ThreatLocker User Guide

Contents

What is ThreatLocker?

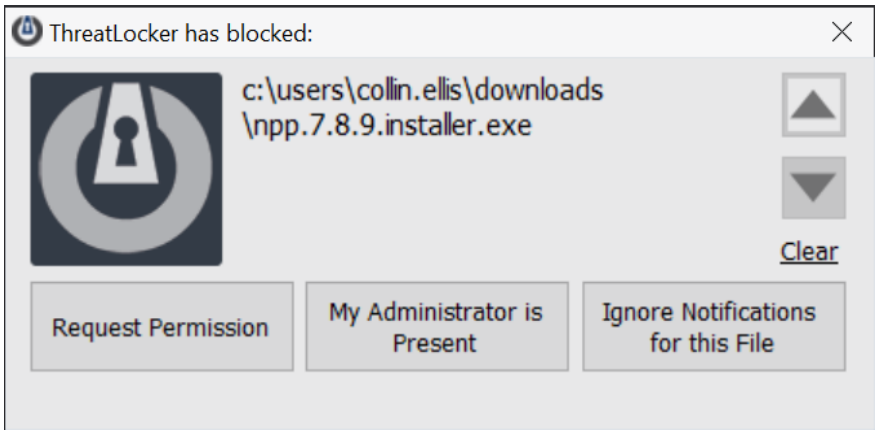
ThreatLocker is an application that enforces a Zero-Trust approach on computers to prevent aggressive malware and viruses from invading businesses. ThreatLocker's Application Control offers a level of protection that makes it increasingly difficult for a user to run ransomware knowingly or unknowingly. Unlike antivirus software, Application Control blocks all untrusted code from executing, so the latest trends in ransomware will not be missed. Whether used in conjunction with Application Control or alone, ThreatLocker's RingFencing increases protection against ransomware to a new level. Rather than simply trying to allow or deny an application from running, RingFencing controls how applications interact with the rest of your systems. If an application attempts to perform unauthorized functions such as accessing your data, it will be blocked.

How does ThreatLocker know what to block?

When ThreatLocker is first deployed, it immediately enters a state called Learning Mode. During this time, ThreatLocker does not block any application functions. Instead, it catalogues and audits all application functions on your computer for review. Well known applications such as Microsoft Office, Adobe, Citrix, and many others are automatically categorized and whitelisted by ThreatLocker engineers. Other lesser known third-party applications are then reviewed on a per case basis to ensure only legitimate activities are authorized to run on your computer. After this review has been completed, Learning Mode is terminated, and computers will enter a state called Secured Mode. Only those applications which have been pre-authorized during the review process will be able to run freely.

How do I request permission for legitimate, but unauthorized activities?

ThreatLocker blocks any unapproved software, including ransomware, viruses, and other malicious software. Should you run any applications that have not been previously approved, you will receive a notification (see image below) prompting you to request permission or ignore it if it is not needed for your day-to-day business functions. Selecting the “Request Permission” button will automatically create a ticket with our Help Desk where a technician can review the request and ensure the application is not malicious in nature and approve it if appropriate. You will then be notified via e-mail once the request has been processed and a determination has been made. To expedite this process, please let us know in advance if you need any new software installed by creating a ticket with the Help Desk.



How do I know ThreatLocker is running on my computer?

ThreatLocker is currently only available for Windows OS. An application icon with they keyhole logo will be visible on the system tray found on the bottom right-hand side of your screen (default).