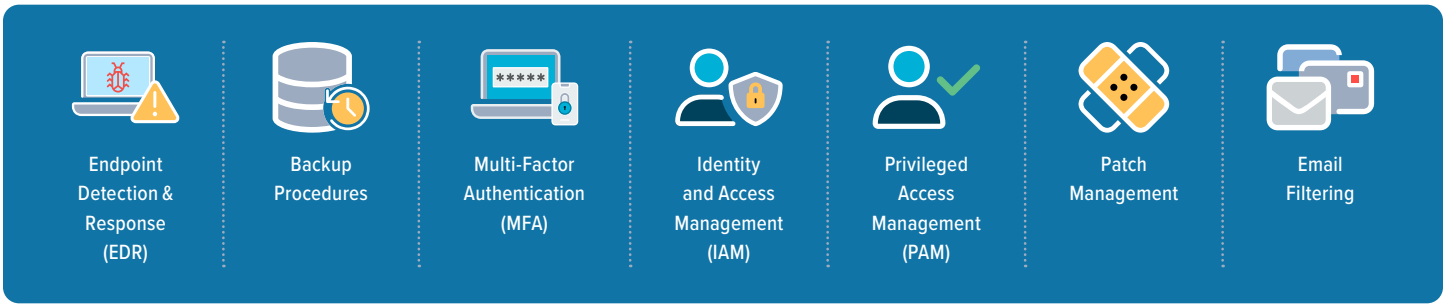
ThreatLocker® & Cyber Insurance



Although cyber insurance requirements will vary depending on the specific coverage and carrier being used, they all include some basic cybersecurity practices. When configured correctly, the ThreatLocker® Endpoint Protection Platform can assist with meeting the core cyber insurance requirements listed below.

Endpoint Detection & Response (EDR) implemented on all endpoints

ThreatLocker® is an Endpoint Protection Platform that uses a default deny approach. All applications, scripts, and libraries will be blocked unless expressly permitted, which stops malware, including zero-days, before they can run. ThreatLocker® Ops can alert that the behavior was attempted. Allowlisting and Ringfencing™ will have stopped threats before they began, and Ops can alert and respond to IOCs based on thresholds set by the IT admin.

Backup Procedures, Offline Backup, or Alternative Backup Solutions

ThreatLocker® Storage Control can be used to help secure backup files. Restrict access to backup files, only permitting specified backup software or users to access them. ThreatLocker® Storage Control can enforce encryption on removable media to protect backups stored there. ThreatLocker® Configuration Manager can alert if full disk encryption is not enabled on computers storing backup files.

Identity and Access Management (IAM) for ad-hoc privileges and restricted network access

Application Allowlisting provides the ability to control which users can run which applications. Storage Control can be used to control which users can access which data locations. Network Control gives the ability to close all ports on all endpoints and create policies to open the port needed for permitted access on-demand, automatically, and closes the ports once they are no longer being used, restricting network access down to the least privileged access. ThreatLocker® Configuration Manager can monitor all logon activity and alert on unsuccessful login attempts. ThreatLocker® Elevation Control provides as-needed admin privileges to specific applications that require it, and only for permitted users.

Privileged Access Management (PAM) to monitor accounts with privileged access

ThreatLocker® Elevation Control is a PAM solution. It enables admins to reduce or eliminate local admin credentials, creating policies that automatically elevate specific applications that require it. The Unified Audit will log all actions performed using elevated privileges.

Email Filtering

ThreatLocker® Configuration Manager can disable downloaded Office macros. ThreatLocker® Allowlisting and Ringfencing™ work in tandem to provide protection against malware, reducing the likelihood of successful malware infection via email. Together, these provide most of the same protection as email filters.

THREATLOCKER®

About Us

ThreatLocker® is a zero trust endpoint protection platform that improves enterprise-level security with zero trust controls, including Allowlisting, Ringfencing™, Elevation, Storage, Network Control, Configuration Management, and Operational Alert solutions.

Learn more about ThreatLocker® at

www.threatlocker.com

sales@threatlocker.com
+1-833-292-7732

ThreatLocker_and_Cyber_Insurance_0622023