IPO Digital Solutions

Your Business I.T. Specialists

THREATLOCKER

Unified Audit

See granular details of every single application, script, or library opened on your endpoints in real-time. Including desktop, servers, and even laptops if they are in or out of the office.

Ringfence Applications

Control application access to resources, including network, registry, and file. Backed up by a real-time audit of all network resources your applications are accessing.

Firewall Like Application Policies

A powerful firewall like policy engine that allows you to permit, deny or restrict application access at a granular level.

Time-based policies

Permit access to applications for a specified amount of time. Automatically block the application after the policy has expired.

Application Control

Features:

- Full granular audit of every executable, script, or library executed on your endpoints
- Default deny application whitelisting approach to deny anything not trusted by your business
- Thirty seconds single click approval
- Stop fileless malware and limit damage from application exploits
- Define how applications can integrate with other applications
- ThreatLocker automatically adds new hashes when application and system updates are released

Storage Control

ThreatLocker gives you granular control over file and storage device access that does more than just blocking USB ports**.**

Most data protection programs on the market are butcher knife solutions to a problem that requires a scalpel. Blocking USB drives and encrypting data-storage servers can help secure your organization's private data, but these tools don't take into account that this data still needs to be utilized and quickly. Waiting for approval or trying to find a device that's allowed to access needed files can drain hours of productivity.

ThreatLocker Storage Control is an advanced storage control solution that protects information. We give you the tools to control the flow and access of data. You can choose what data can be accessed, or copied, and the applications, users, and computers that can access said data. By using ThreatLocker, you are in control of your file servers, USB drives, and your data.

Features:

- A full audit of all file access on USB, Network and Local Hard Drives
- Restrict or deny access to external storage, including USB drives, network shares, or other devices
- Single-click approval for specified devices or users
- Approve for a limited amount of time or permanently
- Restrict access to specific file types, for example only permit access to jpeg files from a camera
- Limit access to a device or file share based on the application
- Enforce or audit the encryption status of USB hard drives and other external storage

Elevation Control

ThreatLocker Elevation Control connects to its cloud-based Application Control Suite to add an extra layer of security by creating access policies for individuals on specific applications.

The addition of PAM combined with ThreatLocker's Application Whitelisting and Ringfencing solutions enables you to control what applications can run, who can access them, and how they interact in an organization's environment.

Features:

- **Complete Visibility of Administrative Rights:**

  Gives you the ability to approve or deny an individual's access to specific applications within an organization even if the user is not a local administrator.

- **Streamlined Permission Requests:**

  Users can request permission to elevate applications and attach files and notes to support their requests.

- **Varied Levels of Elevation:**

  Enables you to set durations for how long users are allowed access to specific applications by granting either temporary or permanent access.

- **Secure Application Integration**

  In combination with ThreatLocker Ringfencing, ensures that once applications are elevated, users cannot jump to infiltrate connected applications within the network.