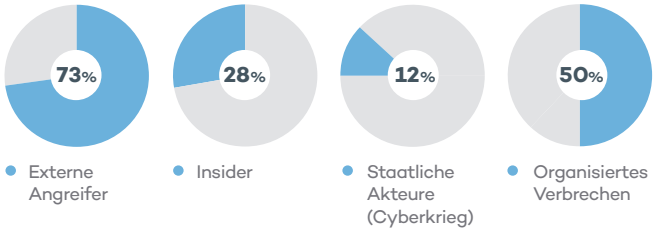
Panda Adaptive Defense 360

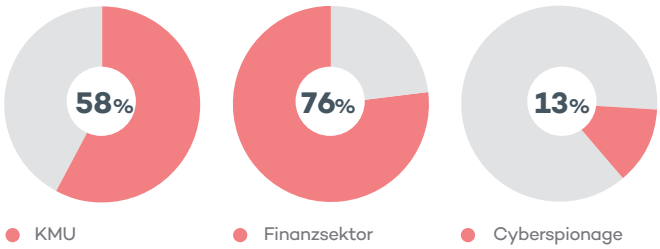
Automatisierte und zentralisierte *Advanced Security*
Schieben Sie Cyber-Bedrohungen einen Riegel vor

CYBERSICHERHEIT FÜR UNTERNEHMEN

Wer steckt hinter der Bedrohung aus dem Internet?[1]



Wer sind die Opfer? Wie lauten die Motive?[1]



Endpoints sind die neue Frontlinie

Mobilität, Datenverarbeitung und Cloud-Speicher haben Unternehmensumgebungen grundlegend verändert. **Endpoints sind die neue Frontlinie**. Sicherheitslösungen für Endpoints müssen **hochentwickelt, anpassungsfähig und automatisiert** sein um eine optimale Angriffsvorbeugung und -erkennung zu ermöglichen. Denn Hacker schaffen es früher oder später immer, die Schutzmechanismen zu umgehen. Entsprechende Lösungen müssen außerdem flexible Tools enthalten, die eine schnelle Reaktion ermöglichen, Schäden eingrenzen und die Angriffsfläche verringern.

Hacker werden immer professioneller

Angreifer werden immer professioneller und ihre Zahl wächst. Dies ist eine Folge der zunehmenden Professionalisierung, einfachen Verfügbarkeit von Exploit Kits und häufigen Datenlecks im Bereich Cybersicherheit.

Cyberbedrohungen der nächsten Generation werden speziell entwickelt, um herkömmliche Lösungen vollkommen unerkannt zu umgehen.

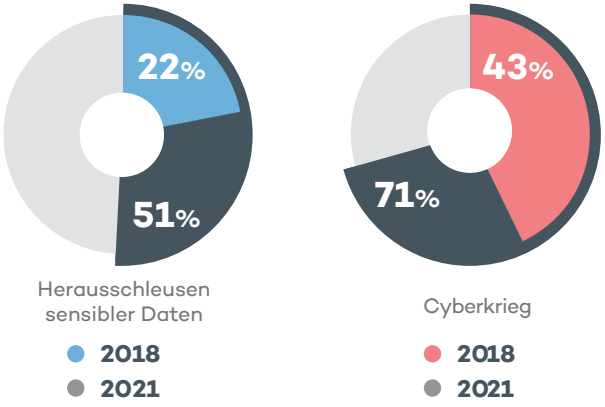
Cyberabwehr für Unternehmen

Hacker haben es ganz besonders auf Computer und Server abgesehen, auf denen sich die wertvollsten Unternehmensdaten befinden. Sicherheitsabteilungen tun sich schwer darin, ihre Angriffe abzuwehren. Auch EDR-Anwendungen (Endpoint Detection and Response) sind alleine keine perfekte Lösung: Sie erhöhen den Arbeitsaufwand und sind daher Personalintensiv. Wer die Sicherheit seines Unternehmens erhöhen will, ohne zugleich die Betriebskosten zu steigern, muss also die Endpoint-Sicherheit automatisieren.

Welche Kosten entstehen den Unternehmen durch Sicherheitsverletzungen?

- **Kosten weltweit:** 600 Mrd. USD[3]
- **Kosten je Sicherheitsverletzung:** 3,86 Mio. USD[4]

Unternehmen und ihre Risikowahrnehmung[4].



In 60 % der Fälle führen Angriffe durch staatliche Akteure zu einem **Cyberkrieg**.

LÖSUNGEN FÜR ENDPOINT DETECTION AND RESPONSE (EDR)

EDR-Lösungen überwachen, protokollieren und speichern die Details der Endpoint-Aktivitäten, wie Benutzerereignisse, Prozesse, Änderungen an der Registrierung, Speicher und Netzwerknutzung. So werden Bedrohungen sichtbar, die ansonsten unbemerkt bleiben würden.

Welche versteckten Probleme lauern in EDR-Lösungen?

Für die Suche nach ereignisbezogenen Sicherheitsanomalien und deren Auslösern bzw. Zurückweisung von Warnhinweisen werden unterschiedliche Verfahren und Tools eingesetzt. Diese erfordern grundsätzlich ein menschliches Eingreifen. EDR-Lösungen müssen rund um die Uhr durch hochqualifiziertes Personal überwacht werden, um jederzeit umgehend reagieren zu können.

Entsprechende Personalressourcen sind allerdings teuer und schwer zu finden. Unterbesetzte Unternehmen mit kleinen Budgets können die Vorteile von EDR-Lösungen also kaum nutzen. Ihre IT-Mitarbeiter sind mit der Implementierung und dem Betrieb entsprechender Lösungen überlastet, anstatt bei der wirklich wichtigen Aufgabe unterstützt zu werden: die Sicherheitslage ihres Unternehmens zu verbessern.

1 2018 Data Breach Investigation Report, Verizon.
2 2018 Economic Impact of Cybercrime — No Slowing Down, CSIC/McAfee.
3 2018 Cost of Data Breach Study: Global Overview, Ponemon Institute/IBM Security.
4 2018 Study on Global Megatrends in Cybersecurity, Ponemon Institute.

Panda Adaptive Defense 360

Panda Adaptive Defense 360 ist eine innovative Sicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Sie **automatisiert die Vorbeugung, Erkennung, Eindämmung und Abwehr** von Angriffen, Zero-Day-Malware, Erpressungssoftware, Phishing, Memory-Exploits und Angriffsversuchen mit und ohne Malware innerhalb sowie außerhalb des Firmennetzwerks.

Sie unterscheidet sich von anderen Lösungen, da sie eine breite Palette an **Schutztechnologien (EPP) und automatisierten EDR-Funktionen bietet**. Ermöglicht wird dies durch zwei in die Lösung eingebundene Serviceangebote **der Panda-Sicherheitsexperten**:

- **100 % Klassifizierung aller Prozesse**
- **Threat Hunting Investigation Service (THIS)**

Dank der Cloud-Architektur ist der **Agent platzsparend** und hat keinerlei Auswirkungen auf die Leistungsfähigkeit der Endpoints, die über eine **einzige Cloud-Konsole** verwaltet werden, selbst wenn sie nicht mit dem Internet verbunden sind.

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

AIRBUS

„Weitsicht ist unser wichtigster Verbündeter, wenn es um die Bestimmung unserer künftigen Anforderungen und die Risikoprävention geht. Adaptive Defense 360 verschafft uns die Transparenz, die wir dafür benötigen."

Jean-Yves Andreoletti

Systems and Networks Integration, Validation and Maintenance Platform Engineer

Panda Adaptive Defense 360
VORTEILE

Weniger Aufwand und geringere Kosten für eine hochentwickelte, anpassungsfähige Sicherheitslösung

- Dank Managed Services sparen Sie Kosten für Fachpersonal. Keine Fehlalarme, keine Weitergabe von Zuständigkeiten.
- Managed Services lernen automatisch aus früheren Angriffen. Keine Zeitverschwendung durch manuelle Konfiguration.
- Bestmögliche Prävention an den Endpoints. Betriebskosten werden praktisch auf Null gesenkt.
- Keine Installation, Konfiguration und Pflege einer Management-Infrastruktur erforderlich.
- Dank ressourcensparendem Agent und Cloud-Architektur keine Einschränkung der Leistungsfähigkeit Ihrer Endpoints.

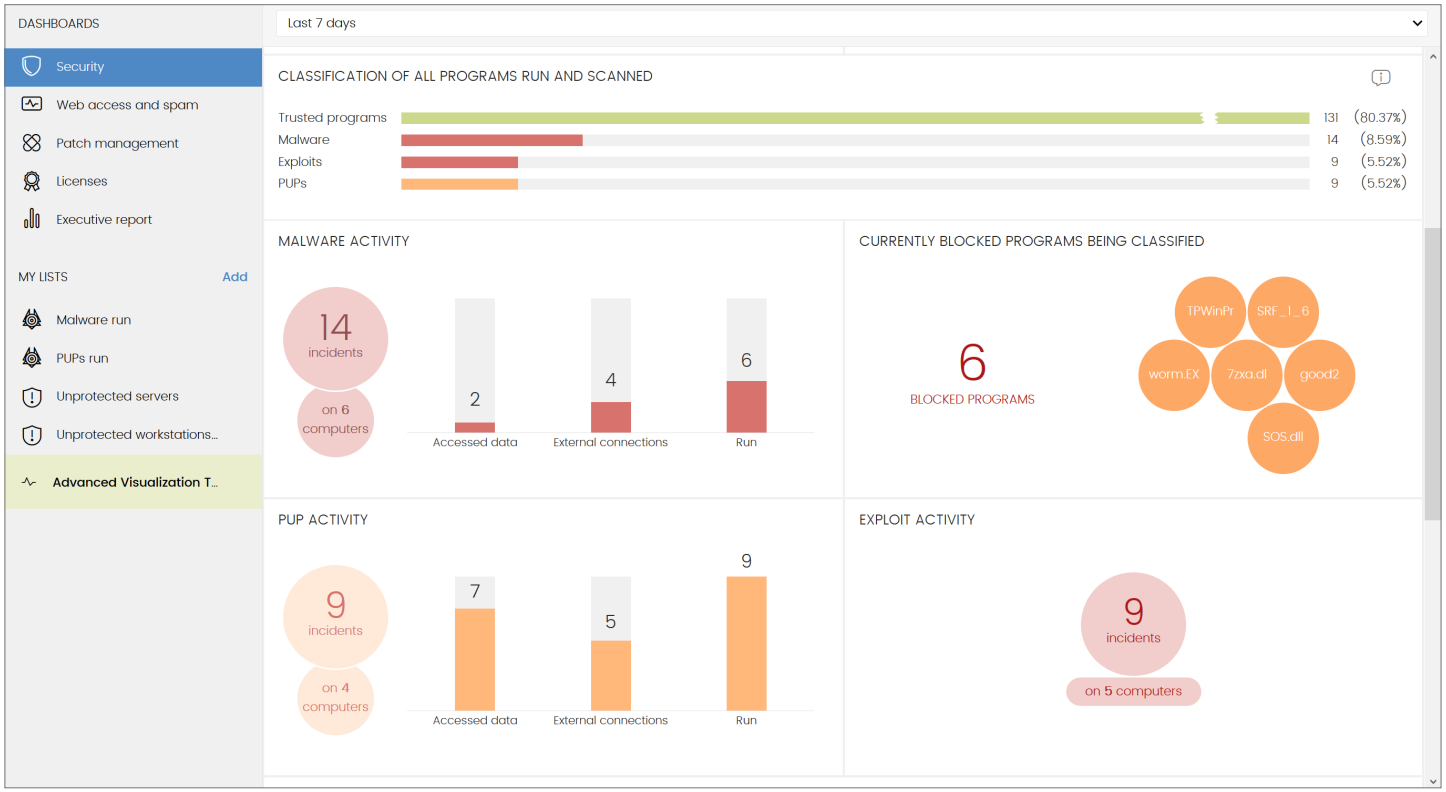
Verkürzung der Erkennungs- und Expositionszeit (Dwell Time) dank Automatisierung

- Verhindert die Ausführung von Angriffen, Zero-Day-Malware, Erpressungssoftware 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 blockiert Hackermethoden und -angriffe

Automatisierung und Verkürzung von Reaktions- und Untersuchungsmaßnahmen

- Automatische und transparente Wiederherstellung.
- Wiederherstellung der Endpoint-Aktivität – sofortige Rückkehr zum Normalzustand.
- Praxisorientierte Einblicke in die Angreifer und deren Vorgehensweise beschleunigen die forensische Untersuchung.
- Verringerung der Angriffsfläche. Unterstützt die Verbesserung und Weiterentwicklung Ihrer Sicherheitsvorkehrungen.

Abbildung 1: Ein Dashboard ermöglicht einen vollständigen Überblick, eine einheitliche Verwaltung und priorisiert erkannte Bedrohungen



Cloud Protection Platform

Hochentwickelte, anpassungsfähige Sicherheit dank Mensch und Maschine

Der 100% Attestation Service überwacht und verhindert die Ausführung bösartiger Anwendungen und Prozesse an den Endpoints. Bei jedem Ausführungsversuch wird in Echtzeit **unmissverständlich entschieden, ob es sich um eine bösartige oder legitime Aktivität handelt**. Der Client wird dabei nicht in Anspruch genommen. Das alles wird dank der Geschwindigkeit, Kapazität, Flexibilität und Skalierbarkeit von KI und Cloud-Processing möglich.

Das Angebot kombiniert **Big Data** und mehrstufiges **maschinelles Lernen** einschließlich **Deep Learning**, die das Panda Security Intelligence Center dank **seiner Erfahrung und seines gebündelten Expertenwissens** zu den Themen Sicherheit und Bedrohungslagen entwickeln konnte.

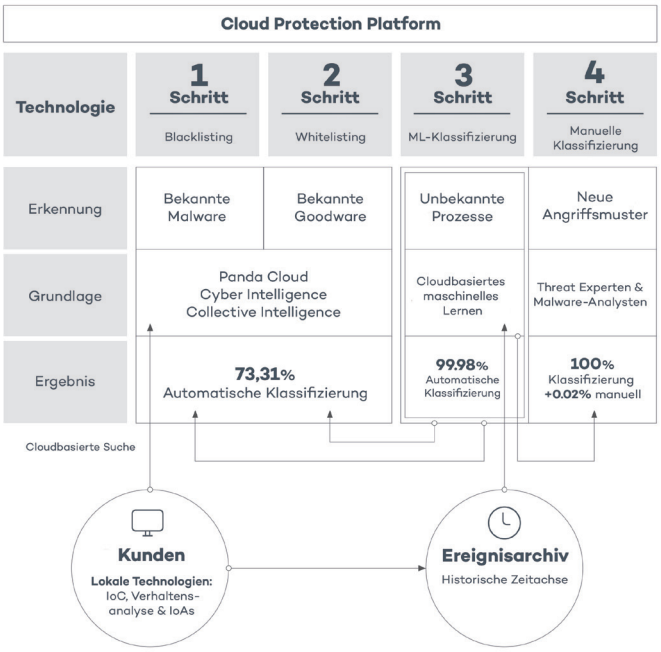


Abbildung 2: Ablauf des Managed Cloud Classification Service

Der Managed Threat Hunting and Investigation Service wird von unseren „Threat Hunters" betrieben und nutzt unterschiedlichste Tools zur Profilerstellung, Auswertung und Ereigniskorrelation, die sowohl in Echtzeit als auch rückblickend eingesetzt werden. Ziel ist es, aktiv neuartige Hacker- und Verschleierungstechniken zu erkennen.

Die Threat Hunter gehen davon aus, dass Unternehmen ständigen Bedrohungen ausgesetzt sind.

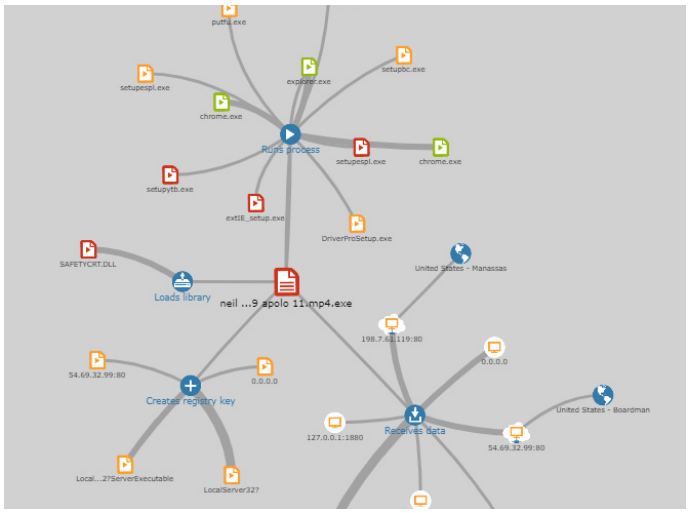


Abbildung 3: Die in Panda Adaptive Defense 360 integrierte Zeitleiste unterstützt forensische Untersuchungen: Wann wurde ein Zwischenfall erstmalig im Netzwerk erkannt? Welche und wie viele Endpoints waren davon betroffen? Welche Einstellungen wurden geändert und wem wurde dies mitgeteilt?

Cloud Protection Platform: Aether

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

Die Aether Platform und ihre Cloud-Konsole, die in allen Endpoint-Lösungen von Panda Security enthalten sind, optimieren die Verwaltung der umfassenden und anpassungsfähigen Sicherheitslösung innerhalb und außerhalb des Netzwerks.

Sie wurden speziell entwickelt, um es den Sicherheitsverantwortlichen zu ermöglichen, sich ganz auf die Sicherheitslage Ihres Unternehmens zu konzentrieren. Sie ist unkompliziert und trotzdem absolut flexibel, detailgenau und skalierbar.

VORTEILE VON AETHER IN Panda Adaptive Defense 360

Erzeugt Wertvorteile in kürzester Zeit. Unkomplizierte Implementierung und sofortige Transparenz

- Bereitstellung, Installation und Konfiguration innerhalb weniger Minuten. Wertvorteil ab dem ersten Tag.
- Platzsparender, produkt- und modulübergreifender Panda Agent. Plattformübergreifend (Windows, Mac, Linux, Android).
- 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 Web-Konsole. Flexible und modulare Verwaltung.
- Voreingestellte und personalisierbare Rollen.
- Genaue Kontrolle der Konsolenaktivität.
- Benutzer mit vollständigen oder eingeschränkten Zugriffs- und Ansichtsberechtigungen.
- Gruppen- und Endpoint-Sezifische Sicherheitsvorschriften.
- Hardware- und Software-Bestandsführung und Änderungsprotokolle.

Unkomplizierte Überwachung. Zügige Reaktion

- Priorisierte Darstellung von Schlüsselkennzahlen und Dashboards.
- Priorisierte und bestätigte Warnungen zu Ihrem Workflow.
- Vollständige und praxisorientierte Vorfallhistorie: Beteiligte Prozesse, Ursprung, Dauer, Verbreitung etc.
- Endpoint-Maßnahmen mit nur einem Mausklick auslösen: neustarten, isolieren, patchen, scannen und so die Reaktionsmaßnahmen beschleunigen.

Abbildung 4: Einheitliche Cloud Management Platform: Aether

Panda Adaptive Defense 360

HOCHENTWICKELTE, AUTOMATISIERTE ENDPOINT-SICHERHEIT

Herkömmliche Sicherheitstechnologien (EPP), die ganz auf Prävention setzen, sind zwar kostengünstig und für bekannte Bedrohungen und bösartige Verhaltensweisen ausreichend, insgesamt jedoch ungenügend. Wenn Sie Ihr Unternehmen wirklich schützen und Cyberangriffen sowohl jetzt und auch in Zukunft einen Riegel vorschieben wollen, müssen Sie sich nicht nur um Prävention, sondern zusätzlich auch um die Erkennung und stetige Abwehr kümmern. Sie sollten davon ausgehen, dass Ihr Unternehmen einer ständigen Bedrohung ausgesetzt ist und Ihre Endpoints kontinuierlich von Hackern angegriffen werden.

Panda Adaptive Defense 360 kombiniert traditionelle Präventionsverfahren mit innovativen Technologien zur Vorbeugung, Erkennung und automatischen Abwehr ausgefeilter Internetangriffe.

Traditionelle Präventionsmethoden

- Persönliche und verwaltete Firewalls. 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.

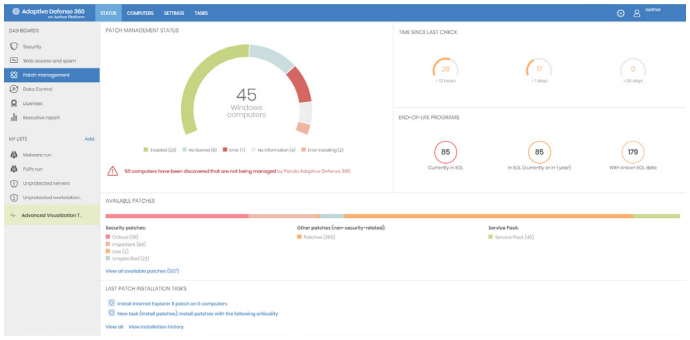
Neuartige Sicherheitstechnologien

- EDR: ständige Überwachung der Endpointaktivität.
- Verhindert die Ausführung unbekannter Prozesse.
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher unbekannter Prozesse (APT, Erpressungssoftware, Rootkits, etc.).
- Cloudbasiertes Sandboxing in realen Umgebungen.
- Verhaltensanalysen und Indicator-of-Attack-Erkennung (Skripte, Makros etc.).
- Automatische Erkennung und Abwehr von Arbeitsspeicher-Exploits.
- Managed Threat Hunting bei Angriffen ohne Malware.

ZUSATZMODULE

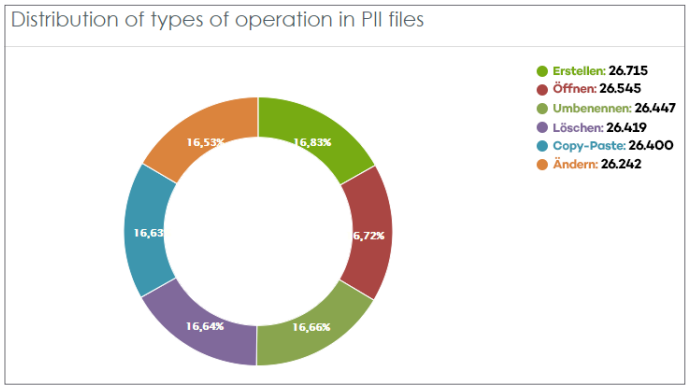
Panda Patch Management

Panda Patch Management ist eine intuitive Verwaltungslösung für Schwachstellen in Betriebssystemen und Drittanbieteranwendungen auf Windows-Endpoints und -Servern. Ergebnis ist eine Verringerung der Angriffsfläche, die Stärkung der Präventionsfähigkeiten und die Eindämmung von Zwischenfällen.



Panda Data Control

Panda Data Control ermittelt, prüft und überwacht unstrukturierte sensible und personenbezogene Daten auf Endpoints: von ruhenden Daten über verwendete Daten bis hin zu in Übertragung befindlichen Daten.



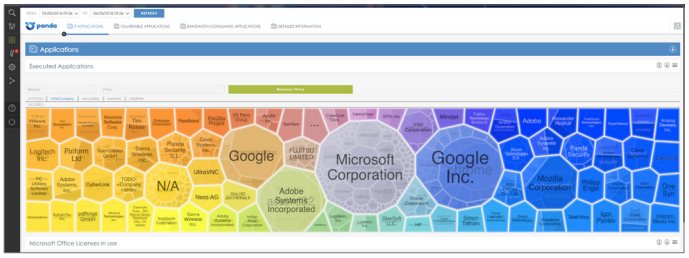
AV-Comparatives empfiehlt Adaptive Defense 360, da „diese Lösung alle ausgeführten Prozesse klassifiziert und daher sämtliche Malware erfasst."

Panda Adaptive Defense 360
Single Product test
Panda Adaptive Defense 360
AV comparatives

Panda Advanced Reporting Tool

Die Erfassungsplattform automatisiert den Abgleich von Daten, die durch die Ausführung von Prozessen und Anwendungen an geschützten Endpoints und deren Netzwerken erzeugt werden. Die Daten werden dann von Panda Adaptive Defense 360 erfasst und in der Cloud Protection Platform angereichert.

Panda Advanced Reporting Tool erzeugt automatisch Informationen zur Unternehmensaktivität und ermöglicht die Suche, den Abgleich und die Konfiguration ereignisbezogener Warnungen.



Das **SIEMFeeder**-Modul übermittelt die an den Endpoints erfassten Ereignisse in Echtzeit und unter Angabe der in der Cloud Protection Platform ergänzten Sicherheitsiformatione. So können sie in das unternehmenseigene SIEM eingespeist werden.

Weitere Informationen erhalten Sie unter www.pandasecurity.com/business/solutions

Mindestanforderungen
Windows-Workstations: XP SP3 oder höher
Windows-Server: Server 2003 (32/64-bit and R2) SP2 oder höher
MacOS-Workstations und -Server: macOS 10.10 Yosemite oder höher
Linux-Workstations und -Server: Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS und 16.10. Fedora 23, 24 und 25. Weitere unterstützte Versionen erfahren Sie von Ihrem Verkaufsberater oder Partner bei Panda Security.
Android: Version 4 oder höher
Plattform-Zertifizierungen: ISO27001, SAS 70

Preise und Auszeichnungen

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 gewonnen.

Panda Adaptive Defense erhielt die Zertifizierung EAL2+ in Rahmen der Prüfung für den Common Criteria Standard.

2018 wurde Panda Security im Gartner Magic Quadrant für Endpoint Protection Platforms (EPP) als visionäres Unternehmen genannt.
https://www.pandasecurity.com/ gartner-magic-quadrant/