Adaptive Defense 360

Moderne Sicherheitslösung zur erfolgreichen Bekämpfung von Cyberbedrohungen

panda a WatchGuard brand

Cybersicherheit für optimalen Schutz mit minimalem Verwaltungsaufwand

Mobilität, Verarbeitung und Cloudspeicher haben die Netzwerkstruktur von Unternehmen revolutioniert. Doch trotz aller Fortschritte gelingt es Hackern immer wieder, sich Zugang zu verschaffen. Woche für Woche erhalten IT-Abteilungen Tausende von Malware-Benachrichtigungen, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % überhaupt untersucht werden. Daher verwundert es nicht, dass ein Administrator für Cybersicherheit typischerweise zwei Drittel der Zeit mit der Verwaltung von Warnmeldungen verbringt.

Endpunktsicherheitslösungen müssen nicht nur die von einem Cyberangriff ausgehenden Bedrohungen bekämpfen, sondern auch den Ressourcenmangel bei der Abwehr solcher Angriffe kompensieren. Vorbeugung und Erkennung spielen eine wesentliche Rolle. Ebenso wichtig ist es jedoch, dass die IT-Abteilung wertvolle Zeit zurückgewinnt, damit sie sich auf andere kritische Bereiche konzentrieren kann. Dies setzt voraus, dass die Aktivitäten zur Verwaltung der Lösung automatisiert werden.

Das Problem bei hoch entwickelten Lösungen zur Cyberabwehr

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**. Auch dies ist darauf zurückzuführen, dass der **Beseitigung von Sicherheitslücken in Systemen** zu wenig Aufmerksamkeit geschenkt wird.

Traditionelle Schutzplattformen (Endpoint Protection Platforms, EPPs) bieten als Mittel gegen ausgeklügelte Angriffe zu wenig, da sie die Prozesse und Anwendungen in Unternehmensnetzwerken nur unzureichend visualisieren und nicht detailliert genug sind. Zur Lösung dieses Problems verstärken IT-Abteilungen den Schutz in Form von Endpoint-Defense-and-Response(EDR)-Lösungen. Das Problem bei den meisten EDR-Plattformen besteht darin, dass sich der Sicherheitsadministrator um das gesamte Management kümmern muss. Seine Arbeitslast steigt dadurch um das Zehnfache, wenn er Warnmeldungen verwalten und Bedrohungen manuell klassifizieren muss.

Die Lösung für fortschrittliche Cyberabwehr: Adaptive Defense 360

Panda Adaptive Defense 360 (AD360) ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. **Sie automatisiert die Vorbeugung, Erkennung, Eindämmung und Abwehr** von hoch entwickelten Bedrohungen, Zero-Day-Malware, Ransomware, Phishing, In-Memory-Exploits und Angriffsversuchen ohne Malware. Dieser hohe Schutz sorgt dafür, dass gegenwärtige und zukünftige Bedrohungen beseitigt werden – sowohl innerhalb als auch außerhalb des Firmennetzwerks.

AD360 unterscheidet sich von anderen Lösungen, da es traditionellen Endpunktschutz (EPP) mit automatisierten EDR-Funktionen der nächsten Generation vereint und so umfassenden Schutz vor bekannten und unbekannten Bedrohungen bietet. Hinzu kommen zwei Kernfunktionen, die bei AD360 als Service bereitgestellt werden – während sich bei anderen Anbietern die IT-Abteilung darum kümmern muss:

- **100 % Klassifizierung aller Prozesse**
- **Threat Hunting and Investigation Service**

Dank der Cloud-Architektur ist der Agent platzsparend und hat keinerlei Auswirkungen auf die Leistungsfähigkeit der Endpoints, die über eine einzige Cloudarchitektur verwaltet werden, selbst wenn sie isoliert sind.

Panda Adaptive Defense 360 ist über eine einzige Webkonsole zugänglich. Die Lösung beinhaltet Cloud Protection und Management Platforms (Aether), die die Prävention, Erkennung und automatische Reaktion optimieren und so den Arbeitsaufwand verringern.

Vorteile

Weniger Aufwand, geringere Sicherheitskosten

- Dank Managed Services lassen sich Kosten für Fachpersonal einsparen, da keine Fehlalarme untersucht und keine Zuständigkeiten weitergegeben werden müssen.
- Die Managed Services lernen automatisch aus früheren Angriffen, sodass keine Zeit mit manueller Konfiguration verschwendet wird.
- Durch bestmögliche Prävention an den Endpunkten werden die Betriebskosten praktisch auf Null gesenkt.
- Installation, Konfiguration und Pflege einer Managementinfrastruktur sind nicht erforderlich.
- Dank ressourcensparendem Agent und Cloud-Architektur wird die Leistungsfähigkeit der Endpunkte nicht beeinträchtigt.

Verkürzung der Erkennungszeit dank Automatisierung

- Blockiert Anwendungen, die ein Sicherheitsrisiko darstellen (durch Hash oder Prozessnamen)
- Verhindert die Ausführung von Angriffen, Zero-Day-Malware, Ransomware Angriffen ohne Datei/Malware und Phishing-Versuchen
- Erkennt und blockiert bösartige Aktivitäten im Arbeitsspeicher (Exploits), bevor diese Schaden anrichten können
- Erkennt bösartige Prozesse, die Ihre Schutzmechanismen umgehen
- Erkennt und unterbindet Techniken, Taktiken und Prozesse von Hackern

Automatisierung und Verkürzung von Reaktions- und Untersuchungsmaßnahmen

- Problemlösung und Reaktion anhand von forensischen Informationen zur Untersuchung jedes Angriffsversuchs sowie Tools zur Verringerung der Auswirkungen (Desinfektion)
- Verfolgung jeder Aktion und Aktivität des Angreifers – erleichtert die forensische Untersuchung
- Verbesserung und Anpassung von Sicherheitsrichtlinien aufgrund der Erkenntnisse aus der forensischen Analyse

WatchGuard

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

Erweiterte und automatisierte Endpunktsicherheit

Traditionelle, auf Vorbeugung ausgerichtete Schutztechnologien (EPPs) sind kostengünstige Maßnahmen gegen bekannte Bedrohungen und böswillige Verhaltensweisen, reichen jedoch alleine nicht aus. Zur erfolgreichen Bekämpfung von Cyberbedrohungen ist eine Abkehr von der traditionellen Prävention hin zu einem Modell der kontinuierlichen Vorbeugung, Erkennung und Reaktion nötig. Dabei wird stets davon ausgegangen, dass dem Netzwerk Schaden zugefügt wurde und alle Endpunkte ständig angegriffen werden.

Mit **Panda Adaptive Defense 360** können IT-Abteilungen die angestrebte Sicherheitslage herstellen, da traditionelle EPP-Technologien und EDR-Funktionen in einer einzigen Lösung integriert sind. Dadurch ist das Netzwerk unanfällig für bekannte und unbekannte Bedrohungen.

Traditionelle Präventionsmethoden

- Persönliche und verwaltete Firewall. IDS
- Gerätesteuerung
- Ständige Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- Managed Blacklisting/Whitelisting
- Schwarmintelligenz
- Vor-Ausführungs-Heuristik
- URL Filtering – Webbrowsing
- Spam- und Phishingschutz
- Manipulationsabwehr
- E-Mail-Inhaltsfilter
- Wiederherstellung und Zurücksetzung

Neuartige Sicherheitstechnologien

- EDR: ständige Überwachung der Endpunktaktivität
- Verhindert die Ausführung unbekannter Prozesse
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher Prozesse (APT, Ransomware, Rootkits usw.)
- Sandboxing in realen Umgebungen
- Verhaltensanalysen und Indicator-of-Attack(IoA)-Erkennung (Skripte, Makros usw.)
- Automatische Erkennung und Abwehr von Arbeitsspeicher-Exploits
- Threat Hunting und forensische Analyse

Abbildung 1: Zentrales Dashboard von Panda Adaptive Defense 360

Zero-Trust-Modell

AD360 agiert auf Basis eines „Zero-Trust-Modells". Der Grundgedanke dahinter besagt, dass Unternehmen niemals einer Einheit innerhalb oder außerhalb ihres Perimeters vertrauen sollten. Diese Methode wird durch den Managed Service umgesetzt, der 100 % der Prozesse klassifiziert, die Aktivitäten an den Endpoints überwacht und die Ausführung von Anwendungen und böswilligen Prozessen unterbindet. Bei jeder Ausführung wird eine Echtzeit-Klassifizierung als böswillig oder rechtmäßig, ohne Unsicherheiten und ohne Eingreifen des IT-Teams gesendet. Möglich ist dies dank der Leistung, Geschwindigkeit, Anpassungsfähigkeit und Skalierbarkeit der KI und der Cloud-Verarbeitung.

Der Service vereint **Big-Data**-Technologien und mehrstufige **Machine-Learning**-Techniken, darunter **Deep Learning** – das Ergebnis der laufenden Überwachung und Automatisierung der Erfahrungen und Kenntnisse, die das interne Sicherheitsteam von Panda erworben hat.

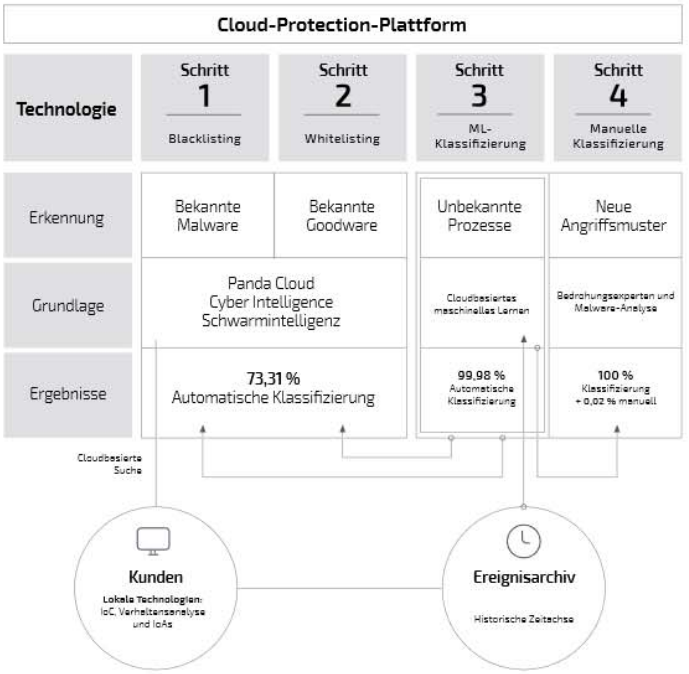

Abbildung 2: Ablauf des Managed Cloud Classification Service

Der verwaltete Service für Threat Hunting und forensische Analyse wird von einem Expertenteam ausgeführt, das anhand von Tools zur Profilerstellung – in Echtzeit und retrospektiv – und Ereigniskorrelation neue Hacking- und Ausweichtechniken/-taktiken proaktiv erkennen.

Die Threat Hunter im Panda Intelligence Center gehen bei ihrer Arbeit davon aus, dass Unternehmen ständig angegriffen werden.

AUSZEICHNUNGEN UND ZERTIFIZIERUNGEN

Panda Security steht regelmäßig auf der Liste der Teilnehmer für die Auszeichnungen von Virus Bulletin, AV-Comparatives, AV-Test und NSSLabs hinsichtlich Sicherheit und Leistung und hat bereits mehrere dieser Auszeichnungen erhalten. Panda Adaptive Defense erhielt die Zertifizierung EAL2+ in Rahmen der Prüfung für den Common Criteria Standard.