Panda Adaptive Defense 360

Automatisierte hochentwickelte Sicherheit Schieben Sie Cyberbedrohungen einen Riegel vor

panda a WatchGuard brand

HERAUSFORDERUNGEN BEI DER CYBERSICHERHEIT FÜR UNTERNEHMEN

Endpoints sind das primäre Ziel der meisten Cyberangriffe. Da die Technologie-Infrastruktur zunehmend komplexer wird, haben Unternehmen Probleme, was Know-how und Ressourcen zur Überwachung von Endpoint-Sicherheitsrisiken und zum Umgang mit diesen angeht. Welche Arten von Herausforderungen müssen Unternehmen bewältigen, wenn sie Endpoint-Sicherheitslösungen einsetzen?

- **Alert Fatigue:** Unternehmen erhalten pro Woche Tausende von Warnmeldungen zu Malware, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % überhaupt geprüft werden. Ein Administrator für Cybersicherheit verbringt zwei Drittel der Zeit mit der Verwaltung von Malware-Warnmeldungen.
- **Komplexität:** Zu viele unverbundene Tools für Cybersicherheit lassen sich von Sicherheitsexperten evtl. nur schwer verwalten – aufgrund der Anzahl der erforderlichen Technologien, der fehlenden internen Fähigkeiten und des Zeitaufwands zur Identifizierung von Bedrohungen.
- **Schlechte Performance:** Häufig erfordern Lösungen für Endpoint-Sicherheit die Installation und Verwaltung mehrerer Agents auf jedem überwachten Computer, Server und Laptop. Dies verursacht schwerwiegende Fehler, eine schlechte Performance und einen hohen Ressourcenverbrauch.

Traditionelle, auf Vorbeugung ausgerichtete Technologien für Endpoint-Schutz sind für bekannte Bedrohungen und böswillige Verhaltensweisen geeignet, bieten jedoch keinen ausreichenden Schutz vor modernen Cyberbedrohungen. Von gängigen Bedrohungsvektoren bis zu neuen Bedrohungen, Angreifer suchen nach immer neuen Möglichkeiten, den wachsamen Augen des IT-Teams zu entgehen, Schutzmaßnahmen zu umgehen und entstehende Schwachstellen auszunutzen.

VON DER VORBEUGUNG BIS HIN ZUR REAKTION – AUTOMATISCHE ENDPOINT-SICHERHEIT

Panda Adaptive Defense 360 ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Die Plattform automatisiert die Vorbeugung, Erkennung, Eindämmung und Abwehr im Zusammenhang mit mannigfaltigen, neuartigen Bedrohungen – von Zero-Day-Malware über Ransomware, Phishing oder In-Memory-Exploits bis hin zu weiteren Angriffsversuchen ohne Dateien und Malware – für optimalen Schutz innerhalb und außerhalb des Unternehmensnetzwerks.

Im Gegensatz zu anderen Lösungen kombiniert sie eine sehr breite Palette an Technologien zum Endpoint-Schutz (EPP) mit automatisierten Funktionen für Erkennung und Reaktion (EDR). Die Lösung umfasst auch zwei Services, die von den Experten von Panda Security verwaltet werden und in die Lösung integriert sind:

- **Zero-Trust Application Service:** 100%ige Klassifizierung von Anwendungen
- **Threat Hunting Service:** Erkennung von Hackern und Insidern

Abbildung 1: Panda Adaptive Defense Haupt-Dashboard.

Panda Adaptive Defense 360 vereint herkömmliche Endpoint-Technologien mit innovativen, adaptiven Methoden der Vorbeugung und EDR-Technologien in einer einzigen Lösung und ermöglicht es IT-Fachkräften, mit fortgeschrittenen Cyberbedrohungen fertigzuwerden :

Traditionelle Präventionsmethoden

- Persönliche oder verwaltete Firewall (IDS)
- Gerätesteuerung
- Collective Intelligence
- Deny list / Allow list
- Permanenter Multi-Vektor Anti-Malware & On-Demand-Scan
- Vor-Ausführungs-Heuristik
- URL Filtering – Webbrowsing
- Anti-Phishing
- Manipulationsabwehr
- Automatische Behebung und Möglichkeit für Rollbacks

Neuartige Sicherheitstechnologien

- Ständige Überwachung der Endpoint-Aktivität mit EDR
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher Prozesse (APT, Ransomware, Rootkits usw.)
- Sandboxing in realen Umgebungen
- Schutz vor Exploits
- Threat Hunting, einschließlich Verhaltensanalysen und Erkennung von IoAs (Indicators of Attack) zur Identifizierung von LotLs (Living off the Land-Angriffen)
- Indicators of Attack werden dem MITRE ATT&CK-Framework zugeordnet
- Erkennung und Abwehr von RDP-Angriffen
- Eindämmungs- und Bereinigungsmöglichkeiten wie Computerisolierung und Programmblockierung nach Hash oder Name

Unterstützte Plattformen und Systemanforderungen von PANDA ADAPTIVE DEFENSE 360

Kompatible Betriebssysteme: Windows (Intel & ARM), macOS, Linux, und, iOS Android. EDR-Funktionen sind auf Windows, macOS und Linux verfügbar, wobei auf der Windows-Plattform alle Funktionen in vollem Umfang verfügbar sind.

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge und Opera.

panda
a WatchGuard brand

VORTEILE

Vereinfacht und maximiert Sicherheit

- Durch die automatischen Services lassen sich Kosten für Fachpersonal einsparen. Es müssen keine Fehlalarme untersucht werden, manuelle Einstellungen sind nicht erforderlich (weniger Zeitaufwand) und es werden keine Entscheidungen delegiert.
- Die Installation, Konfiguration oder Pflege einer Managementinfrastruktur ist nicht erforderlich.
- Dank ressourcensparendem Agent und Cloudarchitektur wird die Leistungsfähigkeit der Endpoints nicht beeinträchtigt.

Benutzerfreundlich und einfach zu verwalten

- Mit dem Endpoint Security-Portfolio lassen sich alle Anforderungen des Endpoint- Schutzes auf bemerkenswert einfache Weise über eine einzige Webkonsole erfüllen.
- Einfach einzurichten. Zentrale plattformübergreifende Endpoint-Verwaltung.
- Es steht eine übersichtliche und selbsterklärende Benutzeroberfläche zur Verfügung, die einfach verständlich ist.

Automatische EDR-Funktionen

- Erkennt und blockiert Techniken, Taktiken und Prozesse von Hackern sowie bösartige In-Memory-Aktivitäten (Exploits), bevor diese Schaden anrichten können.
- Problemlösung und Reaktion: forensische Informationen zur gründlichen Untersuchung jedes Angriffsversuchs sowie Tools zur Verringerung der Auswirkungen (Desinfektion).
- Nachverfolgbarkeit jeder Aktion: verwertbare Erkenntnisse über den Angreifer und dessen Aktivitäten, was die forensische Untersuchung erleichtert.

ZERO-TRUST-MODELL: MEHRSCHICHTIGER SCHUTZ

Die Endpoint Security-Plattform von Panda Security nutzt nicht nur eine einzige Technologie, sondern verschiedene, um die Erfolgschancen eines Angreifers zu reduzieren. Gemeinsam verwenden diese Technologien Ressourcen am Endpoint, um das Risiko einer Sicherheitsverletzung zu minimieren.

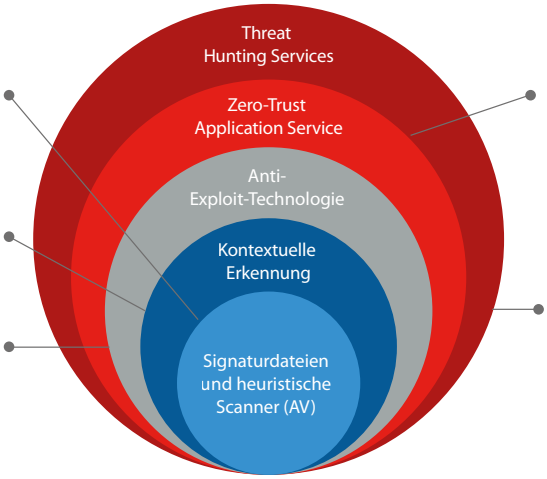
Zero-Trust-Modell: Mehrschichtiger Schutz

ENDPOINT-EBENEN

Ebene 1/Signaturdateien und heuristische Technologien
Effektive, optimierte Technologie zur Erkennung bekannter Angriffe

Ebene 2/Kontextuelle Erkennung
Erkennung von Angriffen ohne Malware und Dateien

Ebene 3/Anti-Exploit-Technologie
Erkennung dateiloser Angriffe, die Schwachstellen ausnutzen



CLOUDNATIVE EBENEN

Ebene 4/Zero-Trust Application Service
Erkennt, ob auf einer vorherigen Ebene ein Verstoß vorliegt, stoppt Angriffe auf bereits infizierten Computern und verhindert laterale Bewegungsangriffe innerhalb des Netzwerks

Ebene 5/Threat Hunting Service
Erkennung von angegriffenen Endpoints, frühen Phasen eines Angriffs, verdächtigen Aktivitäten und IoAs

Signaturdateien und heuristische Technologien, also traditionelle Lösungen zum Endpoint-Schutz (EPP), bilden eine Virenschutztechnologie der nächsten Generation, die sich gegen viele gängige einfache Bedrohungen und böswillige URL-Blockierungen bewährt hat.

Die kontextuelle Erkennung ist sehr effektiv gegen skriptbasierte Angriffe, Angriffe mit Goodware-Betriebssystemtools wie PowerShell, WMI usw., Webbrowser-Schwachstellen und andere häufige Zielanwendungen wie Java, Adobe und mehr.

Die Anti-Exploit-Technologie sucht nach anomalem Verhalten und erkennt es. Sie ist geschäftskritisch auf nicht gepatchten bzw. noch zu patchenden Endpoints sowie auf Endpoints mit Betriebssystemen, die nicht mehr unterstützt werden.patchenden Endpoints sowie auf Endpoints mit Betriebssystemen, die nicht mehr unterstützt werden.

Der Zero-Trust Application Service klassifiziert jeden einzelnen Prozess, wobei standardmäßig jede Ausführung abgelehnt wird, solange sie nicht als vertrauenswürdig zertifiziert wurde. Bedrohungen müssen nicht manuell klassifiziert oder an Sicherheitsadministratoren übergeben werden.

Der Threat Hunting Service basiert auf einer Reihe von Threat-Hunting-Regeln, die von Cybersicherheitsspezialisten entwickelt wurden und die automatisch auf alle durch die Telemetrie erfassten Daten angewendet werden. Hierdurch werden Indicators of Attacks (IoAs) identifiziert, die die Erkennungs- und Reaktionszeit (MTTD und MTTR) verringern.

WatchGuard

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