Panda Adaptive Defense 360

Automatisierte hochentwickelte Sicherheit **Schieben Sie Cyberbedrohungen einen Riegel vor**

panda
a WatchGuard brand

BETRIEBLICHE CYBERSICHERHEIT

Mobilität, Verarbeitung und Cloud-Speicher haben die Geschäftsumgebung revolutioniert. **Endpoints sind das primäre Ziel der meisten Cyberangriffe**. Daher müssen Endpoint-Sicherheitslösungen **hochentwickelt, adaptiv und automatisch** sein und höchstmögliche **Vorbeugung** und **Erkennung** bieten.

Woche für Woche erhalten Organisationen Tausende von Malware-Benachrichtigungen, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % überhaupt untersucht werden. **Ein Administrator für Cybersicherheit verbringt typischerweise zwei Drittel seiner Zeit** mit der **Bearbeitung von Malware-Warnmeldungen**.

AUSGEREIFTHEIT VON CYBERANGRIFFEN

Cyberverteidigung gegen hochentwickelte Bedrohungen

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.

Daher sind **traditionelle Schutzplattformen (EPPs) nicht ausreichend**. Der Grund dafür ist, dass sie **keine ausreichend detaillierte Sicht**. auf die Prozesse und Anwendungen bieten, die in Unternehmensnetzwerken laufen. Zudem führen einige **EDR-Lösungen** statt tatsächlichen Lösungen nur zu **höherer Belastung** und vergrößern die Arbeitslast von Sicherheits-Administratoren, **indem sie die Verantwortung für die Bearbeitung von Warnmeldungen auf die Administratoren verlagern und sie zur manuellen Klassifizierung von Bedrohungen zwingen**.

PANDA ADAPTIVE DEFENSE 360

Die EDR-Lösung - Endpoint Detection & Response

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** mannigfaltiger, fortschrittlicher Bedrohungen – von Zero-Day-Malware über Ransomware, Phishing oder In-Memory-Exploits bis hin zu dateilosen Angriffsversuchen – für optimalen Schutz, heute und morgen, innerhalb und außerhalb des Unternehmensnetzwerks.

Im Gegensatz zu anderen Lösungen **kombiniert** sie eine sehr breite Palette an **Schutztechnologien (EPP) mit automatisierten EDR-Funktionen**. Die Lösung verfügt zudem über **zwei Services, die von Panda Security-Experten** verwaltet werden und im Rahmen der Lösung bereitgestellt werden:

- **Zero-Trust Application Service**
- **Threat Hunting Service**

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

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

VORTEILE

Weniger Aufwand, geringere Sicherheitskosten

- Dank Managed Services lassen sich Kosten für Fachpersonal reduzieren. Es müssen keine Fehlalarme gehandhabt und keine Verantwortung delegiert werden.
- Die Managed Services lernen automatisch aus früheren Angriffen. Kein Zeitaufwand für manuelle Einstellungen.
- Maximaler Schutz am Endpoint. Nahezu keine Betriebskosten.
- Installation, Konfiguration und Pflege einer Managementinfrastruktur sind nicht erforderlich.
- Dank ressourcensparendem Agent und Cloud-Architektur wird die Leistungsfähigkeit der Endpoints 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, dateilosen Angriffen 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 gründlichen Untersuchung jedes Angriffsversuchs sowie Tools zur Verringerung der Auswirkungen (Desinfektion).
- Verfolgung jeder Aktion; Sichtbarkeit des Angreifers und seiner Aktivitäten, was die forensische Untersuchung erleichtert.
- Verbesserung und Anpassung von Sicherheitsrichtlinien aufgrund der Erkenntnisse aus der forensischen Analyse.

panda
a WatchGuard brand

ERWEITERTE UND AUTOMATISIERTE ENDPOINT-SICHERHEIT

Traditionelle, auf Vorbeugung ausgerichtete Schutztechnologien (EPPs) sind kostengünstige Maßnahmen gegen bekannte Bedrohungen und böswillige Verhaltensweisen, reichen jedoch alleine nicht aus. Zur erfolgreichen Verteidigung einer Organisation und Bekämpfung von Cyberbedrohungen ist eine Abkehr von der traditionellen Prävention hin zur kontinuierlichen Vorbeugung, Erkennung und Reaktion nötig. Dabei wird stets davon ausgegangen, dass der Organisation bereits Schaden zugefügt wurde und alle Endpoints jederzeit von Angreifern bedroht sind.

Panda Adaptive Defense 360 integriert in einer Lösung traditionelle Präventionsverfahren mit innovativen, adaptiven Technologien zur Vorbeugung, Erkennung und Abwehr hochentwickelter, sowohl aktueller als auch zukünftiger Cyberbedrohungen:

Traditionelle Präventionsmethoden

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

Hochentwickelte Sicherheitstechnologien

- EDR: Ständige Überwachung der Endpoint-Aktivität
- 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 gezielten Angriffen und Arbeitsspeicher-Exploits
- Threat Hunting und forensische Analyse

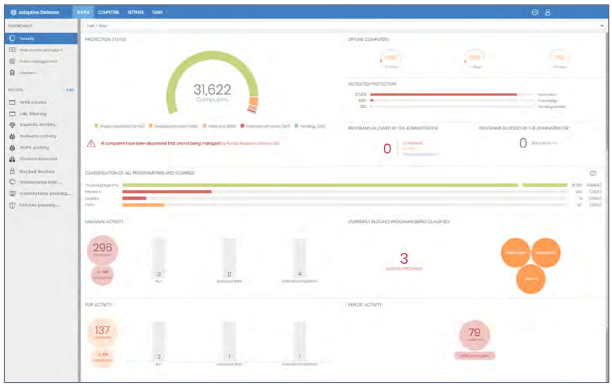

Abbildung 1: Panda Adaptive Defense Haupt-Dashboard.

ZERO-TRUST-MODELL

Dies ist der Managed Service, 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 Delegieren an den Client 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 Sicherheits- und Bedrohungsteam von Panda Security erworben hat.

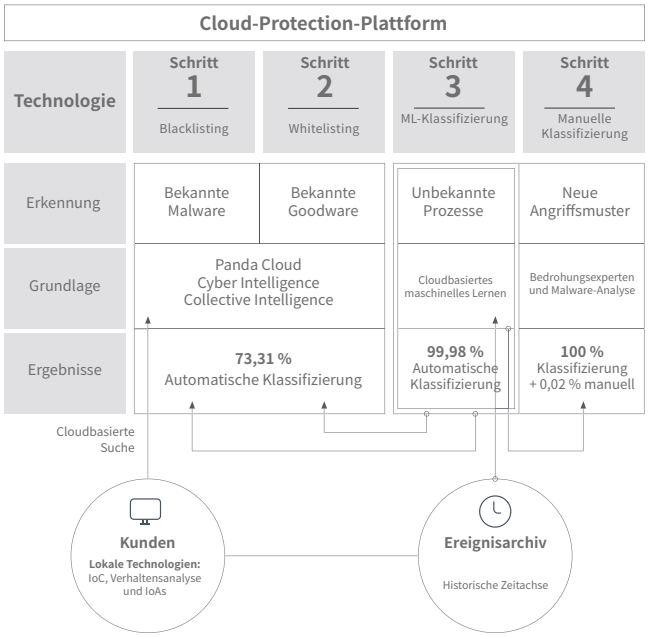

Abbildung 2: Ablauf des Managed Cloud Classification Service.

Der Managed Service für Threat Hunting und forensische Analyse wird von einem Expertenteam ausgeführt, das anhand von Tools zur Profilerstellung und Ereigniskorrelation neue Hacking- und Ausweichtechniken proaktiv erkennen.

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

Unterstützte Plattformen und Systemanforderungen von PANDA ADAPTIVE DEFENSE 360

Kompatible Betriebssysteme: Windows (Intel & ARM), macOS, Linux, und 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.

WatchGuard

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