ENDPOINT SECURITY AND MANAGEMENT

	Panda Endpoint Protection	Panda Endpoint Protection Plus	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Systems Management	Panda Fusion*	Panda Fusion & Adaptive Defense 360*
Protection							
Protection against known and zero-day malware	○	○	●	●		○	●
Protection against known and zero-day ransomware	○	○	●	●		○	●
Protection against known and zero-day exploits	○	○	●	●		○	●
Anti-spyware, anti-phishing protection, etc.	●	●	●	●		●	●
Protection for multiple attack vectors (Web, email, network, devices)	●	●	●	●		●	●
Traditional protection with generic and optimized signatures	●	●	●	●		●	●
Queries to Panda's cloud-based collective intelligence	●	●	●	●		●	●
Behavioral blocking and IoA detection	○	○	●	●		○	●
Personal and managed firewall	●	●		●		●	●
IDS / HIDS	●	●		●		●	●
Device control	●	●		●		●	●
Content filtering for Exchange Serve	●	●		●		●	●
URL filtering by category	●	●		●		●	●
Built-in antivirus protection for Exchange Server		●		●		●	●
Built-in anti-spam protection for Exchange Server		●		●		●	●
Protection against Advanced Persistent Threats (APT)			●	●			●
Managed service: Classification of 100% of applications before execution*			●	●			●
Monitoring							
Web browsing monitoring	●	●		●		●	●
Next-generation endpoint security			●	●			●
Cloud-based continuous monitoring of all process activity			●	●			●
Data retention for one year for retrospective attack investigation			●	●			●
Detection							
Detection of compromised trusted applications			●	●			●
Managed service: Classification of 100% of applications during and after execution (1*)			●	●			●
Managed service for finding and detecting advanced threats (2*)			●	●			●
Fully configurable and instant security risk alerts	●	●	●	●		●	●
Containment							
Real-time computer isolation from the cloud console			●	●			●
Notifications from the Threat Hunting team			●	●			●
Response and remediation							
Ability to roll back and remediate the actions committed by attackers	●	●		●		●	●
Centralized quarantine	●	●		●		●	●
Advanced disinfection and remediation tools					●		
Investigation							
Incident graphs and lifecycle information available from the Web console			●	●			●
Ability to export lifecycle information for local analysis			●	●			●
Real-time integration with most SIEMs (add-on)			●	●			●
Advanced Visualization Tool (add-on)			●	●			●
Discovery and monitoring of unstructured personal data across endpoints (add-on)			●	●			●
Attack surface reduction							
Information about each computer's hardware and software components			●	●			●
Information about the Microsoft updates installed on endpoints			●	●			●
Real-time information about the status of all protections and communications			●	●			●
Unattended, automatic updates	●	●	●	●		●	●
Automatic discovery of unprotected endpoints	●	●	●	●		●	●
Ability to immediately protect unprotected endpoints remotely	●	●	●	●		●	●
Panda native proxy to support endpoints with no Internet connection	●	●	●	●		●	●

Endpoint security management							
Centralized cloud-based console	●	●	●	●	●	●	●
Settings inheritance between groups and endpoints	●	●	●	●		●	●
Ability to configure and apply settings on a group basis	●	●	●	●		●	●
Ability to configure and apply settings on a per-endpoint basis	●	●	●	●		●	●
Real-time deployment of settings from the console to endpoints	●	●	●	●		●	●
Security management based on endpoint views and dynamic filters	●	●	●	●		●	●
Ability to schedule and perform tasks on endpoint views	●	●	●	●		●	●
Ability to assign preconfigured roles to console users	●	●	●	●		●	●
Ability to assign custom permissions to console users	●	●	●	●		●	●
User activity auditing	●	●	●	●		●	●
Installation via MSI packages, download URLs, and emails sent to end users	●	●	●	●		●	●
On-demand and scheduled reports at different levels and with multiple granularity options	●	●	●	●		●	●
Security KPIs and management dashboards	●	●	●	●		●	●
Endpoint system management							
System status reports at different levels and with multiple granularity options	●	●	●	●	●	●	●
Device inventory and audits					●	●	●
Agent and agentless monitoring of devices					●	●	●
Patch management					●	●	●
Centralized software installation					●	●	●
Non-disruptive remote access					●	●	●
Remote Desktop					●	●	●
Built-in chat					●	●	●
Task automation and scripting					●	●	●
Component store					●	●	●
Ticketing/Help Desk					●	●	●
Modules							
Panda Data Control integration (add-on)			●	●			●
Advanced Reporting Tool integration (add-on)			●	●			●
SIEM integration (add-on)			●	●			●
High availability service	●	●	●	●	●	●	●
Security certifications		ISO27001, SAS 70	ISO27001, SAS 70			ISO27001, FISMA, SAS70, PCI DSS	
Supported operating systems							
Windows workstations: XP SP2 or later	●	●	●			●	●
Windows workstations: XP SP3 or later	●	●	●		●	●	●
Windows servers: Windows Server 2003 SP1(32-bit, 64-bit and R2) or later	●	●	●			●	●
Panda - Windows servers: Windows Server 2003 SP2 (32-bit, 64-bit and R2) or later	●	●	●		●	●	●
Mac OS: Mac OS X 10.6 Snow Leopard or later	●	●	●			●	●
Panda native protection - Mac OS: Mac OS X 10.10 Yosemite or later	●	●	●		10.12 +	●	●
Linux Ubuntu, Red Hat, Debian, OpenSUSE, SUSE Enterprise (3*)	●	●	●		●	●	●
Panda native protection: Linux Ubuntu, Fedora (4*)	●	●	●			●	●
Support for virtual environments	●	●	●		●	●	●
Android 4 or later	●	●	●		2.3.3 +	●	●
iOS 7 or later					●	●	●
MDM support for Android and iOS smartphones and tablets					●	●	●

* Fusion is a bundle of Panda Endpoint Protection Plus and Panda Cloud System Management. Fusion - PAD360 is the combination of Fusion and Panda Adaptive Defense 360 that are sold separately

1* 100% Attestation Service.

2* Threat Hunting Service.

○ Functionality extended in other Panda endpoint solutions.

● Full functionality.

○ Functionality extended in other Panda endpoint solutions. Only in Aether-based solutions.

● Full functionality. Only in Aether-based solutions.

3* Ubuntu 12 32/64 bits or later. Red Hat Enterprise Linux 6.0 64 bits or later. Debian 6.0 Squeeze or later. OpenSuse 12 32/64 bits or later. Suse Enterprise Server 11SP2 64 bits or later.

4* Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS & 16.10. Fedora 23, 24 & 25. Panda System Management: Fedora 19 or later, CentOS 7 or later, Debian 7 or later.

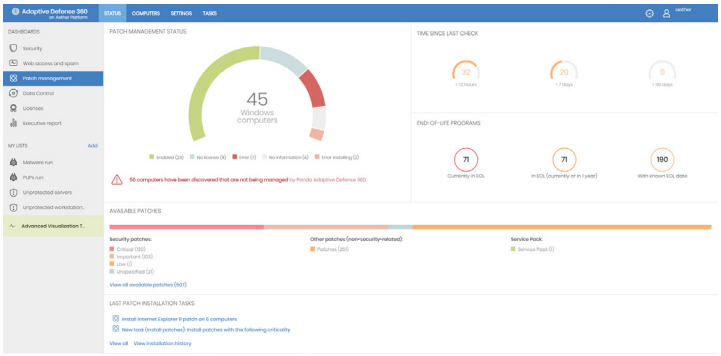
MODULES

Optional modules for Panda Adaptive Defense and Panda Adaptive Defense 360

Panda Patch Management

Panda Patch Management is a module for managing vulnerabilities of the operating systems and third-party applications on Windows workstations and servers.

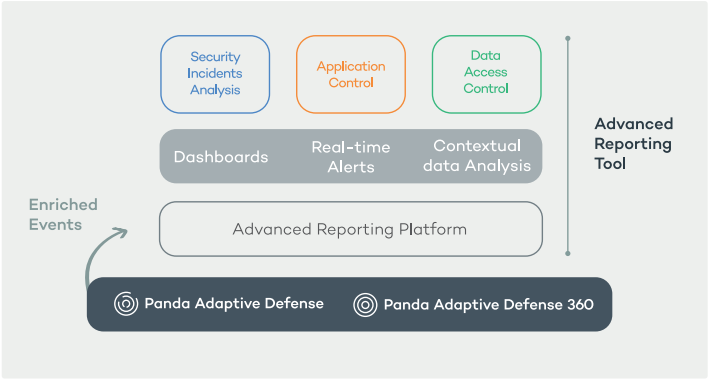
It does not require the deployment of any new endpoint agents or management console as it is fully integrated in all of Panda Security's endpoint solutions. Plus, it provides centralized, real-time visibility into the security status of software vulnerabilities, missing patches, updates and unsupported (EOL3) software. As well as easy-to-use and real-time to install and monitor updates.



More information

Advanced Reporting Tool

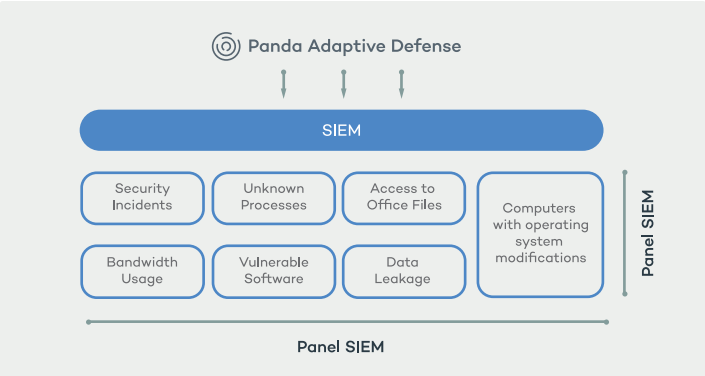
Advanced Reporting Tool stores and correlates of the information related to process execution and its context extracted by Adaptive Defense from endpoints. Automatically generates security intelligence and provides tools that allow organizations to pinpoint attacks and unusual behaviors, detecting internal misuse of the corporate systems and network and go deeper in a security investigation.



More information

SIEM Feeder

SIEMFeeder. Panda Adaptive Defense and Panda Adaptive Defense 360 seamlessly integrate events gathered from protected endpoints with existing corporate SIEM solutions without additional deployments on users' devices. Monitored events are sent securely using the LEEF/CEF formats compatible with most SIEM systems on the market either directly or indirectly via plugins.



More information

EMAIL PROTECTION

Panda Email Protection

Panda Email Protection filters out spam and threat from the inbound and outbound email traffic, through online scans performed on Panda Security's servers. Email Protection requires no client infrastructure. All operations are performed in the cloud.

Key Benefits:

Ensures the highest levels of detection for known and unknown.

Is a cloud-based service, it requires no infrastructure investment or specialized staff.

Security can be managed anytime, anywhere from the Web console

It gives users secure, uninterrupted access to email via webmail

More information