WatchGuard Endpoint-Sicherheit

Erweiterbarer Schutz zur Vorbeugung und Erkennung sowie zur Reaktion auf fortgeschrittene Bedrohungen

Der Endpoint hat eine Vielzahl bekannter Schwachstellen, die sich ausnutzen lassen. Außerdem sind häufig veraltete Softwareversionen installiert. Das macht ihn zu einem beliebten Ziel von Cyberkriminellen. Im Internet sind diese Geräte oft nicht durch Sicherheitsmaßnahmen auf Ebene des Unternehmensperimeters geschützt. Mitarbeiter können Hackern bisweilen sogar unwissentlich den Zugang zu den Endpoints und Netzwerken des Unternehmens ermöglichen. Heute müssen Unternehmen aller Größenordnungen keine leistungsstarke Endpoint-Sicherheit mehr implementieren, die in fortschrittliche Endpoint-Detection-and-Response-(EDR)-Technologien integrierte Endpoint Protection (EPP) umfasst.

Die Endpoint-Sicherheitsplattform von WatchGuard bietet maximalen Schutz bei minimaler Komplexität und macht damit Schluss mit Unsicherheiten bei der Endpoint-Sicherheit. Unsere anwenderzentrierten Sicherheitsprodukte und -dienste bieten fortschrittliche EPP- und EDR-Ansätze mit einem Komplettpaket von Sicherheits- und Betriebstools. Sie schützen Personen, Geräte und die Netzwerke, mit denen sie sich verbinden, vor bösartigen Websites, Malware, Spam und anderen gezielten Angriffen. Die Tools zur Verwaltung von Patches, zur Verschlüsselung der Fernüberwachung und für weitere Funktionen nutzen alle dieselbe Konsole, was die Sicherheit weiter erhöht. Unsere Panda-Adaptive-Defense-Produkte werden durch automatisierte, KI-gesteuerte Prozesse und von Sicherheitsanalysten durchgeführte Investigationsservices gestützt, die einen 100-prozentigen Nachweis bieten. Dieser bestätigt die Legitimität und Sicherheit aller ausgeführten Anwendungen, eine entscheidende Notwendigkeit für jedes Unternehmen, das ein Zero-Trust-Sicherheitsmodell implementiert.

Gut oder schädlich? Zu 100 Prozent verlässlich

Die meisten Endpoint-Sicherheitsprodukte blockieren, was als schädlich bekannt ist, untersuchen, was verdächtig ist, und lassen zu, was nicht bekannt ist. Sie ermöglichen damit Malware, die sich schnell verändert, um die Abwehr zusammen mit anderem unbekannten Datenverkehr zu umgehen. Die Produkte von Panda Adaptive Defense bieten dagegen einen Zero Trust Application Service, der ausführbare Dateien hundertprozentig klassifiziert. Dazu analysiert er alle verdächtigen und unbekannten Prozesse und Anwendungen mithilfe spezieller Algorithmen für maschinelles Lernen in unserer Cloud-Plattform und verifiziert sie bei Bedarf sogar mit unseren Labortechnikern. Alle ausführbaren Dateien werden als „Goodware" oder „Malware" eingestuft, so dass Kunden nur bestätigte Warnmeldungen erhalten. Darüber hinaus genießen sie den ultimativen Schutz, der sich daraus ergibt, dass die Standardeinstellung in einem Zero-Trust-Modell die Ablehnung ist.

Erweiterung der Sicherheits-, Transparenz- und Einsatzfähigkeiten

Panda Adaptive Defense 360 (AD360) ist eine umfassende Lösung, die Virenschutz der nächsten Generation und Endpoint Detection and Response (EDR) sowie die Möglichkeit zum Hinzufügen von Visualisierungstools, Patch-Management, Inhaltsfilterung, E-Mail-Sicherheit, vollständiger Verschlüsselung und mehr kombiniert. Viele dieser Produkte sind auch mit anderen grundlegenden Sicherheitsprodukten erhältlich, einschließlich Panda Endpoint Protection, Endpoint Protection Plus und Adaptive Defense. Damit können sich Kunden, die für ihre konkreten Bedürfnisse am besten passende Lösung erstellen.

Lauernde Bedrohungen ohne zusätzlichess Personal

Threat Hunting erfordert in der Regel hoch qualifizierte Ressourcen und nimmt viele Stunden in Anspruch, bevor Bedrohungen aufgespürt und Erkenntnisse gewonnen werden, die aufzeigen, wie man dieser Bedrohungen Herr werden kann. Unsere fortschrittlichen EDR-Lösungen bieten einen Threat Hunting Service, bei dem unsere Sicherheitsanalytiker die Endpoint-Umgebung des Kunden überwachen und Informationen über potenzielle laufende Angriffe bereitstellen. Dazu gehören eine Ursachenanalyse, festgestellte Anomalien, relevante IT-Erkenntnisse und Pläne zur Reduzierung der Angriffsfläche. Dies ist eine Standardfunktion unserer Produkte Adaptive Defense und AD360. IT-Mitarbeiter brauchen deshalb für die Untersuchung infizierter Endpoints keine Zeit und Energie mehr aufzuwenden.

Die Vorteile von intuitivem cloudbasiertem Management

Unternehmen mit nur wenigen IT-Mitarbeitern und geringem Sicherheits-Know-how profitieren vom Schutz durch die Multifaktor-Authentifizierung, die einfach über die Cloud bereitgestellt und verwaltet werden kann. AuthPoint wird auf der WatchGuard Cloud-Plattform ausgeführt und ist überall verfügbar. Sie müssen keine Software installieren, Upgrades planen oder Patches verwalten. Ferner stellt die Plattform problemlos eine Ansicht eines einzelnen globalen Accounts oder vieler unabhängiger Accounts bereit, sodass dezentrale Unternehmen und Managed Service Provider nur die Daten anzeigen können, die für die Rolle einer Person relevant sind.

Ein Komplettpaket mit flexiblen Optionen für jeden Bedarf

- ✔ vollständig nativ in der Cloud
- ✔ Ressourcensparender Agent
- ✔ Bewertung für maschinelles Lernen
- ✔ EPP, EDR, Threat Hunting, Zero-Trust-fähig

Panda Adaptive Defense und Panda Adaptive Defense 360

- Bietet leistungsstarken Endpoint Detection and Response (EDR)-Schutz vor Zero-Day-Angriffen, Ransomware, Cryptojacking und anderen fortschrittlichen gezielten Angriffen. Genutzt werden hierbei neue und neu entstehende KI-Modelle für maschinelles Lernen und Deep Learning.
- Zur Auswahl stehen Optionen nur für EDR (Panda Adaptive Defense) sowie für EPP + EDR (Panda Adaptive Defense 360)
- 100%ige Klassifizierung mit dem Zero-Trust Application Service – zur Erstellung der Art von Reaktion, die für die Einführung eines Zero-Trust-Modells erforderlich ist
- Optimierung von Einsatz und Effizienz des Personals dank Erkenntnissen aus dem Threat Hunting Service
- Implementierung einer umfassenden Endpoint-Sicherheit mit Adaptive Defense 360, das alle Vorteile unseres Adaptive Defense-Produkts und unseres Endpoint-Sicherheitsprodukts in einem Paket enthält

Panda Endpoint Protection und Panda Endpoint Protection Plus

- Schützt Endpoints vor Viren, Malware, Spyware und Phishing mit Signaturen, lokalem Cache und sogar unseren eigenen proprietären Intelligence-Feeds, die aus der zuvor durch Adaptive Defense-Produkte erkannten Malware stammen
- Zur Auswahl stehen die erweiterten Anti-Malware-Optionen (Panda Endpoint Protection) und die Anti-Malware-Optionen mit URL-Filterung und MS Exchange Anti-Spam-Schutz (Panda Endpoint Protection Plus)
- Findet Zero-Day-Angriffe durch den Einsatz von Verhaltensheuristiken und bekannten Indikatoren für Angriffe als „kontextbezogene Regeln"

Zusätzliche Sicherheitsprodukte für Betriebsabläufe

Fügen Sie optionale Module hinzu, die mit allen EPP- und EDR-Sicherheitsprodukten erhältlich sind:

Panda Patch Management ist eine Lösung zur zentralen Verwaltung von Updates und Patches für Betriebssysteme und für Hunderte von Drittanbieteranwendungen und nicht unterstützte Software-Programme (EOL).

Panda Full Encryption nutzt die BitLocker-Technologie von Microsoft zur Ver- und Entschlüsselung von Endpoint-Informationen, wobei die Wiederherstellungsschlüssel über unsere cloudbasierte Management-Plattform zentral verwaltet werden.

Erweitern Sie mit zusätzlichen optionalen Modulen, die nur bei Adaptive Defense-Produkten verfügbar sind:

Advanced Reporting Tool generiert automatisch Sicherheitsinformationen und stellt Tools bereit, mit denen Angriffe, ungewöhnliche Verhaltensmuster sowie interner Missbrauch des Firmennetzwerks erkannt werden können.

Panda Data Control* erkennt, klassifiziert, prüft und überwacht unstrukturierte personenbezogene Daten, die auf Endpoints und Servern gespeichert werden, während des gesamten Lebenszyklus.

SIEM Feeder bietet eine neue Quelle für wichtige Details zu den Sicherheitsinformationen aller Prozesse, die auf Ihren Geräten ausgeführt werden, während sie kontinuierlich überwacht werden. (Nur verfügbar bei Adaptive Defense 360)

Mehr wirksame Sicherheit mit diesen zusätzlichen Produkten

Panda Systems Management ist ein RMM-Tool für die standortunabhängige Verwaltung, Überwachung und Wartung unserer Endpoint-Sicherheitsprodukte.

WatchGuard DNSWatchGO bietet Schutz auf DNS-Ebene inklusive Content Filtering, mit dem sich Unternehmen auch jenseits des eigentlichen Netzwerks gegenüber Phishing, Ransomware und anderen Angriffen bestmöglich abschirmen können, ohne dass ein VPN benötigt wird.

panda
a WatchGuard brand

WatchGuard übernimmt Panda Security, 1. Juni 2020
Beide Unternehmen waren jahrzehntelang führende Vordenker in ihren entsprechenden Bereichen und stellen gemeinsam eine leistungsstarke Sicherheitsplattform bereit, die Netzwerk und Benutzerperimeter verbindet.

Aether Cloud-Management

- Erstellung von Verbindungen in Echtzeit, um Aufgaben in Sekundenschnelle auf Tausende von Geräten zu verteilen
- Verwaltung aller Produkte von Panda über eine einzige Konsole
- Anzeigen von Geräten auf mehreren Endpoint-Plattformen, einschließlich Windows, Linux, macOS und Android

**Nicht in allen Regionen verfügbar*

Gründe für die Verbesserung Ihrer Sicherheit

1. Fügen Sie Schutz für eine neu verteilte Belegschaft hinzu, wenn die Unternehmenspolitik für die Heimarbeit erweitert wird.

Dieses Paket enthält Panda AD360, WatchGuard DNSWatchGO und WatchGuard AuthPoint für die Multifaktor-Authentifizierung. In Kombination schützen diese Lösungen die Anwender vor den verschiedensten Bedrohungen. Zudem bewahren sie über die Endpoint-Sicherheit hinaus die Unternehmensressourcen vor der Infiltration aufgrund verlorener oder gestohlener Zugangsdaten – einer Angriffsmethode, die bei einigen der größten veröffentlichten Sicherheitsverletzungen angewandt wurde.

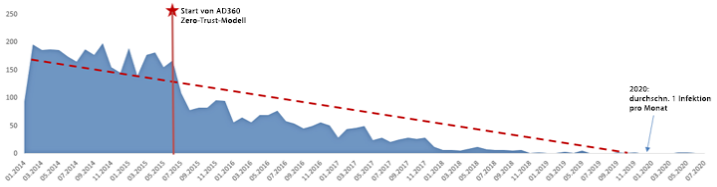
Empfohlene Lösung: **WatchGuard Passport**

2. Erholen Sie sich nach einem Angriff oder nach der Entdeckung von latenter Malware auf Endpoints oder Unternehmensnetzwerken, wenn die Malware von einem Endpoint ausging.

Unternehmen in dieser Position haben zwei Gewissheiten – erstens, dass sie für Cyberkriminelle sicherlich von Interesse sind, und zweitens, dass ihr derzeitiges Schutzniveau nicht angemessen ist. Da sich der erweiterte Schutz von AD360 mit dem Zero Trust Application Service und dem Threat Hunting Service weiterentwickelt hat, ist die Anzahl der auf Malware basierenden Angriffe, die unser Support-Team untersucht/bearbeitet hat, auf nahezu 0 gesunken – unsere Kunden erleben diese Angriffe also gar nicht mehr. In Kombination mit den Sichtbarkeits- und Management-Tools zur Steigerung der Produktivität eines überlasteten IT-Teams ist der Service dafür gerüstet, wiederholte Angriffe und teure Behebungsmaßnahmen zu verhindern.

Empfohlene Lösung:
Adaptive Defense 360
Advanced Reporting Tool
Patch Management
Systems Management

#ANZAHL DER VOM SUPPORT-TEAM BEARBEITETEN MALWARE-BASIERTEN INFEKTIONEN PRO MONAT, 2014 BIS 2020



3. Fügen Sie als geplante Sicherheitsinvestition die EDR-Funktion zu einer vorhandenen AV-Lösung hinzu.

Diese Unternehmen sind sich der Sicherheitsrisiken am Endpoint bewusst und haben ein AV-Produkt eingeführt. Doch sie wissen, dass sie eine EDR-Lösung benötigen, um Hackern einen Schritt voraus zu sein. Es besteht keine Notwendigkeit, auf eine Verlängerung des AV-Vertrags zu warten. Unsere Adaptive Defense EDR-Lösung ergänzt eine vorhandene AV-Bereitstellung, so dass Kunden schnell von unserem fortschrittlichen, differenzierten Ansatz profitieren können.

Empfohlene Lösung: **Adaptive Defense 360**

4. Rüsten Sie ausgehend von einem kostenlosen oder auf private Nutzung ausgerichteten Endpoint-AV-Produkt auf.

Manchmal setzen kleine Unternehmen oder solche, die nur wenige Geräte außerhalb des Netzwerkperimeters haben, auf ein reduziertes Risikoprofil und schieben Investitionen in die Sicherheit auf. Aber die Welt verändert sich. Da Unternehmen immer mehr Risiken ausgesetzt sind und strengere Vorschriften zur Datensicherheit und zum Datenschutz erfüllen müssen, gehen sie zu einer Business-Lösung wie dem Produkt Panda Endpoint Protection Plus über. EPP Plus ist mit starker signaturbasierter Prävention, einschließlich Signaturen von Malware aus unserer Installationsbasis, sowie Verhaltensanalyse, Filterung von Webinhalten und Anti-Spam-Produkten eine kluge Wahl, die zukunftssicher ist, da die Plattform mit dem Geschäftswachstum Schritt hält.

Empfohlene Lösung: **Panda Endpoint Protection Plus**

> Die proaktive Herangehensweise im Kampf gegen Schadsoftware gibt mir Ruhe und Sicherheit. Konfigurieren, Verwalten, Probleme schnell beheben – über die anwenderfreundliche Weboberfläche geht das ganz einfach.
>
> **Jeff Smith**
> Administrator Technologiesysteme, Sacred Heart Schools

Kundenhighlight: BDO

BDO, eine in 162 Ländern tätige Wirtschaftsprüfungs- und Risikoberatungsfirma, ist einer der am schnellsten wachsenden Anbieter professioneller Dienstleistungen weltweit, der sich auf Buchhaltung, Wirtschaftsprüfung, Steuer- und Beratungsdienste spezialisiert hat. Nico Fourie (BDO National IT-Direktor) betrachtet die Informationssicherheit als eine wichtige Säule jedes Unternehmens. „Unternehmen sollten sich davor hüten, selbstgefällig zu werden oder sich in falscher Sicherheit zu wiegen, selbst wenn sie meinen, sie hätten ihre Angelegenheiten geregelt", so Fourie. „Bei der Beurteilung unserer Situation müssen wir unbedingt die Endpoints klar im Blick haben … und die Einhaltung von Vorschriften in Übereinstimmung mit DSGVO und POPIA erfordert auch eine erhöhte Transparenz und Kontrolle der Daten", führt Fourie weiter aus.

Um diesen Herausforderungen gerecht zu werden, hat BDO Panda Adaptive Defense 360 (AD360) und das Advanced Reporting Tool (ART) sowie Panda Patch Management-Module implementiert. „Dieser Multi-Tool-Ansatz sorgt für mehr Transparenz und eine ganzheitliche Berichterstattung und ermöglicht uns, Lücken in unserer Sicherheit zu erkennen", erläutert Fourie. Vor der Einführung von AD360 verfügte BDO über eine signaturbasierte Lösung, die fortgeschrittene und Zero-Day-Bedrohungen weder erkennen noch blockieren konnte. Jetzt ist BDO vor der Art von ausweichender Malware und dateilosen Angriffen geschützt, wie wir sie heute erleben. Fourie erläutert: „Mit AD360 konnten wir einen Zero-Trust-Ansatz umsetzen und Cybersicherheitsrisiken deutlich verringern".

Name des Unternehmens
BDO South Africa

Land
Südafrika

Lösung
Adaptive Defense 360

Lizenzen
1.000

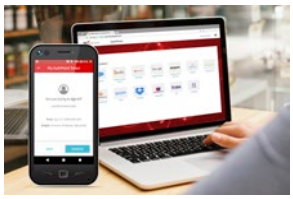
WatchGuard Unified Security Platform™

Netzwerksicherheit

Netzwerk-Sicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

Sicheres WLAN

Die Secure Wi-Fi Solution von WatchGuard ist eine richtungsweisende Neuerung für den Markt von heute: Sie schafft eine sichere, geschützte WLAN-Umgebung, eliminiert den Verwaltungsaufwand und ermöglicht beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.



Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können Sie die passwortgestützte Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones" als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen.

Endpoint-Sicherheit

WatchGuard Endpoint Security ist ein Cloud-natives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung Panda Adaptive Defense 360 verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

Mehr erfahren

Weitere Details erhalten Sie von einem autorisierten WatchGuard-Vertriebspartner oder unter **https://www.watchguard.com.**

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 16.000 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 Pazifikraum. Weitere Informationen finden Sie unter WatchGuard.de.