DATENBLATT

WatchGuard Endpoint Security 360

Autonomer Zero Trust-Schutz für Endpoints

Maximaler Schutz bei minimalem Betriebsaufwand

Moderne Cyberangriffe entwickeln sich schneller als herkömmliche Endpoint-Sicherheitstools sie erkennen können. Angreifer verlassen sich zunehmend auf dateilose Techniken, die Verwendung legitimer Software, um böswillige Aktionen auszuführen, kompromittierte vertrauenswürdige Anwendungen und seitliche Bewegungen, um traditionelle Abwehrmechanismen zu umgehen. WatchGuard Endpoint Security 360 wurde entwickelt, um diese ausgefeilten Bedrohungen automatisch zu stoppen. Durch die Bereitstellung eines autonomen Zero Trust EDR, der unbekannte Anwendungen standardmäßig blockiert, wird kompromittierte vertrauenswürdige Software erkannt und seitliche Bewegungen über das Netzwerk verhindert. Durch die Kombination von KI-gestützter Erkennung mit automatisierter Untersuchung und Reaktion reduziert Endpoint Security 360 die Verweildauer von Angreifern drastisch und minimiert gleichzeitig die betriebliche Arbeitsbelastung.

Es wurde für Unternehmen entwickelt, die maximalen, effizienten Schutz möchten, und bietet einen stärkeren Schutz, eine schnellere Reaktion und einen deutlich geringeren Aufwand für das Sicherheitsmanagement.

Autonomer Schutz beseitigt Risiken

WatchGuard Endpoint Security 360 bietet erweiterte EDR-Funktionen (Endpoint Detection and Response) mit Zero Trust-Ausführungskontrollen, die sicherstellen, dass nur vertrauenswürdige und verifizierte Anwendungen ausgeführt werden können. Dies ermöglicht es Unternehmen, Risiken zu reduzieren und Angriffe frühzeitig zu stoppen, ohne auf ständiges menschliches Eingreifen angewiesen zu sein.

Durch das automatische Blockieren unbekannter Aktivitäten und die kontinuierliche Validierung vertrauenswürdiger Software beseitigt Endpoint Security 360 viele der Angriffstechniken, die bei modernen Sicherheitsverletzungen verwendet werden, einschließlich dateiloser Angriffe, Living-off-the-Land-Techniken und bösartiger Skripte.

Endpoint Security 360 fügt zusätzliche Schutzebenen hinzu, einschließlich der Erkennung kompromittierter vertrauenswürdiger Anwendungen, der Eindämmung seitlicher Bewegungen, der automatisierten Bedrohungssuche und Untersuchungen auf Vorfall-Ebene, um das Risiko weiter zu reduzieren und fortschrittliche Angriffstechniken zu verhindern.

Für MSPs bedeutet dies, dass sie effizienter arbeiten und mehr Kunden schützen können, ohne die Mitarbeiterzahl erhöhen zu müssen. Und für Endkunden bedeutet dies einen besseren Schutz und weniger Sorgen.

WatchGuard Endpoint Security 360 umfasst alle Funktionen der KI-gestützten EDR-Plattform von WatchGuard sowie einen autonomen Zero Trust-Schutz.

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
- Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- URL Filtering und Webbrowsing
- 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
- Integrationen mit ThreatSync (XDR) für Transparenz und Abhilfemaßnahmen
- Isolation, Scannen und Neustart von Computern und Netzwerk in Echtzeit
- Wiederherstellung verschlüsselter Dateien (Schattenkopien)

Autonomer Schutz für moderne Bedrohungen

Unbekannte Aktivitäten standardmäßig blockieren

Cyberkriminelle agieren heutzutage so schnell, dass Tools für den Schutz von Endpoints nicht mithalten können. Aus diesem Grund umfasst WatchGuard Endpoint Security 360 den einzigartigen Zero-Trust Application Service, der Deny-by-Default-Kontrollen implementiert, mit denen nur verifizierte Anwendungen auf Endpoints ausgeführt werden können. Unbekannte Anwendungen werden automatisch blockiert, bis sie als vertrauenswürdig eingestuft werden, wodurch ein großer Teil der modernen Malware- und Ransomware-Angriffe beseitigt wird, bevor sie ausgeführt werden können.

Erkennen und Eindämmen ausgeklügelter Angriffe

Durch die erweiterte Verhaltenserkennung werden Aktivitäten über Endpoints hinweg kontinuierlich analysiert, um verdächtige Verhaltensmuster im Zusammenhang mit modernen Cyberangriffen zu erkennen. Wenn böswillige Aktivitäten erkannt werden, stoppen automatisierte Reaktionsaktionen, wie Isolierung, Eindämmung und Behebung, den Angriff, bevor er sich im gesamten Netzwerk ausbreitet.

Reduzieren Sie die Arbeitsbelastung. Verbessern Sie die Effizienz.

WatchGuard Endpoint Security 360 bietet eine Vielzahl von Automatisierungen, um den Schutz und die Effizienz zu verbessern. Durch die automatische Untersuchung verdächtiger Aktivitäten, die Korrelation von Signalen mit Vorfällen und das standardmäßige Blockieren unbekannter Bedrohungen werden die Anzahl an Warnmeldungen und der Untersuchungsaufwand drastisch reduziert. Das Ergebnis ist ein stärkerer Schutz bei geringerem Betriebsaufwand.

Entwickelt für mehr Skalierbarkeit und Effizienz von MSPs

WatchGuard Endpoint Security 360 wurde entwickelt, um moderne Managed Service Provider (MSPs) zu unterstützen. Das mandantenfähige Cloud-Management ermöglicht es MSPs, Richtlinien bereitzustellen, den Schutz zu überwachen und die Sicherheit über mehrere Kunden hinweg von einer einzigen Konsole aus zu verwalten. Zero Trust-Ausführungskontrollen, automatisierte Untersuchungen und intelligente Reaktionen ermöglichen es MSPs, mehr Endpoints zu schützen und gleichzeitig die Untersuchungsdauer und die Anzahl an Warnmeldungen drastisch zu reduzieren.

Diese Automatisierung ermöglicht es Service Providern, stärkere Endpoint Security Services bereitzustellen und gleichzeitig die betriebliche Effizienz und Rentabilität zu verbessern. Für MSPs bedeutet dies, einen starken Endpoint-Schutz effizient bereitzustellen und gleichzeitig solide Servicemargen aufrechtzuerhalten.

Leistungsstarke, vereinfachte Sicherheit mit der Unified Security Platform von WatchGuard

Die Unified Security Platform-Architektur von WatchGuard bietet eine einzige Plattform für die Bereitstellung moderner Sicherheitsmaßnahmen. Mit unserem Plattformansatz können Sie leistungsstarke Sicherheitsdienste über sämtliche Bedrohungsvektoren hinweg bereitstellen und dabei gleichzeitig die betriebliche Effizienz und die Rentabilität steigern. Weitere Informationen finden Sie unter WatchGuard.com/de.

Unterstützte Plattformen und Systemanforderungen für WatchGuard EDPR

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

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

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

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.