THREATLOCKER

Storage Device Control that is fast, easy and flexible

Blocking all USB Drives is not the Answer... *But having granular control is.*

ThreatLocker® controls which devices are used, and allows advanced policy configuration providing control down to the smallest of detail.

ThreatLocker® Storage Device Control is an advanced storage control solution that protects information by providing tools to manage the flow and access of data. You choose what data can be accessed or copied, and which applications, users, and computers are permitted to access this data. By using ThreatLocker®, you are in control of all file servers, USB drives, and data.

ThreatLocker® takes storage control beyond just blocking USB hard drives, and gives you granular control over what happens on all external storage devices. Whether it's Network Attached Storage, USB drives or secondary hard drives directly connected to your computer, your endpoint is secured.

Lock down USB drives to specific users, groups, or serial numbers

Control data copied to and from storage devices

Audit files that are accessed or changed on storage devices

Reduce data theft by restricting which applications can access data

Rapid Deployment

- 1-Click Deployment
- Push MSI Install
- Get up and running in minutes

Granular Control

- Limit applications access to data
- Create computer, group, or user policies

Simple Approval

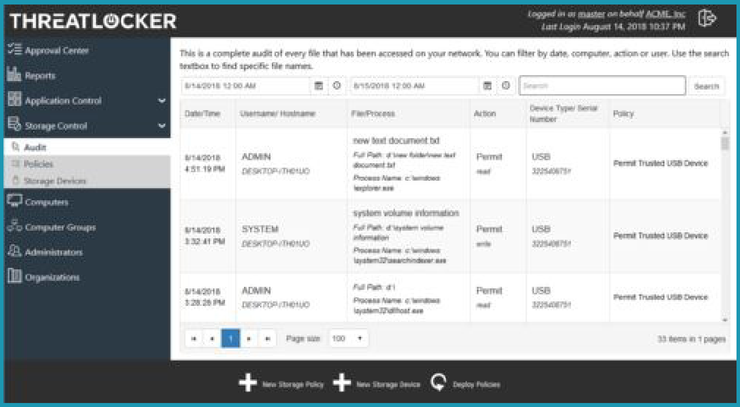
- One-Click Request
- One-Click Approval
- Less than 30 Second Process

THREATLOCKER

Take control over data being transmitted to and from storage devices

Audit Everything

The type of storage device doesn't matter, ThreatLocker® keeps a full audit of every action that users take. We log and store reads, writes, deletes and moves in a simple to use secure cloud portal. By searching the audit you can see what applications, users, and computers are accessing your information. With ThreatLocker® Storage Control you can rest assured that there is a full audit of what's important to your business.



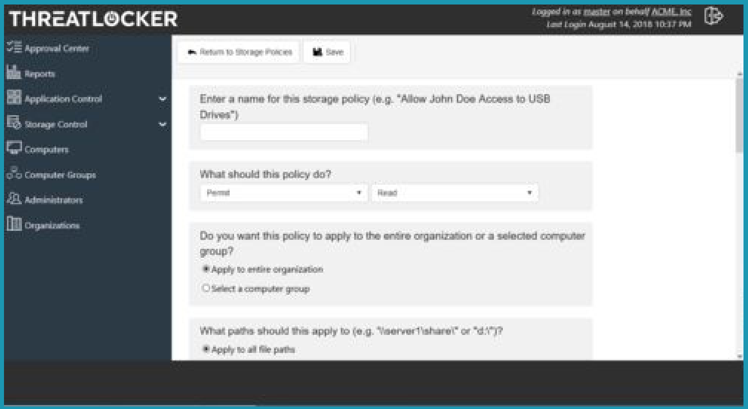
This is a complete audit of every file that has been accessed on your network. You can filter by date, computer, action or user. Use the search textbox to find specific file names.

Date/Time	Username/ Hostname	File/Process	Action	Device Type/ Serial Number	Policy
8/14/2018 4:51:19 PM	ADMIN DESKTOP-[illegible]	new text document.txt Full Path: d:\new folder\new text document.txt Process Name: c:\windows\explorer.exe	Permit read	USB 322540875[illegible]	Permit Trusted USB Device
8/14/2018 3:32:41 PM	SYSTEM DESKTOP-[illegible]	system volume information Full Path: d:\system volume information Process Name: c:\windows\system32\searchindexer.exe	Permit write	USB 322540875[illegible]	Permit Trusted USB Device
8/14/2018 3:28:28 PM	ADMIN DESKTOP-[illegible]	Full Path: d:\ Process Name: c:\windows\system32\dllhost.exe	Permit read	USB 322540875[illegible]	Permit Trusted USB Device

33 items in 1 pages

Firewall Like Policies

Control what happens on file servers, and what devices are being used in your business. With ThreatLocker® firewall like policies, you can configure powerful policies that give granular control of everything from file servers to USB hard drives. Policies can be set to meet your exact requirements and can be configured based on user, computer, file types, device types or serial numbers, and even what application needs access to the device.



Enter a name for this storage policy (e.g. "Allow John Doe Access to USB Drives")

What should this policy do?
Permit ▾ Read ▾

Do you want this policy to apply to the entire organization or a selected computer group?
● Apply to entire organization
○ Select a computer group

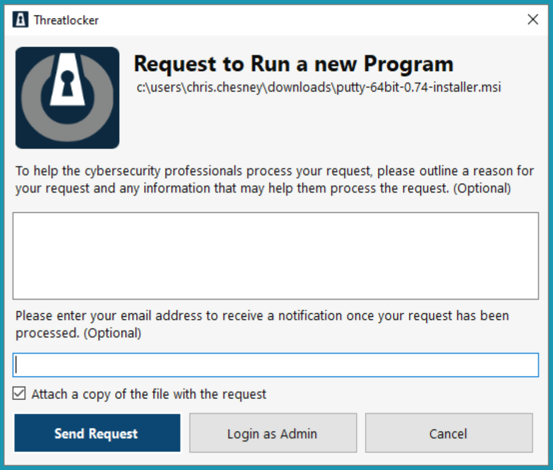
What paths should this apply to (e.g. "\\server1\share\" or "d:\")?
● Apply to all file paths

THREATLOCKER

Take control over data being transmitted to and from storage devices

Granting Access is Fast

When users need to get access to prohibited devices, approval is simple. Users can request permission with a single click, and administrator approval is a single click away. Approval takes seconds and you don't have to worry about having access to the user's computer, you can approve from anywhere, and user will receive updated policies from the cloud immediately.



Request to Run a new Program

c:\users\chris.chesney\downloads\putty-64bit-0.74-installer.msi

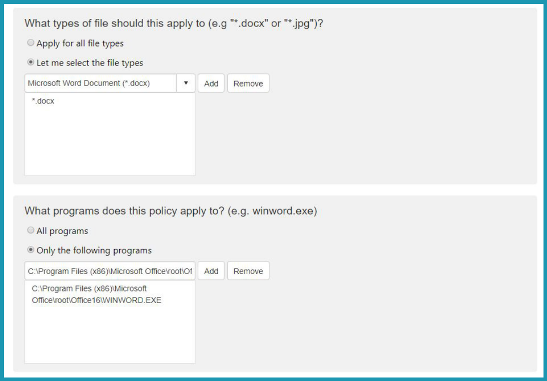
To help the cybersecurity professionals process your request, please outline a reason for your request and any information that may help them process the request. (Optional)

Please enter your email address to receive a notification once your request has been processed. (Optional)

☑ Attach a copy of the file with the request

Restrict Application Access to Important Data

Applications are more of a threat to your valuable data than people are. With ThreatLocker® Storage Control you can control which applications can access your USB Drives and File Servers, preventing damage to your data in the event of a ransomware or cryptolocker attack.



What types of file should this apply to (e.g "*.docx" or "*.jpg")?

○ Apply for all file types

● Let me select the file types

Microsoft Word Document (*.docx) ▾

*.docx

What programs does this policy apply to? (e.g. winword.exe)

○ All programs

● Only the following programs

C:\Program Files (x86)\Microsoft Office\root\Of

C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

THREATLOCKER

Take control over data being transmitted to and from storage devices

A third party enters your premises and plugs a USB drive into a computer. They are able to get full access to your data and systems, including critical safety machinery.

ThreatLocker® gives you control over what USB devices can be used, as well as what type of files they can open. You can limit access to cert document types and block USB drives from running applications.

A user opens a PDF which directly attaches itself to the process by reading code from an HTTPS site. It is impossible for antivirus to detect this code, and it encrypts all files on your shared network drive.

ThreatLocker® gives you the ability to control which applications can access which types of data. In the event a user is infected with malware that processes access to your data,ThreatLocker® will restrict this action.

A rogue employee copies customer data files to a USB drive before leaving for a competitor company.

ThreatLocker® Storage Control lets you block all read and write access, or just write access to USB drives.

An employee needs access to a USB drive to run a backup of the camera system. That employee exploits this privilege to copy customer data to a USB drive.

ThreatLocker® Storage Control lets you decide what data can be copied to storage devices, and data that is copied is recorded in a detailed audit.

Your backup server is infected with ransomware. The ransomware deletes your backups from your USB hard drive, before encrypting your file server.

ThreatLocker® Storage Control provides the ability to lockdown USB access to only specified applications, such as your backup and Disaster Recovery software.