THREATLOCKER® DETECT

DETECT FEATURES

Alerts and Detection

Using industry-known indicators of compromise, ThreatLocker® Detect can identify and alert IT professionals that their organization may be under an attempted attack based on customizable thresholds and notification methods.

Leverage Knowledge

IT admins can easily share their own ThreatLocker® Detect policies or “shop” for vetted policies shared by their industry peers and the ThreatLocker® team.

Respond

Set policies to enable, disable, or create Application Control, Storage Control, or Network Control policies in response to specified observations.

Set Custom Thresholds

Policies can be tailored to alert and respond differently based on the threat level to reduce alert fatigue.

ThreatLocker® Detect

ThreatLocker® Detect is a policy-based Endpoint Detection and Response (EDR) solution. This EDR addition to the ThreatLocker® Endpoint Protection Platform watches for unusual events or Indicators of Compromise (IoCs). ThreatLocker® Detect can send alerts and take automated actions if an anomaly is detected.

ThreatLocker® Detect leverages the vast telemetry data collected from other ThreatLocker® modules and Windows Event logs. This information gives essential insights into an organization’s security, enabling them to identify, respond to and remediate possible cyber threats.

Why ThreatLocker® Detect?

ThreatLocker® Detect has an edge over other EDR tools in detecting and responding to potential threats. Its advanced technology identifies and addresses known malicious activities while providing visibility of threats beyond just known ones.

ThreatLocker® Detect’s automated responses can give information, enforce rules, disconnect machines from the network, or activate Lockdown mode quickly. When Lockdown mode starts, it blocks all activities, including task execution, network access, and storage access, ensuring maximum security.

With the capability of detecting remote access tools or PowerShell elevation, ThreatLocker® Detect also identifies events such as abnormal RDP traffic or multiple failed login attempts, an event log is erased or if Windows Defender finds malware on a device. This proactive approach enables organizations to swiftly identify and respond to potential threats before they can cause significant damage.

Managed Detection and Response with the ThreatLocker® Cyber Hero Team

ThreatLocker® Detect compliments ThreatLocker® Zero Trust functionality and elevates protection of an environment. The 24/7/365 availability of the ThreatLocker® Cyber Hero Team offers an around-the-clock Managed Detection and Response (MDR) service to keep organizations secure and alert, even outside of hours of operation.

How does ThreatLocker® Detect work?

ThreatLocker® Detect continuously monitors the behavior of trusted and untrusted applications across all devices where the ThreatLocker® Agent is installed.

> ***IT experts can make custom rules and policies for decision-making instead of relying on AI or standardized criteria.***

These policies can have a set of conditions or responses that look for behaviors based on a threshold that indicates a compromise may have occurred. When conditions are met, ThreatLocker® Detect will automatically respond based on the rules created.

Policies are continually evaluated in real-time by the ThreatLocker® agent on the endpoint, which means policies are enforced in milliseconds whether or not the endpoint is connected to the internet. IT experts can have complete control over their priorities and event responses. This level of automation and control ensures that incident response actions align with the organization's overall security strategy.

Community-Shared Policies

ThreatLocker® offers recommended policies based on frameworks such as MITRE and CISA Indicators of Compromise. ThreatLocker® has introduced a platform known as "ThreatLocker® Community". IT experts can share policies they created with other members of the ThreatLocker® Community on the platform.

About ThreatLocker®

ThreatLocker® is a Zero Trust endpoint protection platform that improves enterprise-level server and endpoint security with Zero Trust controls, including: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker® Detect, Elevation Control & Configuration Manager.

sales@threatlocker.com

+1-833-292-7732

threatlocker.com