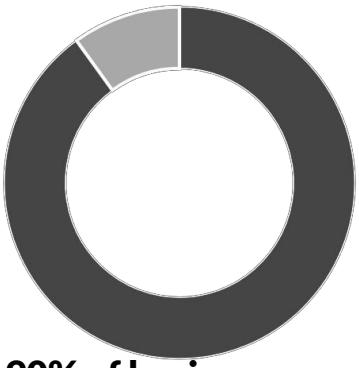
THREATLOCKER®

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 provides an application control solution that allows you to choose what executables and libraries are running. Unlike antivirus software which only blocks known threats, ThreatLocker changes the paradigm to only allowing authorized applications, while giving you a complete insight of everything that runs.

ThreatLocker extends that application control to storage devices. Ensuring your applications are not accessing or destroying your files.



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 authorized access to your 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.
- Application Updates can update apps.

Simple Approval

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

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® puts ring fences around 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® puts ring fences around your applications, so they can only access the data they need to, massively reducing the risk of a data breach from a hijacked process without interrupting users.
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 our 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.