Panda Endpoint Protection Plus

Verwalten Sie die Sicherheit Ihrer IT-Infrastruktur

panda
a WatchGuard brand

Jeden Tag werden über 350.000 neue Schadprogramme (Malware) und potenziell unerwünschte Anwendungen (PUA) gefunden.[1] Hacker zielen auf verwundbare Endpoints, auf denen Unternehmen ihre wertvollsten Assets aufbewahren. Der Grund? Wie so oft: **wirtschaftliche Motive**.

Unternehmen hängen in steigendem Maße von neuen Technologien ab und sind daher gegenüber neuen Arten von Malware, die ihre Sicherheit **gefährden**, **exponiert**. Dies macht Sicherheitsansätze erforderlich, die die **Angriffsoberfläche verkleinern**.

EVOLUTION DER IT-UMGEBUNGEN VON UNTERNEHMEN

Über die letzten Jahre haben die technologische Entwicklung und die umfassende Nutzung des Internets, von Mobilgeräten sowie cloudbasierter Speicher und Apps zu einer echten Revolution der Unternehmensumgebung geführt. Diese Revolution geht jedoch mit Risiken einher. Diese Vorteile sind jedoch nicht nur für Unternehmen wertvoll, sondern werden auch von Cyberkriminellen genutzt.

Die Ursache für die wachsende Anzahl an Cyberangriffen ist der höhere Wert der von Unternehmen gespeicherten digitalen Assets. Das bedeutet auch, dass Cyberkriminelle hier eine Chance sehen, ihren Ertrag zu steigern. Malware und Ransomware gehören mittlerweile zu den häufigsten Bedrohungen, obwohl die direkten Kosten nicht das Hauptproblem darstellen. Viel kostspieliger sind die verursachten Ausfallzeiten. Dies zwingt Unternehmen, Maßnahmen zu ergreifen, um ihre Sicherheitslage zu verbessern.

SCHÜTZEN SIE IHR UNTERNEHMEN VOR MALWARE UND RANSOMWARE

Panda Endpoint Protection Plus stellt eine vollständige, hochentwickelte Sicherheitslösung für Desktop-Geräte, Laptops und Server dar. Sie dient zum zentralen Management der Endpoint-Sicherheit sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks.

Dieser Dienst bietet einen Satz von EPP-Technologien zur Kontrolle von Malware, Ransomware und Bedrohungen, die unbekannte Schwachstellen (Zero Day) ausnutzen. Es müssen keine neuen Hardwareressourcen auf der Infrastruktur des Unternehmens installiert oder gewartet werden.

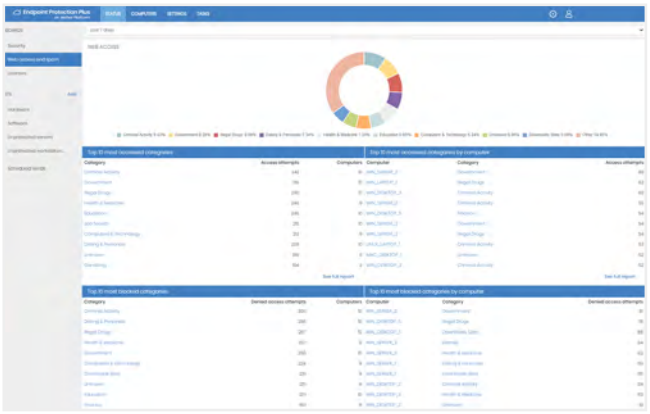

Abbildung 1: Webzugang und Spam-Dashboard.

VORTEILE

Sicherheit auf mehreren Plattformen

- Schutz vor unbekannten hochentwickelten Bedrohungen: erkennt und blockiert Malware, Trojaner, Phishing und Ransomware.
- Sicherheit über alle Angriffsvektoren hinweg: Browser, E-Mail, Dateisysteme und mit Endpoints verbundene externe Geräte.
- Automatische Analyse und Desinfektion von Computern. Verhaltensanalyse zur Erkennung bekannter und unbekannter Malware.
- Sicherheit für Windows-Systeme, Linux, macOS, iOS, Android und virtuelle Umgebungen (VMware, Virtual PC, MS Hyper-V, Citrix) – sowie für sowohl persistente als auch nicht persistente Virtualisierungs-Infrastruktur (VDI).

Produktivitätssteigerung

- Die Lösung überwacht und filtert Web-Traffic und verhindert, dass Mitarbeiter sich mit unproduktiven Tätigkeiten beschäftigen oder Sicherheitsbedrohungen wie Bots oder Phishing zum Opfer fallen.
- Es ist keine spezielle Infrastruktur oder Wartung erforderlich; die IT-Abteilung kann sich auf wichtigere Aufgaben konzentrieren.

Einfachere Verwaltung

- Einfache Wartung: Keine spezielle Infrastruktur zum Hosten der Lösung erforderlich; die IT-Abteilung kann sich auf wichtigere Aufgaben konzentrieren.
- Einfacher Schutz von Remote-Anwendern: Jeder mit Panda Endpoint Protection Plus geschützte Computer kommuniziert mit der Cloud; Remote-Büros und -Anwender lassen sich ohne zusätzliche Installationen schnell und einfach schützen.
- Einfache Bereitstellung: Mehrere Bereitstellungsmethoden mit automatischen Deinstallationsprogrammen für Konkurrenzprodukte ermöglichen eine schnelle Migration von Drittanbieterlösungen.

[1] **AV-Test**: https://www.av-test.org/en/statistics/malware/

ZENTRALE ENDPOINT-SICHERHEIT

Umfasst zentrale Verwaltung der Sicherheits- und Produktaktualisierungen aller Workstations und Server im Unternehmensnetzwerk. Verwalten Sie den Schutz von Windows-, Linux-, macOS-, iOS- und Android-Geräten über eine einzige, webbasierte Administrationskonsole.

SCHUTZ VOR MALWARE UND RANSOMWARE

Panda Endpoint Protection Plus analysiert Verhaltensweisen und Hacking-Techniken, um sowohl bekannte als auch unbekannte Malware sowie Ransomware, Trojaner und Phishing zu erkennen und zu blockieren. Zudem stellt Malware Freezer erkannte Malware sieben Tage lang unter Quarantäne und die betroffene Datei wird bei einem false-positive Treffer automatisch wieder hergestellt.

FORTGESCHRITTENE DESINFEKTION

Bei einer Sicherheitsverletzung ermöglicht Panda Endpoint Protection Plus es Unternehmen, betroffene Computer schnell auf den vorherigen Zustand zurückzusetzen. Dazu werden fortschrittliche Desinfektionstools und Quarantäne eingesetzt, die verdächtige und gelöschte Elemente speichert. Zudem können Administratoren Workstations und Server aus der Ferne neu starten, um sicherzustellen, dass aktuelle Produkt-Aktualisierungen installiert sind.

ÜBERWACHUNG UND WEBFILTERUNG

Detaillierte Netzwerksicherheitsüberwachung in Echtzeit lässt sich über umfassende Dashboards und einfach ablesbare Diagramme durchführen.

Webfilter steigern die Produktivität im Unternehmen und überwachen Aktivität, um Zugriff auf gefährliche oder unproduktive URLs zu verhindern.

ZENTRALE GERÄTESTEUERUNG

Blockieren Sie ganze Gerätekategorien (Flash-Laufwerke, USB-Modems, Webcams, DVD/CD usw.), richten Sie Whitelists für Geräte ein oder konfigurieren Sie Berechtigungen mit Lesezugriff, Schreibzugriff oder Lese-/Schreibzugriff, um Malware und Datenlecks zu verhindern und potenziell riskante Aktivitäten zu blockieren.

SCHNELLE, FLEXIBLE INSTALLATION

Stellen Sie den Schutz über E-Mail und eine Download-URL bereit oder nehmen Sie über das integrierte Distributionstool der Lösung eine automatische Bereitstellung für ausgewählte Endpoints vor. Das MSI-Installationsprogramm ist mit Drittanbieter-Tools kompatibel (Active Directory, Tivoli, SMS usw.)

GARANTIERTE VERFÜGBARKEIT RUND UM DIE UHR GEMÄSS ISO 27001 UND SAS 70

Die Lösung wird auf einer Aether-Plattform mit garantiertem vollständigen Datenschutz gehostet. Unsere Rechenzentren sind gemäß ISO 27001 und SAS 70 zertifiziert, wodurch Kunden kostspielige Ausfallzeiten und Malware-Infektionen vermeiden können.

BEHEBUNG VON RANSOMWARE UND WIEDERHERSTELLUNG

Um zu verhindern, dass korrumpierte Systeme wiederhergestellt werden, versuchen Angreifer nicht nur Dateien zu verschlüsseln, sondern auch von Administratoren erstellte Sicherungs- und VSS-Dateien zu löschen und Dienste zu deaktivieren, die bei der Wiederherstellung unterstützen sollen.

Die Funktion für Schattenkopien nutzt die Technologie des Betriebssystems und schützt diese Dateien mit unserer Technologie für den Schutz vor Manipulation. So können Benutzer Daten nach einem Ransomware-Angriff wiederherstellen.

IT-Experten verwenden die Schattenkopien, um Dateien nach einem kritischen Systemausfall wiederherzustellen, allerdings eignet sich diese Technologie auch hervorragend zur Wiederherstellung von Dateien, dir durch Ransomware verschlüsselt wurden.

Kompatible Lösungen auf der Aether-Plattform:

Panda Endpoint Protection **Panda Endpoint Protection Plus**

Windows-Workstations und -Server:
http://go.pandasecurity.com/endpoint-windows/requirements

macOS-Geräte:
http://go.pandasecurity.com/endpoint-macos/requirements

Linux-Workstations und Server:
http://go.pandasecurity.com/endpoint-linux/requirements

Android-Mobilgeräte:
http://go.pandasecurity.com/endpoint-android/requirements

iOS-Mobilgeräte:
https://www.pandasecurity.com/support/card?id=700123

VERTRIEB DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.com | pandasecurity.com