Zero-Trust Application Service

Ausgereifte Cyberangriffe

Abwehr neuartiger 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 zu wenig Aufmerksamkeit geschenkt wird. Aus diesem Grund reichen traditionelle Schutzplattformen nicht aus. Sie liefern 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.

KI als disruptive Innovation im Sicherheitsbereich

Der Zero-Trust Application Service ist ein Managed Service, der Teil der WatchGuard EPDR- und WatchGuard EDR-Lösung ist. Dieser Service klassifiziert Anwendungen als Malware oder vertrauenswürdig, sodass nur die vertrauenswürdigen Anwendungen an den jeweiligen Endpoints ausgeführt werden. Da der Service vollständig automatisiert ist, muss weder der Endanwender noch die Sicherheitsanalysten oder das IT-Team aktiv werden oder eine Entscheidung treffen.

Dieser Service klassifiziert 100 % der ausgeführten Prozesse in Echtzeit, überwacht die Aktivitäten an den Endpoints und unterbindet die Ausführung von Anwendungen und böswilligen Prozessen (vor, während und nach der Ausführung).

Der Zero-Trust Application Service umfasst drei Hauptkomponenten:

1. Ständige Überwachung der Aktivitäten an den Endpoints über eine Cloudplattform.

Die Aktivität jeder Anwendung am Endpoint wird überwacht und zur ständigen Klassifizierung an die Cloud gesendet. Auf diese Weise kann die Ausführung von Malware und sogar von ausgereiften Bedrohungen wie Angriffen auf die Lieferkette unterbunden werden.

Der Zero-Trust Application Service lässt die standardmäßige Ablehnung von Prozessen zu, die am Endpoint ausgeführt werden, und unterbindet so die Ausführung potenziell schädlicher Anwendungen und Prozesse. Bei jeder Ausführung wird eine Echtzeit-Klassifizierung als böswillig oder rechtmäßig gesendet, ohne Unsicherheiten und ohne Delegierung manueller Prozesse an den Kunden. Dieser Klassifizierungsprozess lässt die Ausführung von Anwendungen zu, die als rechtmäßig eingestuft werden. Doch was, wenn eine rechtmäßige Anwendung später zu Malware mutiert?

Häufig wird rechtmäßige Software genutzt, um böswillige Aktionen aus finanziellen Motiven auszuführen, darunter auch Software von bekannten Anbietern.

Dieses anomale Verhalten von scheinbar rechtmäßiger Software wird dank ständiger Überwachung und Neubewertung auf unserer Big Data-Plattform erneut klassifiziert.

2. Automatische, KI-basierte Klassifizierung.

Automatische Klassifizierungen erfolgen in einem cloudbasierten KI-System, in dem eine Reihe von Algorithmen für maschinelles Lernen (ML) Hunderte von statischen, Verhaltens- und Kontextattributen in Echtzeit verarbeiten. Extrahiert werden die Attribute aus der Telemetrie der geschützten Umgebung und aus physischen Sandboxes, in denen ausführbare Dateien untersucht werden.

Die Rate der automatischen Klassifizierung liegt aktuell bei 99,98 %. Nur 0,02 % der Prozesse erfordern also das Eingreifen unserer Experten. Das KI-Klassifizierungssystem ist somit autark und skalierbar für große Dateimengen und funktioniert in Echtzeit ohne Eingreifen des Endanwenders.

3. Risikobasierte Anwendungskontrolle.

Bezieht sich auf die Betriebsweise des Schutzmechanismus an den Endpoints.

Es gibt zwei Schutzebenen:

- **Verstärkung:** standardmäßige Ablehnung unbekannter Anwendungen oder Binärdateien von außen (Webdownloads, E-Mails, Wechseldatenträger, dezentrale Standorte usw.).
- **Sperre:** standardmäßige Ablehnung unbekannter Anwendungen oder Binärdateien unabhängig von ihrem Ursprung (aus dem Netzwerk, vom Endpoint selbst oder von außen). Damit wird sichergestellt, dass alle ausgeführten Prozesse vertrauenswürdig sind.

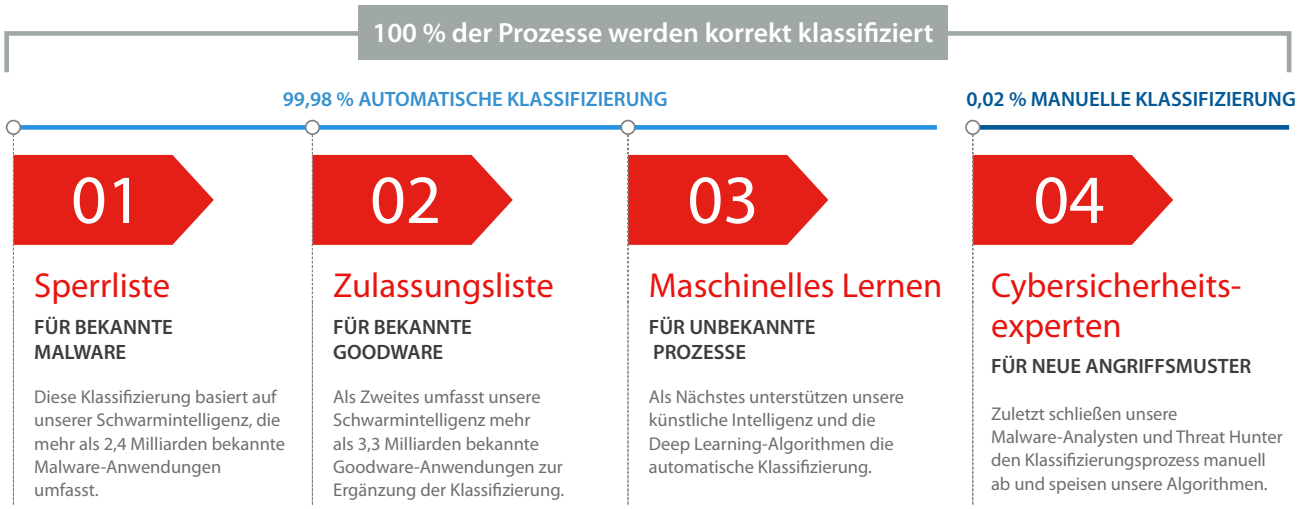
Schwarmintelligenz für die WatchGuard Endpoint-Security

Dies ist eine weitere in der Cloud gehostete Hauptkomponente, die die Effizienz des Zero-Trust Application Service erhöht.

Schwarmintelligenz ist diesem Fall das konsolidierte und immer weiter wachsende Wissens-Repository aller Anwendungen, Binärdateien und anderer Dateien, die interpretierten Code enthalten – vertrauenswürdigen wie bösartigen.

Dieses Repository in der Cloud wird kontinuierlich vom KI-System und von kompetenten Analysten befüllt und gleichzeitig vor jeder Ausführung von den WatchGuard Endpoint-Sicherheitslösungen und -diensten laufend abgefragt.

Funktionsweise:



Die Grafik oben zeigt, wie Technologien im Stack nahtlos zusammenarbeiten, was die Klassifizierung aller Anwendungen, Binärdateien und Dateien, die interpretierten Code enthalten, in Echtzeit sicherstellt.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von mehr als 250.000 Kunden. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Weitere Informationen finden Sie unter WatchGuard.com/de.

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.com/de