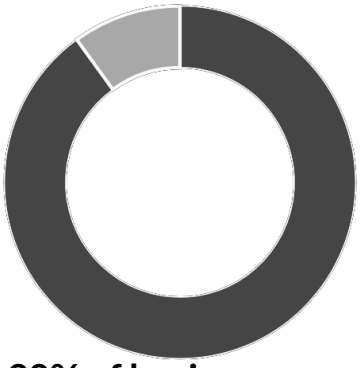
THREATLOCKER®

ThreatLocker® changes the paradigm from only blocking known threats, to giving you the choice of what is running on your network. Not only can you control what software is running, but you can also control what that software can do.

ThreatLocker® puts your business ahead in the fight against malware and exploits by combining Application Whitelisting and RingFencing™ together into our Application Control. The solution is fast to deploy and has a low total cost of ownership solution.

RingFencing™ limits applications from performing functions that are not required for normal use. This is extremely effective at stopping exploits of known or unknown vulnerabilities



90% of business were affected by malware in the last 2 years

Only run applications approved by I.T Department

Control data copied to and from storage devices

Audit all access to files on the network, and opened applications

Ringfence applications so they cannot gain unauthorized access to data.

Rapid Deployment

- 1-Click Deployment
- Push Install
- Auto Profiling Apps
- Audit of What's Running

Automatic Updates

- ThreatLocker® maintains a database of applications, that is automatically updated.
- Whitelists are automatically updated.

Simple Approval

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

THREATLOCKER®

Protect Your Business from Ransomware and Cryptolocker

Ransomware and CryptoLocker malware and viruses are some of the most aggressive threats that businesses face. Businesses that have been affected by this malware are often left in ruins as they try to recover from huge losses.

Ransomware is packaged in various forms and attacks systems by various methods. Ransomware can infect PCs through user-downloaded software, a macro in an office document, a script in a PDF file, or even an exploit such as the EternalBlue exploit.

ThreatLocker® Application Control helps businesses put a stop to ransomware in multiple ways. Our Application Whitelisting offers a superior level of protection, making it virtually impossible for a user to knowingly or unknowingly run ransomware. Unlike antivirus software, our Application Whitelisting blocks all untrusted code from executing, so the latest trends in ransomware will not be missed.

Whether used in conjunction with our Application Whitelisting or alone, ThreatLocker® RingFencing™ increases protection against Ransomware to a new level. Rather than simply trying to allow or deny an application from running, ThreatLocker® RingFencing™ controls what applications can and cannot do in the system. If an application attempts to perform unauthorized functions such as accessing or encrypting your data, it will be blocked.

When ThreatLocker® RingFencing™ is used with ThreatLocker® Application Whitelisting, businesses enjoy well above enterprise-level security without the overhead of traditional application control.

THREATLOCKER®

Stop Zero-day Malware

ThreatLocker® uses Application Control techniques such as RingFencing™ and Application Whitelisting to stop zero-day malware threats.

Malware creators are getting faster and faster at releasing new threats. Last year, nearly 1 million new pieces of malware were created each day. Antivirus vendors use methods such as definition files with a list of known viruses and heuristic methods to try and identify if a file is a virus.

Unfortunately, this kind of old school way of thinking leaves you vulnerable and at risk of being infected by a virus or malware from zero-day attacks. It only takes a few minutes for malware to copy your data or encrypt your files, but it takes hours or even days for antivirus vendors to update their definitions.

ThreatLocker® uses a more logical approach to stop viruses and malware from affecting your business. ThreatLocker® Application Control uses a combination of Application Whitelisting and RingFencing™ to protect your business from known and unknown malware threats.

With ThreatLocker® RingFencing™ software applications are ring fenced inside a perimeter, preventing them from launching attacks on your system and severely limiting any damage caused by malware or vulnerabilities in applications.

ThreatLocker® Application Whitelisting stops any application files, script files or libraries from running that are not explicitly trusted by your business. If a user opens a file that appears to be a Microsoft Word document but turns out to be a virus, it is blocked by ThreatLocker Application Whitelisting.

Our "default deny" approach gives you, the IT administrator, control over what software is running. Regardless of whether the virus appears as a macro in a word document, disguised as good software that is downloaded by the user, or is opened by an attacker who exploited your system, the ThreatLocker® Application Control blocks the file from running and keeps your system safe.

THREATLOCKER®

Protecting Against Fileless Malware Threats

ThreatLocker® RingFencing™ protects businesses against fileless malware by controlling what applications and code a hijacked processes can run.

Fileless Malware is a type of malware that only exists in memory. It does not run from the computer's hard drive like most types of malware.

Malware embedded in a Microsoft Office document that downloads and executes a file, then removes itself, is often considered as fileless. However, this is not technically accurate, and this type of malware is dealt with differently from true fileless malware (see our Macro Viruses and Malware section). True fileless malware does not save any files to the hard drive and is often very difficult to detect by an antivirus.

Fileless malware can operate using several methods. The most common method is when the application that opens a document is able to download and run a script using a built-in windows application such as Rundll32. The script is loaded into memory using RunDll32 and continues to run unbeknownst to the user.

A less common method in fileless malware operation is active when a vulnerability is exploited in an application, such as a PDF reader. A script attaches itself to that process and can be used to copy or CryptoLocker your data. This method is more relevant for computers that are not patched.

ThreatLocker Application Control, in combination with our RingFencing™ technology, is able to control fileless malware by monitoring application behavior and stopping it from stepping outside its normal boundaries. If an application attempts to perform actions that fall outside of acceptable behavior, ThreatLocker® Application Control blocks the action, stopping the threat in its tracks. In addition, even if the application is vulnerable, ThreatLocker is able to RingFence™ the application, so the amount of damage caused by fileless malware or a rogue application is massively reduced.

THREATLOCKER®

"ThreatLocker has given us the control we needed, without causing overhead on our I.T. Resources" - Danielle Hutcheson, Business Manager - Lake Forrest Preparatory School"

How ThreatLocker® helps with real life problems

A user receives an email with a file that executes a program on your computer. Antivirus is unable to detect most of today's malware, which can allow an attacker remote access to your system.	ThreatLocker® blocks all software that is not allowed by your I.T department, virtually eliminating the risk of malware enabling an attacker to gain control. ThreatLocker's whitelisting solution is as close to a silver bullet as you can get.
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, which encrypts all of the files on your shared network drive.	ThreatLocker® Ring Fences your applications, so they can only access the data they need to. This massively reduces the risk of a data breach from a hijacked process without interrupting users.
A rogue employee copies customer data files to a USB drive before leaving for a competitor company.	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.
When trying to download some legitimate software, a user accidentally clicks on the Ad link which has a similar download button. The software contains malware.	ThreatLocker® identifies applications from our built-in database and blocks the user from executing software that is not permitted
A user receives a Word document by email, that when opened swaps out a system DLL file to malware.	ThreatLocker® maintains a system database of all Windows Update files and their matching hash. In the case of a file modified or replaced ThreatLocker® blocks the modified file.