

# Visibilidad sin Límites, Control Absoluto

## Panda Adaptive Defense 360

### Protección, Detección, Respuesta & Remediación

Las organizaciones siguen siendo víctimas de ataques: Pese a las capas de seguridad de última generación, los hackers, los ataques dirigidos y los ataques de día cero siguen sembrando el caos.

Panda Adaptive Defense 360 es la única solución de seguridad avanzada y adaptativa en el endpoint que integra servicios gestionados de clasificación del 100% de los procesos ejecutados.

## Panda Patch Management

### Simplifica la aplicación de parches y reduce la superficie de ataque

Panda Patch Management es una solución de gestión de vulnerabilidades y sus correspondientes actualizaciones y parches, tanto de los sistemas operativos como de cientos de aplicaciones. Fortalece las capacidades de prevención, contención y remediación de las amenazas y de reducción de la superficie de ataque en servidores y estaciones Windows.

Proporciona visibilidad de la salud de los endpoints en tiempo real en cuanto a vulnerabilidades, parches o actualizaciones pendientes y software no soportado (EoL). Descubre, planifica, instala y monitoriza.

## Panda Data Control

### Seguridad, visibilidad y control de los datos personales en tiempo real

Los robos masivos de datos se han convertido en un problema demasiado frecuente: El acceso incontrolado a la información de carácter personal (PII) y sensible (IP) almacenada por las empresas es una amenaza cotidiana que puede traducirse en importantes pérdidas económicas y daños a su reputación.

Panda Data Control ayuda a las organizaciones a cumplir con las normativas de protección de datos, descubriendo y protegiendo la información de carácter personal almacenada en sus equipos y servidores tanto en tiempo real como durante todo su ciclo de vida.

## Panda Full Encryption

### Refuerza la seguridad contra accesos no autorizados centralizadamente

Una eficiente medida para minimizar la exposición de los datos es cifrando automáticamente los discos en portátiles, estaciones de trabajo y servidores, para que el acceso a los datos sea segura y conforme a los mecanismos de autenticación establecidos.

Panda Full Encryption permite la gestión centralizada del cifrado y descifrado completo de discos a través de BitLocker de Microsoft, así como la gestión centralizada y el control de las claves de recuperación almacenadas en la plataforma cloud de gestión de Panda Security, Aether.

## Advanced Reporting Tool

### Convierte los datos en conclusiones de Seguridad y Gestión IT

El personal informático se ve superado: La cantidad creciente de datos y los ataques avanzados hacen que información esencial se pase por alto, amenazando la seguridad de todo el sistema.

Panda Advanced Reporting Tool correlaciona información, generando inteligencia de seguridad de forma automática y ofreciendo herramientas que permiten tanto localizar ataques y comportamientos extraños, como descubrir el uso incorrecto de los equipos y la red corporativa.



	Advanced Protection		Traditional Protection		Device Mgmt	Protection & Mgmt		IT Operations & Privacy & Data Control				Email
	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Endpoint Protection	Panda Endpoint Protection+	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Panda Adv Reporting Tool	Panda Data Control	Panda Email Protection
Gestión centralizada desde una única consola en la nube	● <sup>1</sup>	● <sup>1</sup>	● <sup>1</sup>	● <sup>1</sup>	● <sup>2</sup>	● <sup>3</sup>	● <sup>3</sup>	● <sup>1</sup>	● <sup>1</sup>	● <sup>1</sup>	● <sup>1</sup>	● <sup>4</sup>
Único agente ligero en el endpoint	●	●	●	●	●	2 Agentes	2 Agentes	●	●	●	●	
Protección de aplicaciones maliciosas (malware, phishing, ransomware, troyanos,...)		●	●	●		●	●					●
Protección de scripts y macros maliciosos en documentos office, etc	●	●	●	●		●	●					
Protección de ataques sofisticados y dirigidos en pre-ejecución y en ejecución	●	●					●					
Detección de Exploits desconocidos por comportamiento de los procesos	●	●					●					
Parcheado Virtual en sistemas no soportados (Virtual Patching)	●	●				●	●					
Detección de Indicadores de Ataques (IoAs) en pre-ejecución	●	●	●	●		●	●					
Detección de IoAs por comportamiento y contexto en ejecución	●	●				●	●					
Monitorización de actividad en Windows, macOS y Linux	●	●					●					
Machine Learning y Deep Learning en miles de atributos estáticos, dinámicos y contextuales	●	●					●					
Servicio de clasificación 100% de procesos: previene o detecta aplicación maliciosa	●	●					●					
Servicio gestionado de Threat Hunting que detecta actividades de hackers e insiders	●	●					●					
Cortafuegos personal y administrado		●	●	●		●	●					
IDS / HIPS <sup>5</sup>		●	●	●		●	●					
Antitamper	●	●	●	●		●	●					
Control de dispositivos		●	●	●		●	●					
Filtrado de URL por categorías		●		●		●	●					
Monitorización de la navegación web		●		●		●	●					
Integración SIEM opcional	●	●					●					
Protección phishing, malware y amenazas avanzadas en correo		Exchange		Exchange		Exchange	Exchange					●
Protección antispam en correo		Exchange		Exchange		Exchange	Exchange					●
Desinfección y remediación automatizada	●	●	●	●		●	●					
Cuarentena centralizada integrada en la lista de detecciones (Malware Freezer)	●	●	●	●		●	●					
Timeline de ejecución y Análisis Forense	●	●					●					
Contención desde consola: aislar equipos de forma controlada	●	●				●	●					
Contención desde consola: reiniciar equipos de forma controlada	●	●	●	●		●	●					
Aplicación de políticas de seguridad y actualizaciones en tiempo real	●	●	●	●		●	●	●	●			
Descubrimiento de dispositivos no administrados	●	●	●	●		●	●	●	●			
Dashboard, informes y alertas en tiempo real	●	●	●	●		●	●	●	●	●	●	●
Inventario de Hardware y Software	●	●	●	●	●	●	●					
Antirrobo - alarma remota (Android)		●	●	●		●	●					
Foto al ladrón (Android)		●	●	●		●	●					
Monitorización de dispositivos con/sin agente					●	●	●					
Instalación y control de licencias centralizada de software					●	●	●					
Scripting y automatización de tareas					●	●	●					
Tienda de componentes - ComStore					●	●	●					
Ticketing / Help Desk / Chat					●	●	●					
Soporte MDM para móviles y tablets (iOS y Android)					●	●	●					



	Advanced Protection		Traditional Protection		Device Mgmt	Protection & Mgmt		IT Operations & Privacy & Data Control				Email	
	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Endpoint Protection	Panda Endpoint Protection+	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Panda Adv Reporting Tool	Panda Data Control	Panda Email Protection	
Control remoto					●	●	●						
Monitorización de equipos y servidores (CPU, Memoria, VMI, EventLog, etc)					●	●	●						
Gestión de Parches de Sistemas Operativos Windows y aplicaciones					Solo SO	Solo SO	Solo SO	●					
Gestión de aplicaciones en EoL								●					
Roll-back de aplicación de parches								●					
Posibilidad de deshabilitar Windows Update de forma centralizada								●					
Parcheo en tiempo real y mediante tareas programadas								●					
Cifrado/Descifrado completos de discos mediante BitLocker									●				
Administración, gestión y recuperación de claves centralizada									●				
Aplicación de políticas de cifrado centralizadas									●				
Dashboards, listados e informes sobre cifrado									●				
Dashboard, widget y consultas predefinidas de KPI's de seguridad										●			
KPI's de aplicaciones instaladas, ejecutadas y vulnerables										●			
KPI's de acceso a datos en los endpoints										●			
KPI's de aplicaciones ejecutadas - Shadow IT										●			
Inventario y Clasificación de ficheros con información personal (PII) <sup>1</sup>											●		
Monitorización de ficheros PII (datos en uso, reposo y tránsito) <sup>2</sup>											●		
Búsquedas guiadas por el usuario sobre ficheros PII y no PII											●		
Eliminación de ficheros con PII											●		
Consolas de administrador y usuario												●	
Técnicas avanzadas contra suplantación de identidad (antispoofting, DKIM, DMARC, etc)												●	
Antispam avanzado tecnología propietaria												●	
Cuarentena centralizada gestionada por el administrador o por cada usuario												●	
Comunicación segura obligatoria (TLS) para destinatarios elegidos												●	
Backup de correo entrante												●	
Notificador de correo en los endpoints												●	
Validación estricta de emisores de correo												●	
Compatible con Windows	●	●	●	●	●	●	●	●	●	●	●	●	Perimetral
Compatible con Exchange		●		●	●	●	●			●	●	●	Perimetral
Compatible con macOS X		●	●	●	●	●	●			●	●	●	Perimetral
Compatible con Linux		●	●	●	●	●	●			●	●	●	Perimetral
Compatible con Virtual systems	●	●	●	●		●	●			●	●	●	Perimetral
Compatible con Android		●	●	●	●	●	●			●	●	●	Perimetral
Compatible con iOS					●	●	●						Perimetral

Los módulos Panda Advanced Reporting Tool y Panda Data Control están disponibles únicamente para Panda Adaptive Defense y Panda Adaptive Defense 360. Los módulos de Panda Patch Management y Panda Full Encryption están disponible para Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Fusion, Panda Adaptive Defense y Panda Adaptive Defense 360.

Para más información o para solicitar una prueba gratuita de Panda Security Solutions, visita: [pandasecurity.com/business](https://pandasecurity.com/business)

<sup>1</sup> Consola única en la nube: Gestión centralizada independientemente de la ubicación que reduce el coste en infraestructura y mantenimiento

<sup>2</sup> Datos en reposo (data at rest), operaciones sobre ellos (data in use) y en tránsito (data in motion)

<sup>3</sup> Consola Aether en la nube y única para todas las soluciones y módulos endpoint de Panda Security

<sup>4</sup> Consola en la nube de Panda Cloud Systems Management

<sup>5</sup> Consola en la nube Panda Cloud de la cual se accede a las consolas de Panda Cloud System Management y de Panda Endpoint Protection Plus y de Panda Adaptive Defense 360

<sup>6</sup> Consola en la nube de Panda Email Protection

<sup>7</sup> Intrusion Detection System/ Host-based Intrusion Prevention System

<sup>8</sup> Personally Identifiable Information (Información personalmente identificable)