THREATLOCKER®
ZERO TRUST PLATFORM

LÖSUNGSÜBERSICHT ZUSAMMENFASSUNG

Einleitung

Erkennungsbasierte Lösungen (Detection) sind nicht mehr ausreichend im modernen Cybersecurity Stack. Es ist Zeit, “Lebwohl” zu traditionellen Erkennungstools zu sagen und „Hallo“ zur nächsten großen Innovation in der Cybersicherheit.

Die frühen Tage des Internets, in denen eine Antivirensoftware die einzige Schutzmaßnahme gegen Cyber-Bedrohungen war, sind längst vorbei. Da Antivirus-Lösungen nicht mehr in der Lage sind, moderne Formen von Cyberangriffen wie Ransomware zu stoppen, wurden neue Tools, z.B. Endpoint Detection and Response (EDR), entwickelt.

Doch selbst EDR-Systeme haben Schwächen – allen voran die Tatsache, dass Bedrohungen erst erkannt werden, nachdem sie bereits in Ihr System eingedrungen sind. Ihr Unternehmen braucht eine Zero-Trust-Sicherheitslösung für alle Endpunkte, die Bedrohungen stoppt, bevor sie in Ihrer Umgebung ausgeführt werden können.

Stoppe Ransomware, betrügerische Apps und Zero-Day-Exploits, bevor sie ausgeführt werden.

Wir haben die ThreatLocker® Zero Trust Protection Platform entwickelt, weil es unmöglich ist, jeder neuen Malware einen Schritt voraus zu sein. Mit ThreatLocker haben wir den Spieß umgedreht. Anstatt Cyberkriminelle aktiv per Detection und Threathunting zu jagen, blockieren wir sie. Lassen Sie in Ihrem Unternehmen die Applikationen zu, die Sie ausdrücklich brauchen und auf die Sie vertrauen. Alles andere wird standardmäßig blockiert.

ThreatLocker und unser Cyber Hero® Team sind rund um die Uhr an 365 Tagen im Jahr im Einsatz und helfen Ihnen in 60 Sekunden bei jedem Problem. Unsere proaktive, richtliniengesteuerte Sicherheit ist darauf ausgelegt, Abläufe zu vereinfachen und Ihre Umgebung sicher abzuriegeln. All dies wird durch unseren erstklassigen, einmaligen Support von echten Menschen unterstützt, die wissen, wie man schnell handelt, wenn es für Sie am wichtigsten ist.

THREATLOCKER® PROTECT

Application Allowlisting

ThreatLockers Application Allowlisting ist eine leistungsstarke Deny-by-Default-Lösung, die die Anwendungskontrolle (Application Control) vereinfacht. Nur vertrauenswürdige, erlaubte Software kann ausgeführt werden. Alles andere, einschließlich Ransomware, wird standardmäßig blockiert. Sie behalten die Kontrolle über Ihre Umgebung.

- **Deployment und Lernmodus:** Automatisches Katalogisieren von Anwendungen und deren Abhängigkeiten. Mit der Erkennung von Tausenden vorgefertigten Applikationen erhalten Sie sofortige Sichtbarkeit und optimierte Policy-Vorschläge ohne manuellen Aufwand.
- **Genehmigen Sie, worauf Sie vertrauen:** Wählen und genehmigen Sie Applikationen und Software mit einem Klick. Alles andere - unerlaubte Apps, Skripte oder Bibliotheken werden standardmäßig blockiert.
- **Neue Applikationen einfach hinzufügen:** End-User fragen den Zugriff auf neue Apps einfach über ein Popup an. Die IT-Abteilung kann zustimmen oder das Cyber Hero®-Team kann in etwa 60 Sekunden antworten..

Das Ergebnis? Eine schnelle Bereitstellung und Konfiguration des Allowlisting-Ansatzes. Einfacher zu skalieren. Leicht und leistungsstark. Einsatzfähig in 2 bis 6 Wochen.

Ringfencing™

ThreatLocker Ringfencing ist Ihre Strategie zur uneingeschränkten Anwendungskontrolle. Es ermöglicht bereits erlaubten Applikationen die Ausführung und beschränkt dabei die Interaktionen ausschließlich auf die benötigten Dateien, Registrierungsschlüssel, Netzwerkressourcen oder Apps. Es stellt sicher, dass Anwendungen nur das tun, wozu sie bestimmt sind, und nichts darüber hinaus. Dadurch hebt es Ihre Application Control auf ein ganz neues, in der Cybersecurity-Industrie bisher unerreichtes Niveau.

- **Bereitstellung mit Standard-Ringfencing-Policies:** Basisrichtlinien gelten sofort für gängige Apps wie Microsoft Office, PowerShell und Zoom; eine Einrichtung oder Konfiguration ist nicht von Ihnen erforderlich.
- **Mit Präzision anpassen:** Möchten Sie, dass PowerShell ausgeführt wird, aber offline bleibt? Oder Word, um Dokumente zu öffnen, ohne andere Apps zu starten? Sie legen die Regeln fest.

Bonus: Das rund um die Uhr verfügbare Cyber Hero ® Team von ThreatLocker hilft bei der schnellen Feinabstimmung von Richtlinien mit einer Reaktionszeit von etwa 60 Sekunden. Die Ergebnisse? Weniger Risiko. Strengere Kontrolle. Keine übermäßige Anwendung mehr.

Network Control

ThreatLocker® Network Control ist eine hostbasierte Firewall, die für Endpunkte und Server entwickelt wurde. Sie ermöglicht Ihnen die vollständige Kontrolle über den gesamten Netzwerkverkehr. Sperren Sie den Zugriff nach Port, Quell-IP-Adresse oder dynamisch mit ACLs, die sich bei Änderungen der IP-Adressen automatisch aktualisieren. Kurz gesagt: Sie entscheiden, wer reinkommt.

- Legen Sie Endpoint-Firewall-Richtlinien für jeden Endpunkt von einer zentralen Konsole fest.
- Wenn eine Verbindungsanfrage eingeht, prüft ThreatLocker®, ob das Gerät autorisiert ist.
- Wenn dies der Fall ist, öffnet sich der Port automatisch. Falls nicht, bleibt der Port geschlossen und unsichtbar
- Sobald eine autorisierte Verbindung endet, schließt sich der Port innerhalb von Minuten automatisch.

Das Ergebnis? Eine sicherere Umgebung und mehr Schutz vor unberechtigtem Netzwerkzugriffen.

Mehr Möglichkeiten, deine Zero-Trust-Strategie zu stärken

Entdecken Sie zusätzliche Tools, die Ihre Zero Trust-Umgebung intelligenter und sicherer machen und dabei einfacher zu verwalten sind.

Storage Control

Verhindern Sie unerwünschte Datenzugriffe mit differenzierter Speicherkontrolle

ThreatLocker® Storage Control gibt Ihnen die volle Kontrolle darüber, auf welche Daten wann und wie zugegriffen werden darf. Legen Sie präzise, granulare Richtlinien fest, die auf Benutzern, Anwendungen, Geräten und Kontexten basieren, und zwar für lokale Ordner, Netzwerkfreigaben, USB-Geräte und Cloud-Speicher. Das Ergebnis? Ein stärkerer Schutz vor Datenschutzverletzungen, Insider-Bedrohungen und unbefugten Zugriffen.

Elevation Control

Stoppen Sie den Missbrauch von Admin-Rechten: Erhöhen Sie die Rechte von einzelnen Anwendungen, nicht von gesamten Benutzern

ThreatLocker® Elevation Control stoppt den Missbrauch lokaler Administratorrechte, indem es Anwendungen – nicht Benutzern – erweiterte Rechte gewährt. Genehmigte Anwendungen können mit erhöhten Rechten ausgeführt werden. Braucht eine neue Anwendung erweiterte Rechte? Dann kann der User eine einfache Anfrage per Popup stellen, für die keine weiteren Administratoranmeldeinformationen erforderlich sind. Darüber hinaus kann Elevation Control unnötige oder ungenutzte Administratorkonten entfernen und macht die Eingabe von Anmeldeinformationen an Endgeräten durch Administratoren überflüssig. Weniger Privilegien, ein reduziertes Risiko und mehr Kontrolle - so härten Sie Ihre Umgebung gegen unerwünschte Angriffe und Missbrauch.

Configuration Manager

Erzwinge Best-Practice-Sicherheit über eine leistungsstarke Konsole

Der ThreatLocker® Configuration Manager gibt Ihnen die volle Kontrolle über eine einzige, zentrale Konsole, um bewährte Sicherheitsrichtlinien und Konfigurationen auf jedem Gerät durchzusetzen. Dabei spielt es keine Rolle, ob das Gerät mit einem einzelnen Active.

Directory verbunden ist oder nicht. Konfigurationsrichtlinien können einfach pro Gerät, Gruppe, Organisation oder für die gesamte Umgebung festgelegt und verwaltet werden. Über eine leistungsstarke Schnittstelle können Sie schnell Einstellungen wie das Deaktivieren von Universal Plug and Play, das Blockieren von SMBv1, das Erzwingen automatischer Sperrrichtlinien und vieles mehr festlegen. Vereinfachen Sie das Management, stärken Sie die Sicherheit, übernehmen Sie die Kontrolle.

Threatlocker Detect

Bedrohungen sofort erkennen und neutralisieren

ThreatLocker® Detect ist eine leistungsstarke Endpoint Detection and Response (EDR)-Lösung, die entwickelt wurde, um Bedrohungen sofort zu identifizieren, zu reagieren und sie automatisch in Echtzeit zu isolieren. Threatlocker Detect analysiert unermüdlich Telemetriedaten, Verhaltensmuster und Indikatoren für Kompromittierungen (IoCs) und wird sofort aktiv, sobald verdächtige Aktivitäten erkannt werden. Keine kritischen Zeitverzögerungen mehr für eine schnelle Bedrohungsneutralisierung, denn im Ernstfall zählt jede Sekunde.

Cloud Detect

Microsoft 365 gegen Bedrohungen schützen

ThreatLocker® Cloud Detect durchleuchtet Ihre Microsoft-365-Umgebung und bietet Ihnen umfassende Transparenz und Kontrolle. Es überwacht kontinuierlich M365-Protokolle und kennzeichnet echte Bedrohungen, wie z.B. abgeflossene Anmeldeinformationen, verdächtige Anmeldungen, unmögliche Reisen oder riskantes Verhalten.

Und das Beste: Sie legen die Regeln fest. Mit vollständig anpassbaren Richtlinien (Policies), die Microsoft 365- und Graph-API-Protokollfelder verwenden, benachrichtigt Sie Cloud Detect umgehend, sodass Sie schneller reagieren und neuen Bedrohungen immer einen Schritt voraus sind.

Cyber Hero® MDR

Elite-MDR mit einer Response in 60 Sekunden

ThreatLocker® Cyber Hero MDR ist ein vollständig gemanagter Detection-and-Response-Service (MDR), der auf ThreatLocker Detect aufgebaut. Der Service bietet Ihnen eine direkte Verbindung zu unserem Elite-Cyber Hero®-Team von ausgebildeten Sicherheitsexperten, die Alarme überwachen, Bedrohungen validieren und schnell gemäß Ihrem Playbook handeln. Wie schnell? Wir reagieren in 60 Sekunden auf jede Bedrohung, schneller als jeder andere in der Branche. Während andere noch Telemetriedaten mit der Cloud synchronisieren, isolieren wir bereits kompromittierte Geräte und stoppen Bedrohungen, bevor sie sich ausbreiten.

Cloud Control

Schützen Sie Microsoft 365 vor Phishing und Token-Diebstahl

Cloud-Control ist Ihr neuer leistungsstarker Verbündeter, um Ihren Microsoft 365-Tenant vor Phishing-Angriffen und Token-Diebstahl zu schützen. Mit einer hochmodernen im Kern integrierten Intelligenzfunktion verfolgt ThreatLocker Cloud Control automatisch die geschützten Geräte Ihrer Benutzer, zeichnet deren IP-Adressen auf und ermittelt mit hoher Präzision die vertrauenswürdigen Verbindungen. Alle Aktualisierungen erfolgen automatisch, ohne eine manuelle Konfiguration im Conditional Access zu benötigen.

Patch Management

Vereinfachen Sie Ihr Patching mit einer automatisierten, zentralisierten Verwaltung

ThreatLocker® Patch Management fungiert als wachsamer Wächter, der Ihre Geräte ständig auf veraltete Software scannt und Anwendungen identifiziert, die gepatcht werden müssen. Es übernimmt die mühsame Arbeit und beseitigt die Notwendigkeit, verschiedene Quellen für unterschiedliche Warnungen zu überprüfen, indem es alles an einem Ort zusammenführt. Anstatt unnötige Zeit mit der Recherche und Entscheidung über jeden ausstehenden Patch zu verbringen, übernimmt das Patch-Management alles für Sie.

Insights

Unterüberschrift: Leistungsstarke Endpunkt-Intelligenz für bessere Security-Entscheidungen

ThreatLocker® Insights greift auf Daten von Millionen Endpunkten weltweit zu und bietet Ihnen einen klaren Überblick über die Nutzung und Trends bei der Einführung von Anwendungen. Durch das Benchmarking von realen Daten und Entscheidungen von IT-Fachleuten befähigt Threatlocker Insights Sie, klügere und schnellere Sicherheitsentscheidungen zu treffen, damit Ihr Netzwerk ohne Rätselraten und mühsame Recherchen geschützt bleibt. Sie sparen viel Zeit an mühsamer Recherche und machen Ihre Umgebung zukunftssicher, indem Sie die bessere Entscheidungen treffen

Web Control

Blockieren Sie Phishing und schützen Sie jedes Gerät in Ihrem Netzwerk

ThreatLocker® Web Control vereinfacht Ihnen die Verwaltung des Webzugriffs, ohne auf zusätzliche Drittanbieter-Tools angewiesen zu sein. Es blockiert Phishing-Bedrohungen mit Echtzeitinformationen und setzt Richtlinien auf sowohl verwalteten als auch nicht verwalteten Geräten durch.

Umfangreiche, automatisch aktualisierte Bibliotheken und vordefinierte Kategorien ermöglichen es Ihnen, unerwünschte Websites einfach zu blockieren. Benutzer werden auf eine Unternehmensseite umgeleitet (keine DNS-Weiterleitung), wodurch Zertifikatsfehler vermieden werden. Brauchen Sie eine blockierte Website? Dann geben Sie diese mit nur wenigen Klicks frei.

Web Control wendet Ihre Richtlinien (Policies) auch auf private und Gastgeräte in Ihrem Netzwerk an, reduziert das Risiko und hilft Ihnen, die DSGVO, HIPAA und PCI DSS einzuhalten – mit weniger Aufwand.

Threatlocker User Store

Unterüberschrift: Supportanfragen reduzieren und Schatten-IT verhindern

Der ThreatLocker® User Store ist ein Katalog (Repository) vorab genehmigter Anwendungen, der es End-Usern ermöglicht, die benötigten Apps selbständig zu installieren und auszuführen, ohne Ihre Cybersicherheitslage zu gefährden oder unnötige Arbeit für die IT zu verursachen.

Nach der Konfiguration fungiert der User Store als zentraler Hub für die Genehmigung von Apps und die Verwaltung von Lizenzschlüsseln. Er verwaltet aktiv den Zugriff und weist Lizenzschlüssel zu, sodass Ihre User die genehmigte Software problemlos und ohne Verzögerungen oder zusätzliche Supportanfragen installieren können.

Kein Hin und Her mehr zwischen Benutzern und der IT. Kein Risiko mehr durch Schatten-IT oder unautorisierte Installationen. Benutzer erhalten, was sie zum Arbeiten benötigen, ohne die Zero-Trust-Prinzipien zu verletzen.

Über ThreatLocker®

ThreatLocker ist eine Zero-Trust-Plattform zum Schutz von Endpunkten, die die Sicherheit von Servern und Endgeräten auf Unternehmensebene mit Zero-Trust-Kontrollen verbessert, darunter: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker Detect, Elevation Control und Configuration Manager.

sales@threatlocker.com

threatlocker.com