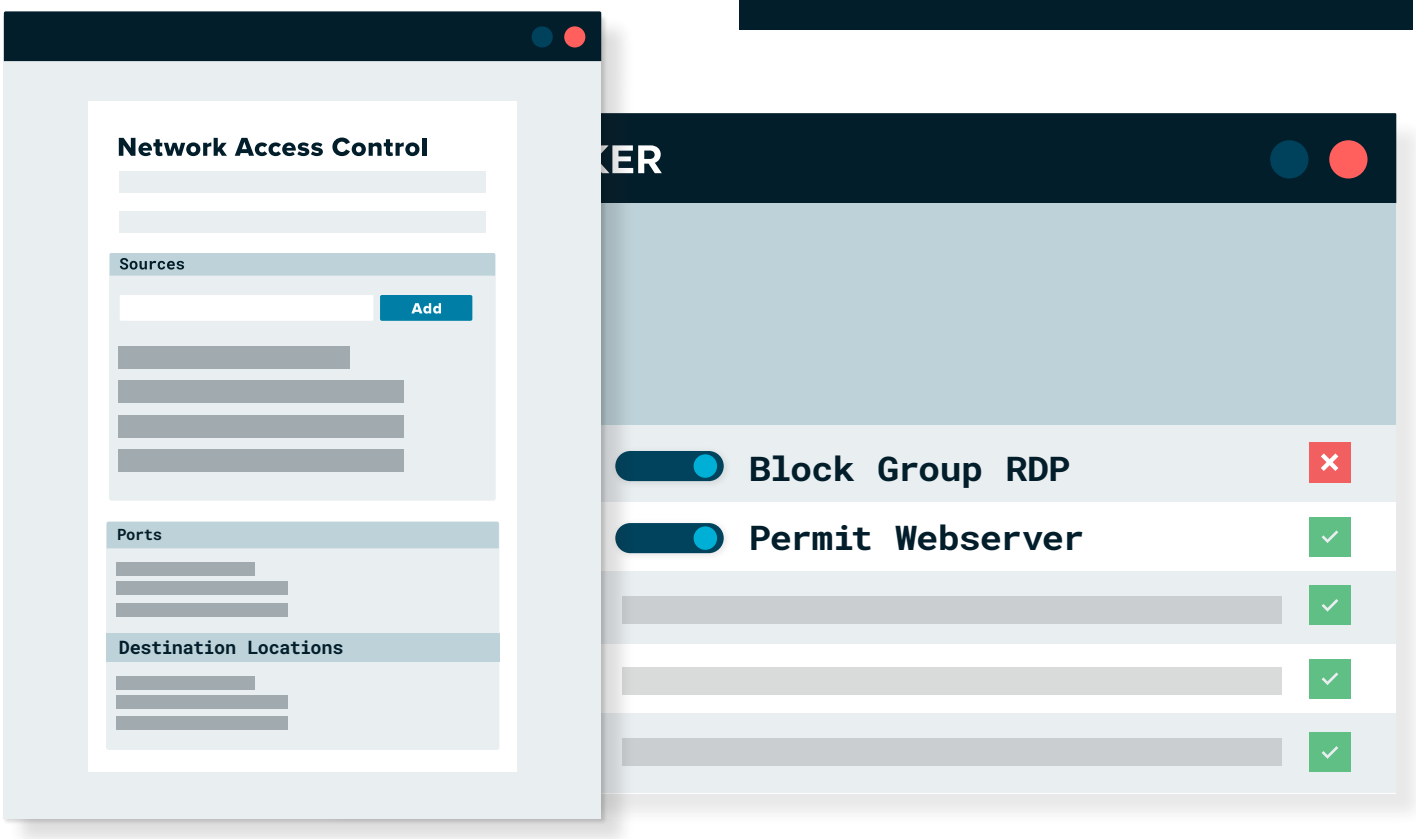
The cloud-managed solution provides customers with a centralized view of endpoint policies and network traffic across your organization.

Dynamic

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

Enhanced Network Security

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



About ThreatLocker®

ThreatLocker® is a leader in endpoint security technologies, providing enterprise-level cybersecurity tools to improve the security of servers and endpoints. ThreatLocker's combined Application Allowlisting, Ringfencing™, Storage Control, Elevation Control, and Endpoint Network Access Control (NAC) solutions are leading the cybersecurity market towards a more secure approach of blocking the exploits of unknown application vulnerabilities. To learn more about ThreatLocker® visit: www.threatlocker.com

If you're interested in learning more about how ThreatLocker® can help you better protect your business, reach out to a Cyber Hero today: www.threatlocker.com/demo-sign-up

THREATLOCKER