THREATLOCKER

USE CASES

Introduction

As ransomware, malware, and data encryption have become more prevalent over the past few years, organizations of all sizes and industries need to reevaluate their internal IT security stacks to remain compliant with industry standards and protected from rising threats.

ThreatLocker's number one goal is to equip you with solutions that proactively defend your organization against countless cyber threats and provide rapid 24/7 support needed for your dynamic operations. Each solution on the ThreatLocker platform is founded on the basis of operating with a zero trust, default deny strategy. This puts you in command of how your organization facilitates its internal and external cyber defenses and protocols.

Key Uses

Proactive Approach to Cybersecurity

Unlike antivirus or traditional EDR, ThreatLocker's Allowlisting solution puts you in control of what software, scripts, executables, and libraries can run on your endpoints and servers. This approach stops not only malicious software in its tracks but also stops other unpermitted applications from running. This process greatly minimizes cyber threats and other rogue applications from running on your network.

Preventing the Weaponization of Legitimate Tools

ThreatLocker's Ringfencing™ solution controls what applications are able to do once they are running. By limiting how software can interact on your devices, ThreatLocker® can reduce the likelihood of an exploit being successful or an attacker weaponizing legitimate tools such as PowerShell.

Limiting Application Hopping For Administrators

Elevation Control puts IT administrators in the driver's seat, enabling them to control specific applications that can run as a local admin without giving users local admin rights.

With applications such as Quickbooks that need to run with local admin access; Elevation control can limit that access without impacting operational workflow, which can prevent the further spread of an attack, like application hopping, in case there is a breach in the endpoint.

Control Over Storage Devices and Data Access

ThreatLocker® 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. Storage Control allows you to set granular policies, such as blocking USB drives or blocking access to your backup share except when your backup application is accessed.

Solution Benefits

Save Time & Money
Reduce time dedicated to endpoint security by 25% and reevaluate annual spending on multiple licensing for antivirus and EDR solutions.

Increased Security
Increasing endpoint security coverage and reduce the risk of potential security breaches.

Streamlining workflows
Permit any files or applications blocked by ThreatLocker® within 60 seconds by an administrator if an approval request is submitted.

Seamless Onboarding & Deployment
ThreatLocker's Learning Mode and Unified Audit simplifies setting up your Zero Trust environment during the initial onboarding and deployment.

24/7 Cyber Hero Support
Resolve any questions or issues with ThreatLocker's Cyber Heroes, who are available within 30 seconds via the admin portal chat or telephone 24/7/365.

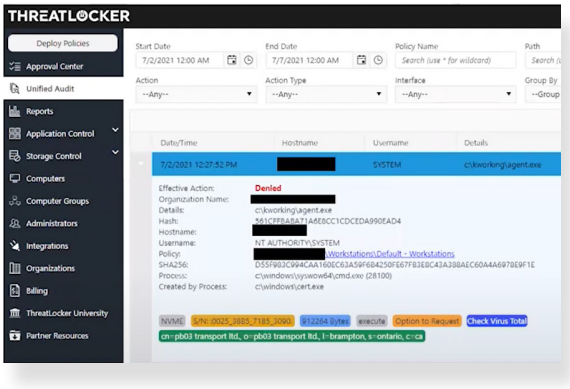
KEY EXAMPLES

Kaseya VSA Attack

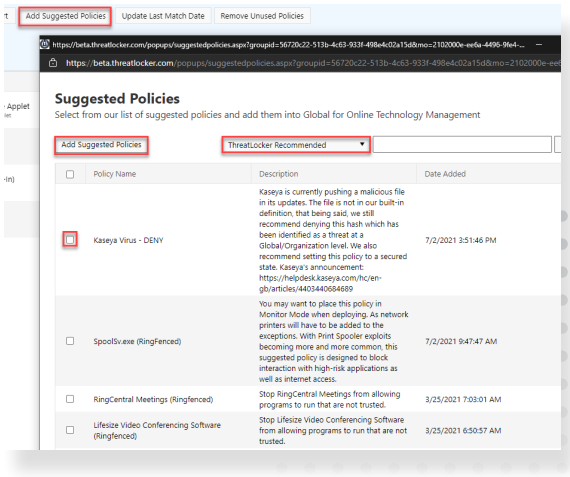
The ransomware gang known as REvil attacked Kaseya's VSA SaaS platform using zero-day exploits to gain access and distribute malicious software to their customers and their systems. They used an authentication bypass vulnerability to compromise the VSA and distribute a malicious payload to hosts using the remote monitoring and management software, amplifying the reach of the initial foothold.

The Kaseya VSA agent (C:\PROGRAM FILES (X86)\KASEYA\<ID>\AGENTMON.EXE) was deployed to Kaseya's customers and then deployed to the MSP customer's systems. This agent is responsible for pulling from Kaseya servers, which are hosted in the cloud. Since the malware was already wrapped in the platform, it was signed by Kaseya's platform. As a result, the malware was able to pass everything on to these clients' systems. To normal users, it looked like legitimate Kaseya traffic when it was installers for malware.

This Kaseya VSA attack impacted between 800 and 1500 companies. Each customer was asked to pay a ransom of between $50,000 and $5 million. There was also a $70 million master key available as a bundled deal paid in Bitcoin.



- Unified Audit showing *c:\kworking\agent.exe* being denied



- Adding *Kaseya Virus - Deny* suggested policies at the Global/ Organizational Level

How ThreatLocker® Mitigated This Exploit

During this incident, ThreatLocker® noticed a file c:\kworking\agent.exe being blocked on multiple devices. EDRs and other threat detection tools weren't able to effectively detect the Kaseya breach due to the fact that the malicious code was signed off and appeared to be a part of a reputable company. ThreatLocker's Allowlisting solution was able to mitigate the attack because an executable file changed within the program folder. Whether or not the application is reputable or is signed off with a certification, ThreatLocker's solution can deny all applications from running except those that are explicitly allowed by hash. This means untrusted software, including ransomware and other malware, will be denied by default.

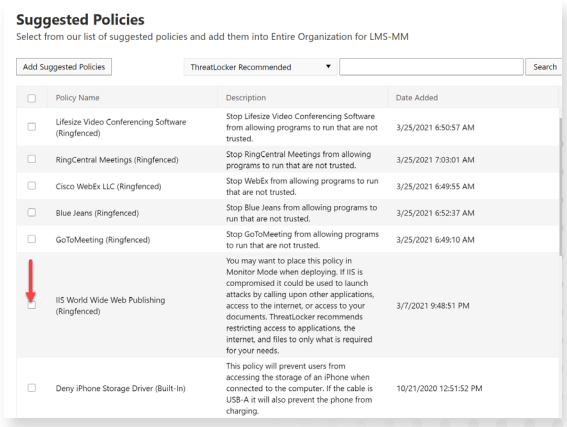
> ThreatLocker® stops ransomware. It allows you to mitigate most application vulnerabilities, and it allows you to gain unprecedented control over your existing applications. ThreatLocker® is our last bastion of defense.
>
> **- Zachary Kinder, Net Tech**

Microsoft Exchange Server Attack

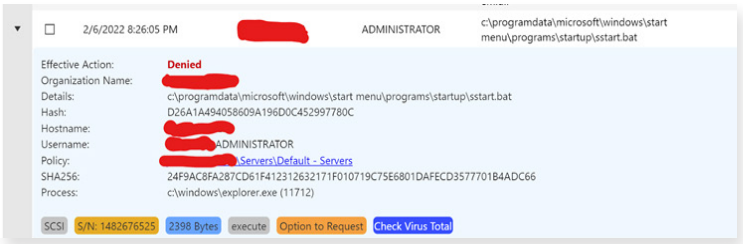
The Microsoft Exchange Server on-premises editions were attacked using several zero-day exploits discovered by Microsoft in 2021. Due to these exploits, over 30,000 organizations in the US were targeted, which gave cybercriminals access to email accounts where they were able to install web shell malware, giving them ongoing administrative access to the victims' servers.

How ThreatLocker® Mitigated This Exploit

ThreatLocker® was able to mitigate this attack with its Ringfencing™ solution. By using Ringfencing™ to limit Internet Information Services(IIS), ThreatLocker® was able to stop the execution of the remote web shells by blocking/limiting access to other applications, the internet, and user files, mitigating the damage the threat attacker had intended to do post-exploitation.



- Adding *IIS World Wide Web Publishing* suggested policies at the Global/Organizational Level.



-Unified Audit showing *c:\programdata\microsoft\windows\start menu\programs\startup\sstart.bat* being denied.

SolarWinds Orion Attack

SolarWinds Orion was the target of a software supply chain attack against American software company SolarWinds, which develops and maintains network monitoring tools used by major corporations and governments. The hack was carried out by threat actors outside of the nation and exploited SolarWinds' Orion software updates. The updates that were exploited ended up being installed by more than 250 of SolarWinds' customer base, including Fortune 500 businesses.

How ThreatLocker® Mitigated This Exploit

ThreatLocker® mitigated the SolarWinds Orion Attack by limiting what the application was able to do, which was accessing the internet. The code that was placed in the SolarWinds Orion software would reach out to the internet, which happened to be an A-to-B server in the U.S.. By using the Ringfencing™ solution, the SolarWinds Orion application was unsuccessful because the attack was blocked from interacting with the internet or browser applications that hindered its ability to download the intended malware.

> If I had an EDR we would know the attackers are inside our house but wouldn't we rather have someone hitting the intruder with a baseball bat before they get in? The biggest benefit of ThreatLocker® to me is I don't have the fear I used to whenever I would hear about ransomware attacks like Kaseya and Exchange on-premises server.
>
> **- David Stinner, US itek**

THREATLOCKER Platform

READY FOR A DEMO?

Visit the ThreatLocker® website for more details.