DATENBLATT

WatchGuard Endpoint Security Elite

Erweiterte EDR für Sicherheitsteams

Umfassende Transparenz und erweiterte Bedrohungsuntersuchung

Für Unternehmen mit ausgereiften Sicherheitsprogrammen oder Partner, die fortschrittliche Sicherheitsdienste bereitstellen, sind Funktionen für umfassende Transparenz und Untersuchung von entscheidender Bedeutung. Sicherheitsteams benötigen Präventions-, Erkennungs- und Reaktionslösungen, um Bedrohungen in ihren Umgebungen zu untersuchen und darauf zu reagieren, den Sicherheitsstack zu verbessern und die Verweildauer von Angreifern zu minimieren.

WatchGuard Endpoint Security Elite bietet eine voll funktionsfähige EDR-Plattform (Endpoint Detection and Response) mit erweiterter Telemetrie, erweiterten Abfragetools und KI-gestützten Untersuchungsfunktionen, damit Sicherheitsteams komplexe Angriffe schnell verstehen, Ereignisse über Endpoints hinweg korrelieren und präzise reagieren können. Durch die Kombination von leistungsstarken Analysen mit automatisierter Reaktion und erweiterter Datentransparenz bietet Endpoint Security Elite Sicherheitsteams die Tools, die sie benötigen, um komplexe Bedrohungen auf Unternehmensebene zu erkennen, zu untersuchen und zu stoppen.

Erweiterte EDR-Funktionen für Sicherheitsvorgänge

WatchGuard Endpoint Security Elite wurde für Unternehmen und Managed Security Service Provider (MSSP) entwickelt, die umfassenden Einblick in die Sicherheit und erweiterte Untersuchungsfunktionen benötigen. Aufbauend auf der KI-gestützten EDR-Grundlage von WatchGuard bietet die Lösung erweiterte Telemetrie, erweiterte historische Transparenz und erweiterte Tools zur Erkennung von Bedrohungen, mit denen Sicherheitsteams komplexe Angriffe effektiver erkennen, untersuchen und darauf reagieren können.

Mit detaillierter Endpoint-Telemetrie und kontextbezogenen Vorfallsdaten können Analysten Angriffszeitpläne anzeigen, Ursachen identifizieren und verstehen, wie sich Angreifer über Systeme hinweg bewegen. Integrierte MITRE ATT&CK-Zuordnung und automatisierte Verhaltenskorrelation bieten Einblick in die Taktiken, Techniken und Verfahren von Angreifern und helfen Sicherheitsteams, Bedrohungen schnell zu priorisieren und zuverlässig zu reagieren.

Zu den erweiterten Untersuchungstools gehören die STIX- und YARA-basierte Bedrohungserkennung und ein integrierter generativer KI-Assistent, mit dem Analysten Sicherheitsdaten in natürlicher Sprache abfragen können. Diese Funktionen beschleunigen die Untersuchungsabläufe erheblich und ermöglichen es Sicherheitsteams, versteckte Bedrohungen zu identifizieren, die Verweildauer zu verkürzen und die allgemeine Sicherheit zu verbessern.

Für MSPs und Unternehmen, die erweiterte Sicherheitsdienste bereitstellen, bietet WatchGuard Endpoint Security Elite den Grad an Transparenz und Analyseleistung, der für die Unterstützung moderner Sicherheitsvorgänge erforderlich ist, ohne die Komplexität fragmentierter Tools.

Fortschrittliche Untersuchungstools

- GenAI-Assistent zur Abfrage von Telemetrie
- Suche nach STIX-Angriffsindikatoren (IoAs) und YARA-Regeln
- CAPA-Tool zur Analyse von Dateiinformationen (Verhaltensweisen, Zeichenfolgen, Importe, Exporte)
- Remote Shell für reduzierte MTTR und Verweildauer

WatchGuard Endpoint Security Elite bietet erweiterte Untersuchungs- und Reaktionsfunktionen für Sicherheitsteams.

Reduzierung der Angriffsfläche

- Anpassbares Dashboard mit Risiken für Endpoints
- Erkennung nicht verwalteter Endpoints
- Schwachstellenanalyse

Integrierte Präventionstechnologien

- Firewall, IDS und Gerätekontrolle
- Schutz für mehrere Angriffsvektoren (Web, E-Mail, Netzwerk, Geräte)
- Signaturdateien, Heuristik vor der Ausführung und kollektive Intelligenz
- KI-gestützte Erkennung, die bösartige Installationsprogramme und Skripte identifiziert und blockiert
- Anti-Phishingschutz
- URL und Web Filtering
- Erkennung mithilfe von Analysen des Netzwerkverkehrs
- Deny-by-Default-Ausführung

Funktionen für Erkennung und Reaktion

- Ständige Überwachung von Endpoints
- Selbstlernende KI mit kontextbezogener Verhaltensanalyse zur Erkennung und Abwehr von dateilosen und Living-off-the-Land-Angriffen (LotL)
- Blockiert automatisch Versuche, Schwachstellen in aktiven Prozessen auf dem Gerät auszunutzen
- Schutz vor Netzwerkangriffen, bei denen Schwachstellen in über das Internet zugänglichen Diensten ausgenutzt werden
- Automatische Erkennung von RDP-Angriffen und Vorbeugung
- Eindämmung lateraler Bewegungen
- Automatische Erkennung und Korrelation eines Angriffs mit Warnmeldungen, die dem MITRE ATT&CK® Framework entsprechen
- Interaktive Vorfallansicht mit mehreren Signalen für eine umfassende Ursachenanalyse
- Umfassende Kontext- und Echtzeit-Computerforensik-Telemetrie zur Beschleunigung von Untersuchungen
- Integrationen mit ThreatSync (XDR) für Transparenz und Abhilfemaßnahmen
- Isolation, Scannen und Neustart von Computern und Netzwerk in Echtzeit
- Wiederherstellung verschlüsselter Dateien (Schattenkopien)

Unterstützte Betriebssysteme: Windows (Intel und ARM), macOS (Intel und ARM), Linux, iOS und Android.

Strategische Vorteile

Umfassende Telemetrie für schnellere Untersuchungen

Endpoint Security Elite bietet Zugriff auf angereicherte und forensische Telemetrie sowie eine längere Aufbewahrung von Daten, sodass Analysten die Angriffsaktivität im Laufe der Zeit analysieren und das Angreiferverhalten über Endpoints hinweg rekonstruieren können.

Erweiterte Bedrohungserkennung

Sicherheitsteams können mit fortschrittlichen Tools proaktiv nach neuen Bedrohungen suchen, wobei Endpoint-Telemetrie auf Anzeichen von Kompromittierung und verdächtigem Verhalten analysiert werden. Mit Unterstützung für strukturierte Erkennungs-Frameworks, wie STIX und YARA, können Sicherheitsteams versteckte Bedrohungen aufdecken und Aktivitäten in der gesamten Umgebung untersuchen.

Umfassender, visueller Angriffskontext

Interaktive Zeitleisten, Prozessbäume und seitliche Bewegungskarten bieten einen klaren visuellen Kontext, um zu verstehen, wie sich Angriffe über Endpoints hinweg entwickeln. Dies ermöglicht es Sicherheitsteams, die Ursache schnell zu identifizieren, das Verhalten von Angreifern zu verstehen und Untersuchungen zu beschleunigen.

KI-gestützte Sicherheitsanalyse

Ein integrierter generativer KI-Assistent ermöglicht es Analysten, Sicherheitsdaten in natürlicher Sprache abzufragen, was die Untersuchungen beschleunigt und die Zeit zum Verständnis von Vorfällen verkürzt – es sind keine komplexen Abfragen erforderlich.

Granulare Richtlinienkontrollen

Endpoint Security Elite ermöglicht es Administratoren, detaillierte Sicherheitsrichtlinien durchzusetzen, die die Ausführung von Anwendungen, den Gerätezugriff und das Systemverhalten über verschiedene Endpoints hinweg steuern. Diese granularen Kontrollen reduzieren die Angriffsfläche und gewährleisten gleichzeitig eine konsistente Sicherheitsdurchsetzung für Anwender, Geräte und Umgebungen.

Speziell für Managed Security Services entwickelt

Endpoint Security Elite bietet die umfassende Telemetrie, Untersuchungstools und Automatisierung, die MSPs benötigen, um hochwertige Sicherheitsdienste bereitzustellen. Mit zentralisiertem Multi-Tenant Management und erweiterten Untersuchungsfunktionen können Partner Bedrohungen in verschiedenen Kundenumgebungen effizient überwachen, untersuchen und darauf reagieren.

Zero Trust-Modell: Mehrschichtiger Schutz

Die Endpoint Security-Plattform von WatchGuard nutzt nicht nur eine einzige Technologie. Wir kombinieren verschiedene Tool-Ebenen miteinander, um die Erfolgschancen von Angreifern zu reduzieren. Gemeinsam verwenden diese Technologien Ressourcen am Endpoint, um das Risiko einer Sicherheitsverletzung zu minimieren.

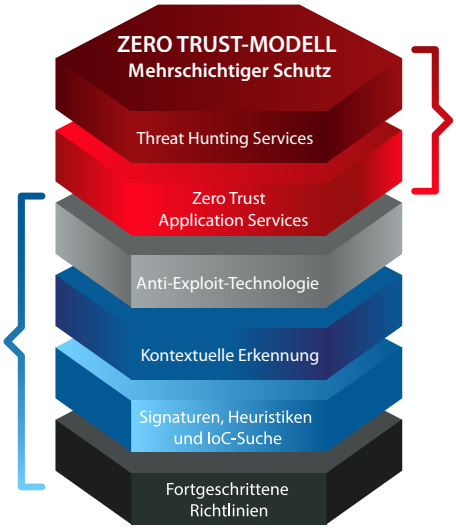
Endpoint-Ebenen:

Ebene 1/Verbesserte Sicherheitsrichtlinien
Erkennen oder Blockieren der Ausführung verbreiteter Angriffstechniken

Ebene 2/Signaturdateien, heuristische Technologien und STIX IoCs-Suchmaschine
Ermöglichen die Suche nach kürzlich bekannt gewordenen Angriffen anhand von Hash, Dateinamen, Pfad, C2-Domäne, IP und YARA-Regeln

Ebene 3/Kontextbasierte Erkennung
Identifiziert bösartige Angriffe, die legitime Tools wie PowerShell, WMI und Webbrowser missbrauchen

Ebene 4/Anti-Exploit-Technologie
Erkennung dateiloser Angriffe, die Schwachstellen ausnutzen



Endpoint-Ebenen:

Ebene 5/Zero-Trust Application Service
Klassifiziert jeden einzelnen Prozess, bevor er ausgeführt wird, wobei jede Ausführung abgelehnt wird, solange sie nicht als vertrauenswürdig zertifiziert wurde.

Ebene 6/Integrierter Threat Hunting Service
Erkennung kompromittierter Endpoints, IoAs, Angriffe im Frühstadium und verdächtige Aktivitäten. IoAs werden in der cloudbasierten Konsole mit der zugehörigen Telemetrie kontextualisiert, sodass Sicherheitsanalysten potenzielle Angriffsversuche untersuchen können

Informationen zu WatchGuard

WatchGuard Technologies ist ein weltweit führendes Unternehmen für einheitliche Cybersicherheit, das speziell für Managed Service Provider (MSPs) entwickelt wurde. Seit mehr als 30 Jahren definiert WatchGuard, wie MSPs Sicherheit in großem Maßstab bereitstellen, und entwickelt kontinuierlich Innovationen, um jeder größeren Veränderung in der Bedrohungslandschaft einen Schritt voraus zu sein. Die KI-gestützte Unified Security Platform® von WatchGuard bietet an Zero-Trust-Prinzipien ausgerichteten Netzwerk-, Endpoint- und Identitätsschutz in einer einzigen, integrierten Plattform, die es MSPs ermöglicht, die betriebliche Komplexität zu reduzieren, Sicherheitsergebnisse zu verbessern und ihr Geschäft effizienter auszubauen. WatchGuard genießt das Vertrauen von mehr als 25.000 MSPs, die weltweit über 1,5 Millionen Kunden schützen, und ermöglicht es Partnern, starke, messbare Sicherheitsergebnisse für Kunden auf der ganzen Welt zu liefern. Weitere Informationen finden Sie unter WatchGuard.com/de.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.com/de
WatchGuard Technologies, Inc.