# Panda Adaptive Defense 360

Seguridad Automatizada y Avanzada
**Ponga fin a las amenazas informáticas**

panda
a WatchGuard brand

## SEGURIDAD CIBERNÉTICA ORGANIZACIONAL

La movilidad, el procesamiento y el almacenamiento en la nube revolucionaron el entorno empresarial. **Los endpoints son el objetivo principal de la mayoría de los ataques informáticos**. Es por eso que las soluciones de seguridad de endpoint deben ser **avanzadas, adaptables y automáticas**, con los máximos niveles posibles de **prevención** y **detección**.

**Las organizaciones reciben miles de alertas de malware cada semana**, de las cuales solo el 19% se considera confiable y solo el 4% se investiga. **Dos tercios del tiempo de un administrador de seguridad cibernética** se dedica **a la administración de las alertas de malware**.

## SOFISTICACIÓN DE LOS ATAQUES INFORMÁTICOS

### Ciber-Defensa contra las Amenazas Avanzadas

Los **ataques informáticos** de avanzada están diseñados para evadir la protección que proporcionan las soluciones de seguridad tradicionales. Estos ataques se están haciendo **más frecuentes** y **más sofisticados** a medida que los hackers se vuelven más profesionales. Esto también se debe a la falta de enfoque en la corrección de la **vulnerabilidades de seguridad en los sistemas**.

En este contexto, **las plataformas de protección tradicionales (EPP) no alcanzan**. Esto se debe a que **no proporcionan suficiente visibilidad y detalles** de los procesos y las aplicaciones que se ejecutan en las redes corporativas. Además, **algunas soluciones de EDR**, lejos de brindar soluciones, **generan mayor estrés** y aumentan la carga de trabajo de los administradores de seguridad, **ya que delegan la responsabilidad de administrar alertas y los obligan a clasificar las amenazas manualmente**.

## PANDA ADAPTIVE DEFENSE 360

### La solución de EDR: Detección y Respuesta en el Endpoint

**Panda Adaptive Defense 360** es una solución de seguridad cibernética innovadora para computadoras, computadoras portátiles y servidores que se entrega desde la nube. **Automatiza la prevención, detección, contención y respuesta relacionadas** con cualquier amenaza avanzada, malware de día cero, ransomware, suplantación de identidad, vulnerabilidad en la memoria o ataque sin malware, tanto presentes como futuros y dentro y fuera de la red corporativa.

A diferencia de otras soluciones, **combina** la más amplia variedad de **tecnologías de protección (EPP) con capacidades automatizadas de EDR**. Además, tiene **dos servicios, administrados por los expertos de Panda Security**, que se ofrecen como funcionalidad de la solución:

- **Servicio de Implementación de Confianza Cero**
- **Servicio de Búsqueda de Amenazas**

Gracias a su arquitectura en la nube, el agente es liviano y tiene poco impacto en los endpoints, que se administran mediante una arquitectura de nube única, incluso cuando están aislados.

Es posible acceder a **Panda Adaptive Defense 360** desde una consola web única. **Integra plataformas de administración y protección en la nube** (Aether), que maximizan la prevención, detección y respuesta automatizada, lo cual, a su vez, minimiza el esfuerzo necesario.

## BENEFICIOS

### Simplifica y Minimiza los Costos de Seguridad

- Sus servicios administrados reducen los costos de personal especializado. No hay falsas alertas que administrar y no se delegan responsabilidades.
- Los servicios administrados aprenden sobre las amenazas de manera automática. No se pierde tiempo en configuraciones manuales.
- Máxima prevención de endpoints. Los costos operativos se reducen casi a cero.
- No es necesario instalar, configurar ni mantener ninguna infraestructura de administración.
- El rendimiento del endpoint no se ve afectado, ya que se basa en un agente liviano y arquitectura nativa de la nube.

### Automatiza y Reduce el Tiempo de Detección

- Las aplicaciones que representan un riesgo de seguridad se bloquean (mediante hash o nombre de proceso).
- Bloquea la ejecución de amenazas, malware de día cero, ataques sin archivos/sin malware, ransomware y suplantación de identidad.
- Detecta y bloquea la actividad maliciosa en la memoria (vulnerabilidades) antes de que pueda causar daño.
- Detecta los procesos maliciosos que evadieron las medidas preventivas.
- Detecta y bloquea las técnicas, tácticas y procedimientos de ataque.

### Automatiza y Reduce el Tiempo de Respuesta e Investigación

- Resolución y respuesta: información forense para investigar a fondo cada intento de ataque y herramientas para mitigar sus efectos (desinfección).
- Rastreabilidad de cada acción y visibilidad práctica del atacante y su actividad, lo que facilita la investigación forense.
- Mejora y ajuste de políticas de seguridad, gracias a las conclusiones del análisis forense.

panda
a WatchGuard brand

## SEGURIDAD DE ENDPOINTS AVANZADA Y AUTOMATIZADA

Las técnicas de protección tradicional (EPP), enfocadas en la prevención, son medidas de bajo costo que resultan válidas para amenazas conocidas y comportamiento malicioso, pero no son suficientes. Para defender correctamente una organización y lograr que las amenazas cibernéticas lleguen a su fin, es necesario alejarse de la prevención tradicional y virar hacia la prevención, detección y respuesta continuas, asumiendo en todo momento que la organización está en peligro y que todos los endpoints sufren la amenaza constante de los atacantes.

**Panda Adaptive Defense 360** integra tecnologías preventivas tradicionales con tecnologías de prevención, detección y respuesta innovadoras, adaptables en una única solución para lidiar con las amenazas cibernéticas avanzadas, tanto presentes como futuras:

### Tecnologías Preventivas Tradicionales

- Firewall personal o administrado. IDS
- Control de dispositivos
- Antimalware y análisis a pedido multivector permanentes
- Listas negras/blancas administradas.
- Inteligencia Colectiva
- Heurística previa a la ejecución
- Filtrado de URL y navegación web
- Filtro de correo no deseado y protección contra suplantación de identidad
- Protección contra alteraciones
- Filtro de contenido del correo electrónico
- Corrección y reversión

### Tecnologías de Seguridad Avanzadas

- EDR: supervisión continua de endpoints
- Prevención de la ejecución de procesos desconocidos
- Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.)
- Sandboxing en entornos reales
- Análisis del comportamiento y detección de indicadores de ataques (IoA), como scripts, macros, etc.
- Detección y respuesta automáticas de los ataques dirigidos y las vulnerabilidades en la memoria
- Búsqueda de amenazas y análisis forense

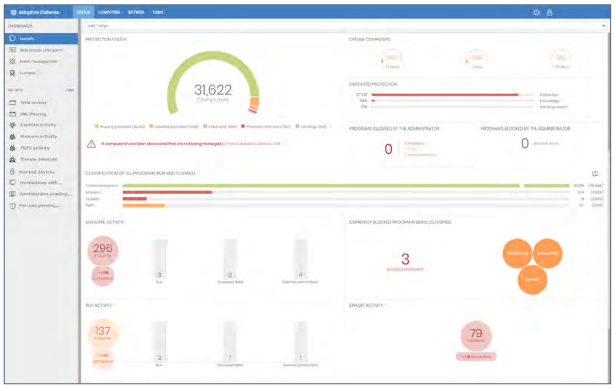


**Figura 1:** Panel de Control Principal de Panda Adaptive Defense.

## MODELO DE CONFIANZA CERO

**Se trata del servicio administrado que clasifica el 100% de los procesos, supervisa la actividad del endpoint y bloquea la ejecución de aplicaciones y procesos maliciosos**. Para cada ejecución, envía un veredicto de clasificación en tiempo real de "malicioso" o "legítimo", sin incertidumbre y sin delegarlo al cliente. Todo esto es posible gracias a la capacidad, la velocidad, la capacidad de adaptación y la escalabilidad de la IA y el procesamiento en la nube.

El servicio unifica tecnología de **grandes datos** y técnicas de **aprendizaje automático** multinivel, incluido el **aprendizaje profundo**, que es el resultado de la supervisión y la automatización continuas de la experiencia y el conocimiento acumulados por el equipo de seguridad y amenazas de Panda.

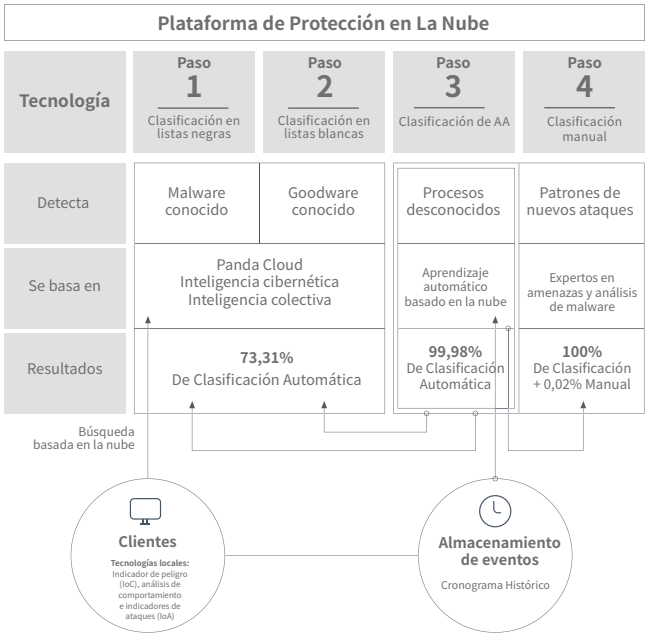


**Figura 2:** Secuencia de Servicio de Clasificación de la Nube.

**El servicio administrado de búsqueda de amenazas y análisis forense** está a cargo de un equipo de expertos que usan herramientas de correlación de eventos de análisis y elaboración de perfiles para detectar de manera proactiva nuevas técnicas de ataques y evasión.

Los cazadores del Centro de Inteligencia de Panda trabajan con la premisa de que las organizaciones están constantemente en peligro.

**Plataformas compatibles y requisitos de sistema de PANDA ADAPTIVE DEFENSE 360**

Sistemas operativos compatibles: Windows (Intel & ARM), macOS, Linux y Android. Las capacidades de EDR están disponibles en Windows, macOS y Linux, mientras que Windows es la plataforma que ofrece todas las capacidades completas.

Lista de exploradores compatibles: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge y Opera.

WatchGuard

VENTAS DE EE. UU.: 1.800.734.9905 VENTAS INTERNACIONALES: +1-206-613-0895 www.watchguard.com | pandasecurity.com