

LÖSUNGSÜBERSICHT ZUSAMMENFASSUNG



Einleitung

Erkennungsbasierte Lösungen sind nicht mehr prominent im modernen Sicherheitsarsenal. Es ist Zeit, „Lebwohl“ zu traditionellen Erkennungstools zu sagen und „Willkommen“ zur nächsten großen Innovation in der Cybersicherheit.

Die frühen Tage des Internets, in denen Antivirensoftware die einzige Schutzmaßnahme gegen Online-Bedrohungen war, sind längst vorbei. Neue Tools wie Endpoint Detection and Response (EDR) wurden entwickelt, um die Lücken zu füllen, da Antivirus-Software nicht mehr in der Lage ist, moderne Formen von Cyberangriffen wie Malware zu stoppen.

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

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

Wir haben die ThreatLocker® Zero Trust Endpoint Protection Plattform entwickelt, weil es unmöglich ist, jeder Bedrohung einen Schritt voraus zu sein. Mit ThreatLocker haben wir also den Spieß umgedreht. Anstatt Cyberkriminelle zu jagen, blockieren Sie sie stattdessen. Sie lassen zu, was Sie ausdrücklich brauchen und worauf Sie vertrauen. Alles andere? Standardmäßig blockieren.

ThreatLocker und unser Cyber Hero® Team, das rund um die Uhr an 365 Tagen im Jahr im Einsatz ist und in etwa 60 Sekunden reagiert, haben nichts Traditionelles an sich. Unsere proaktive, richtliniengesteuerte Sicherheit ist darauf ausgelegt, Ihre Abläufe zu vereinfachen und Ihre Umgebung sicher abzuriegeln. All dies wird durch branchenverändernden, erstklassigen Support von echten Menschen unterstützt, die wissen, wie man schnell handelt, wenn es für Sie am wichtigsten ist.



THREATLOCKER® PROTECT

Zulassungslisten für Anwendungen

ThreatLocker Application Allowlisting ist eine leistungsstarke Deny-by-default-Lösung, die die Anwendungskontrolle vereinfacht. Nur vertrauenswürdige Software wird ausgeführt. Alles andere, einschließlich Ransomware, wird standardmäßig blockiert. Sie behalten die Kontrolle.

- ▶ **Bereitstellen im Lernmodus:** Automatisches Katalogisieren von Anwendungen und Abhängigkeiten. Mit der Erkennung von Tausenden vorgefertigter Apps erhalten Sie sofortige Sichtbarkeit, optimierte Listen und Richtlinienvorschläge ohne manuellen Aufwand.
- ▶ **Genehmigen Sie, worauf Sie vertrauen:** Wählen und genehmigen Sie Apps mit einem Klick. Alles andere, nicht genehmigte Apps, Skripte oder Bibliotheken, wird standardmäßig blockiert.
- ▶ **Neue Apps einfach hinzufügen:** Benutzer beantragen den Zugriff auf neue Apps über ein Popup. Die IT-Abteilung kann zustimmen, oder das Cyber Hero®-Team kann in etwa 60 Sekunden antworten.

Die Ergebnisse? Schnellere Bereitstellung von Allowlisting-Lösungen. Einfacher zu skalieren. Leicht und leistungsstark.



Ringfencing™

ThreatLocker Ringfencing ist Ihre Strategie zur Anwendungseindämmung. Es ermöglicht vertrauenswürdigen Apps die Ausführung, jedoch nur die Interaktion mit den Dateien, Registrierungsschlüsseln, Netzwerkressourcen oder Apps, die sie tatsächlich benötigen. Es stellt sicher, dass Apps nur das tun, wozu sie bestimmt sind, und nichts darüber hinaus.

- ▶ **Bereitstellung mit Standardschutzmaßnahmen:** Basisrichtlinien gelten sofort für gängige Apps wie Microsoft Office, PowerShell und Zoom; eine Einrichtung ist nicht 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.



Netzwerksteuerung

ThreatLocker® Network Control ist eine hostbasierte Firewall, die für Endpunkte und Server entwickelt wurde und Ihnen die vollständige Kontrolle über den gesamten Netzwerkverkehr ermöglicht. 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.

- ▶ Lege Firewall-Richtlinien für jeden Endpunkt von einer Konsole aus 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 die Tür geschlossen und unsichtbar.
- ▶ Sobald eine autorisierte Verbindung endet, schließt sich der Port innerhalb von Minuten automatisch.

Die Ergebnisse? Sicherere Umgebung und mehr Schutz vor unberechtigttem Netzwerkverkehr.

Mehr Möglichkeiten, deine Zero-Trust-Strategie zu stärken

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



Speicherkontrolle

Verhindern Sie Sicherheitsverletzungen mit differenzierter Speicherkontrolle

ThreatLocker® Storage Control gibt Ihnen die volle Kontrolle darüber, auf welche Daten wann und wie zugegriffen werden kann. Legen Sie präzise Richtlinien fest, die auf Benutzern, Anwendungen, Geräten und Kontexten basieren, und zwar für lokale Ordner, Netzwerkfreigaben, USB-Geräte und Cloud-Speicher. Nichts kommt durch, es sei denn, es erfüllt Ihre Sicherheitsregeln. Das Ergebnis? Stärkerer Schutz vor Datenschutzverletzungen, Insider-Bedrohungen und unbefugtem Zugriff.



Höhenkontrolle

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

ThreatLocker® Elevation Control stoppt den Missbrauch lokaler Administratorrechte, indem es Anwendungen – nicht Benutzern – erweiterte Rechte gewährt. Genehmigte Apps werden mit erhöhten Rechten ausgeführt. Benutzer benötigen nie vollen lokalen Administratorzugriff. Müssen Sie eine neue App verbessern? Es ist eine einfache Ein-Klick-Anfrage, für die keine Administratoranmeldeinformationen erforderlich sind. Darüber hinaus kann Elevation Control unnötige oder ungenutzte Administratorkonten entfernen und macht die Eingabe von Anmeldeinformationen an Standardendpunkten durch Administratoren überflüssig. Weniger Privilegien für weniger Risiken und mehr Kontrolle.



Konfigurationsmanager

Erzwingen Best-Practice-Sicherheit über eine leistungsstarke Konsole

Der ThreatLocker® Configuration Manager gibt Ihnen die volle Kontrolle über eine einzige, zentrale Konsole, um bewährte Sicherheitsrichtlinien auf jedem Gerät durchzusetzen, unabhängig davon, ob es 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.



Erkennen

Bedrohungen sofort erkennen und neutralisieren

ThreatLocker® Detect ist eine leistungsstarke, richtliniengesteuerte Endpoint Detection and Response (EDR)-Lösung, die entwickelt wurde, um Bedrohungen sofort zu identifizieren, darauf zu reagieren und sie automatisch und in Echtzeit zu isolieren. Sie analysiert unermüdlich Telemetriedaten, Verhaltensmuster und Indikatoren für Kompromittierungen (IoCs) und wird sofort aktiv, sobald verdächtige Aktivitäten erkannt werden. Verabschieden Sie sich von kritischen Zeitverzögerungen und begrüßen Sie die schnelle Bedrohungsneutralisierung.



Cloud Detect

Microsoft 365 gegen Bedrohungen schützen

ThreatLocker® Cloud Detect dringt tief in Ihre Microsoft 365-Umgebung ein und bietet Ihnen umfassende Transparenz und Kontrolle. Es überwacht kontinuierlich M365-Protokolle und kennzeichnet echte Bedrohungen, wie durchgesickerte Anmeldeinformationen, verdächtige Anmeldungen, unmögliche Reisen und riskantes Verhalten, das oft unbemerkt bleibt.

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



Cyber Hero® MDR

Elite-Bedrohungsreaktion in etwa 60 Sekunden

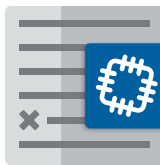
ThreatLocker® Cyber Hero MDR ist ein vollständig verwalteter Erkennungs- und Reaktionsdienst (MDR), der auf ThreatLocker Detect aufgebaut ist. Er bietet Ihnen eine direkte Verbindung zu unserem Elite-Cyber Hero®-Team, ausgebildeten Sicherheitsexperten, die Alarme überwachen, Bedrohungen validieren und schnell gemäß Ihrem Playbook handeln. Wie schnell? Wir antworten in etwa 60 Sekunden, 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-Kontrolle

Schützen Sie Microsoft 365 vor Phishing und Token-Diebstahl

Ihr neuer leistungsstarker Verbündeter, um Ihren Microsoft 365-Mandanten vor Phishing-Angriffen und Token-Diebstahl zu schützen. Mit einer hochmodernen integrierten Intelligenzfunktion im Kern verfolgt ThreatLocker Cloud Control automatisch die geschützten Geräte Ihrer Benutzer, zeichnet ihre IP-Adressen auf und ermittelt mit hoher Präzision die vertrauenswürdigen Verbindungen. Es hält Sie auf dem Laufenden. Keine manuellen Updates mehr.



Patch-Verwaltung

Vereinfachen Sie das Patchen mit automatisierter, zentralisierter Verwaltung

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



Insights

Unterüberschrift: Leistungsstarke Endpunkt-Intelligenz für klügere Sicherheitsentscheidungen

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 wie Ihnen befähigt Insights Sie, klügere und schnellere Sicherheitsentscheidungen zu treffen, damit Ihr Netzwerk ohne Rätselraten und mühsame Recherchen geschützt bleibt. Sie sparen Stunden – möglicherweise Tage – an mühsamer Recherche, vermeiden Rätselraten und machen Ihre Umgebung zukunftssicher, indem Sie die besten Entscheidungen treffen, um Ihre Sicherheitslage zu stärken.



Websteuerung

Blockieren Sie Phishing und schützen Sie jedes Gerät in Ihrem Netzwerk

ThreatLocker® Web Control vereinfacht 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, sich automatisch aktualisierende Bibliotheken und vororganisierte Kategorien ermöglichen es Ihnen, unerwünschte Websites einfach zu blockieren. Benutzer werden auf eine Unternehmensseite umgeleitet (keine DNS-Weiterleitung), wodurch Zertifikatsfehler und Verwirrung vermieden werden. Brauchen Sie eine Ausnahme? Erstellen Sie Ausschlüsse in nur wenigen Klicks.

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



Benutzerladen

Unterüberschrift: Supportanfragen reduzieren und Schatten-IT verhindern

Der ThreatLocker® User Store ist ein Katalog vorab genehmigter Anwendungen, der es Benutzern ermöglicht, die benötigten Apps 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 Benutzer 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 benötigen, um produktiv zu bleiben, ohne die Sicherheit zu gefährden oder 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

+1-833-292-7732

threatlocker.com