Datengestützte Analysen als Schlüssel zum Schutz vor Sicherheitsver-letzungen

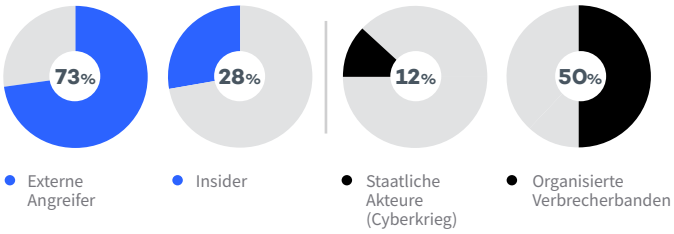
PANDA ADAPTIVE DEFENSE 360

Panda Adaptive Defense 360 vereint traditionelle Antivirustechnologie und das fortschrittliche Modell der Endpoint Detection and Response (EDR) in einer einzigen Lösung zur Abwehr bekannter und unbekannter Bedrohungen.

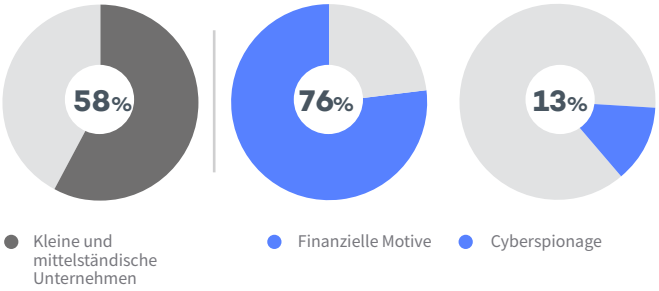
panda
a WatchGuard brand

DIE BEDROHUNGSLANDSCHAFT

Woher kommen die Angriffe?[1]



Wer sind die Opfer? Was sind die Beweggründe?[1]



Welche Kosten entstehen den Unternehmen?

- **Kosten weltweit:** 600.000 Mio. USD[2]
- **Kosten einer Datensicherheitsverletzung:** 3,86 Mio. USD[3]

DIE EVOLUTION VOM HACKERN

Hacker werden immer raffinierter und immer zahlreicher. Dies ist das Ergebnis ihrer Professionalisierung, der gemeinsamen Nutzung von Technologien und der ständigen Cyberintelligence-Lücken.

ELIMINIERUNG DER ANGRIFFSFLÄCHE

Die von den Hackern ausgehenden Cyberbedrohungen der nächsten Generation sind so konzipiert, dass sie **herkömmliche Lösungen** völlig unbemerkt umgehen und Netzwerke überall anfällig machen, ohne dass geeignete Abwehrmechanismen vorhanden sind.

Traditionelle Schutzplattformen sind 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 Lösungen für Endpoint Detection and Response (EDR). EDR-Funktionen umfassen die kontinuierliche Überwachung und Datenanalyse von Netzwerkaktivitäten. So verfügen IT-Abteilungen über die Daten und Erkennungsmöglichkeiten, die sie zur Bekämpfung hoch entwickelter Bedrohungen benötigen.

BEWÄLTIGUNG DER IT-ARBEITSLAST

Da die Zahl der Computer innerhalb der Unternehmensinfrastruktur jährlich zunimmt, ist es für Sicherheitsteams problematisch, Geräte innerhalb und außerhalb des Netzwerks zu verwalten und vor Angriffen zu schützen. Hinzu kommt, dass EDR-Lösungen zwar ein wichtiger Baustein beim Schutz vor komplexen Bedrohungen sind, jedoch in den meisten Fällen das Management der IT-Umgebung zusätzlich erschweren. Zurückzuführen ist dies vor allem auf die unzureichende Automatisierung von Plattformmanagements, da das Team die erzeugten Warnmeldungen verwalten und Bedrohungen manuell klassifizieren muss.

LÖSUNGEN FÜR ENDPOINT DETECTION AND RESPONSE (EDR)

Was leisten EDR-Lösungen hauptsächlich?

EDR-Lösungen überwachen, protokollieren und speichern die Details der Endpoint-Aktivitäten, beispielsweise Anwenderereignisse, Prozesse, Änderungen am Registrierungsschlüssel, Speicher- und Netzwerknutzung. Durch diese Visualisierung werden Bedrohungen aufgedeckt, die andernfalls unbemerkt bleiben würden.

Welche versteckten Probleme gibt es bei EDR-Lösungen?

Zur Suche nach sicherheitsrelevanten Auffälligkeiten bei Ereignissen und zur Bestätigung oder Zurückweisung von Warnmeldungen werden mehrere Techniken und Tools eingesetzt. Dies geht nicht ohne manuellen Eingriff.

EDR-Lösungen erfordern eine permanente Überwachung und schnelle Reaktionen durch hoch qualifiziertes Personal.

Diese Ressourcen sind kostspielig und schwer zu finden. Organisationen mit dünner Personaldecke und geringem Budget sind nicht darauf vorbereitet, die Vorzüge von EDR-Lösungen ohne Hilfe von außen zu nutzen. Die Mitarbeiter werden durch die Implementierung und Ausführung dieser Lösungen stärker belastet, statt bei ihrer wichtigsten Aufgabe unterstützt zu werden: den Sicherheitsstatus ihrer Organisation zu verbessern.

Wie lautet die Antwort auf dieses Problem?

Adaptive Defense 360 von Panda.

[1] „2018 Data Breach Investigation Report“ (Bericht zu Datensicherheitsverletzungen 2018). Verizon
[2] „2018 Economic Impact of Cybercrime – No Slowing Down“ (Wirtschaftliche Auswirkungen von Cyberkriminalität 2018 – Keine Verlangsamung). CSIC/McAfee
[3] „2018 Cost of a Data Breach Study: Global Overview“ (Studie zu den Kosten einer Datensicherheitsverletzung: weltweiter Überblick). Ponemon Institute/IBM Security

PANDA ADAPTIVE DEFENSE 360

Panda Adaptive Defense 360 ist eine innovative Cybersicherheitslösung für Desktop-Geräte, Laptops und Server, die über die Cloud bereitgestellt wird. Sie automatisiert die Prävention, Erkennung, Eindämmung und Abwehr aller aktuellen oder zukünftigen Arten von Bedrohungen, darunter hoch entwickelte Angriffe, Zero-Day-Malware, Ransomware, Phishing, Speicher-Exploits und Angriffe ohne Malware innerhalb und außerhalb des Firmennetzwerks.

Dank der Cloudarchitektur ist der Agent ressourcensparend und hat keinerlei Auswirkungen auf die Leistungsfähigkeit der Endpoints, die über eine zentrale Cloudkonsole verwaltet werden, selbst wenn sie nicht mit dem Internet verbunden sind.

Panda Adaptive Defense 360 beinhaltet Cloud-Protection- und Cloud-Management-Plattformen (Aether). Diese optimieren die Prävention, Erkennung und automatische Reaktion und verringern so den Arbeitsaufwand.

Sie unterscheidet sich von anderen Lösungen, da sie eine breite Palette an Endpoint-Schutztechnologien (EPP) und automatisierten EDR-Funktionen bietet. Ermöglicht wird dies durch ein in die Lösung eingebundenes Serviceangebot, das von Panda Security-Experten verwaltet wird: Zero-Trust Application Service. Dadurch werden die Verwaltung von Warnmeldungen und die damit verbundene Entscheidungsfindung automatisiert.

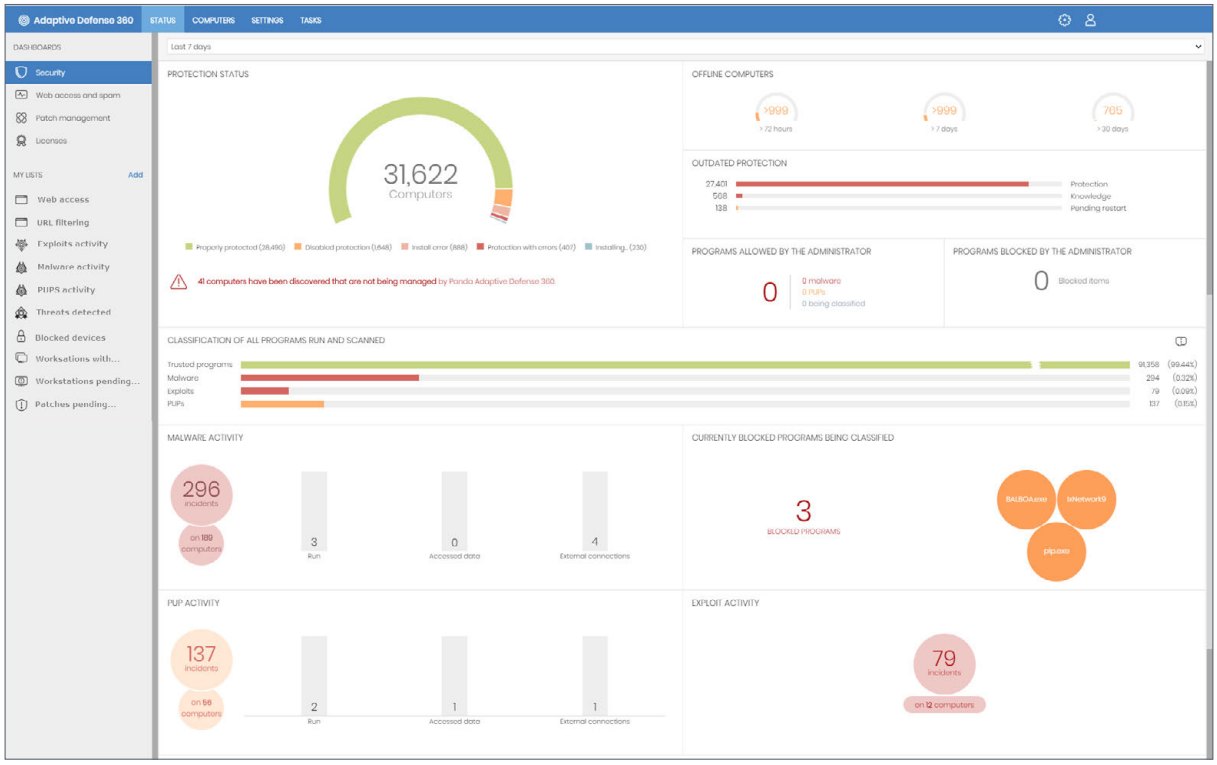


Abbildung 1: Zentrales Dashboard von Panda Adaptive Defense 360

VORTEILE PANDA ADAPTIVE DEFENSE 360

Weniger Aufwand und geringere Kosten für eine hoch entwickelte, anpassungsfähige Sicherheitslösung

- Dank Managed Services lassen sich Kosten für Fachpersonal einsparen, da das Untersuchen von Fehlalarmen und das Treffen entsprechender Entscheidungen wegfallen.
- Die Managed Services lernen automatisch aus früheren Angriffen, sodass keine Zeit mit manueller Konfiguration verschwendet wird.
- Durch bestmögliche Prävention an den Endpoints werden die Betriebskosten praktisch auf null gesenkt.
- Keine Installation, Konfiguration oder Pflege einer Managementinfrastruktur erforderlich
- Dank ressourcensparendem Agent und Cloudarchitektur wird die Leistungsfähigkeit der Endpoints nicht beeinträchtigt.

Verkürzung der Erkennungs- und Expositionszeit (Dwell Time) dank Automatisierung

- Verhinderung der Ausführung von Bedrohungen, Zero-Day-Malware, Ransomware und Phishing-Versuchen
- Erkennung und Blockierung bösartiger Aktivitäten im Arbeitsspeicher (Exploits), bevor diese Schaden anrichten können
- Erkennt bösartige Prozesse, die Ihre Schutzmechanismen umgehen
- Erkennt und blockiert Hackermethoden und -angriffe

Automatisierung und Verkürzung von Reaktions- und Untersuchungsmaßnahmen

- Automatische und transparente Wiederherstellung
- Wiederherstellung der Endpunktaktivität – sofortige Rückkehr zum Normalzustand
- Schnellere forensische Untersuchung durch praxisorientierte Einblicke in die Angreifer und deren Vorgehensweise
- Verringerung der Angriffsfläche, dadurch Verbesserung und Weiterentwicklung Ihrer Sicherheitsvorkehrungen

ENTLASTUNG DER IT: ZERO-TRUST APPLICATION SERVICE

Mit dem **Zero-Trust Application Service** wird die Ausführung bösartiger Anwendungen und Prozesse auf Endpoints überwacht und verhindert. Für jede Ausführung wird automatisch eine Echtzeit-Klassifizierung von bösartigen oder rechtmäßigen Anwendungen und Prozessen ausgegeben. Menschliches Eingreifen ist somit nicht mehr erforderlich. Möglich ist dies dank der Geschwindigkeit, Kapazität, Flexibilität und Skalierbarkeit der KI und der Cloud-Verarbeitung.

Der Dienst führt Big Data und maschinelles Lernen, einschließlich Deep Learning, auf mehreren Ebenen zusammen. Dabei stützt sich die Klassifizierung auf die laufende Überwachung und Automatisierung der Erfahrung, der Einblicke und des gesammelten Wissens der Sicherheits- und Bedrohungsexperten im Intelligence Center von Panda Security.

Wie sonst keine Lösung auf dem Markt kann der Zero-Trust Application Service IT-Abteilungen vor dem Risiko schützen, dass Malware auf Endpoints innerhalb und außerhalb des Firmennetzwerks ausgeführt wird.

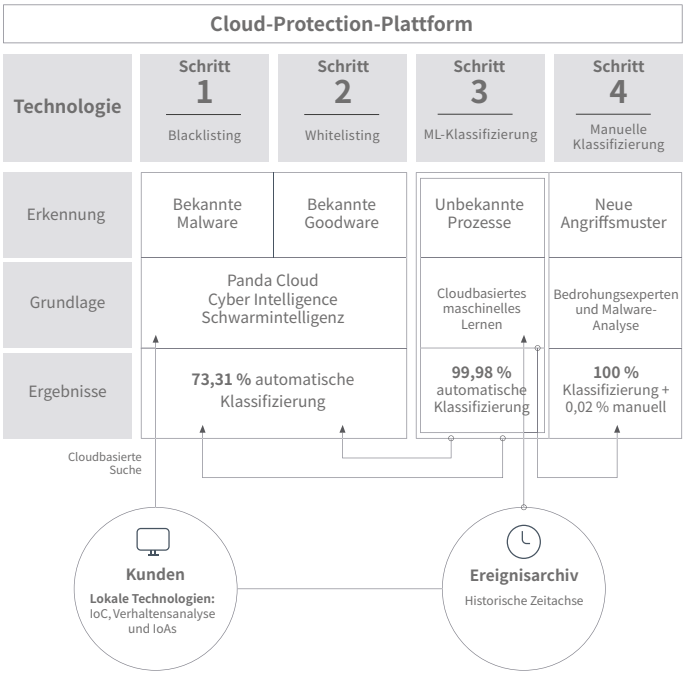


Abbildung 2: Ablauf des Managed Cloud Zero-Trust Application Service

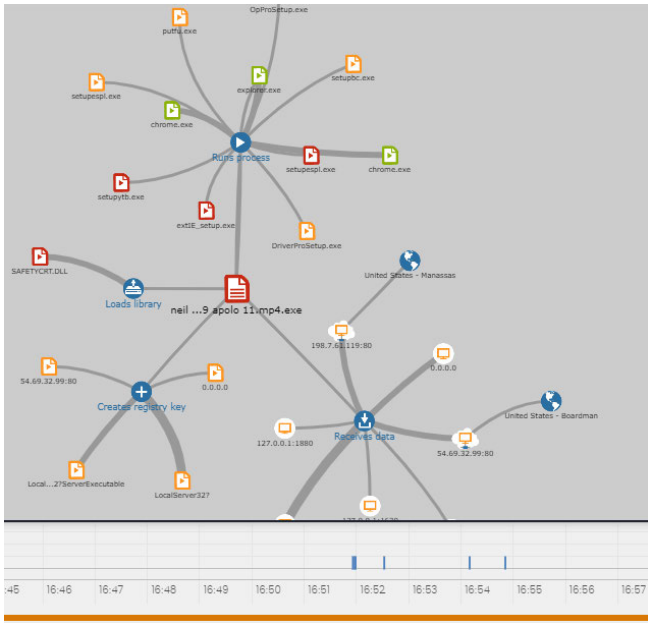


Abbildung 3: Die in Panda Adaptive Defense 360 integrierte Zeitleiste unterstützt forensische Untersuchungen: Wann wurde ein Zwischenfall erstmalig im Netzwerk erkannt? Welche und wie viele Endpoints waren davon betroffen? Welche Einstellungen wurden geändert und wem wurde dies mitgeteilt?

HOCH ENTWICKELTE AUTOMATISIERTE SICHERHEIT AUF ENDPOINTS

Panda Adaptive Defense 360 integriert in einer einzigen Lösung traditionelle Präventionsverfahren mit innovativen Technologien zur Vorbeugung, Erkennung und automatischen Abwehr ausgefeilter Internetangriffe.

Traditionelle Präventionsmethoden

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

Neuartige Sicherheitstechnologien

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

CLOUD–MANAGEMENT-PLATTFORM: AETHER

Sicherheit, Transparenz und Kontrolle der nächsten Generation Umfassend und skalierbar aus der Cloud – ein Mehrwert mit sofortiger Wirkung

Die Plattform Aether und deren Cloud-Konsole optimieren die Verwaltung der umfassenden und anpassungsfähigen Sicherheitslösung innerhalb und außerhalb des Netzwerks.

Sie wurden speziell entwickelt, damit sich die Sicherheitsverantwortlichen ganz auf die Sicherheitslage Ihres Unternehmens konzentrieren können. Sie ist unkompliziert und trotzdem absolut flexibel, detailgenau und skalierbar.

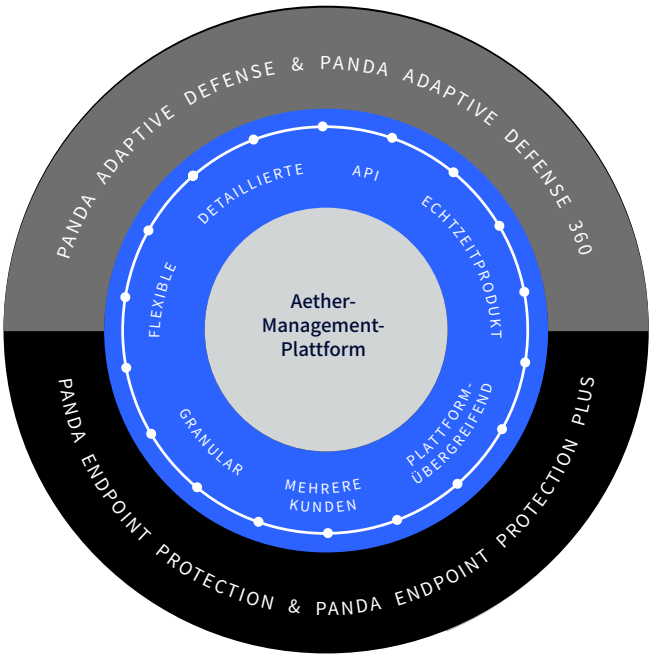


Abbildung 3: Einheitliche Cloud-Management-Plattform: Aether

VORTEILE VON AETHER

Erzeugt Wertvorteile in kürzester Zeit. Unkomplizierte Implementierung und sofortige Transparenz

- Bereitstellung, Installation und Konfiguration innerhalb weniger Minuten – Wertvorteil ab dem ersten Tag
- Ressourcensparender, produkt- und modulübergreifender Agent, der plattformübergreifend (Windows, Mac, Linux, Android) einsetzbar ist
- Automatische Erkennung ungeschützter Endpoints, Remote-Installation
- Speziell entwickelte Proxy-Technologie auch für Computer ohne Internetanschluss
- Traffic-Optimierung dank proprietärer Repository-/Cache-Technologie

Anpassungsfähig und einfach in der Anwendung

- Intuitive cloudbasierte Konsole für flexible und modulare Verwaltung
- Voreingestellte und personalisierbare Rollen
- Genaue Kontrolle der Konsolenaktivität
- Anwender mit vollständigen oder eingeschränkten Zugriffs- und Ansichtsberechtigungen
- Gruppen- und Endpoint-spezifische Sicherheitsvorschriften
- Hardware- und Software-Bestandsführung und Änderungsprotokoll

Schnellere Reaktion dank unkomplizierter Überwachung

- Priorisierte Darstellung von Schlüsselkennzahlen und Dashboards
- Priorisierte und bestätigte Warnungen zu Ihrem Workflow
- Vollständige und praxisorientierte Vorfallhistorie: Beteiligte Prozesse, Ursprung, Dauer, Verbreitung usw.
- Auslösen von Endpoint-Maßnahmen mit nur einem Klick: neustarten, isolieren, patchen, scannen und so die Reaktionszeit verkürzen

PREISE UND AUSZEICHNUNGEN

WatchGuard und Panda haben sich verpflichtet, ihre Lösungen konsequent unabhängigen Tests und Prüfungen durch Dritte zu unterziehen. Wir sind stolz auf die Anerkennung, die wir von führenden Testlaboren wie Virus Bulletin, AV-Comparatives, AV-Test und NSS Labs erhalten.

AV-Comparatives empfiehlt Adaptive Defense 360, da „diese Lösung alle ausgeführten Prozesse klassifiziert und daher sämtliche Malware erfasst“.

Unterstützte Plattformen und Systemanforderungen von Panda Adaptive Defense 360

Die unterstützten Plattformen entwickeln sich kontinuierlich weiter, um so weit wie möglich die Anforderungen der neuesten Betriebssysteme zu erfüllen. Über die folgenden Links können Sie auf den Online-Support für unsere Produkte zugreifen:

Windows-Server und -Workstations: http://go.pandasecurity.com/endpoint-windows/requirements
MacOS-Geräte: http://go.pandasecurity.com/endpoint-macos/requirements
Linux-Server und -Workstations: http://go.pandasecurity.com/endpoint-linux/requirements
Android-Mobilgeräte: http://go.pandasecurity.com/endpoint-android/requirements
Panda Patch Management: http://go.pandasecurity.com/patch-management/requirements
Panda Cloud Systems Management: http://go.pandasecurity.com/systems-management/requirements
SIEM Feeder: http://go.pandasecurity.com/siem-feeder/requirements
Advanced Reporting Tool: http://go.pandasecurity.com/reporting-tool/requirements
Panda Full Encryption: http://go.pandasecurity.com/full-encryption/requirements

WatchGuard

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