

| WatchGuard
Endpoint-
Sicherheitslösungen
für Unternehmen



Schutz	Panda Adaptive Defense 360	Panda Adaptive Defense	Panda Endpoint Protection Plus	Panda Endpoint Protection	Panda Systems Management	Panda Fusion*	Panda Fusion 360**
Schutz vor bekannter und Zero-Day-Malware	■	■	□	□		□	■
Schutz vor bekannter und Zero-Day-Ransomware	■	■	□	□		□	■
Schutz vor bekannten und Zero-Day-Exploits	■	■	□	□		□	■
Anti-Spyware, Anti-Phishing-Schutz usw	■	■	■	■		■	■
Schutz mehrere Angriffsvektoren (Web, E-Mail, Netzwerk, Geräte)	■	□	■	■		■	■
Traditioneller Schutz mit generischen und optimierten Signaturen	■	■	■	■		■	■
Schutz vor Advanced Persistent Threats (APT)	■	■					■
Zero-Trust Application Service	■	■					■
Threat Hunting Service (Indikatoren für Angriffe)	■	■					■
Abfragen der cloudbasierten Collective Intelligence von Panda	■	■	■	■		■	■
Verhaltensblockierung und IoA-Erkennung	■	■	□	□		□	■
Persönliche und verwaltete Firewall	■		■	■		■	■
IDS/HIDS	■		■	■		■	■
Autorisierte Software nach Hash bzw. Programmeigenschaften	■	■					■
Möglichkeit zum Blockieren unbekannter und unerwünschter Anwendungen	■	■					■
Gerätesteuerung	■		■	■		■	■
URL Filtering nach Kategorie (Webbrowsing-Überwachung)	■		■			■	■
Überwachung							
Hochentwickelte Endpoint-Sicherheit	■	■					■
Cloudbasierte ständige Überwachung aller Prozessaktivitäten	■	■					■
Einjährige Aufbewahrung von Daten für retrospektive Angriffsuntersuchungen	■	■					■
Erkennung							
Erkennung kompromittierter vertrauenswürdiger Anwendungen	■	■					■
Zero-Trust Application Service	■	■					■
Vollständig konfigurierbare und sofortige Sicherheitsrisiko-Warmmeldungen	■	■	■	■		■	■
Eindämmung							
Echtzeitisolierung von Computern über die Cloud-Konsole	■	■					■
Reaktion und Abhilfe							
Möglichkeit zum Zurücksetzen und Beheben der von Angreifern durchgeführten Aktionen	■	■	■	■		■	■
Zentrale Quarantäne	■	■	■	■		■	■
Automatische Analyse und Desinfektion	■	■	■	■		■	■
Untersuchung							
Threat Hunting Service (Indikatoren für Angriffe)	■	■					■
Ereignisdiagramme und Lebenszyklus-Informationen über die Web-Konsole	■	■					■
Möglichkeit zum Export von Lebenszyklus-Informationen zur lokalen Analyse	■	■					■
Advanced Visualization Tool (Add-on)	■	■					■
Entdeckung und Überwachung unstrukturierter personenbezogener Daten über Endpoints hinweg (Add-on)	■	■					■
Verkleinerung der Angriffsfläche							
Informationen zu den Hardware- und Softwarekomponenten jedes Computers	■	■	■	■		■	■
Informationen zu den auf Endpoints installierten Microsoft-Aktualisierungen	■	■	■	■		■	■
Echtzeitinformationen zum Status aller Schutzmaßnahmen und Kommunikationen	■	■	■	■		■	■
Automatisierte Aktualisierungen	■	■	■	■		■	■
Automatische Erkennung ungeschützter Endpoints	■	■	■	■		■	■
Möglichkeit zum unmittelbaren Remote-Schutz ungeschützter Endpoints	■	■	■	■		■	■
Panda native Proxy zur Unterstützung von Endpoints ohne Internetverbindung	■	■	■	■		■	■

ENDPOINT-SICHERHEIT UND -MANAGEMENT

Panda Adaptive Defense 360 Panda Adaptive Defense Panda Endpoint Protection Plus Panda Endpoint Protection Panda Systems Management Panda Fusion* Panda Fusion 360**

Endpoint-Sicherheitsmanagement	Panda Adaptive Defense 360	Panda Adaptive Defense	Panda Endpoint Protection Plus	Panda Endpoint Protection	Panda Systems Management	Panda Fusion*	Panda Fusion 360**
Zentrale cloudbasierte Konsole	■	■	■	■	■	■	■
Vererbung von Einstellungen zwischen Gruppen und Endpoints	■	■	■	■		■	■
Möglichkeit zur Konfiguration und Anwendung von Einstellungen auf Gruppenbasis	■	■	■	■		■	■
Möglichkeit zur Konfiguration und Anwendung von Einstellungen pro Endpoint	■	■	■	■		■	■
Echtzeit-Bereitstellung von Einstellungen der Konsole zu Endpoints	■	■	■	■		■	■
Sicherheitsmanagement basierend auf Endpoint-Ansichten und dynamischen Filtern	■	■	■	■		■	■
Möglichkeit zur Planung und Ausführung von Aufgaben in Endpoint-Ansichten	■	■	■	■		■	■
Möglichkeit zur Zuweisung vorkonfigurierter Rollen für Konsolenanwender	■	■	■	■		■	■
Möglichkeit zur Zuweisung benutzerdefinierter Berechtigungen für Konsolenanwender	■	■	■	■		■	■
Möglichkeit zur individuellen Konfiguration lokaler Warnmeldungen	■	■	■	■		■	■
Anwender-Aktivitätsaudits	■	■	■	■		■	■
Installation über MSI-Packages, Download-URLs und an Endanwender gesendete E-Mails	■	■	■	■		■	■
On-Demand-Berichte und geplante Berichte auf verschiedenen Ebenen und mit mehreren Granularitätsoptionen	■	■	■	■		■	■
Sicherheits-KPIs und Management-Dashboards	■	■	■	■		■	■
API-Verfügbarkeit	■	■	■	■			
Endpoint-Systemmanagement							
Systemstatus-Berichte auf verschiedenen Ebenen und mit mehreren Granularitätsoptionen	■	■	■	■	■	■	■
Gerätebestände und Audits					■	■	■
Agenten- und agentenlose Geräteüberwachung					■	■	■
Patch-Management (eingeschränkte Funktion, kein vollständiges Patch-Management-Add-on)					■	■	■
Zentrale Softwareinstallation					■	■	■
Unaufdringlicher Fernzugriff					■	■	■
Remote-Desktop					■	■	■
Eingebaute Chatfunktion					■	■	■
Aufgabenautomatisierung und Skripterstellung					■	■	■
Komponenten-Store – ComStore					■	■	■
Ticketsystem/Helpdesk					■	■	■
Module (erfordert Zusatzkauf)							
Panda Data Control-Integration	■	■					■
Advanced Reporting Tool-Integration	■	■					■
SIEM-Integration	■	■					■
Panda Patch Management-Integration	■	■	■	■		■	■
Panda Full Encryption-Integration	■	■	■	■		■	■
Hochverfügbarkeitsdienst	■	■	■	■	■	■	■
Hostplattform-Zertifizierungen			ISO27001, SAS 70 ISO27001, SAS 70			ISO27001, FISMA, SAS70, PCI DSS	
Kompatible Betriebssysteme							
Unterstützt Windows Intel	■	■	■	■	■	■	■
Unterstützung für Windows ARM	■	■	■	■		■	■
Unterstützung für macOS ARM	■	■	■	■	■	■	■
Unterstützt macOS	■	■	■	■	■	■	■
Unterstützt Linux	■	■	■	■	■	■	■
Unterstützt Android	■		■	■	■	■	■
Unterstützt iOS					■	■	■
Unterstützt virtuelle Umgebungen – persistent und nicht persistent (VDI)***	■	■	■	■		■	■

- Nur Basisfunktionen. Zusätzlicher Schutz verfügbar mit anderen Panda-Produkten.
- Volle Funktionalität. Nur bei Aether-basierten Lösungen.

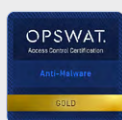
* Panda Fusion ist ein Bundle bestehend aus Panda Endpoint Protection Plus und Panda Systems Management.

** Panda Fusion 360 ist eine Kombination aus Panda Systems Management und Panda Adaptive Defense 360, separat erhältlich

***Kompatible Systeme mit folgenden virtuellen Maschinen: VMware Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop und MS Virtual Servers. Panda Adaptive Defense 360 & Panda Fusion 360 Lösungen sind mit Citrix Virtual Apps, Citrix Desktops 1906 & Citrix Workspace App für Windows kompatibel; Panda Security ist als Citrix Ready Partner zertifiziert

AUSZEICHNUNGEN UND ZERTIFIZIERUNGEN

Panda Security steht regelmäßig auf der Liste der Teilnehmer für die Auszeichnungen von Virus Bulletin, AV-Comparatives, AV-Test und NSS Labs 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.



ZUSÄTZLICHE MODULE UND PRODUKTE VON WATCHGUARD FÜR ENDPOINT-SICHERHEIT

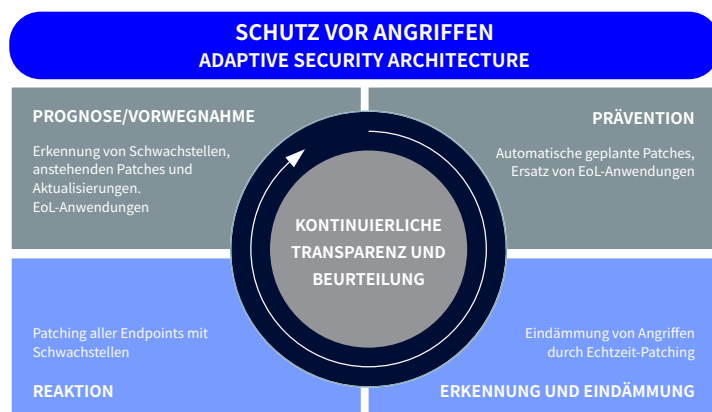
Panda Patch Management

Panda Patch Management ist ein Modul zum Schwachstellenmanagement von Betriebssystemen und Drittanbieter-Anwendungen auf Windows-Workstations und -Servern.

Die Lösung erfordert keine neuen Endpoint-Agents oder Managementkonsolen, da sie vollständig in alle Endpoint-Lösungen von Panda Security integriert ist. Zudem bietet sie zentrale Echtzeit-Transparenz des Sicherheitsstatus hinsichtlich Software-Schwachstellen, fehlender Patches, Aktualisierungen und nicht unterstützter EOL-Software. Sie ist einfach zu verwenden und installiert und überwacht Aktualisierungen in Echtzeit.

[Weitere Informationen](#)

[Unterstützte Plattformen und Anforderungen](#)

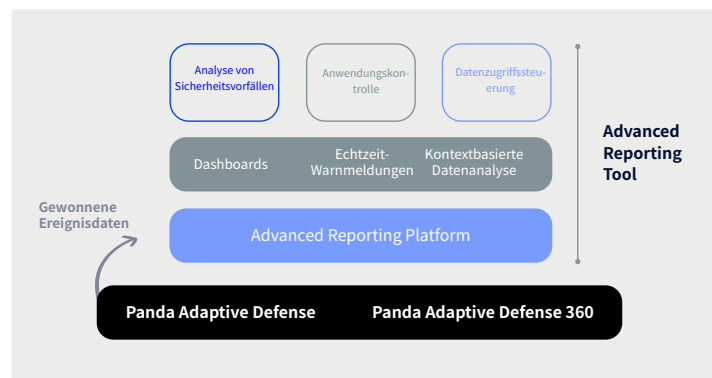


Advanced Reporting Tool

Das **Advanced Reporting Tool** speichert und korreliert die Informationen in Zusammenhang mit der Prozessausführung und dem Kontext, der von Adaptive Defense von Endpoints extrahiert wird. Erzeugt automatisch Sicherheitsinformationen und bietet Tools, mit denen Organisationen Angriffe und ungewöhnliche Verhaltensmuster präzise bestimmen sowie internen Missbrauch der Firmennetzwerke und -systeme erkennen können, um umfassendere Sicherheitsuntersuchungen zu ermöglichen.

[Weitere Informationen](#)

[Unterstützte Plattformen und Anforderungen](#)



Panda Data Control

Panda Data Control ist ein Modul für unstrukturierte Datensicherheit und ist darauf ausgelegt, Unternehmen bei der Einhaltung von Datenschutzrichtlinien zu helfen sowie personenbezogene und vertrauliche Daten zu entdecken und zu schützen, sowohl in Echtzeit als auch über den Lebenszyklus der Daten auf Endpoints und Servern hinweg. Panda Data Control entdeckt, auditiert und überwacht unstrukturierte personenbezogene Daten auf Endpoints: Von ruhenden Daten bis hin zu verwendeten Daten und Daten in Bewegung.

[Weitere Informationen](#)

[Unterstützte Plattformen und Anforderungen](#)



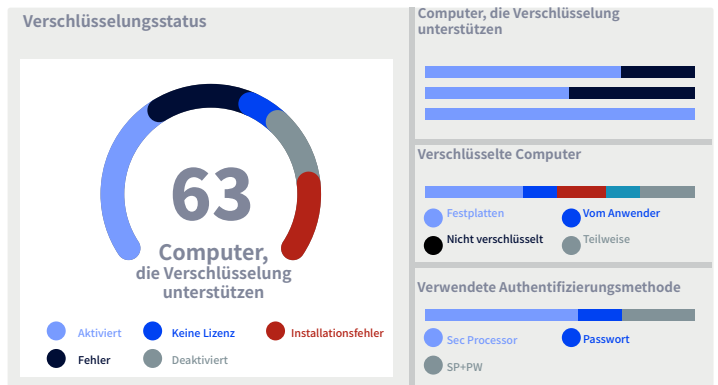
***Panda Data Control** ist in den folgenden Ländern verfügbar: Spanien, Deutschland, Vereinigtes Königreich, Schweden, Frankreich, Italien, Portugal, Niederlande, Finnland, Dänemark, Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.

Panda Full Encryption

Panda Full Encryption ist ein zusätzliches Modul für den Panda Security Endpoint-Schutz und hochentwickelte, anpassungsfähige Sicherheitslösungen, das auf zentrales Management der vollständigen Festplattenverschlüsselung ausgelegt ist. Es bietet die folgenden Funktionen: Vollständige Festplattenverschlüsselung und -Entschlüsselung, zentrale Verwaltung und Wiederherstellung von Verschlüsselungsschlüsseln, Listen und Berichte und zentrale Anwendung von Richtlinien.

[Weitere Informationen](#)

[Unterstützte Plattformen und Anforderungen](#)



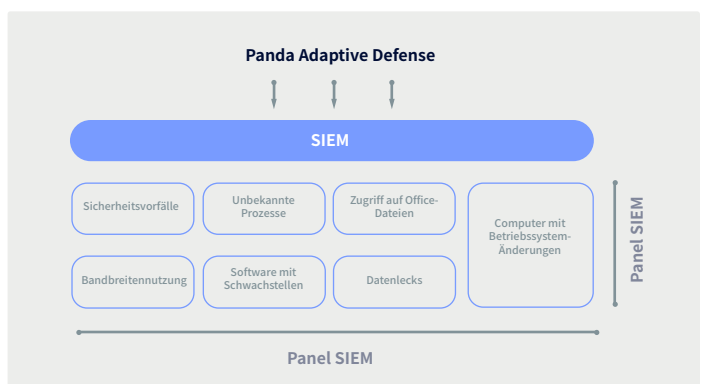
SIEM Feeder

SIEM Feeder. Panda Adaptive Defense und Panda Adaptive Defense 360 integriert auf geschützten Endpoints erfasste Ergebnisse nahtlos in bestehende Unternehmens-SIEM-Lösungen, ohne weitere Bereitstellungen auf Anwendergeräten. Überwachte Ereignisse werden sicher, entweder direkt oder indirekt über Plug-Ins, über das LEEF/CEF-Format gesendet, das mit den meisten SIEM-Systemen auf dem Markt kompatibel ist.

[Weitere Informationen](#)

[Unterstützte Plattformen und Anforderungen](#)

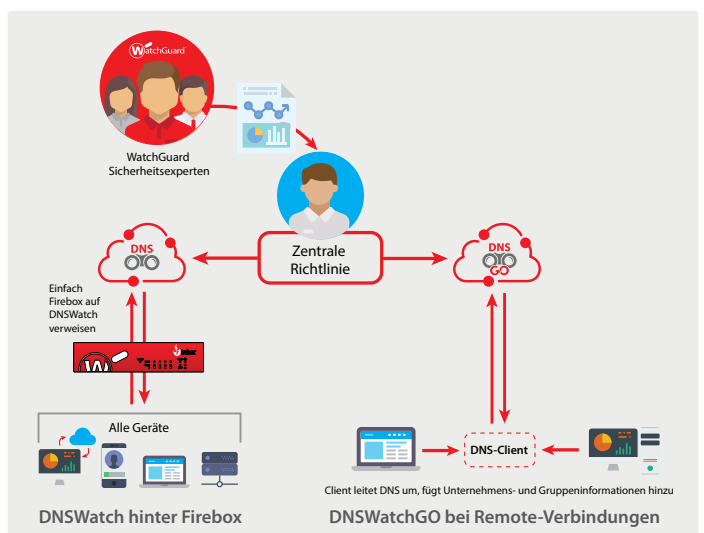
WatchGuard-Verteilung. Kauf und Einrichtung benötigen Unterstützung durch WatchGuard-Mitarbeiter.



DNSWatchGO

DNSWatchGO ist ein cloudbasierter Dienst, der Schutz auf Domain-Ebene, Inhaltsfilterung und integrierte Schulungen zur Förderung des Sicherheitsbewusstseins bietet, damit Ihre Benutzer auch außerhalb Ihres sicheren Netzwerkperimeters geschützt sind. Im Fall kritischer Warnmeldungen führen die Sicherheitsexperten von WatchGuard eine maßgeschneiderte Analyse der potenziellen Bedrohung durch und dokumentieren dann potenzielle Infektionen in einfacher Sprache und mit detaillierten Informationen. Wenn ein Benutzer auf einen bösartigen Link klickt, wird er von DNSWatchGO automatisch auf eine sichere Seite umgeleitet. Außerdem werden ihm Ressourcen angeboten, mit denen er sein Sicherheitswissen vertiefen kann.

[Weitere Informationen](#)



PANDA-LÖSUNGEN: PLATTFORMEN UND ANFORDERUNGEN

[Windows Server & Workstations](#) | [macOS-Geräte](#) | [Linux Server & Workstations](#) | [Android-Mobilgeräte](#)



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

Mit diesem Dokument werden keine ausdrücklichen oder implizierten Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2021 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo und Panda Security sind Marken oder eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Marken und Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilen: WGCE67378_072121