Panda Endpoint Protection

Die Endpoint-Sicherheit entwickelt sich weiter

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.

Im Jahr 2020 **werden über 350.000 neue Schadprogramme** pro Tag erfasst[1]. Hacker zielen auf verwundbare Endpoints, auf denen Unternehmen ihre **wertvollsten Assets** aufbewahren. Der Grund? Wie so oft: wirtschaftliche Motive. **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

Die steigende Exposition von Unternehmen gegenüber neuen Typen von Malware und Bedrohungen beeinträchtigt ihre Sicherheitslage und erfordert neue Ansätze, um die Auswirkungen potenzieller Angriffe zu mindern.

Panda Endpoint Protection ist eine effektive, cloudnative Sicherheitslösung für Desktops, Laptops und Server. Sie dient dem zentralen Management der Endpoint-Sicherheit, sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks.

Sie umfasst ein Reihe von EPP-Technologien zum Schutz vor Malware, Ransomware und aktuellen Bedrohungen. Eine dieser Technologien überprüft in Echtzeit die Panda Threat Intelligence, ein umfangreiches Repository, das über die neuesten Machine-Learning-Algorithmen verfügt, um schädliche Angriffe schneller zu erkennen.

Zudem muss keine Hardware und Software gewartet werden. Der ressourcensparende Agent hat keine Auswirkungen auf die Endpoint-Leistung, was das Sicherheitsmanagement vereinfacht und die betriebliche Effizienz verbessert.

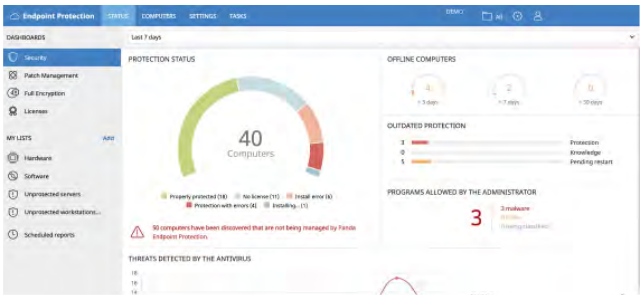

Abbildung 1: Dashboard zum Status des Netzwerkschutzes.

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

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.
- Plattformübergreifende Sicherheit: Windows-Systeme, Linux, macOS, iOS, Android und virtuelle Umgebungen (VMware, Virtual PC, MS Hyper-V, Citrix). Verwaltung von Lizenzen für persistente und nicht persistente Virtualisierungs-Infrastruktur (VDI).

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 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.
- Flache Lernkurve: Intuitive, einfache webbasierte Management-Schnittstelle, bei der die meistgenutzten Optionen nur einen Klick entfernt sind.

Geringere Beeinträchtigung der Leistung

- Der Agent weist nur minimale Netzwerk-, Arbeitsspeicher- und CPU-Auslastung auf, da alle Vorgänge in der Cloud ausgeführt werden.
- Panda Endpoint Protection erfordert keine Installation, Management oder Wartung neuer Hardwareressourcen in der Infrastruktur der Organisation.

panda
a WatchGuard brand

ZENTRALE GERÄTESICHERHEIT

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 analysiert Verhaltensweisen und Hacking-Techniken, um sowohl bekannte als auch unbekannte Malware sowie Ransomware, Trojaner und Phishing zu erkennen und zu blockieren.

FORTGESCHRITTENE DESINFEKTION

Bei einer Sicherheitsverletzung ermöglicht Panda Endpoint Protection 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 BERICHTE IN ECHTZEIT

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

Berichte zu Schutzstatus, Erkennungen und unsachgemäßer Nutzung von Geräten werden automatisch erstellt und zugestellt.

GRANULARE PROFILKONFIGURATION

Weisen Sie spezifische Schutzrichtlinien nach Anwenderprofil zu, was sicherstellt, dass jede Anwendergruppe geeignete Richtlinien erhält.

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.

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.)

MALWARE FREEZER

Malware Freezer stellt erkannte Malware sieben Tage lang unter Quarantäne und stellt die betroffene Datei bei einem falsch positiven Treffer automatisch wieder her.

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

Die Lösung wird auf der Aether-Plattform mit garantiertem vollständigen Datenschutz gehostet. Unsere Datenzentren 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

WatchGuard

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