

THREATLOCKER®

FAILURE
IS NOT AN
OPTION

Simplifying Cybersecurity

Rob Allen | CPO of ThreatLocker®



Change the
paradigm of
Endpoint Security
from **Default Allow**
to **Default Deny**



The future of endpoint security is **Zero Trust**



Allowlisting

- **Block untrusted software including ransomware.**
- Updates are automatically checked.
- Applications are not just blocked at the user level, but also at the system level.
- Users can easily request and get new apps approved.



Ringfencing™

- **Applications are restricted in what they can do.**
- Applications require permission to access file locations.
- Communication is restricted between applications.
- Network access is limited.



ThreatLocker® Detect

- **Detection and Response will be used as a validation to primary Zero Trust controls.**
- SOC resources will be reduced.
- Attackers shift focus to other methods of attack or targets.

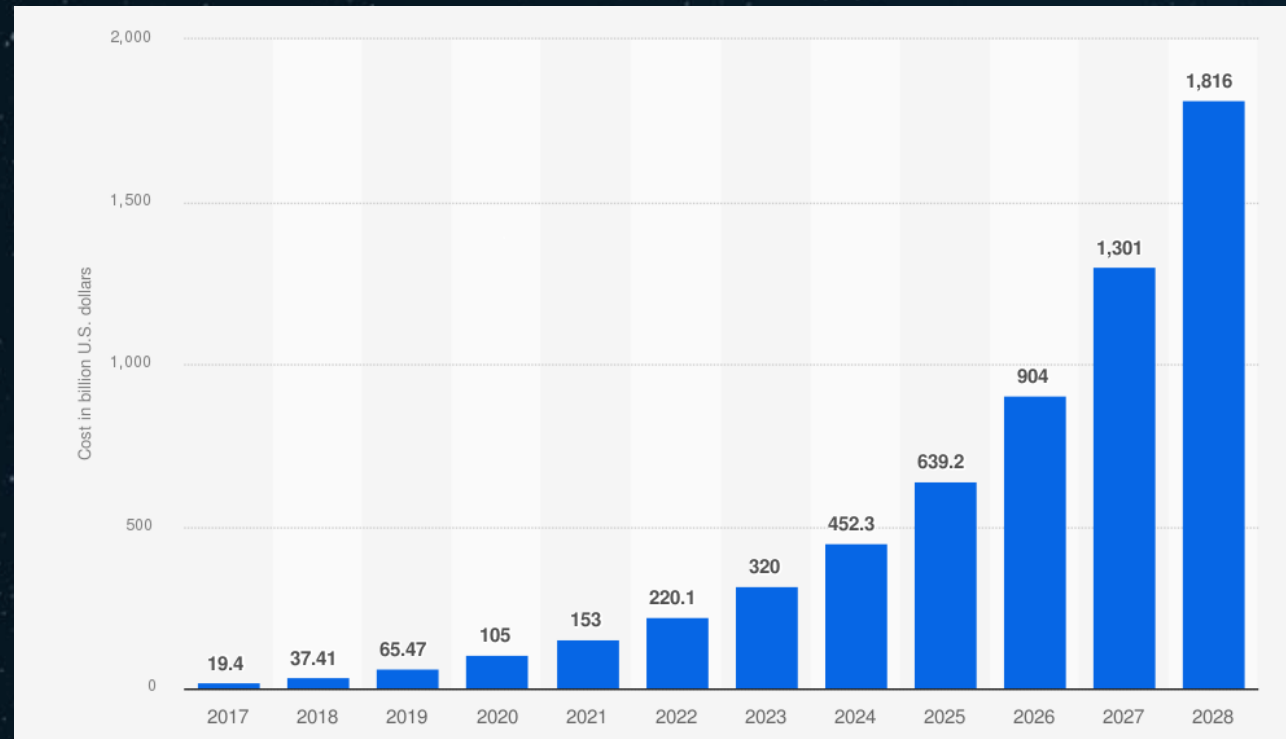


11 Seconds



Estimated annual cost of cybercrime in the US from 2017 to 2028.

In billion US dollars.



Sources

Statista; Statista Technology Market Insights
©Statista 2025

Additional Information

United States; Statista Technology Market Insights; 2017 to 2025



Applications

- Know what is running
- Block untrusted software
- Prevent applications from talking to each other



Allowlisting



Ringfencing™

Know what is running

The screenshot displays the 'Application Control' interface. At the top, there's a '+ New Policy' button and a 'Search By' dropdown set to 'Application Name'. Below this, a table lists applications. Two callout boxes are overlaid on the interface:

- Left Callout Box:** Contains information for '7-Zip All Versions', labeled as 'Built-In' and 'Compression Software'. It features a green 'Compression Software' button and a red 'Missing Updates' button.
- Right Callout Box:** Titled 'Countries', it shows a flag representing Russia.

The background table lists applications with columns for 'Computers', 'Policies', and 'Access'. Visible entries include 'Advanced IP Scanner' and 'Angry IP Scanner', both marked as 'Built-In' and 'Networking Software'. The bottom of the interface shows a pagination bar indicating 'Showing 1 to 25 of 126 records'.



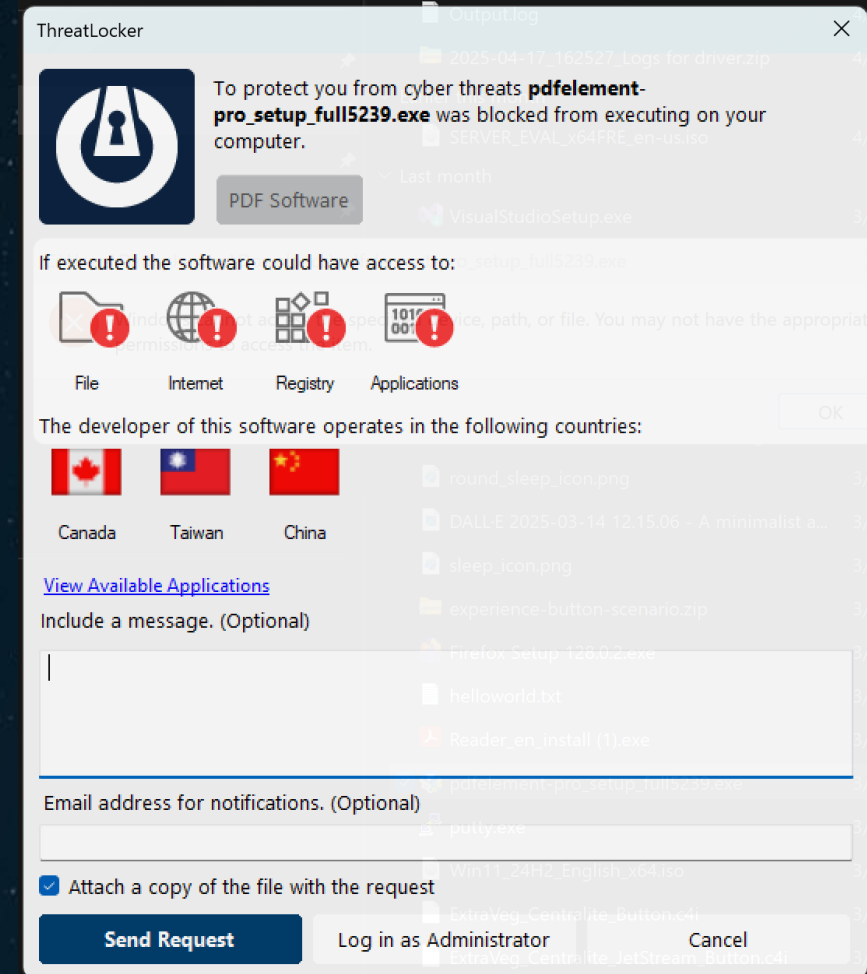
Block untrusted software



RANSOMWARE



RCLONE



Prevent application interaction



Actions

Permit Permit with Ringfence Deny

Restrict this application from interacting with other applications?

☒

Allow All Except Below Allow Only the Below

Windows Command Prompt (Built-In) (x) Windows CScript (Built-In) (x)

Windows RegSVR32 (Built-In) (x) Windows Forfiles (Built-In) (x)

Windows Scheduled Tasks (Built-In) (x) Windows RunDLL (Built-In) (x) msdt.exe (Built-In) (x)

Curl (Built-In) (x) PowerShell Version 7 (Built-In) (x) Windows WScript.exe (Built-In) (x)

Windows PowerShell Full Language Mode (Built-In) (x)

Exclusions Tags

Tag	Port	Action
ThreatLocker\Microsoft 365 (Built-In)	All	✓ Permit



Control file access with Ringfencing™



Control network access with Ringfencing™

Restrict this application from accessing the internet?

☒

Exclusions Tags

Domain +

8.8.8.8

www.google.com

Restrict this application from accessing the internet?

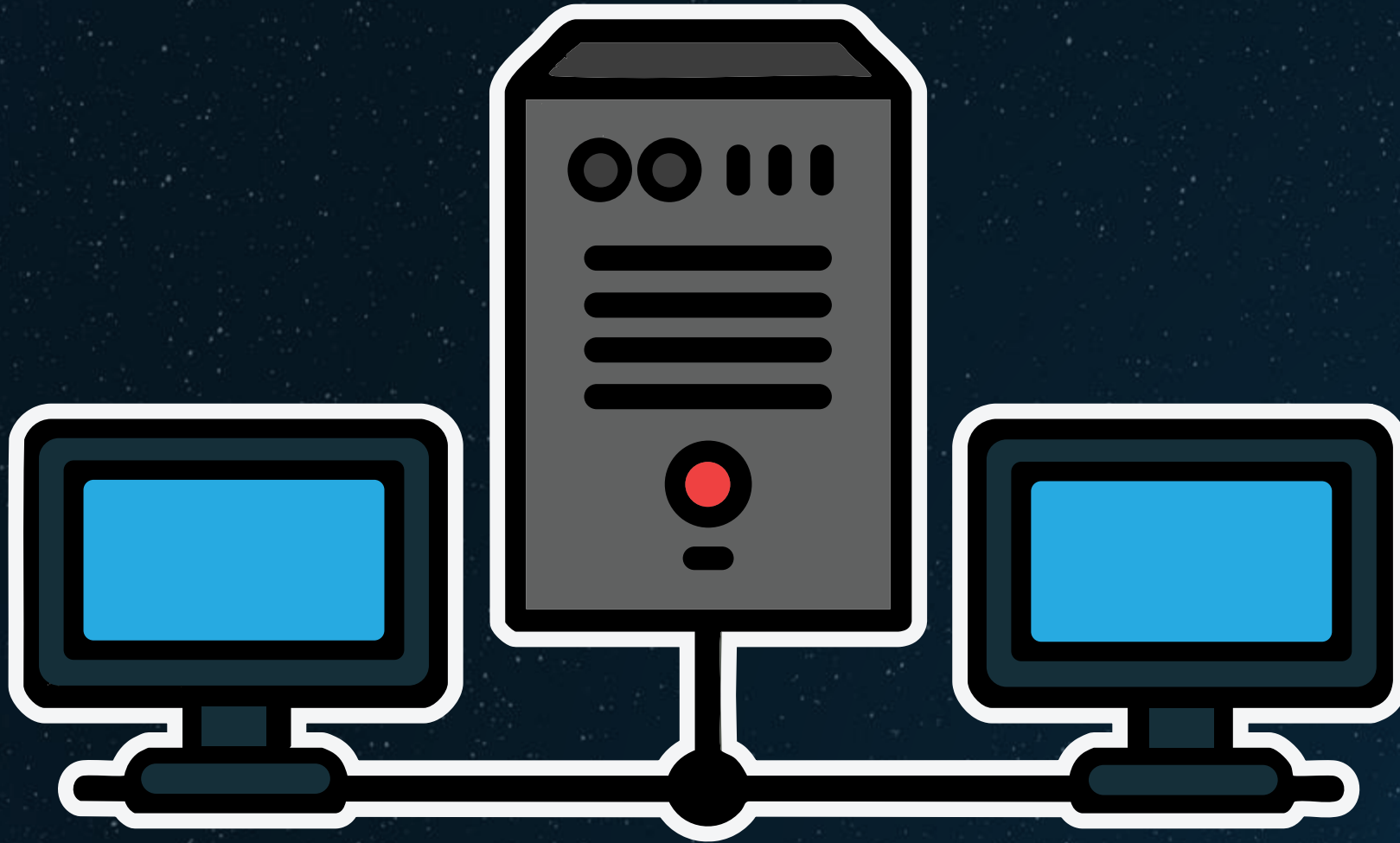
☒

Exclusions Tags

Tag	Port	Action	
<input type="text" value="Required"/>	All	<input type="text" value="Deny"/>	
ThreatLocker\Instagram (Built-In)	All	Deny	
ThreatLocker\Omegle (Built-In)	All	Permit	
Test Tag	All	Permit	



Network



Audit all network traffic

FAILURE
IS NOT AN
OPTION

Unified Audit							
Start Date		End Date		Action Type			
04/27/2025 12:00 AM		04/27/2025 11:59 PM		Action		Network	
				Group By		Hostname	
						Search	

Block SMB ports by default

According to the 2024 Microsoft Digital Defence Report, over 70% of ransomware attacks involved remote encryption.

IPv4

Location

+

Object

Culchie Global

Destination

All

Selected

All Ports

Selected Ports

Ports or Ranges

+

445

139

138

137

Communication Protocol

TCP/UDP

Conditions

No Policy Expiration

Set Policy Expiration

Schedule Policy

Source

All

Selected

All

Selected

All Ports

Selected Ports

Ports or Ranges

+

445

139

138

137

Communication Protocol

TCP/UDP

Conditions

No Policy Expiration

Set Policy Expiration

Schedule Policy

Actions

Permit

Deny



Block outbound network traffic on servers



SOLARWINDS®



Block all inbound traffic to Workstations

+

New Policy

⚙️

Settings

☰

🔌

Network Control

🔌 Policies

🔗 Auth Host

🏷️ Tags

↺

Applies To

🖥️ Workstations

▼

Search

🔍

☐ Inactive / Expired

<input type="checkbox"/>	Order	Active	Policy Name	Policy Action	Description	Created	Delete
<input type="checkbox"/>	-1	<input checked="" type="checkbox"/>	<div>🔌</div> <div>Deny All Inbound</div>	<div>🚫</div>	-	9/6/24, 10:58 AM	🗑️

Showing 1 to 1 of 1 policies

<<

<

1








>








>>

25 ▼



Filter web content

er	Policy Action ⓘ	Policy Name
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 Malicious (Built-In)
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 Explicit Content (Built-In)
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 Advertising Trackers (Built-In)
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 LLMs and AI Tools (Built-In)
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 Business (Built-In)
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 Technology (Built-In)
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	 Project Management (Built-In)

Applies To	Created	Delete
Entire Organization	4/27/25, 4:03 PM	
Entire Organization	4/27/25, 4:03 PM	
Entire Organization	4/27/25, 4:03 PM	
Entire Organization	4/27/25, 4:03 PM	
Entire Organization	4/27/25, 4:03 PM	
Entire Organization	4/27/25, 4:03 PM	
Entire Organization	4/27/25, 4:03 PM	



Audit and control file access

Unified Audit

Start Date: 02/01/2025 12:00 AM End Date: 04/27/2025 11:59 PM Action: Write X Group By: Hostname Search

<input type="checkbox"/>	Date/Time	Hostname	Username	Details	Action Type	Policy Action
<input type="checkbox"/>	4/27/25 10:15:37 PM	WINDEV2407EVAL	USER	c:\users\user\documents\[taskhostw.exe system]	Write	Permit
<input type="checkbox"/>	4/27/25 10:15:37 PM	WINDEV2407EVAL	USER	c:\users\user\desktop\[taskhostw.exe system]	Write	Permit
<input type="checkbox"/>	4/27/25 11:26:01 AM	TLSS-SJ01	DANNYJENKINS	c:\users\public\documents\adobegcinfo\consentrecord	Write	Permit
<input type="checkbox"/>	4/27/25 1:48:06 AM	TLSS-SJ01	SAMUJENKINS	c:\users\samijenkins\documents\outlook files\[taskhostw.exe]	Write	Permit
<input type="checkbox"/>	4/27/25 1:48:06 AM	TLSS-SJ01	SAMUJENKINS	c:\users\samijenkins\documents\[taskhostw.exe]	Write	Permit
<input type="checkbox"/>	4/27/25 1:48:06 AM	TLSS-SJ01	DANNYJENKINS	c:\users\dannyjenkins\documents\github\namedlocationprocessing\namedlocationprocessing\objid ebug\[taskhostw.exe]	Write	Permit
<input type="checkbox"/>	4/27/25 1:48:06 AM	TLSS-SJ01	DANNYJENKINS	c:\users\dannyjenkins\documents\github\namedlocationprocessing\gitlogs\refs\remotes\[taskhostw.exe]	Write	Permit

Showing 1 to 100 of 101+ records < 1 2 > 100 Show Count

TLSS-SJ01

Username
AZUREAD\DANNYJENKINS

Action & Policy

Action Type
Write

Date/Time
3/14/25 8:48:55 AM

Policy
Culchie Global\Workstations\Local Folders - Workstations

Policy Action
Permit

Effective Action
Permitted

Application & File

Full Path:
c:\users\dannyjenkins\documents\hello123.txt.txt

Process Path
c:\program files\windowsapps\microsoft.windowsnotepad_11.2412.16.0_x64__8wekyb3d8bbwe\notepad\notepad.exe (26980)

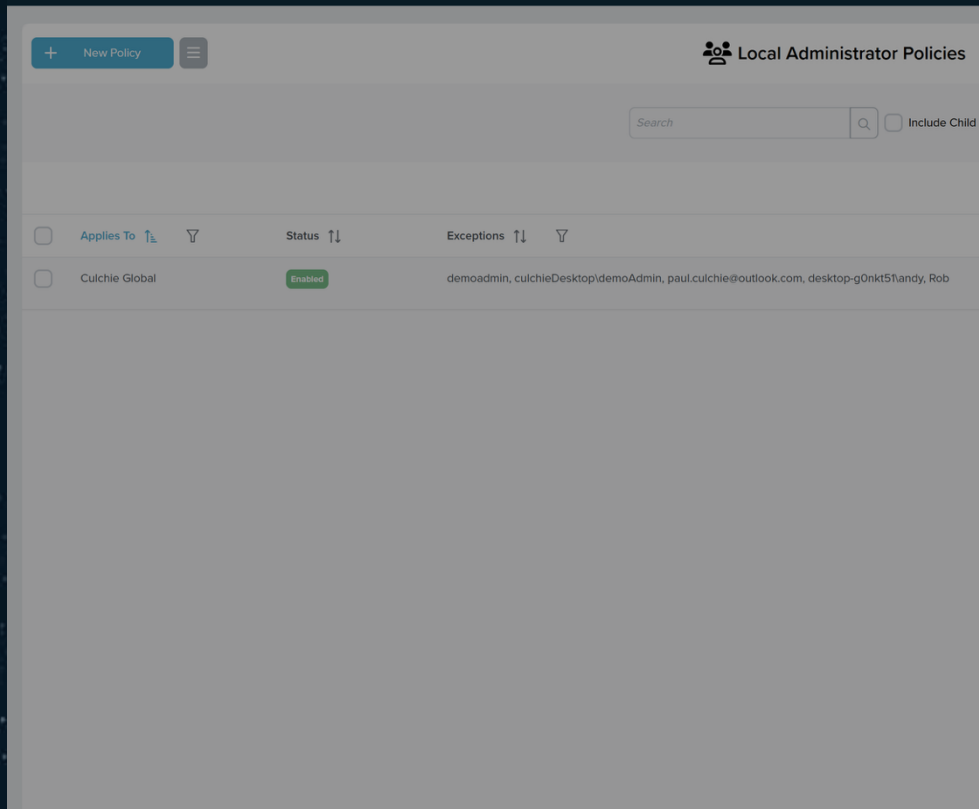
[More Details >](#)

Additional Details

NVME S/N: 1074291363:0025_38B2_4100_EDC3 Not Encrypted



Take away administrator rights



Edit Local Administrator Policy

Applies To

Entire Organization

This policy will automatically remove all users and groups from the Local Administrator group on the selected machines, except for the usernames and groups listed below. We recommend you try this on a test computer before applying it in production.

Enabled Disabled

Details

Windows Agent 9.5 and lower will remove the Domain Admin group from the Local Administrator group unless it is added as an exclusion below.

Exclusions ⓘ

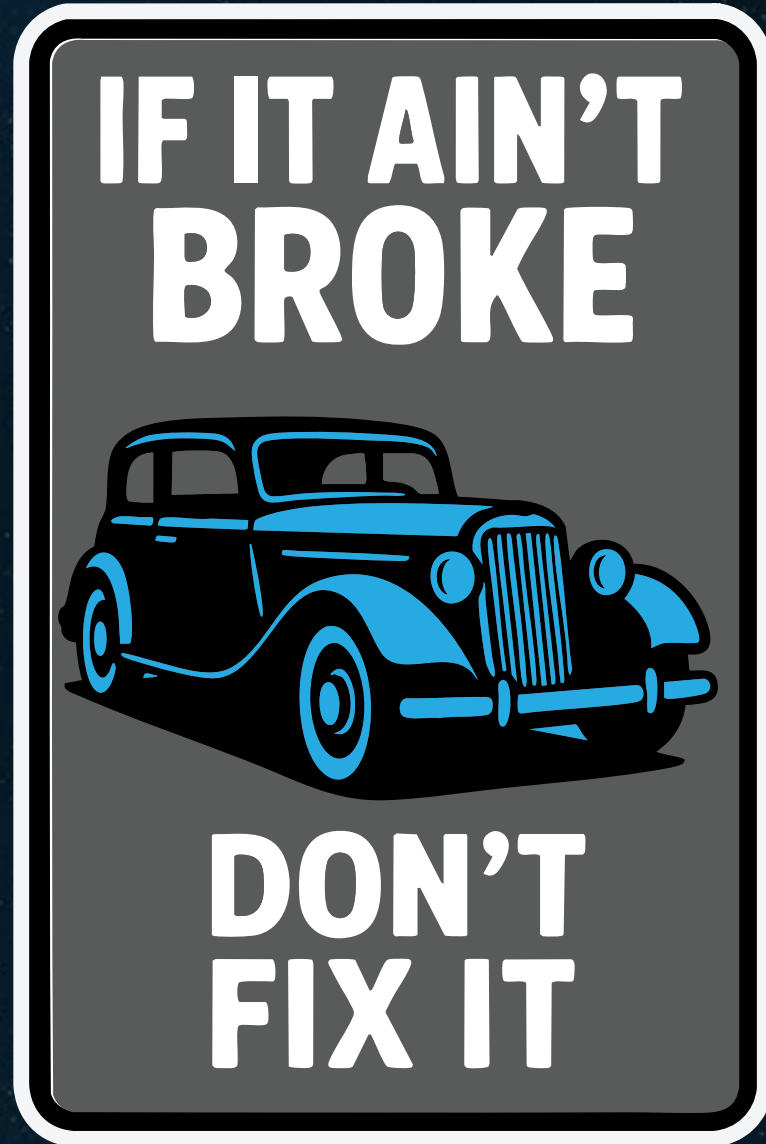
Username *

Add

Exclusions are case-sensitive on Windows Agent 9.5 and lower.

Username / Group	Delete
demoadmin	
culchieDesktop\demoAdmin	
paul.culchie@outlook.com	
desktop-g0nkt5tandy	
Rob	





Patch

- Monitor for unpatched software
- Don't forget about portable apps
- Implement automated patching schedule with testing
- Don't forget firewalls, Access Points, printers, etc.



Detection and response for mass change or exfiltration

If ALL Conditions Are True

Action Type Matches Read

Occurrences Greater than or equal to 10

Within 20 Minutes

AND

If ANY Conditions Are True

Process Path Contains msedge

Parent Process: Application Matches BUILT-IN\Mozilla Firefox...

Policy Actions

Action 1

Create Alert

Severity Warning

Threat Level 0

TLSS-SJ01

Alerts Executes Installs Baseline Network Elevation Storage Exclusions

Alert Details ☐ Show All Alerts

Search Severity All Sort By Select Sort By

Automatically Block Data Exfiltration Warning

Someone is stealing data

View Full Log Threat Level Impact: 0

Date/Time: Apr 27, 2025, 4:47:08 PM Number of Occurrences: 30

Exclusion Count: 0

Automatically Block Data Exfiltration Warning

Someone is stealing data

View Full Log Threat Level Impact: 0

Date/Time: Apr 27, 2025, 4:28:59 PM Number of Occurrences: 28

Exclusion Count: 0

Automatically Block Data Exfiltration Warning

Someone is stealing data

View Full Log Threat Level Impact: 0

Date/Time: Apr 27, 2025, 4:27:31 PM Number of Occurrences: 27

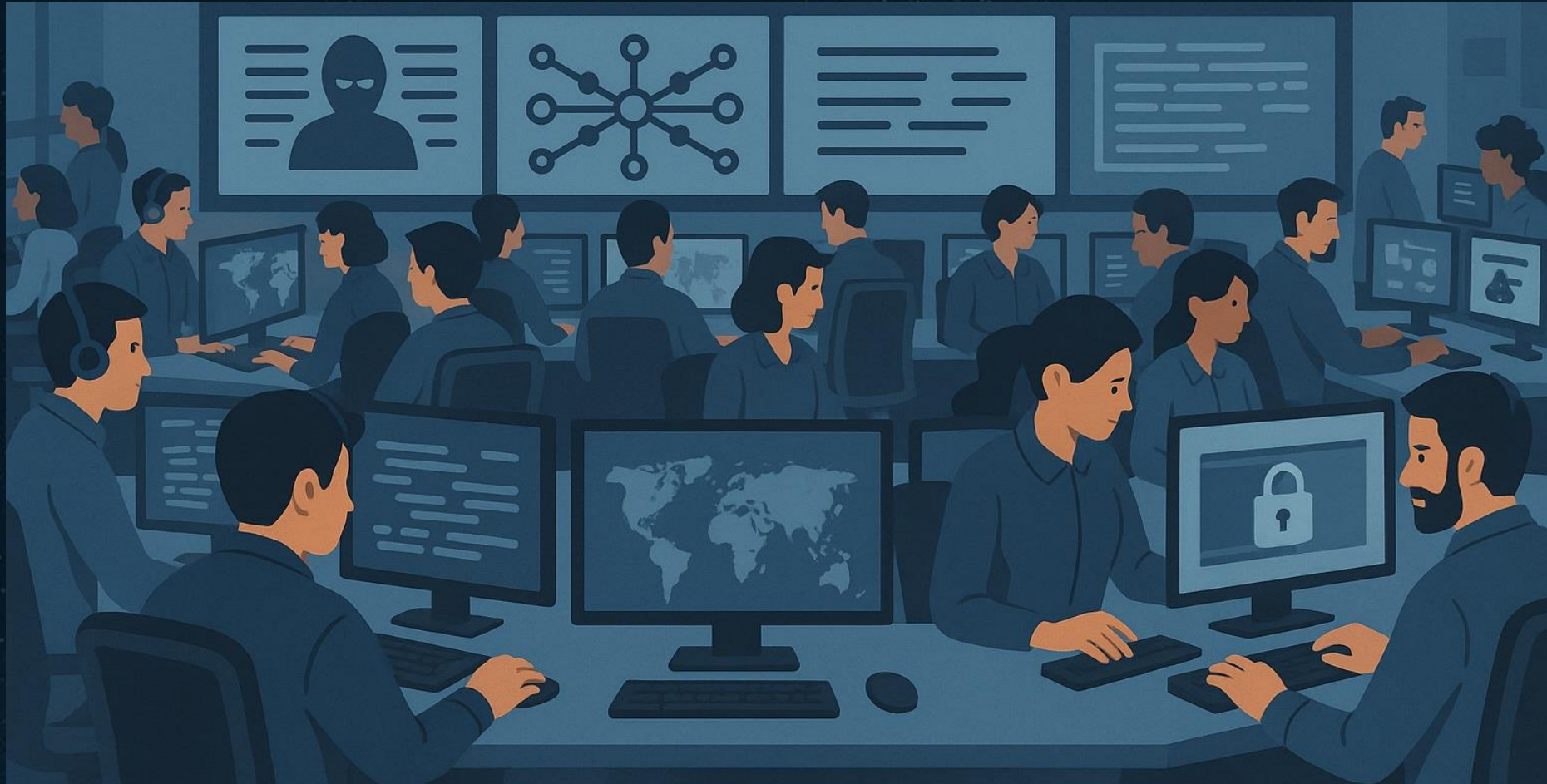
Exclusion Count: 0

Response Details

Clear All Alerts Cancel



Managed Detection and Response



ThreatLocker® enables you to deliver seamless technology to your users, while blocking what is not needed... including cyberattacks.



THREATLOCKER®

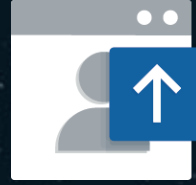
Platform



Allowlisting



Ringfencing™



Elevation Control



Storage Control



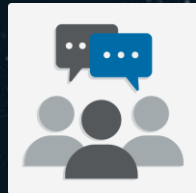
Network Control



ThreatLocker®
Detect



Configuration
Manager



Community

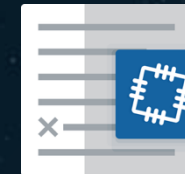


Defense Against
Configurations (DAC)

What's new



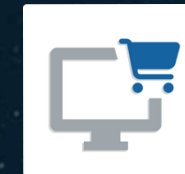
ThreatLocker
Web Control



ThreatLocker
Patch Management



ThreatLocker
Insights



ThreatLocker
User Store



ThreatLocker
Cloud Control



THREATLOCKER® Defense Against Configurations (DAC)



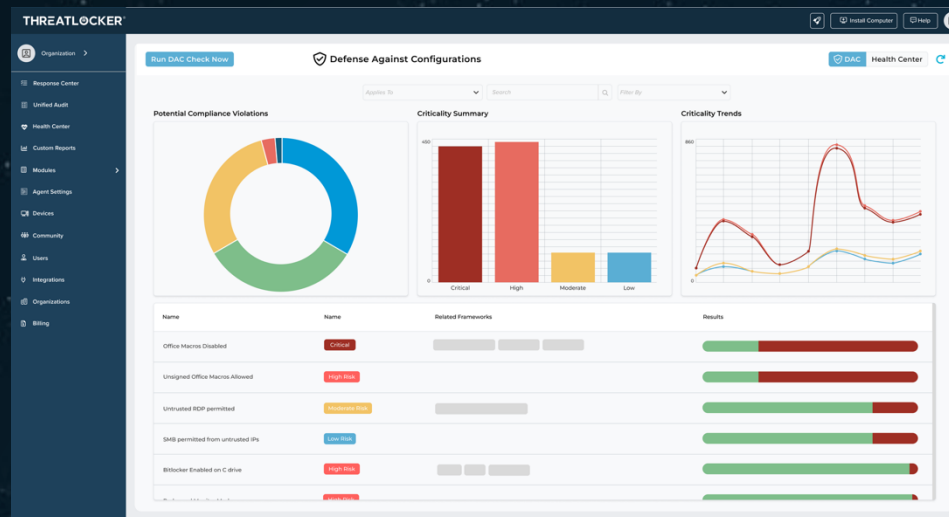
**Less stress, less
headaches**



Stronger security



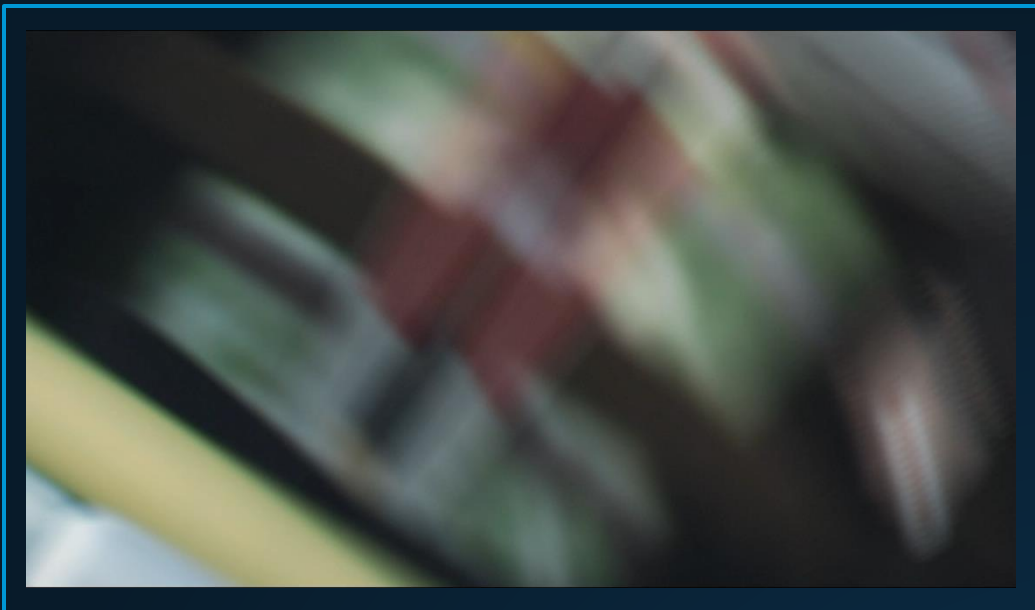
One-click compliance



ThreatLocker® DAC is a powerful dashboard, built right into the ThreatLocker agent. It shows you exactly how your systems are configured and what needs fixing.

DAC removes the guesswork by flagging risky settings, highlighting dormant admin rights, and mapping gaps against compliance standards.





threatlocker.com



Book a demo

