DATENBLATT

WatchGuard EDR

Endpoint Detection and Response

Cyberabwehr Gegen Fortschrittliche Bedrohungen

Mit modernen Mitteln geplante und ausgeführte Cyberangriffe sind darauf ausgelegt, dass sie den von traditionellen Sicherheitslösungen geleisteten Schutz umgehen. Diese Angriffe werden aufgrund der zunehmenden Professionalisierung der Hacker immer häufiger und ausgefeilter. Dies liegt auch daran, dass der Beseitigung von Sicherheitslücken in Systemen zu wenig Aufmerksamkeit geschenkt wird.

Im Rahmen dieses Szenarios liefern herkömmliche Endpoint Protection Platforms (EPPs) nicht ausreichend detaillierte Einblicke in die Prozesse und Anwendungen der Unternehmensnetzwerke. Hinzu kommt, dass einige EDR-Lösungen ineffizient sind, unnötigen Stress verursachen und die Arbeitsbelastung von Sicherheitsadministratoren erhöhen, da die Verantwortung für die Verwaltung von Warnmeldungen auf sie delegiert wird und sie Bedrohungen manuell klassifizieren müssen.

Optimieren Sie Ihre Sicherheit – Steigen Sie Um Auf Automatisierte EDR

WatchGuard EDR ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Die Plattform automatisiert die Prävention, Erkennung, Eindämmung und Abwehr mannigfaltiger, neuartiger Bedrohungen – von Zero-Day-Malware über Ransomware, Phishing oder In-Memory-Exploits bis hin zu weiteren Angriffsversuchen ohne Malware – für optimalen Schutz, heute und morgen, innerhalb und außerhalb des Unternehmensnetzwerks.

WatchGuard EDR wurde entwickelt, um umfassende Transparenz im Hinblick auf Endpoints zu schaffen, indem böswillige Aktivitäten, die herkömmliche Lösungen umgehen, überwacht und erkannt werden. WatchGuard EDR wird zusätzlich zu vorhandenen Virenschutzlösungen installiert, um diese durch umfangreiche EDR-Funktionen zu ergänzen, einschließlich folgender automatischer Services:

- **Zero-Trust Application Service: 100 %ige Klassifizierung von Anwendungen**
- **Threat Hunting Service: Erkennung von Hackern und Insidern**

WatchGuard EDR bietet die Werkzeuge, um Bedrohungen effektiv zu bekämpfen und auf böswillige Angriffe zu reagieren, indem es die folgenden modernen Sicherheitstechnologien unterstützt:

- Ständige Überwachung der Endpoint-Aktivität mit EDR
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher Prozesse (APT, Ransomware, Rootkits usw.)
- Sandboxing in realen Umgebungen
- Schutz vor Exploits
- Netzwerkangriffsschutz: Verhindern, dass Angriffe Schwachstellen in über das Internet exponierten Diensten ausnutzen
- Threat Hunting: Verhaltensanalysen und Erkennung von IoA (Indicators of Attack) zur Identifizierung von LotL (Living off the Land-Angriffen)
- Zwölfmonatige Datenspeicherung und physisches Sandboxing in Echtzeit, um unbemerkte Hacker-Aktionen zu vermeiden
- Indicators of Attack die dem MITRE ATT&CK-Framework zugeordnet sind
- Erkennung und Verhinderung von RDP-Angriffen
- Eindämmungs- und Abhilfemöglichkeiten wie Computerisolierung und Programmblockierung nach Hash oder Name
- Verschlüsselte Dateien über Schattenkopien wiederherstellen

Vorteile

Weniger Aufwand, geringere Sicherheitskosten

- Durch die verwalteten Services lassen sich Kosten für Fachpersonal einsparen. Außerdem müssen keine Fehlalarme untersucht werden und es werden keine Entscheidungen delegiert.
- Zentrale plattformübergreifende Endpoint-Verwaltung.
- Dank ressourcensparendem Agent und Cloudarchitektur wird die Leistungsfähigkeit der Endpoints nicht beeinträchtigt.

Verkürzung der Erkennungszeit dank Automatisierung

- Anwendungen, die ein Sicherheitsrisiko darstellen , können blockiert werden (durch Hash oder Name).
- Verhindert die Ausführung von Angriffen, Zero-Day-Malware, Angriffen ohne Datei/ Malware, Ransomware und Phishing-Versuchen.
- Erkennt und unterbindet Techniken, Taktiken und Prozesse von Hackern.

Automatisierung und Verkürzung von Problemlösung und Reaktion

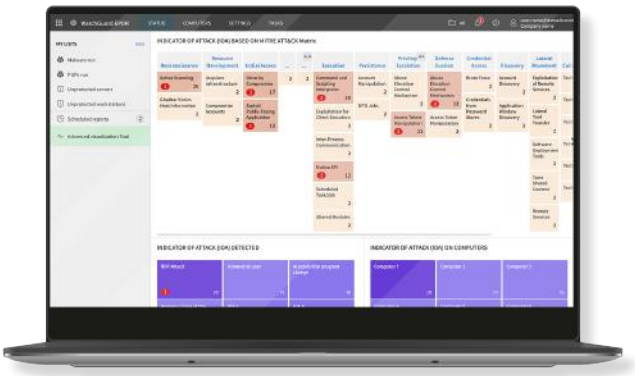
- Problemlösung und Reaktion: forensische Informationen zur gründlichen Untersuchung jedes Angriffsversuchs sowie Tools zur Verringerung der Auswirkungen (Desinfektion).
- Nachverfolgbarkeit jeder Aktion: verwertbare Erkenntnisse über den Angreifer und dessen Aktivitäten. Erweiterte Nachforschungen zu Indicators of Attack (IoAs).
- Verbesserung und Anpassung von Sicherheitsrichtlinien aufgrund der Erkenntnisse aus der forensischen Analyse.

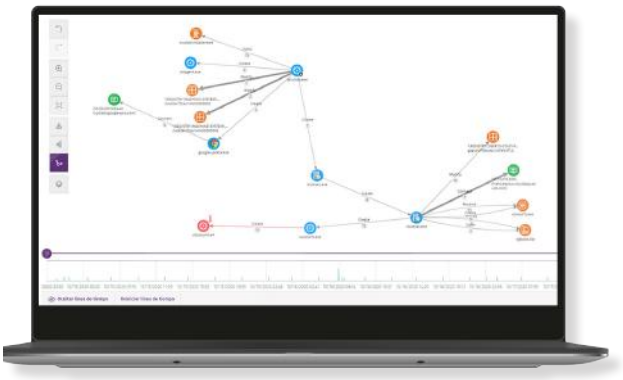
Zero Trust-Sicherheit Und Threat Hunting

Die Endpoint Security-Plattform von WatchGuard nutzt nicht nur eine einzige Technologie, sondern verschiedene, um die Erfolgschancen eines Angreifers zu reduzieren. Gemeinsam verwenden diese Technologien Ressourcen am Endpoint, um das Risiko einer Sicherheitsverletzung zu minimieren.

Der **Zero-Trust Application Service** klassifiziert 100 % der Prozesse, überwacht die Aktivitäten an den Endpoints und unterbindet die Ausführung von Anwendungen und böswilligen Prozessen. Bei jeder Ausführung wird eine Echtzeit-Klassifizierung als böswillig oder rechtmäßig, ohne Unsicherheiten und ohne Delegierung von Entscheidungen an den Kunden versendet, wobei manuelle Prozesse vermieden werden. Möglich ist dies dank der Leistung, Geschwindigkeit, Anpassungsfähigkeit und Skalierbarkeit der KI und der Cloud-Verarbeitung.

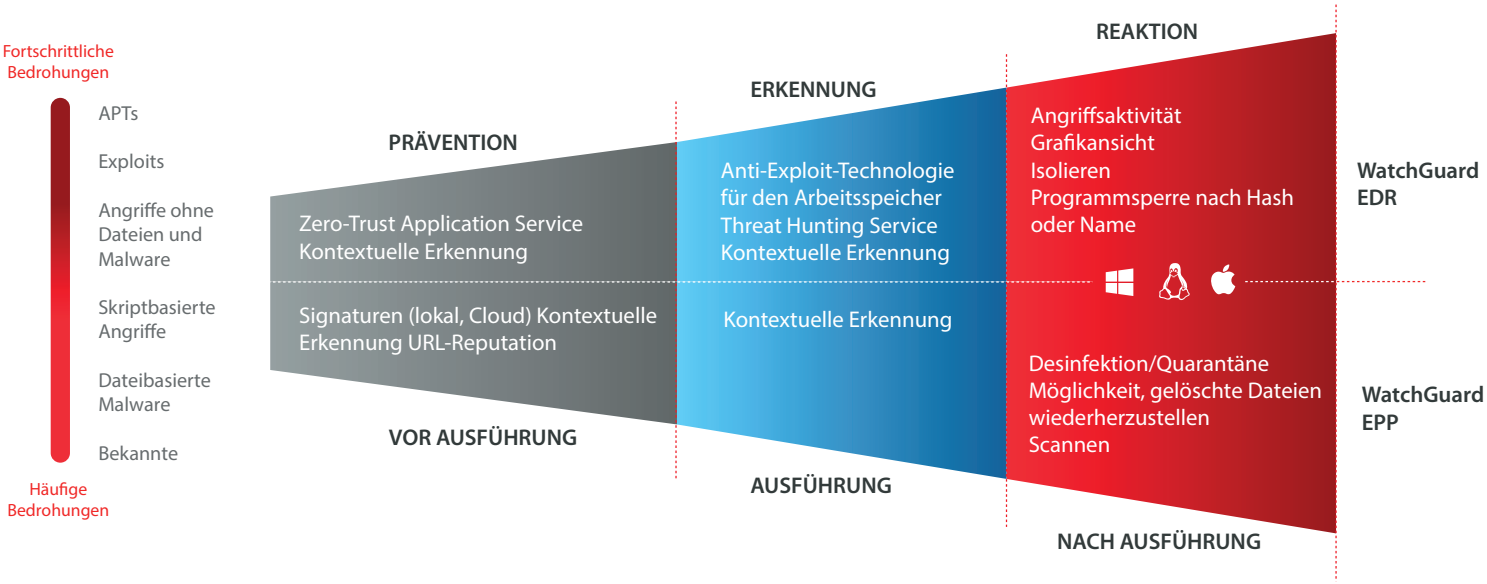
Der Service vereint Big-Data-Technologien und mehrstufiges maschinelles Lernen einschließlich Deep Learning – das Ergebnis der laufenden Überwachung und Automatisierung der Erfahrungen und Kenntnisse, die das Bedrohungsteam von WatchGuard erworben hat.





Der **Threat Hunting Service** basiert auf einer Reihe von Threat-Hunting-Regeln, die von Cybersicherheitsspezialisten entwickelt wurden und die automatisch auf alle durch die Telemetrie erfassten Daten angewendet werden. Hierdurch werden höchst zuverlässige IoAs ausgelöst und die Anzahl der falsch positiven Meldungen verringert, um MTTD und MTTR zu minimieren („Mean Time To Detect“ und „Mean Time To Respond“).

Diese Angriffsindikatoren sind ein Ergebnis des fortlaufenden Prozesses zur Erkennung von Angreifern anhand einer fortschrittlichen Datenanalyse, unserer eigenen Bedrohungsanalyse und dem Fachwissen unserer Analysten. Die Threat Hunter bei WatchGuard gehen bei ihrer Arbeit davon aus, dass Unternehmen ständig angegriffen werden.



Unterstützte Plattformen und Systemanforderungen von WatchGuard EDR

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

Unterstützung von älteren Systemen ab Windows XP SP3 und Server 2003

EDR-Funktionen sind unter Windows, macOS und Linux verfügbar, wobei Windows sämtliche Funktionen uneingeschränkt unterstützt.

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Microsoft Edge und Safari.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.