THREATLOCKER®

Managed Detection & Response
by The Cyber Hero Team

Unleash the full potential of the ThreatLocker® Detect Endpoint Detection and Response (EDR) solution with managed services from the 24/7/365 ThreatLocker® Cyber Hero Team.

MDR 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.

What is ThreatLocker® Cyber Hero Managed Detection & Response? (MDR)

CHMDR is an add-on to ThreatLocker® Detect that allows organizations to opt for the ThreatLocker® Cyber Heroes to monitor and respond to Indicators of Compromise (IoC).
When ThreatLocker® Detect identifies suspicious activity in your environment, the Cyber Hero Team will review the alert to determine if there is a true IoC or a false positive. In the event of a cyber incident, the Cyber Hero will follow the customer’s runbook to either isolate or lock down the device and notify the customer. They will be able to identify additional information for the customer, including:

- What the threat was
- How initial access was gained
- Where the threat originated
- What the threat attempted to do
- How the threat was blocked and mitigated

Prompt Notifications 24/7/365

The 24/7/365 availability of the ThreatLocker® Cyber Hero Team offers around-the-clock Managed Detection and Response (MDR) services to keep organizations secure and alert even outside of standard hours of operation.

The Cyber Hero Team has an average response time of less than 60 seconds.

This metric is unique to ThreatLocker® and provides a significant advantage when responding to threats. By augmenting the ThreatLocker® Zero Trust Endpoint Protection Platform with managed detection and response services, customers can reduce agent fatigue while hardening their environment to the highest standards, ensuring the mitigation and notification of attempted attacks.

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