DATASHEET

WATCHGUARD ADVANCED EPDR

HERAUSFORDERUNGEN BEI DER CYBERSICHERHEIT

Endpoints sind das primäre Ziel der meisten Cyberangriffe. Da die Technologieinfrastruktur immer komplexer wird, fällt es Unternehmen schwer, das nötige Fachwissen für die Überwachung und Verwaltung von Endpoint-Sicherheitsrisiken zu finden. Welche Arten von Herausforderungen müssen Sicherheitsteams bewältigen, wenn sie Endpoint-Sicherheitslösungen einsetzen?

- **Sich ständig verändernde, komplexe Bedrohungen:** Effiziente, proaktive Sicherheitspraktiken können den Unterschied zwischen einem kleinen Sicherheitsvorgehen und der Rolle als Opfer ausmachen. Diese Praktiken reichen von der Reduzierung der Angriffsoberfläche bis zum Erkennen sich entwickelnder Bedrohungen, bevor es zu einer tatsächlichen Kompromittierung kommt.
- **Alarmmüdigkeit, fehlende Effizienz:** Unternehmen erhalten pro Woche Tausende von Warnmeldungen, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % geprüft werden. Sicherheitsteams verbringen zwei Drittel der Zeit mit der Verwaltung von Warnmeldungen und der manuellen Klassifizierung verdächtiger Dateien.
- **Schlechte Performance:** Häufig erfordern Lösungen für Endpoint-Sicherheit die Installation und Verwaltung mehrerer Agenten auf jedem überwachten Computer, Server und Laptop. Dies verursacht schwerwiegende Fehler, eine schlechte Performance und einen hohen Ressourcenverbrauch.

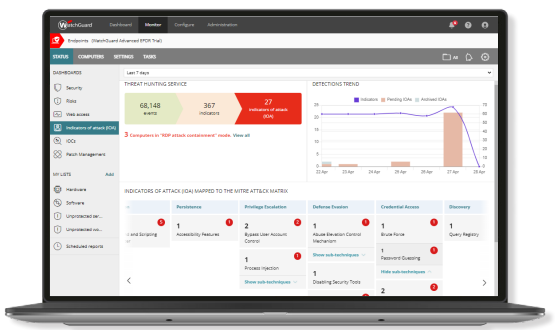
Zur Verteidigung benötigen Sicherheitsteams autonome Präventions-, Erkennungs- und Reaktionslösungen sowie entsprechende Mittel, damit sie Bedrohungen, die in Umgebungen lauern, leicht aufspüren, untersuchen und darauf reagieren sowie die Sicherheitsstruktur weiter optimieren können, um die Verweildauer von Angreifern zu minimieren.

VERBESSERN SIE IHRE CYBERSICHERHEITSDIENSTE

WatchGuard Advanced EPDR ist eine in der Cloud bereitgestellte Lösung für Computer, Laptops und Server, die Prävention, Erkennung, Eindämmung und Reaktion auf fortschrittliche Bedrohungen automatisiert. Die Lösung vereint präventive und EDR-Technologien mit fortschrittlichen, KI-gestützten Diensten:

- **Zero-Trust Application Service:** Cloud-basiertes KI-System, das automatisch alle Dateien klassifiziert.
- **Threat Hunting Service:** Verhaltensanalyse in der Cloud zur Aufdeckung von Bedrohungsakteuren, die Living-Off-The-Land (LOTL)-Techniken verwenden.
- **KI/ML-Analysen:** Erkennt Living-Off-The-Land (LOTL)-Angriffe, dateilose und skriptbasierte Angriffe und blockiert versteckte Bedrohungen in Installationsprogrammen, PDFs und Office-Dateien.
- **Automatisierte Rekonstruktion von Vorfällen:** Visualisierung des Angriffspfads, um die Anzahl an Alarmmeldungen zu reduzieren und dafür zu sorgen, dass Vorfälle schnell nachvollzogen werden können.
- **GenAI-Assistent:** Abfragen in natürlicher Sprache über Telemetrie, Steigerung der Benutzerfreundlichkeit und Teameffizienz.

WatchGuard Advanced EPDR erweitert EPDR mit Threat Hunting- und Untersuchungstools, einschließlich IoC-Suche, fortschrittlicher IoA-Erkennung, angereicherter Telemetrie und auf MITRE ATT&CK zugeschnittener Analysen sowie Remote-Zugriff auf Windows, macOS und Linux für eine schnellere Untersuchung und Reaktion.



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

WatchGuard Advanced EPDR vereint präventive und EDR-Technologien in einer einzigen, in der Cloud bereitgestellten Lösung und automatisiert Prävention, Erkennung, Eindämmung und Reaktion auf fortschrittliche Bedrohungen über verschiedene Endpoints hinweg.

Werkzeuge zur Reduzierung der Angriffsfläche

- Zentralisierte Erkennung und Bewertung von Endpoint-Sicherheitsrisiken
- Proaktive Erkennung nicht verwalteter Endpoints
- Bewertung der Schwachstellen von Betriebssystemen und Hunderten von Anwendungen

Prävention

- Firewall (IDS), Geräte- und Anwendungskontrolle
- Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- Heuristik vor der Ausführung und kollektive Intelligenz
- Selbstlernende KI mit Verhaltensanalysen erkennt Malware, Ransomware, dateilose und skriptbasierte Angriffe
- ML-Analyse von Installationsprogrammen, PDFs und Office-Dateien, um versteckte Bedrohungen zu erkennen und automatisch zu blockieren
- URL- und Webfilterung, Schutz vor Phishing und Manipulationsabwehr
- Erkennung mithilfe von Analysen des Netzwerkverkehrs
- Endpoint Access Enforcement, um laterale Bewegungen zu blockieren

Threat Hunting, Erkennung und Untersuchung von Gefahren

- Ständige Überwachung von Endpoints mit EDR
- Zero Trust Application und Threat Hunting Services
- Sandboxing in realen Umgebungen und Schutz vor Exploits
- Automatisierte Erkennung und Eindämmung von RDP-Angriffen
- Suche nach STIX-Angriffsindikatoren (IoAs) und YARA-Regeln
- Ausführungsüberwachung oder Verweigerung gängiger LotL-Anwendungen
- Zugriff auf angereicherte Telemetrie
- Abstimmung von Ereignissen und Angriffsindikatoren (IoAs) auf MITRE ATT&CK
- CAPA-Tool: Dateiinformationen (Verhaltensweisen, Zeichenfolgen, Importe, Exporte)
- Automatische Rekonstruktion des Angriffspfads von Vorfällen
- GenAI-Assistent zur Abfrage von Telemetrie

Eindämmung und Abhilfe

- Endpoint-Isolation, Neustart und Remote Shell
- Automatische Behebung und Rollback
- Wiederherstellung verschlüsselter Dateien (Schattenkopien)