DATENBLATT

WatchGuard EDR

Endpoint Detection and Response

KI-gestützte Abwehr neuartiger Bedrohungen

Herkömmliche Endpoint Protection- und Antivirenlösungen sind zwar für die Abwehr bekannter Malware unerlässlich, bieten jedoch nicht die Transparenz und fortschrittlichen Technologien, die für die Früherkennung und automatisierte Reaktion auf ausgeklügelte Angriffe erforderlich sind. Cyberbedrohungen werden immer häufiger und komplexer, da Angreifer ihre Methoden kontinuierlich verfeinern.

Einzellösungen für Endpoint Security generieren häufig Warnungen mit niedriger Priorität, die für IT- und Sicherheitsadministratoren einen hohen Aufwand bedeuten und sie dazu zwingen, Bedrohungen manuell zu verwalten und zu klassifizieren. Dies erhöht nicht nur den Stress, sondern bedeutet auch, dass kritische Warnungen möglicherweise übersehen werden.

Optimieren Sie Ihre Sicherheit – steigen Sie um auf automatisierte EDR

WatchGuard EDR ist eine Cloud-basierte Cybersicherheitslösung für mehrere Geräte. Sie automatisiert Prävention, Erkennung, Eindämmung und Reaktion auf erweiterte Bedrohungen wie Zero-Day-Malware, Ransomware, Phishing, In-Memory-Exploits und dateilose Angriffe. Mit vollständiger Endpoint-Transparenz identifiziert und stoppt WatchGuard EDR Cyberangriffe, die von herkömmlichen Sicherheitslösungen übersehen werden.

WatchGuard EDR lässt sich nahtlos in bestehende Antivirenlösungen integrieren und verbessert Ihr Sicherheits-Framework mit umfangreichen EDR-Funktionen und Managed Services:

- **Zero-Trust Application Service: 100-%ige Klassifizierung von Anwendungen**
- **Threat Hunting Service: erkennt Hacker und Insider**

Wichtige Funktionen

- KI-gesteuerte Bedrohungserkennung: verwendet Cloud-basierte KI und maschinelle Lerntechnologien für eine 100-%ige Klassifizierung von Prozessen und Anwendungen.
- Physisches Sandboxing: Verhaltensanalyse von Anwendungen in sicheren Umgebungen zur Identifizierung von Bedrohungen.
- Anti-Exploit-Schutz: schützt vor Exploit-basierten Angriffen.
- Netzwerkangriffsschutz: verhindert, dass Angriffe Schwachstellen in über das Internet exponierten Diensten ausnutzen.
- IoAs-Erkennung: Analysen, die auf dem Mitre ATT&CK™ Framework basieren, bieten Indikatoren für Angriffe, um laufende Bedrohungen zu mindern und zukünftige Angriffe zu verhindern.
- Erkennung und Verhinderung von RDP-Angriffen: gewährleistet Sicherheit vor Angriffen auf das Remote-Desktop-Protokoll.
- Eindämmung und Abhilfe: beinhaltet Funktionen wie Programmblockierung und Geräteisolierung.
- Dateiwiederherstellung: stellt verschlüsselte Dateien mithilfe von Schattenkopien wieder her.

Vorteile

Weniger Aufwand, geringere Sicherheitskosten

- Managed Services reduzieren den Bedarf an Fachpersonal und eliminieren Fehlalarme, um sicherzustellen, dass Entscheidungen nicht delegiert werden.
- Zentrale plattformübergreifende Endpoint-Verwaltung.
- Dank ressourcensparendem Agent und Cloud-nativer Architektur wird die Leistungsfähigkeit der Endpoints nicht beeinträchtigt.

Verkürzung der Erkennungszeit dank Automatisierung

- Blockiert Anwendungen, die ein Sicherheitsrisiko darstellen, durch Hash oder Name
- Verhindert die Ausführung von Zero-Day-Malware, dateilosen Angriffen, Ransomware und Phishing-Versuchen.
- Erkennt und unterbindet Techniken, Taktiken und Prozesse von Hackern.

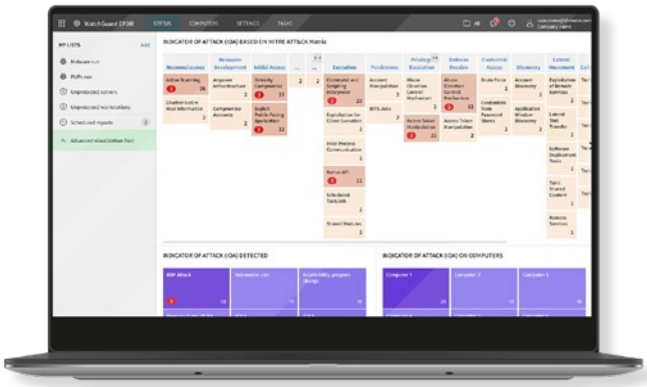
Verkürzt die Zeit für Problemlösung und Reaktion

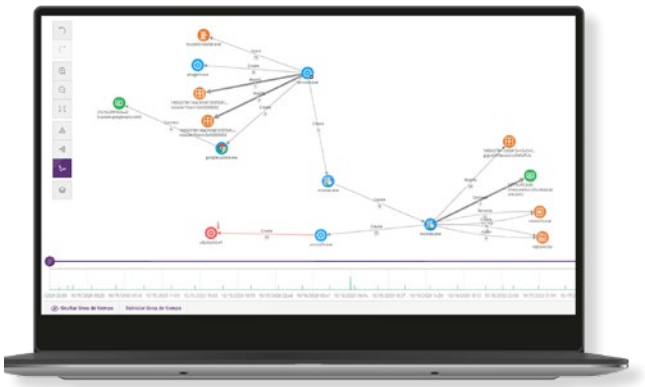
- Bietet forensische Informationen zur gründlichen Untersuchung sowie Tools zur Verringerung der Auswirkungen eines Angriffsversuchs (Desinfektion).
- Bietet verwertbare Erkenntnisse über die Aktivitäten der Angreifer und erweiterte Nachforschungen zu Indicators of Attack (IoAs).
- Ermöglicht Verbesserungen der Sicherheitsrichtlinien auf der Grundlage von Erkenntnissen aus forensischen Analysen.

Zero Trust und Threat Hunting

Die Endpoint Security 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 manuellen Eingriff versendet, unter Nutzung von KI-Technologien und Cloud-Verarbeitung für Skalierbarkeit und Verarbeitung.

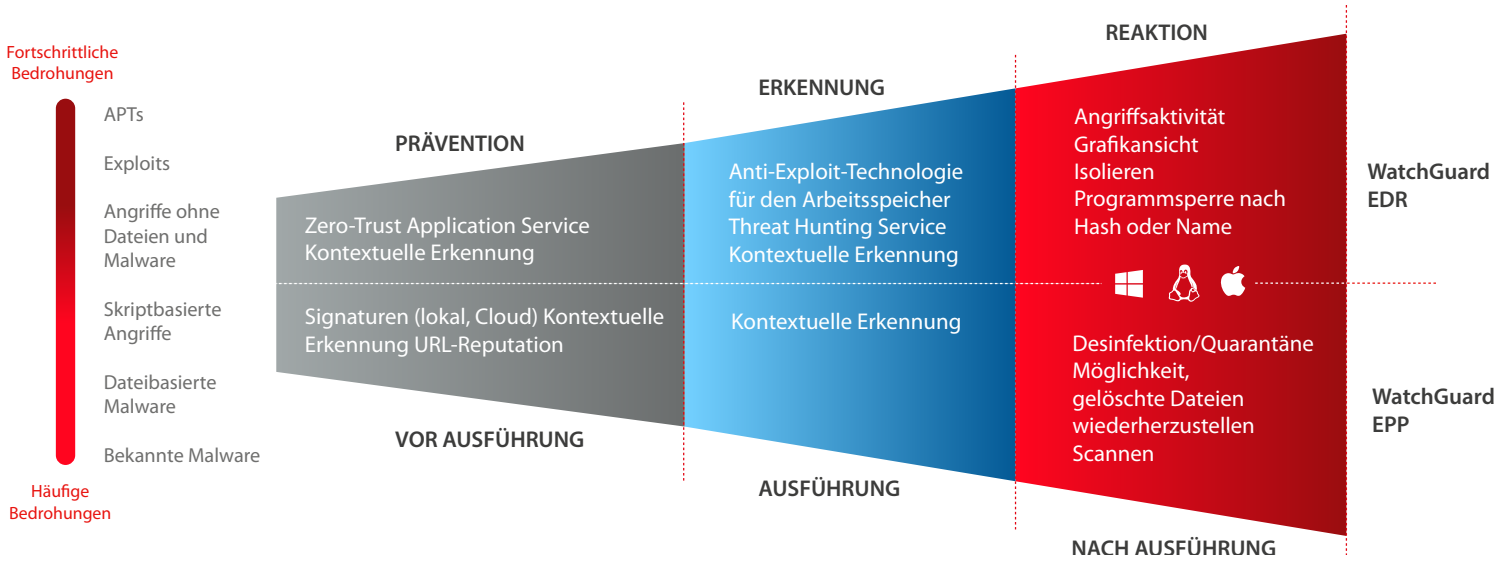




Der **Threat Hunting Service** verwendet Regeln, die von Spezialisten für Cybersicherheit entwickelt wurden und die automatisch auf alle durch die Telemetrie erfassten Daten angewendet werden, um höchst zuverlässige IoAs auszulösen und die Anzahl der falsch positiven Meldungen zu verringern. Dieser fortlaufende Prozess verwendet fortschrittliche Analysen, proprietäre Bedrohungsinformationen und Expertenanalysen, um MTTD und MTTR zu entdecken und zu minimieren, wobei davon ausgegangen wird, dass Unternehmen ständig ins Visier genommen werden.

Beseitigen Sie übersehene Bedrohungen mit vollständiger EDR-Sicherheit

Aktualisieren Sie Ihre Sicherheit mit WatchGuard EDR. Erweitern Sie Ihr traditionelles Antivirenprogramm mit modernsten EDR-Funktionen, um fortschrittlichen Bedrohungen einen Schritt voraus zu sein. Mit automatisierter Erkennung, Reaktion und kontinuierlicher Überwachung bietet WatchGuard EDR umfassenden Schutz für Ihre Geräte, Benutzer und Daten. Unsere einzigartigen Services für Zero-Trust Application und Threat Hunting tragen dazu bei, die Auswirkungen moderner Cybersicherheitsherausforderungen zu minimieren und eine robuste und proaktive Sicherheit für Ihr Unternehmen zu gewährleisten. Schützen Sie schon heute Ihr Morgen.



Unterstützte Plattformen und Systemanforderungen für WatchGuard EDR

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

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.