The Intelligence You Need To Be Breach Proof

The Data And Tools To Stay Ahead Of Hackers

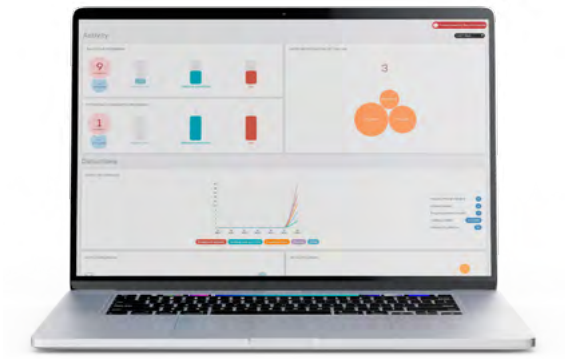
Panda Adaptive Defense 360

Today' s threat landscape is sophisticated and the volume of new viruses unprecedented. To combat this new reality, it takes the right resources, technology and the ability to manage both. And while advanced threats keep appearing at alarming numbers, there is a shortage of IT professionals and IT budget to protect against them.

Panda' s answer to this problem?

Panda Adaptive Defense 360, a cybersecurity model based on three principles: continuous monitoring of applications on a company' s computers and servers, automatic classification using machine learning on our big data platform in the Cloud, and expert analysis by Panda' s Threat Hunting team to analyze those applications that haven' t been classified automatically, delivered as a service.

Download the datasheet >



Panda Patch Management

Simplify patching to reduce your network' s attack surface

Panda Patch Management is a solution to manage updates and patches, both for operating systems and hundreds of third-party applications. Strengthens threat prevention, containment and remediation capabilities, reducing the attack surface on Windows servers and workstations.

Provides visibility of endpoint health status in real time, in terms of vulnerabilities, patches or pending updates, and unsupported software (EOL). Discover, plan, install, and monitor.

Download the datasheet >

Panda Data Control

Real-time data security, visibility and control

Massive data breaches occur too often. Uncontrolled access to company personal (PII) & sensitive (IP) data is an everyday threat leading to serious financial loss & reputational damage.

Panda Data Control assists organizations in complying with data protection regulations, discovering and protecting personal and sensitive data, both in real time and throughout its lifecycle on endpoints and servers.

Download the datasheet >

Panda Full Encryption

Strengthen security from unauthorized access

One of the most efficient ways to minimize data exposure is to automatically encrypt the hard disks of desktops, laptops and servers, in order to ensure data access is secure and compliant with the authentication mechanisms implemented.

Panda Full Encryption leverages BitLocker, a proven and stable Microsoft technology, to encrypt and decrypt disks without impacting end users and providing organizations with the added value of centrally controlling and managing the recovery keys stored on Panda Security' s Cloud-based management platform, Aether.

Download the datasheet >

Advance Reporting Tool

From Data to Actionable IT and Security Insight

IT staff is overwhelmed. Increasing volume of data and advanced attacks causes vital details to be overlooked, compromising the security of the entire system.

Panda Advanced Reporting Tool correlates data to automatically generate security intelligence, to pinpoint attacks and unusual behaviors, and detect internal misuse of the corporate systems.

Download the datasheet >

panda
a WatchGuard brand

	Advanced Protection		Traditional Protection		Device Mgmt	Protection & Mgmt		IT Operations & Privacy & Data Control			
	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Endpoint Protection	Panda Endpoint Protection Plus	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Panda Adv Reporting Tool	Panda Data Control
Centralized management from a single, Cloud-based console	■[1]	■[1]	■[1]	■[1]	■[2]	■[3]	■[3]	■[1]	■[1]	■[1]	■[1]
Single, lightweight endpoint agent	■	■	■	■	■	2 Agents	2 Agents	■	■	■	■
Protection of malicious apps (malware, phishing, ransomware, trojans, etc.)		■	■	■		■	■				
Protection against scripts and malicious macros in MS Office documents, etc.	■	■	■	■		■	■				
Protection of sophisticated targeted attacks in the pre-execution and execution phases	■	■					■				
Detection of unknown exploits based on the behavior of compromised processes in memory	■	■					■				
Virtual patching for unsupported systems	■	■				■	■				
Detection of Indicators of Attack (IoAs) in the pre-execution phase	■	■	■	■		■	■				
Behavior- and context-based detection of IoAs in the execution phase	■	■				■	■				
Activity monitoring on Windows, macOS and Linux systems	■	■					■				
Machine learning and deep learning on static, dynamic and contextual attributes	■	■					■				
Zero-Trust Application Service	■	■					■				
Threat Hunting & Investigation Service	■	■					■				
Personal and managed firewall		■	■	■		■	■				
IDS/HIPS[4]		■	■	■		■	■				
Anti-tamper protection	■	■	■	■		■	■				
Device Control		■	■	■		■	■				
Ability to block unknown and unwanted applications	■	■					■				
Authorized software by hash or program properties	■	■					■				
URL filtering by category (web browsing monitoring)		■		■		■	■				
Integration with existing SIEM systems (optional)	■	■					■				
Email protection against phishing, malware and advanced threats		■		Exchange		Exchange	Exchange				
Anti-spam protection		Exchange		Exchange		Exchange	Exchange				
Automated disinfection and remediation	■	■	■	■		■	■				
Centralized quarantine accessible from the list of detections (Malware Freezer)	■	■	■	■		■	■				
Execution timeline and forensic analysis	■	■					■				
Containment from the console: isolate computers in a controlled way	■	■					■				
Containment from the console: restart computers in a controlled way	■	■	■	■		■	■				
Real-time deployment of configuration policies and tasks	■	■	■	■		■	■	■	■		■
Discovery of unmanaged devices	■	■	■	■	■	■	■	■	■		
Real-time preconfigured & customizable dashboards, reports and alerts	■	■	■	■		■	■	■	■	■	■
Hardware and software inventory	■	■	■	■	■	■	■				
Anti-theft - remote alarm (Android)		■	■	■		■	■				
Snap the thief (Android)		■	■	■		■	■				
Anti-theft (iOS)					■	■	■				
Applications usage control (iOS)					■	■	■				
Agent and agentless monitoring of devices					■	■	■				
Centralized software installation and license control					■	■	■				
Task automation and scripting					■	■	■				
Component store - ComStore					■	■	■				
Ticketing/Help Desk/Chat					■	■	■				
Remote control					■	■	■				
Computer and server monitoring (CPU, memory, VMI, Event log, etc.)					■	■	■				

panda
a WatchGuard brand

	Advanced Protection		Traditional Protection		Device Mgmt	Protection & Mgmt		IT Operations & Privacy & Data Control			
	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Endpoint Protection	Panda Endpoint Protection Plus	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Panda Adv Reporting Tool	Panda Data Control
Patch and service pack management for Windows operating systems and third-party applications					Only OS	Only OS	Only OS	■			
EOL (End of Life) application management								■			
Patch rollback								■			
Ability to centrally disable Windows Update								■			
Ability to exclude specific patches and software								■			
Real-time and scheduled patching								■			
Full disk encryption/decryption using BitLocker									■		
Centralized management and recovery of encryption keys									■		
Centralized application of encryption policies									■		
Ability to encrypt removable storage drives									■		
Encryption dashboards, widgets and reports									■		
Dashboard, widget and predefined queries for ecurity KPIs										■	
KPIs on vulnerable, installed and run applications										■	
KPIs for unusual access to data files on endpoints										■	
KPIs on shadow IT applications run										■	
Inventory and classification of PII[5] files											■
Monitoring of PII files (data at rest, in use and in transit)**											■
User-defined guided searches for PII and non-PII files											■
Ability to delete PII files											■
Control writing information in removable storage drives only if they are encrypted											■
User and administrator consoles											
Advanced anti-phishing techniques (antispoofing, SPF, DKIM and DMARC, etc.)											
Advanced anti-spam proprietary technology											
Centralized quarantine managed by the administrator or the local user											
Mandatory secure communication (TLS) for selected recipients											
Incoming email backup											
Email notifier on endpoints											
Strict email sender validation											
Supports Windows Intel	■	■	■	■	■	■	■	■	■	■	■
Support Windows ARM	■	■	■	■		■	■	■	■	■	■
Supports Exchange		■		■	■	■	■				
Supports macOS	■	■	■	■	■	■	■			■***	
Supports Linux	■	■	■	■	■	■	■			■***	
Supports virtual systems - persistent and non-persistent (VDI)****	■	■	■	■		■	■				
Supports Android		■	■	■	■	■	■				
Supports iOS					■	■	■				

Panda Advanced Reporting and Panda Data Control modules are available for Panda Adaptive Defense and Panda Adaptive Defense 360 only. Panda Patch Management and Panda Full Encryption are available for Panda Endpoint Protection & Endpoint Protection Plus, Panda Fusion & Fusion 360, Panda Adaptive Defense and Panda Adaptive Defense 360. 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.

* Single, Cloud-based console: centralized management from anywhere. Reduces infrastructure and maintenance costs. **Data at rest, the actions taken on it (data in use) and data in motion. *** Limited telemetry. **** Compatible systems with the following types of virtual machines: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp,XenServer, MS Virtual Desktop y 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 Securtity has been verified as Citrix Ready partner.

[1]: Single, Cloud-based Aether console for all of Panda Security' s endpoint solutions and modules
[2]: Cloud-based Panda Cloud Systems Management console
[3]: Cloud-based Panda Cloud console. Provides access to the Panda Systems Management, Endpoint Protection Plus and Adaptive Defense 360 consoles.
[4]: Intrusion Detection System/Host-Based Intrusion Prevention System
[5]: Personally Identifiable Information

WatchGuard

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com