THREATLOCKER®

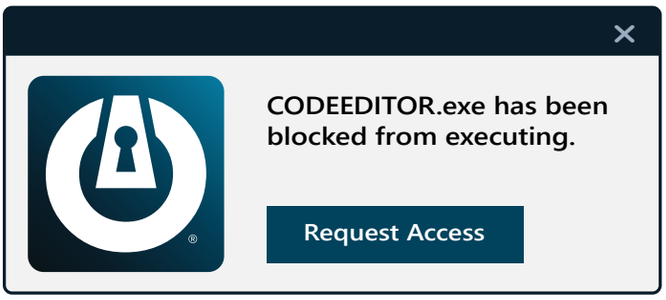
ZERO TRUST ENDPOINT PROTECTION PLATFORM

Introducing Zero Trust

As part of an ongoing effort to ensure all systems are secure, we are now adding a Zero Trust approach to your security stack. As attackers become more sophisticated, so do the complexities in stopping software-based threats. The techniques and solutions we are implementing are regularly adopted by large governments and other enterprise organizations. As your managed service provider, we understand the use of a higher grade of security is fundamental in protecting you from the latest threats.

What is Zero Trust?

Zero Trust is a security framework which states that organizations should not trust any entity inside or outside of their perimeter at any time. It is necessary in today's environment to provide the visibility and IT controls needed to secure, manage and monitor every device, user, app and network being used to access business data.



ThreatLocker® Helps With:

- Layered Security
- Ransomware Prevention
- Compliance
- Internal Disputes
- Storage Control
- Data Privacy

What Does This Mean for You?

As of today, ThreatLocker® will be running on your PCs, and blocking any unapproved software, including ransomware, viruses, and other malicious software.

Should you run any applications that are not approved, you will receive a notification prompting you to request access or ignore if it's not needed for your day-to-day business functions.

Selecting the "Request Access" button will notify us. We will review the request and ensure the application is not malicious in nature and approve if appropriate.

As such, it is vital to let us know in advance if you need any new software installed by entering a ticket with the service desk.