




EDR CORE Aktualisierung Ihres Sicherheitskonzepts durch Hinzufügen von EDR-Funktionen

Sicherheit für Netzwerke und Endpoints. Warum nicht beides?

Unternehmen konzentrieren sich zunehmend auf die Entwicklung robuster Cybersicherheitsverfahren, um ihre Netzwerke vor externen Bedrohungen zu schützen und ihre Endpoints zu überwachen, um Cyberkriminelle zu identifizieren, die mit fortschrittlichen Methoden eine Erkennung zu umgehen versuchen. Aber was passiert, wenn ein Cyberangriff unsere Verteidigungslinien überwindet? Verfügen wir über die geeigneten Technologien, um Angriffe zu erkennen, sobald sie sich innerhalb des Unternehmensnetzwerks befinden?

Ein durchschnittliches IT-Sicherheitsteam verwaltet Tausende von Endpoints in nur einem Netzwerk. Mit zunehmender Komplexität von Cyberbedrohungen, einschließlich Malware und Ransomware, die traditionelle Sicherheitsmaßnahmen wie Firewalls und Antivirensoftware umgehen können, merken Unternehmen, dass sie eine zusätzliche Sicherheitsebene benötigen – eine, die einen weitaus umfassenderen Einblick in die Aktivitäten auf den Endpoints bietet und verdächtiges Verhalten in Echtzeit erkennen und darauf reagieren kann.

Wesentliche Herausforderungen




Fortschrittliche
Bedrohungen

Viele fortschrittliche Bedrohungen, wie datei- und malwarelose Angriffe, Ransomware und APTs (Advanced Persistent Threats), sind so konzipiert, dass sie eine Erkennung auf Netzwerkebene umgehen und von traditionellen Endpoint-Lösungen nicht erkannt werden.



Eingeschränkte
Visualisierung

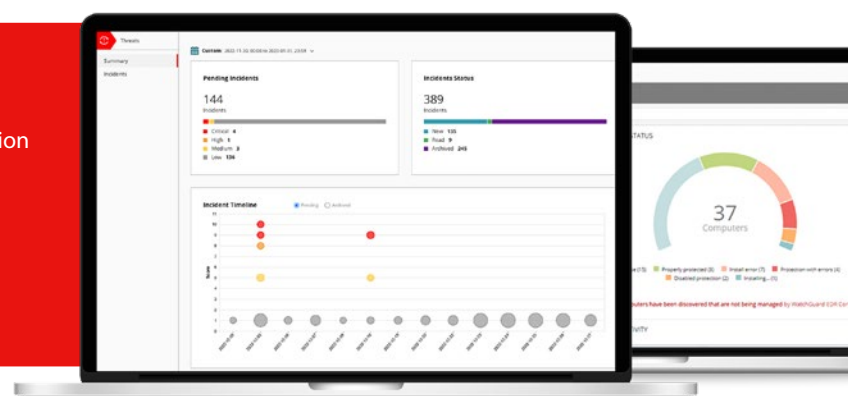
Netzwerksicherheit und AV-Lösungen der nächsten Generation bieten möglicherweise keinen ausreichenden Einblick in die Aktivitäten in Bezug auf Endpoints, was es schwierig macht, Bedrohungen zu erkennen und auf Bedrohungen zu reagieren, die von diesen Geräten ausgehen oder diese betreffen.



Getrennte Tools

Für ein Unternehmen, das über mehrere separate Sicherheitstools verfügt, kann es schwierig sein, einen umfassenden Überblick über die Sicherheitslage zu erhalten und effektiv auf Bedrohungen zu reagieren.

Der Umgang mit den heutigen fortschrittlichen Bedrohungen erfordert koordinierte Maßnahmen bei der Erkennung und Reaktion zwischen Netzwerk- und Endpoint-Tools. Das Hinzufügen von **WatchGuard EDR Core** zu einer Antivirenlösung der nächsten Generation oder einer **EDR-Lösung** schließt die Lücken für eine umfassende und effektive Netzwerk- und Endpoint-Sicherheit.



Ein umfassender Ansatz zur Maximierung der Sicherheit

Moderne Cyberbedrohungen sind eine ernste Angelegenheit und können nicht nur mit traditionellen Sicherheitsmaßnahmen wie Firewalls und Antivirensoftware gestoppt werden. Um sich ihnen erfolgreich zu stellen, ist eine umfassende und fortschrittliche End-to-End-Sicherheitslösung erforderlich, die über den Netzwerkperimeter hinausgeht und Endpoints einbindet, damit Netzwerk- und Endpoint-Tools zusammenarbeiten, um verdächtige Aktivitäten zu identifizieren, rechtzeitig darauf zu reagieren und zu verhindern, dass Sicherheitsverletzungen auftreten. Durch die Kombination von Endpoint Detection and Response (EDR)-Technologien und Netzwerksicherheit erhalten Sie die erforderliche Transparenz, um böswillige Aktivitäten, die die Infrastruktur Ihres Unternehmens bedrohen, in Echtzeit zu erkennen und darauf zu reagieren.

WatchGuard EDR Core bietet einen zusätzlichen Schutz vor fortschrittlichen Bedrohungen, indem es Einblick in die Aktivitäten an Ihren Endpoints bietet, verdächtiges Verhalten in Echtzeit erkennt und eine Reaktionskoordination zwischen Ihren Netzwerk- und Endpoint-Tools ermöglicht. Die Lösung erweitert das Netzwerkportfolio um EDR-Funktionen und stattet Kunden mit produktübergreifenden Erkennungs- und Reaktionsmöglichkeiten aus, um über ThreatSync ein XDR-basiertes Sicherheitskonzept aufzubauen.

Hauptvorteile

Überblick über Endpoint-Aktivitäten, um verdächtige Aktivitäten zu identifizieren, die auf Netzwerkebene möglicherweise nicht sichtbar sind.

Verbesserung der Bedrohungserkennung gegenüber ausgeklügelten Angriffen, die sich der Erkennung entziehen und von Netzwerk- und AV-Lösungen der nächsten Generation nicht erkannt werden können.

Verbesserung der Reaktion auf Bedrohungen mit einer Vielzahl von Maßnahmen, um eine effektive Reaktion zur Neutralisierung von Bedrohungen zu bieten.

Stärkung des Sicherheitskonzepts durch Hinzufügen von Visualisierung, Erkennung und Reaktion für einen besseren Schutz vor fortschrittlichen Bedrohungen.

Wesentliche Funktionen von EDR Core

WatchGuard EDR Core wurde entwickelt, um umfassende Transparenz im Hinblick auf Endpoints zu schaffen, indem es böswillige Aktivitäten überwacht und erkennt, die herkömmliche Lösungen umgehen. EDR Core wird auf vorhandenen AV- oder anderen EDR-Lösungen der nächsten Generation installiert, um diese durch umfassende Endpoint Detection and Response-Funktionen zu erweitern. WatchGuard EDR Core bietet die Werkzeuge, um Bedrohungen effektiv zu bekämpfen und auf böswillige Angriffe zu reagieren, indem es die folgenden modernen Sicherheitstechnologien unterstützt.



VPN-Durchsetzung

Das hybride Arbeitsmodell hat die Notwendigkeit eines sicheren Fernzugriffs auf das Unternehmensnetzwerk erhöht. Mit EDR Core können Sie erzwingen, dass VPN-Verbindungen nur von Endpoints mit dem richtigen Endpoint-Sicherheitskonzept aus erlaubt sind.



Fortschrittliche Reaktionen

Reagieren Sie schnell auf potenzielle Bedrohungen. Beenden Sie einen Prozess, der sich böswillig verhält, verschieben Sie Dateien an einen sicheren Ort in Quarantäne und isolieren Sie betroffene Endpoints oder Hosts, um effektiv zu reagieren und die Auswirkungen eines Sicherheitsvorfalls zu minimieren.



Schutz vor Manipulationen

Viele Ransomware-Angriffe versuchen, den auf Endpoints installierten Schutz auszuschalten, bevor sie versuchen, sich über das Netzwerk auszubreiten. Der Manipulationsschutz verhindert, dass Hacker Ihre Prozesse stoppen oder Services aussetzen und unbefugte Änderungen an Ihren Systemen vornehmen können.



Kontextuelle Erkennung und Anti-Exploit-Technologie

Aktivieren Sie die verhaltensbasierte Erkennung zur Verhinderung und Blockierung von dateilosen Angriffen, die auf in Office-Dateien eingebetteten Skripten basieren, sowie von Angreifern, die LotL-Techniken (living-off-the-land) verwenden. Die Anti-Exploit-Technologie erkennt dateilose Angriffe, die darauf abzielen, ungepatchte Schwachstellen auszunutzen.



SIND SIE BEREIT, XDR IN AKTION ZU SEHEN? Weitere Einzelheiten finden Sie auf der WatchGuard-Website

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security und Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung und sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter www.watchguard.de.

