THREATLOCKER®
ZERO TRUST PLATFORM

YOUR GUIDE TO INDUSTRY-LEADING

APPLICATION CONTROL

The foundation of Zero Trust security.

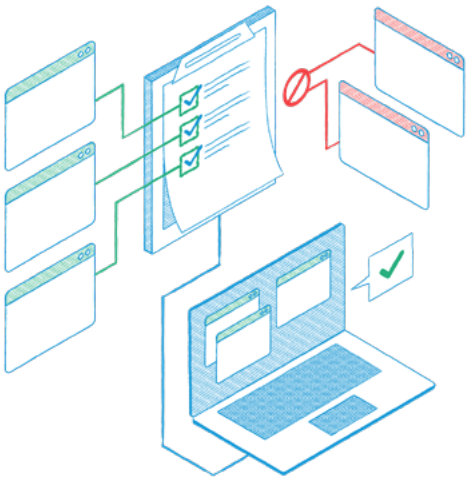
Allowlisting, Ringfencing™, and Privileged Access Management.

The ThreatLocker® Application Control suite, built on a Zero Trust, deny-by-default model, prevents unauthorized software from running, tightly defines what approved applications can do, and who can use elevated privileges.

Together, ThreatLocker Allowlisting, Ringfencing, and Privileged Access Management (PAM) capabilities provide you with a powerful, yet agile layered application control strategy:

- Determine what applications can execute on your endpoints with **Allowlisting.**
- Define precisely what approved applications are allowed to do with **Ringfencing.**
- Control when and how applications can run with elevated privileges with **Privileged Access Management.**

This layered approach dramatically reduces attack surface, limits lateral movement, prevents software exploitation, and gives your organization granular control over its environment.



Application Allowlisting

Control what runs

Application Allowlisting is a powerful and practical solution that blocks all unapproved software from executing.

Instead of trying to identify malicious files among millions of legitimate applications, permit only trusted software and deny everything else by default. You can deploy this solution in hours to days, not months to years.

This approach stops:

- Ransomware
- Zero-day attacks
- Unauthorized software
- Shadow IT
- Malicious scripts
- Fileless malware
- Remote access tools used by attackers

If you do not approve the software, it does not run.

Learning Mode

Simplify Allowlisting deployment through ThreatLocker® Learning Mode. Historically, allowlisting deployments have been challenging and time consuming, with administrators forced to manually create application inventories and policies. ThreatLocker Learning Mode completely changes the experience.

When deployed in Learning Mode, ThreatLocker automatically:

- Catalogs applications and dependencies already running in the environment
- Creates suggested policies based on observed activity
- Builds visibility into software usage
- Reduces manual policy creation
- Accelerates deployment from months to days

You review discovered applications, remove anything unnecessary, and then transition endpoints into a secured state once they are confident the baseline is complete.

Built-in applications

ThreatLocker® recognizes thousands of commonly used applications (15,000+) and software publishers.

Built-in applications help you:

- Automatically trust known software publishers
- Simplify policy creation
- Reduce administrative overhead
- Streamline software updates
- Maintain security without constantly rebuilding policies

As approved applications update, policies can remain effective without requiring extensive manual intervention.

Testing unknown software with sandbox VDI

Users frequently request applications that IT has never seen before.

Instead of approving software blindly, you can leverage the ThreatLocker cloud-based testing environment using a Virtual Desktop Infrastructure (VDI).

Within the isolated environment, administrators can:

- Execute requested software safely
- Observe application behavior
- Review network activity
- Identify file and registry access
- Analyze application interactions
- Determine whether software should be approved, restricted, or denied

This allows you to evaluate software without exposing production systems to unnecessary risk.

User requests and fast approvals

When users need new software:

- The application is blocked
- The user receives a request prompt
- IT reviews the request
- The application can be approved, denied, or tested

You can also leverage Cyber Hero® Approvals for rapid response and reduced operational disruption.

Ringfencing™

Controlling what approved applications can do

Allowlisting prevents unauthorized software from running. But what happens if a trusted application is exploited?

Attackers frequently abuse legitimate tools such as:

- Microsoft Office
- PowerShell
- Command Prompt
- Browsers
- PDF Readers
- Remote management tools

Ringfencing acts as a second layer of defense by controlling how approved applications interact with the operating system, data, network resources, and other applications.

Set clearly defined boundaries for the applications that are allowed to run, further protecting your environment.

Application containment

Ringfencing applies granular controls that limit an application's behavior after execution. You can control:

File access
Limit which files and folders applications can read, modify, or delete.

- Prevent PowerShell from accessing file shares
- Restrict browsers from sensitive document repositories
- Stop applications from encrypting protected data locations

Registry access
Control which registry locations applications can access or modify.

- Prevent unauthorized persistence mechanisms
- Stop applications from changing startup locations
- Restrict access to critical system settings
- Block unauthorized outbound communications

Network access

Limit internet and network connectivity.

- Allow a business application to reach required services only
- Prevent PowerShell from connecting to the internet
- Block unauthorized outbound communications

Application-to-application interaction

Control which applications can launch or communicate with other applications.

- Prevent Microsoft Word from launching PowerShell
- Stop browsers from spawning command-line utilities
- Restrict scripting engines from executing other tools

Ringfencing™ in action

Ringfencing helps mitigate attacks even when a trusted application has been compromised. For example:

A user receives a malicious Word document	
Without containment	**With Ringfencing**
1. Word launches PowerShell.	1. Word is prevented from launching PowerShell.
2. PowerShell downloads malware.	2. The attack chain is broken.
3. The attacker gains access.	3. The compromise is contained.

The application remains usable for legitimate purposes while dangerous behavior is blocked.

Default protection and customization

ThreatLocker® provides powerful default Ringfencing policies for many commonly abused applications.

Customize policies to fit their environment by defining:

- Allowed file access
- Registry permissions
- Network connectivity
- Child process execution
- Application interactions

This enables strong security controls without disrupting your business' workflows.

Privileged Access Management (PAM)

Controlling elevated privileges

Historically, users were granted local administrator rights because certain applications required elevated permissions.

Unfortunately, attackers also rely on those same privileges.

You can provide controlled elevation when required and eliminate the need for permanent administrative access with ThreatLocker® Privileged Access Management.

Instead of giving users full administrator rights, you can elevate only specific applications under defined conditions.

Application elevation

Elevate trusted applications without elevating the user.

Examples include:

- Software installers
- Legacy business applications
- Administrative utilities
- Vendor support tools

Users can perform required tasks without receiving unrestricted administrative access.

Just-in-time elevation

Elevation can be granted only when needed.

Examples include:

- Approve an installer for a specific task
- Allow elevated access during a maintenance window
- Grant temporary administrative permissions for a defined period

Once the task is complete, elevated access expires automatically.

Policy-based elevation

Elevation decisions can be based on:

- Specific users
- Security groups
- Endpoints
- Applications
- Time restrictions
- Business requirements

This ensures privileges are granted only when justified.

Reducing risk

By eliminating standing administrator rights, you:

- Reduce attack surface
- Limit privilege escalation opportunities
- Improve compliance
- Prevent unauthorized system changes
- Strengthen Zero Trust security

Users receive the access they need without exposing the organization to unnecessary risk.

How the three features work together

ThreatLocker Application Control is most effective when Allowlisting, Ringfencing™, and Privileged Access Management work together.

Step 1: Allowlisting

Determine whether software can run.
Question: Is this application approved?

- If not approved: Execution is denied.
- If approved: Execution is allowed.

Step 2: Ringfencing

Control how approved software behaves.
Question: What is this application allowed to do?
Policies determine:

- Which files it can access
- Which registry keys it can modify
- Which applications it can launch
- Which network resources it can contact

Step 3: Privileged Access Management

Control elevated permissions.
Question: Does this application need administrative privileges?
If elevation is required:

- Elevate the application, not the user
- Only when needed, under approved conditions

A practical example

An employee downloads a new application.

1. Allowlisting blocks execution because the software is not approved.
2. IT reviews the request and tests the application in the ThreatLocker® VDI environment.
3. The application is approved.
4. Ringfencing™ restricts the application's access to only the files, network resources, and processes it legitimately requires.
5. If the application requires administrative privileges, PAM elevates only that application rather than granting the user local administrator rights.

The result is a layered Zero Trust model that controls:

- What can run
- What it can do
- How it can be elevated

All while minimizing disruption to end users and reducing operational burden on IT teams.

The result

Your organization will have a practical, scalable Zero Trust security framework with the ThreatLocker Application Control suite.

By combining Allowlisting, Ringfencing, and Privileged Access Management, you will gain:

- Greater visibility
- Stronger endpoint security
- Reduced attack surface
- Protection against ransomware and fileless malware
- Control over software behavior
- Elimination of unnecessary administrative rights
- Faster deployments through Learning Mode and built-in applications
- Safer software evaluation through sandbox VDI testing

Take control of your environment with closely observed approvals, granular boundaries over application interactions, and strict governance over elevation. Visit **threatlocker.com/demo** to request your personalized 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