|WatchGuard Endpoint Security Solutions for Companies

panda
a WatchGuard brand

ENDPOINT SECURITY AND MANAGEMENT

	Panda Adaptive Defense 360	Panda Adaptive Defense	Panda Endpoint Protection Plus	Panda Endpoint Protection	Panda Systems Management	Panda Fusion*	Panda Fusion 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	■	■	■	■		■	■
Protection against advanced persistent threats (APT)	■	■					■
Zero-Trust Application Service*	■	■					■
Threat Hunting Service**	■	■					■
Queries to Panda's Cloud-based collective intelligence	■	■	■	■		■	■
Behavioral blocking and IoA detection	■	■	□	□		□	■
Personal and managed firewall	■		■	■		■	■
IDS / HIDS	■		■	■		■	■
Ability to block unknown and unwanted applications	■	■					■
Device control	■		■	■		■	■
URL filtering by category (web browsing monitoring)	■		■			■	■
Content, virus and spam filtering for Exchange Server	■		■			■	■
Built-in antivirus protection for Exchange Server	■		■			■	■
Built-in anti-spam protection for Exchange Server	■		■			■	■
Monitoring							
Advanced 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	■	■					■
Zero-Trust Application Service*	■	■					■
Fully configurable and instant security risk alerts	◼	◼	◼	◼		◼	◼
Containment							
Real-time computer isolation from the Cloud console	◼	◼					◼
Response and remediation							
Ability to roll back and remediate the actions committed by attackers	■	■	■	■		■	■
Centralized quarantine	■	■	■	■		■	■
Automatic analysis and disinfection	■	■	■	■		■	■
Investigation							
Threat Hunting Service*	■	■					■
Incident graphs and lifecycle information available from the web console	■	■					■
Ability to export lifecycle information for local analysis	■	■					■
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	◼	◼	◼	◼		◼	◼
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 AND MANAGEMENT

	Panda Adaptive Defense 360	Panda Adaptive Defense	Panda Endpoint Protection Plus	Panda Endpoint Protection	Panda Systems Management	Panda Fusion*	Panda Fusion 360**
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 - ComStore					■	■	■
Ticketing/Help Desk					■	■	■
Modules							
Panda Data Control integration	■	■					■
Advanced Reporting Tool integration	■	■					■
SIEM integration	■	■					■
Panda Patch Management integration	■	■	■	■		■	■
Panda Full Encryption inregration	■	■	■	■		■	■
High availability service	■	■	■	■	■	■	■
Host platform certifications	ISO27001, SAS 70	ISO27001, SAS 70			ISO27001, FISMA, SAS70, PCI DSS		
Supported operating systems							
Supports Windows	■	■	■	■	■	■	■
Suppots Exchange	■		■		■	■	■
Supports macOS	■	■	■	■	■	■	■
Supports Linux	■	■	■	■	■	■	■
Supports Android	■		■	■	■	■	■
Supports iOS					■		■
Support for virtual environments - persistent and non-persistent (VDI)***	■	■	■	■		■	■

□ 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.

* Panda Fusion is a bundle of Panda Endpoint Protection Plus and Panda Systems Management.

** Panda Fusion 360 is the combination of Panda Systems Management and Panda Adaptive Defense 360 that are sold separately.

*** Compatible systems with the following types of virtual machines: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop and MS Virtual Servers. Panda Adaptive Defense 360 & Panda Fusion 360 solutions are compatible with Citrix Virtual Apps, Citrix Desktops 1906 & Citrix Workspace App for Windows, Panda Security has been verified as Citrix Ready partner.
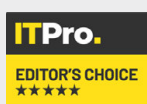
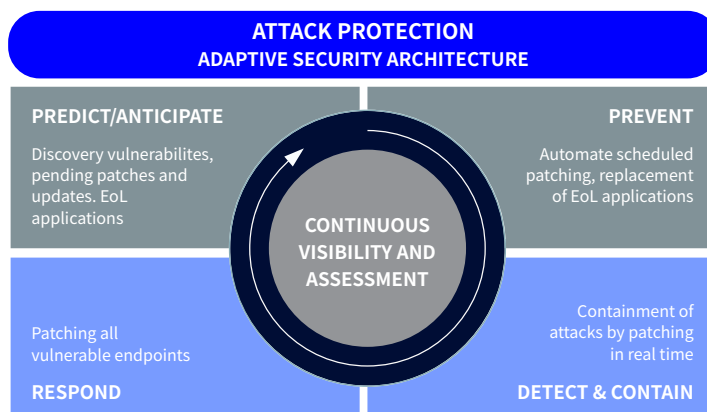# ADDITIONAL WATCHGUARD ENDPOINT SECURITY MODULES AND PRODUCTS

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 end of life (EOL) software. As well as easy-to-use and real-time to install and monitor updates.

ATTACK PROTECTION
ADAPTIVE SECURITY ARCHITECTURE

PREDICT/ANTICIPATE		PREVENT
Discovery vulnerabilites, pending patches and updates. EoL applications	CONTINUOUS VISIBILITY AND ASSESSMENT	Automate scheduled patching, replacement of EoL applications
Patching all vulnerable endpoints		Containment of attacks by patching in real time
RESPOND		DETECT & CONTAIN

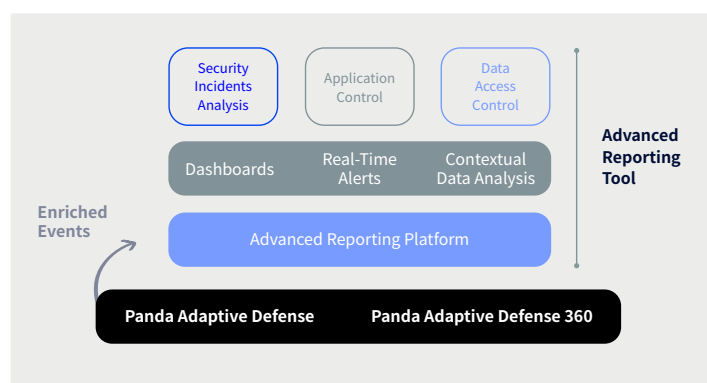[More information]

Supported platforms & requirements

Advanced Reporting Tool

The **Advanced Reporting Tool** stores and correlates 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 to go deeper in a security investigation.

Security Incidents Analysis | Application Control | Data Access Control

Advanced Reporting Tool

Dashboards | Real-Time Alerts | Contextual Data Analysis

Advanced Reporting Platform

Enriched Events

Panda Adaptive Defense   **Panda Adaptive Defense 360**

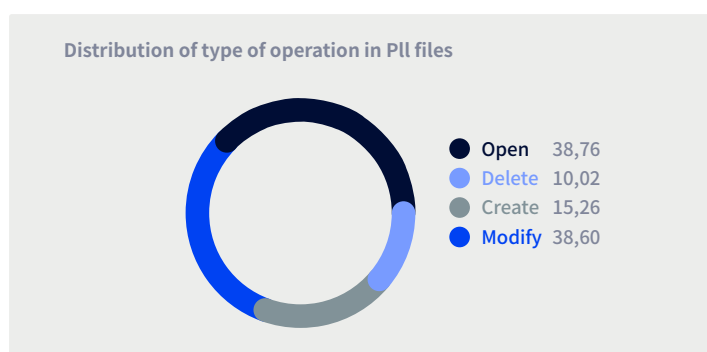[More information]

Supported platforms & requirements

Panda Data Control

Panda Data Control is an unstructured data security module, designed to assist organizations in complying with data protection regulations, as well as discovering and protecting personal and sensitive data both in real time and throughout its lifecycle on endpoints and servers. Panda Data Control discovers, audits and monitors unstructured personal data on endpoints: from data at rest to data in use and data in motion.

Distribution of type of operation in Pll files

- ● Open 38,76
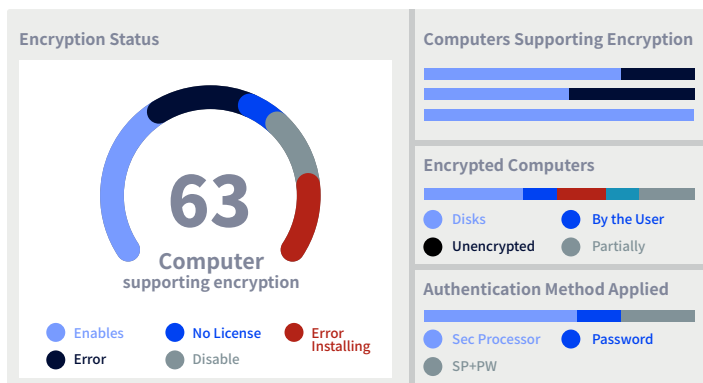- ● Delete 10,02
- ● Create 15,26
- ● Modify 38,60

*****Panda Data Control** is available in the following countries: Spain, Germany, UK, Sweden, France, Italy, Portugal, Holland, Finland, Denmark, Switzerland, Norway, Austria, Belgium, Hungary and Ireland.*

[More information]

Supported platforms & requirements

panda
a WatchGuard brand

Panda Full Encryption

Panda Full Encryption is an additional module for Panda Security's endpoint protection and advanced adaptive security solutions, designed to centrally manage full disk encryption and provide the following features: Full drive encryption and decryption, centralized management and recovery of encryption keys, Lists and reports and centralized policy application.

More information

Supported platforms & requirements

Encryption Status

63
Computer
supporting encryption

- Enables
- No License
- Error Installing
- Error
- Disable

Computers Supporting Encryption

Encrypted Computers

- Disks
- By the User
- Unencrypted
- Partially

Authentication Method Applied

- Sec Processor
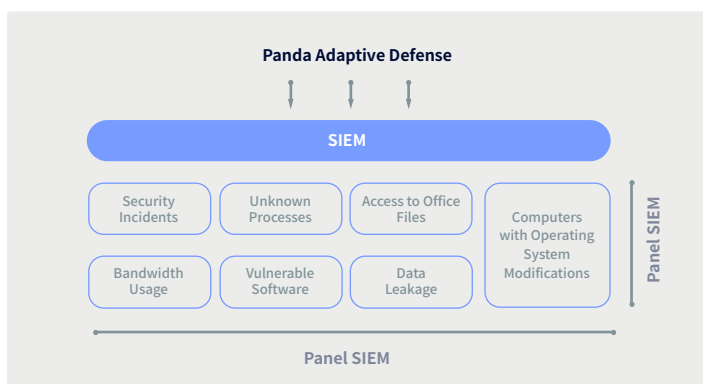- Password
- SP+PW

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

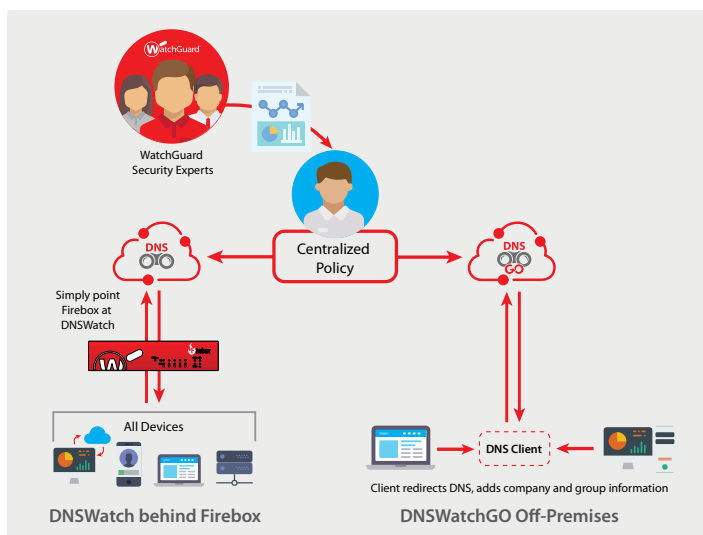Supported platforms & requirements

WatchGuard distribution. Purchase and set up requires assistance from WatchGuard staff.

Panda Adaptive Defense

SIEM

| Security Incidents | Unknown Processes | Access to Office Files | Computers with Operating System Modifications |
| Bandwidth Usage | Vulnerable Software | Data Leakage | |

Panel SIEM

Panel SIEM

DNSWatchGO

DNSWatchGO is a Cloud-based service that provides domain-level protection, content filtering, and integrated security awareness training to keep your users safe when they travel outside of your secure network perimeter. When critical alerts are seen, WatchGuard's team of security experts performs a tailored analysis of the potential threat, following up with an easy-to-understand accounting that includes detailed insights about the potential infection. When a user clicks a malicious link, DNSWatchGO automatically redirects them to a safe page and offers resources that reinforce security education.

More information

WatchGuard Security Experts

Centralized Policy

Simply point Firebox at DNSWatch

All Devices

DNS Client

Client redirects DNS, adds company and group information

DNSWatch behind Firebox   **DNSWatchGO Off-Premises**

WatchGuard®

UK SALES +44 (0) 203 608 9070   EMAIL uksales@watchguard.com   www.watchguard.com/uk | pandasecurity.com