THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

Sample Report

REPORT SUMMARY

Devices running ThreatLocker® vs. not running ThreatLocker® **206 out of 42,000**. To capture a complete picture of the environment, all devices should run the ThreatLocker® Agent.

Devices **NOT** Running ThreatLocker®

0.47%

Devices in Secured mode

When devices are not secured, users can run any software or code that isn't flagged as malicious by antivirus software. Allowing shadow IT activities, ransomware attacks, and the misuse of built-in tools like PowerShell. It is recommended after a learning period and review; all devices are secured. Failing to secure a computer can lead to potential negative consequences, including data breaches and cyberattacks.

103/206

Unused Software

There is no value in permitting unused software within the environment. We recommend restrictively allowing only the essential applications for everyday business operations. By doing so, you can substantially reduce your vulnerability to attacks.

9,986 policies unused out of 17,432 Total

No Default Deny Network Policies

Network Access policies are not being utilized on the organization. Activating this product will not only log and monitor all inbound network traffic, but also give the ability to control that traffic based on organizational needs.

0/206

Devices with no default deny network policies

Restricted Storage

Portable storage should be blocked where it is not required as it can allow data theft from your environment very easily. Permitting unencrypted portable storage could lead to data theft if the devices are lost.

0/206

Devices with restricted storage policies

Ringfenced™ Policies

Software applications may have access to your data, the internet, and other applications on your computer. Allowing untethered access from all of the software you run allows vulnerable applications or application back doors to extract data, execute instructions from attackers and expose your organization to cybersecurity attacks.

Recommended action, Ringfence™ applications so they can only access the data they require to perform their function.

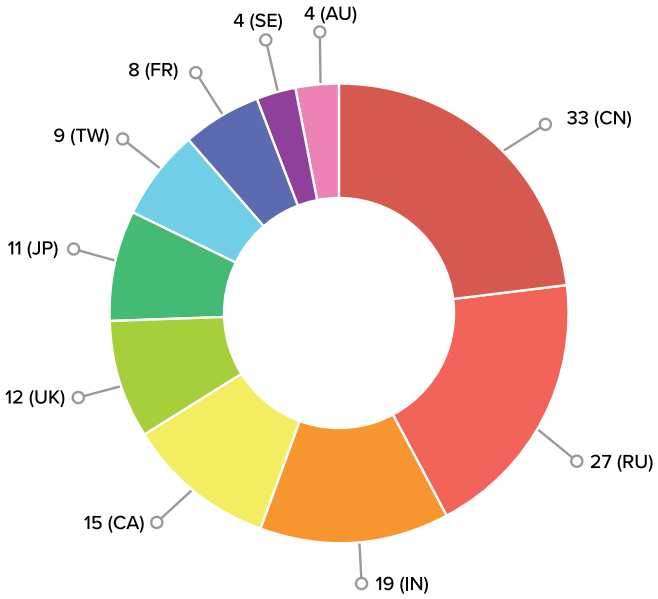
64/17,432

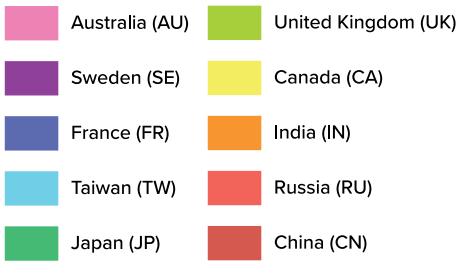
Executes	Network	Reads & Writes	Moves & Deletes
Permitted: 387,806 Items Denied: 1,741 Items	Permitted: 1,651,588 Items Denied: 146,231 Items	Reads Permitted: 1,687,920 Items Reads Denied: 11 items Writes Permitted: 189,738 Items Writes Denied: 69 Items	Moves Permitted: 45,690 Items Moves Denied: 0 Items Deletes Permitted: 181,363 Items Deletes Denied: 91 Items

Data Collected From: [Last 7 Days]

APPLICATION REPORT SUMMARY

Foreign Applications by Country of Origin





17,432 TOTAL POLICIES

Average Policy Count: 39

Ideal Policy Count: 22

ThreatLocker® best practices involve removing unused software, as well as limiting functionality with Ringfencing™ to allow programs to only access what they need, and blocking everything else.

AREAS RECOMMENDED FOR REVIEW

Known Vulnerabilities

Devices in the organization still have files present that are vulnerable to the Apache Log4Shell exploit (CVE-2021-44228).

- PaperCut NG
- Apache Log4j
- FortiSOAR
- FortiConverter
- eCatcher

Browser Extensions

There are 105 browser extensions being utilized in the environment.

- 12, Productivity extensions
- 8, Gaming extensions
- 11, Shopping extensions
- 6, VPN extensions
- 3, ChatGPT extensions
- 17, Custom Browser Theme extensions

Gaming and Entertainment

There are 25 types of gaming and entertainment software being used. Some include open-source software, which allows developers from around the world to modify the code.

- Chromium Extension Beyond
- Epic Games
- Candy Crush
- Minecraft

Windows Store Apps

There are multiple Windows Store Apps being used in your environment. It is important to note that these apps can be developed by various third parties, which may expose them to potential security flaws and vulnerabilities.

- Windows App Microsoft Windows Terminal
- Windows App Candy Crush Saga
- Windows App Splashtop

VPN Tools

There are more than one VPN tool being used in your environment. They are widely used for enhancing privacy and security. However, they may have the capability to bypass security measures, hindering visibility and exposing sensitive data.

- Nord VPN
- Express VPN
- CyberGhost
- Hotspot Shield
- Azure VPN
- ProtonVPN

Remote Desktop Apps

There are multiple remote access tools found in your organization. While being commonly used for legitimate purposes, they can also be exploited and used for malicious purposes, making them a security risk if not used or managed properly.

- TeamViewer
- Anydesk
- Splashtop
- UltraVNC
- Bomgar
- ConnectWise Control

APPLICATIONS TO PRIORITIZE & REVIEW

7-Zip

An open-source file compression system that allows users to compress and decompress files and folders.

Russia

Potential Risks

It has been used historically for password cracking, allowing remote code distribution, encrypting files, and data exfiltration. (CVE-2018-10115)

Mitigation Strategy

Explicitly block this application if it is not required. If it is required for business, limit its access to the internet and other files to prevent data exfiltration.

Browser Extension Coupert

Mainly used for applying coupon codes and discounts when online shopping. It automatically finds and applies any valid coupons to your checkout.

China

Potential Risks

This extension can view and modify all data on websites that you visit, and read all of your browser history.

Mitigation Strategy

Evaluate the need for this software to run in your environment. If it is not required for business use, explicitly deny this software from running.

PuTTY

An open-source terminal emulator and network file transfer tool used for secure remote connections to servers and devices. It supports SSH, Telnet, and serial connections.

United Kingdom

Potential Risks

This has the capability to connect to remote systems using SSH and Telnet Protocols. It can also transmit data outside of the organization.

Mitigation Strategy

Block and limit interactions with other software. Only use required ports and devices for a secure environment. Schedule this tool for operation during business hours.

TightVNC

An open-source remote access software that allows you to have complete access over targeted endpoints.

Russia

Potential Risks

This has the potential for unauthorized access to your systems and sensitive data if it is not properly controlled and monitored.

Mitigation Strategy

Evaluate the need for this software. If it is required for business use, restrict its access to high-risk applications, files, and internet communication.

Wave Browser

A chromium-based browser that is marketed as a privacy-focused browser.

United States

Potential Risks

This has the capability to store browser history, cookies, passwords, and other sensitive information.

Mitigation Strategy

Evaluate the need for this software. If it is required for business use, restrict its access to high-risk applications, files, and internet communication.

Autohotkey

An open-source software that can create keyboard remappings, and program other peripheral macros to run scripts with the push of a button.

United States
Canada...

Potential Risks

This has the potential for the misuse of unauthorized or malicious scripting actions, which can lead to disruptions in business operations.

Mitigation Strategy

Evaluate the need for this software. If it is required for business use, restrict its access to high-risk applications, files, and internet communication.

Levels of Access

Web Data | Applications | File | Internet | Registry | Passwords

Sample Report

NETWORK TRAFFIC SUMMARY

We have found machines communicating with the following countries. This information is pulled directly from the policies with ThreatLocker® Network Control and Ringfencing™ settings applied.

ThreatLocker® Network Control includes additional logging information such as Port traffic. Common examples of information that could be valuable to see usage on include:

- Port 3389 (Remote Desktop Protocol)
- Port 135 (Remote Procedure Call Service)
- Ports 139 & 445 (SMB Protocol)

ThreatLocker® best practices involve Ringfencing™ Applications from reaching out to the Internet. This will prevent unwarranted communication to particular IP's or Domains. Utilize Network Control policies to only allow traffic that's trusted, while denying everything else.

Inbound Network Traffic

WebServer

The following hostname is accepting incoming connections on the following ports:

- Ports: 3389, 445, and 139

Inbound connections coming from:

- China, Russia, Mexico, etc.

Dev-Workstation

The following hostname is accepting incoming connections on the following ports:

- Ports: 3389

Inbound connections coming from:

- France, India, Russia, etc.

Marketing-Laptop

The following hostname is accepting incoming connections on the following ports:

- Ports: 139

Inbound connections coming from:

- Canada, China, Singapore, etc.

Sales-Workstation

The following hostname is accepting incoming connections on the following ports:

- Ports: 139

Inbound connections coming from:

- Germany, United States, Japan etc.

Remote-Laptop

The following hostname is accepting incoming connections on the following ports:

- Ports: 445 and 139

Inbound connections coming from:

- Ukraine, Estonia, Taiwan etc.

FileServer

The following hostname is accepting incoming connections on the following ports:

- Ports: 3389 and 445

Inbound connections coming from:

- Local IP Addresses.

IT-Laptop

The following hostname is accepting incoming connections on the following ports:

- Ports: 3389

Inbound connections coming from:

- United States, Russia, China, France, Germany, Canada, and Singapore.

Accounting-PC

The following hostname is accepting incoming connections on the following ports:

- Ports: 135 and 445

Inbound connections coming from:

- Russia and China.

Dev-Laptop

The following hostname is accepting incoming connections on the following ports:

- Ports: 3389

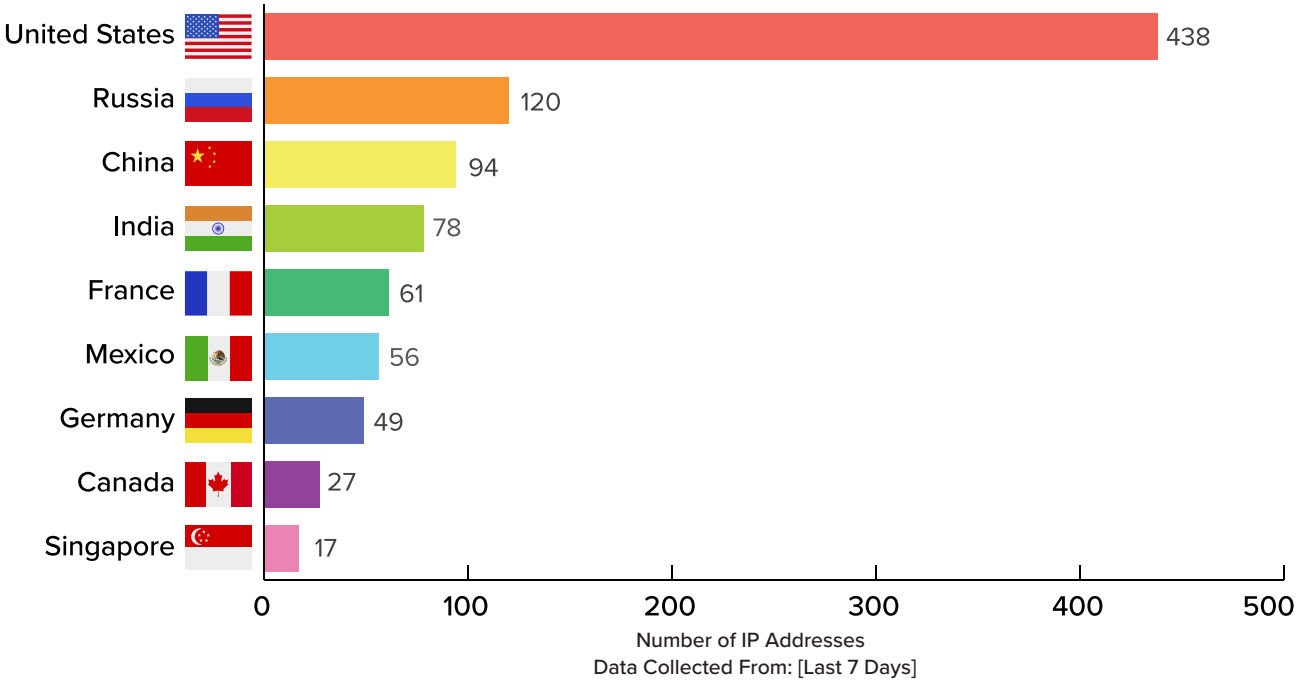
Inbound connections coming from:

- France, India, and Russia.

NETWORK TRAFFIC SUMMARY

Outbound Network Traffic

This graph displays the number of IP Addresses that your machines have communicated with across the following countries.



TikTok

We have found instances of TikTok being used in your organization. Within the past 30 days, 78 computers have reached out to TikTok. Included in this report is the United States Government Executive Ban for TikTok on all Government devices.

Over the last 7 days, the Unified Audit has detected devices making connections to TikTok. Here is a sample of some of these devices:

Hostname	User	Process
Marketing-Laptop2	REYNALDO	chrome.exe
FrontDesk-Desktop1	VIVIAN	msedge.exe
FrontDesk-Desktop3	SANDRA	brave.exe

Scan the QR Code to view the official Executive Order.

Risks of Allowing Ports 139 & 445

Ports 139 & 445 facilitate the Server Message Block (SMB) Protocol for file and printer sharing across networks. However, enabling access to these ports poses risks like unauthorized access, data theft, malware spread, and potential denial-of-service attacks. To uphold network security, it is advisable to block or limit access to these ports.

APPLICATIONS OVERVIEW

Application Name	Details	Access	Country(s) of Operation	Review Rating
7-Zip	**Description:** An open-source file compression system that allows users to compress and decompress files and folders. **Potential Risks:** It has been used historically for password cracking, allowing remote code distribution, encrypting files, and data exfiltration. (CVE-2018-10115) **Risk Mitigation Strategy:** Explicitly block this application if it is not required. If it is required for business, limit its access to the internet and other files to prevent data exfiltration.		Russia	8
Wave Browser	**Description:** A chromium-based browser that is marketed as a privacy-focused browser. **Potential Risks:** This has the capability to store browser history, cookies, passwords, and other sensitive information. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is required for business use, restrict its access to high-risk applications, files, and internet communication.		United States	8
Autohotkey	**Description:** An open-source software that can create keyboard remappings, and program other peripheral macros to run scripts with the push of a button. **Potential Risks:** This has the potential for the misuse of unauthorized or malicious scripting actions, which can lead to disruptions in business operations. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is required for business use, restrict its access to high-risk applications, files, and internet communication.		United States, Canada	8
Angry IP Scanner	**Description:** An open-source network scanner that scans IP addresses and ports, providing information about devices on a network. **Potential Risks:** Unauthorized network scanning, and the ability to identify weaknesses that can be used for exploitation. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is not required for business use, Explicitly deny this software from running.		Estonia	8

*Review Rating is based on a scale from 0 to 10, with the higher the rating on the scale, the more attention needed to review the application in question.

Levels of Access

APPLICATIONS OVERVIEW

Application Name	Details	Access	Country(s) of Operation	Review Rating
Browser Extension Coupert	**Description:** Mainly used for applying coupon codes and discounts when online shopping. It automatically finds and applies any valid coupons to your checkout. **Potential Risks:** This extension can view and modify all data on websites that you visit, and read all of your browser history. **Risk Mitigation Strategy:** Evaluate the need for this software to run in your environment. If it is not required for business use, explicitly deny this software from running.		China	7
TightVNC	**Description:** An open-source remote access software that allows you to have complete access over targeted endpoints. **Potential Risks:** This has the potential for unauthorized access to your systems and sensitive data if it is not properly controlled and monitored. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is required for business use, restrict its access to high-risk applications, files, and internet communication.		Russia	7
Filezilla FTP Client	**Description:** An open-source FTP Client that allows the upload and download of files to and from a remote server. It supports various file transfer protocols. **Potential Risks:** Security vulnerabilities, potential data exposure, possible breaches, and malware distribution. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is required for business use, limit access to high risk applications, files, and the ability to reach out to the internet.		Germany	7
Browser Extension LastPass	**Description:** An extension that allows users to generate strong passwords, store passwords, and autofill login credentials on multiple websites. **Potential Risks:** Can allow access to view and modify all data on websites that you visit, read all of your browser history, and display notifications. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is not required for business use, explicitly deny this software from running.		United States	7

*Review Rating is based on a scale from 0 to 10, with the higher the rating on the scale, the more attention needed to review the application in question.

Levels of Access

Sample Report

APPLICATIONS OVERVIEW

Application Name	Details	Access	Country(s) of Operation	Review Rating
PuTTY	**Description:** An open-source terminal emulator and network file transfer tool used for secure remote connections to servers and devices. It supports SSH, Telnet, and serial connections. **Potential Risks:** This has the capability to connect to remote systems using SSH and Telnet protocols. It can also transmit data outside of the organization. **Risk Mitigation Strategy:** Block and limit interactions with other software. Only use required ports and devices for a secure environment. Schedule this tool for operation during business hours.		United Kingdom	7
Teamviewer	**Description:** A remote access and support software that allows users to access and control other computers and devices. **Potential Risks:** Unauthorized access to your systems and sensitive data if it is not properly controlled and monitored in your environment. **Risk Mitigation Strategy:** Evaluate the need for this software. If it is required for business use, limit access to high risk applications, files, and the ability to reach out to the internet.		Germany	7
Microsoft Office	**Description:** Suite of producitivity software applications. It includes software, such as Word, Excel, PowerPoint, Outlook, and more. **Potential Risks:** Potential for phishing attempts, data leakage, and potential security vulnerabilities if not used and monitored properly. **Risk Mitigation Strategy:** Only permit the required applications that are included in the Office Suite. Limit access to high risk applications, files, and the ability to reach out to the internet.		United States, United Kingdom, india	5
PowerShell	**Description:** A command-line shell and scripting language for automating administrative tasks and managing Windows Systems. **Potential Risks:** Carries the potential for misuse by individuals with malicious intent, as it can be used to run commands that may compromise overall security. **Risk Mitigation Strategy:** Further evaluate the need for this software. If it is required for business use, limit access to high risk applications, files, and the ability to reach out to the internet. Limit the use of this application to those who are authorized.		United States	5

*Review Rating is based on a scale from 0 to 10, with the higher the rating on the scale, the more attention needed to review the application in question.

Levels of Access

Sample Report

Appendix:

Allowlisting

The approach of allowlisting with ThreatLocker® focuses on permitting required software while blocking everything else. This ensures smooth business operations without the risk of unauthorized or malicious software infiltrating the devices in the organization.

This Default Deny approach enhances security by blocking both known and unknown malware, including ransomware, whether it's triggered by an unknown vulnerability or human error.

The Importance of Allowlisting

UHS Hospitals

UHS Hospitals encountered a significant disruption as a result of a ransomware attack. UHS Hospitals, a healthcare network encompassing 400 medical facilities in both the United States and the United Kingdom, fell victim to the Ryuk ransomware variant. The infiltration of Ryuk into the hospitals computer systems is suspected to have occurred through a phishing attack. Subsequently, the malware remained dormant until nighttime, when it initiated the process of encrypting critical files.

Colonial Pipeline

The U.S. Colonial pipeline, which stretches from Texas to the southeastern coast and onwards to Washington D.C., faced a security breach resulting from a blend of phishing, weak passwords, and vulnerabilities. Once the hackers infiltrated the pipeline, they held it hostage, attempting to extort money. Consequently, the pipeline was forced to halt its operations in response to the attack, impacting oil and gas prices for many.

Ringfencing™

Ringfencing™ restricts the actions of an application after it starts running. This includes controlling its access to data, the internet, and interactions with other applications.

By implementing Ringfencing™, organizations can prevent exploited or vulnerable applications from accessing and extracting data, as well as prevent zero-day vulnerabilities from being exploited.

Historic Examples of Apps Being Weaponized

SolarWinds

The SolarWinds breach was a supply chain attack, internally compromised due to an intern who had used the same password for seven years. Hackers may have brute forced the password to gain access. Another supporting factor to compromise was because of a misconfigured GitHub repository which was made accessible - and was leaking FTP credentials of the company's download website in clear text. This allowed hackers to use these credentials to upload compromised/malicious updates to SolarWinds download sites. The compromised version of SolarWinds Orion plug-in was used to execute dubious commands, transfer files, disable system services, and gather information about the machine. By misleading vendors into thinking that it was an uncompromised version, they were able to target multiple organizations simultaneously gathering sensitive information from a wide range of machines by means outside of what the software would normally do.

3CX

3CX was also compromised by a supply chain attack. Hackers managed to hijack the 3CX Electron Windows app, and used it to download malicious software from a unrelated GitHub repository. It is believed that they were able to compromise 3CX by using another supply chain attack from a company, called X Trader, which experienced a similar compromise. This false update allegedly was written in a way that forced the malicious content to wait a certain amount of time before actually doing anything, increasing the distribution of the update, then attacking all infected platforms at once. Both examples related involved compromised software, but also had access to more than it needed, and could change the intent of how it performed as a result.