La Inteligencia Impulsada por Datos que Necesita para Estar Fuera del Alcance de las Vulneraciones

PANDA ADAPTIVE DEFENSE 360

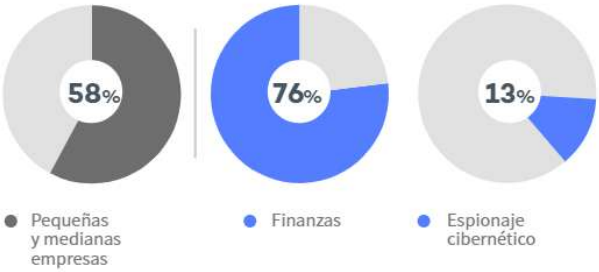
Panda Adaptive Defense 360 combina la tecnología de antivirus tradicional con el modelo de protección avanzado de detección y respuesta de endpoints en una solución única a fin de brindar protección contra las amenazas conocidas y desconocidas.

panda
a WatchGuard brand

EL PANORAMA DE AMENAZAS

¿De dónde vienen los ataques?[1]

¿Quiénes son las víctimas? ¿Cuáles son los fines?[1]



¿Qué costo tiene para las empresas?

- **Costo global:** 600.000 millones de dólares[2]
- **Costo de una vulneración de datos:** 3,86 millones de dólares[3]

LA EVOLUCIÓN DE LOS HACKERS

Los hackers son cada vez más sofisticados y numerosos como resultado de su profesionalización, las tecnologías que comparten y las permanentes filtraciones de inteligencia cibernética.

CÓMO ELIMINAR LA SUPERFICIE DE ATAQUE

Las amenazas cibernéticas de última generación que los hackers elaboran, están diseñadas para impedir que **las soluciones tradicionales** las detecten; por lo tanto, dejan a todas las redes vulnerables y sin las defensas apropiadas.

Las plataformas de protección tradicionales no alcanzan para hacer frente a los ataques avanzados, ya que no proporcionan suficiente visibilidad y detalles de los procesos y aplicaciones que se ejecutan en las redes corporativas. Para atender este problema, los departamentos de TI agregan protección adicional como las soluciones de detección y respuesta de endpoints (EDR). Las capacidades de EDR incluyen supervisión continua y análisis de datos de la actividad de la red, lo que ofrece a los departamentos de TI la información y la detección que necesitan para combatir amenazas avanzadas.

ADMINISTRACIÓN DE CARGA DE TRABAJO DE TI

Con la cantidad de máquinas que se implementan en la infraestructura corporativa cada año, los equipos de seguridad se enfrentan a dificultades para administrar y proteger a los dispositivos que residen tanto dentro como fuera de la red. Y a pesar de que las soluciones de EDR son parte esencial de la protección contra amenazas, la mayoría de ellas aumenta la dificultad para administrar el entorno de TI. Esto se debe, en gran medida, a la falta de automatización de la administración de la plataforma, ya que el equipo debe administrar las alertas que se generan y clasificar las amenazas manualmente.

SOLUCIONES DE DETECCIÓN Y RESPUESTA DE ENDPOINTS (EDR)

¿Cuál es la principal funcionalidad de las soluciones de EDR?

Las soluciones de EDR supervisan, registran y almacenan los detalles de la actividad de los endpoints, como los eventos de usuarios, los procesos, los cambios en el registro y el uso de memoria y de red. Esta visibilidad revela amenazas que, de otra manera, pasarían inadvertidas.

¿Cuáles son los problemas ocultos de las soluciones de EDR?

Se utilizan múltiples técnicas y herramientas para buscar anomalías de seguridad en los eventos y confirmar o rechazar alertas. Todo esto requiere intervención humana.

Las soluciones de EDR requieren supervisión durante las 24 horas, todos los días, además de personal altamente calificado que pueda brindar una rápida respuesta.

Estos recursos son costosos y difíciles de encontrar. Las organizaciones que disponen de personal limitado y cuentan con bajos presupuestos no están preparadas para aprovechar los beneficios de las soluciones de EDR por sus propios medios. El personal se encuentra ante mayores cargas de trabajo como resultado de la implementación y la ejecución de estas soluciones, en lugar de poder usarlas para lo importante: mejorar la posición de seguridad de su organización.

¿Cuál es la respuesta a este problema?

Panda Adaptive Defense 360.

[1] "2018 Data Breach Investigation report". Verizon
[2] "2018 Economic Impact of Cybercrime — No Slowing Down". CSIC/McAfee
[3] "2018 Cost of a Data Breach Study: Global Overview". Ponemon Institute/IBM Security

PANDA ADAPTIVE DEFENSE 360

Panda Adaptive Defense 360 es una innovadora solución de seguridad cibernética para computadoras de escritorio, computadoras portátiles y servidores que se ofrece desde la nube. Automatiza la prevención, la detección, la contención y la respuesta relacionadas con cualquiera de los ataques avanzados presentes o futuros, el malware de día cero, el ransomware, la suplantación de identidad, las vulnerabilidades de memoria y los ataques sin malware (dentro y fuera de la red corporativa).

Gracias a su arquitectura en la nube, el agente es liviano y no afecta el rendimiento de los endpoints, que se administran a través de una consola única en la nube, incluso cuando no están conectados a Internet.

Panda Adaptive Defense 360 integra plataformas de protección y administración en la nube (Aether) que maximizan la prevención, la detección y la respuesta automatizada, lo cual minimiza el esfuerzo requerido.

Se diferencia de otras soluciones ya que combina la más amplia variedad de tecnologías de protección del endpoint (EPP) con capacidades automatizadas de EDR, gracias a un servicio administrado por los expertos de Panda Security que se ofrece como funcionalidad de la solución: Servicio de Aplicaciones de Confianza Cero, que automatiza la administración de alertas y la toma de decisiones respecto a esas alertas.

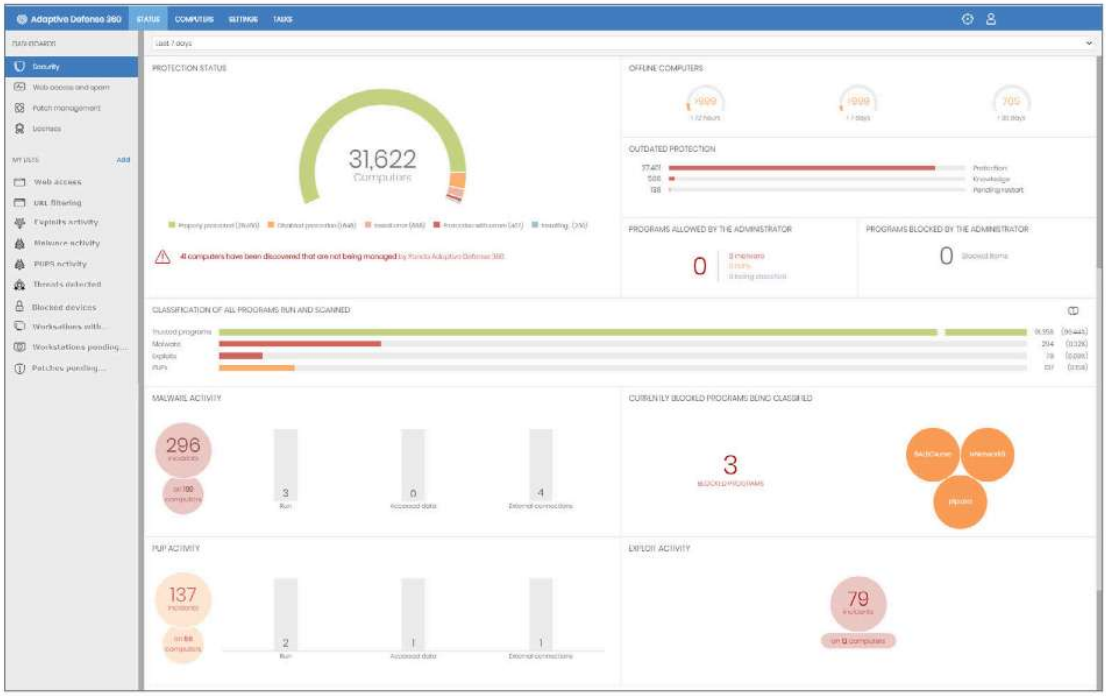


Figura 1: Panel de control principal de Panda Adaptive Defense 360.

BENEFICIOS PANDA ADAPTIVE DEFENSE 360

Simplifica y Minimiza el Costo de la Seguridad Avanzada y Adaptable

- Sus servicios administrados reducen el costo de personal especializado, lo cual elimina la responsabilidad de administrar alertas y tomar decisiones sobre qué hacer con ellas
- Los servicios administrados aprenden sobre las amenazas de manera automática, de modo que no se pierde tiempo en configuraciones manuales
- La máxima prevención en los endpoints reduce los costos operativos casi a cero
- No es necesario instalar, configurar ni mantener ninguna infraestructura de administración
- El rendimiento de los endpoints no se ve afectado, ya que se basa en un agente liviano y en la arquitectura en la nube

Automatiza y Reduce el Tiempo de Detección y Exposición (Tiempo de Permanencia)

- Impide la ejecución de amenazas, malware de día cero, ransomware y suplantación de identidad
- Detecta y bloquea la actividad maliciosa en la memoria (vulnerabilidades) antes de que cause problemas
- Detecta procesos maliciosos que evaden las medidas preventivas
- Detecta y bloquea técnicas y procedimientos de ataques informáticos

Automatiza y Reduce el Tiempo de Respuesta e Investigación

- Corrección automática y transparente
- Recuperación de actividad de endpoints y recuperación inmediata de actividad normal
- Insights prácticos de los atacantes y su actividad, lo que acelera la investigación forense
- Reducción de superficie de ataque, lo cual mejora de manera instantánea la posición de seguridad

REDUCCIÓN DE CARGA DE TRABAJO DE TI: SERVICIO DE CONFIANZA CERO DE APLICACIONES

El Servicio de Aplicaciones de Confianza Cero supervisa y evita la ejecución de aplicaciones y procesos maliciosos en los endpoints. Por cada ejecución, se emite de manera automática una clasificación en tiempo real, ya sea maliciosa o legítima, lo cual elimina la necesidad de intervención humana. Todo esto es posible gracias a la velocidad, la capacidad, la flexibilidad y la escalabilidad de la IA y el procesamiento en la nube.

El servicio combina big data con el aprendizaje automático de múltiples niveles, incluido el aprendizaje profundo, y está impulsado por la continua supervisión y automatización de la experiencia, la inteligencia y el conocimiento acumulados de expertos en seguridad y amenazas del centro de inteligencia de Panda Security.

Como ninguna otra solución del mercado, el Servicio de Aplicaciones de Confianza Cero puede liberar a los departamentos de TI del riesgo de ejecutar malware en endpoints dentro y fuera de la red corporativa.

Figura 2: Flujo de trabajo del Servicio de Aplicaciones de Confianza Cero en la nube.

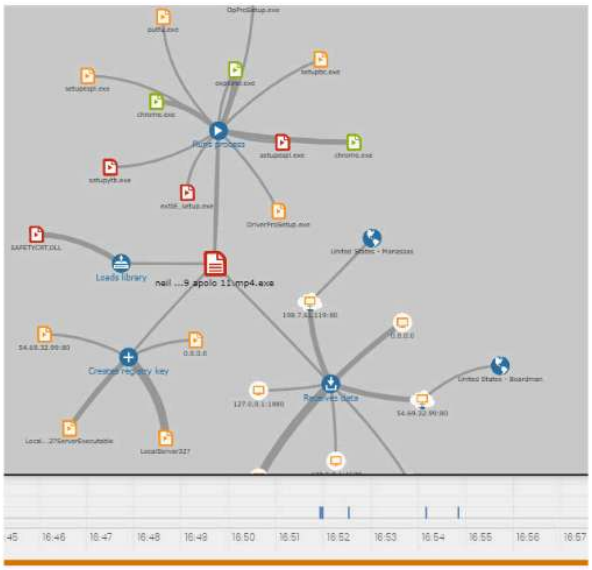


Figura 3: El cronograma de incidentes de la consola de Panda Adaptive Defense 360 permite la investigación forense: la fecha en que el incidente apareció por primera vez en la red, los nombres y el número de endpoints afectados, los cambios de configuración y con quién se comunicó.

SEGURIDAD AUTOMATIZADA AVANZADA EN LOS ENDPOINTS

Panda Adaptive Defense 360 integra, en una solución única, tecnologías preventivas tradicionales con capacidades de última generación para lograr prevención, detección y respuestas automatizadas contra las amenazas cibernéticas avanzadas.

Tecnologías Preventivas Tradicionales

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

Tecnología de Seguridad Avanzadas

- EDR: supervisión continua de la actividad del endpoint
- Prevención de la ejecución de procesos desconocidos
- Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.)
- Sandboxing basado en la nube en entornos reales
- Análisis de comportamientos y detección de IoA (scripts, macros, etc.)
- Detección automática de vulnerabilidades de memoria y respuesta automática a esas vulnerabilidades

PLATAFORMA DE PROTECCIÓN EN LA NUBE: AETHER

Seguridad, visibilidad y control de última generación. Integral y escalable desde la nube, para ofrecer servicios valiosos de inmediato.

La plataforma Aether y su consola en la nube optimizan la administración de seguridad avanzada y adaptable dentro y fuera de la red.

Está diseñada para que los equipos de seguridad se concentren solo en administrar la posición de seguridad cibernética de la organización, por lo que minimiza la complejidad y maximiza la flexibilidad, la granularidad y la escalabilidad.

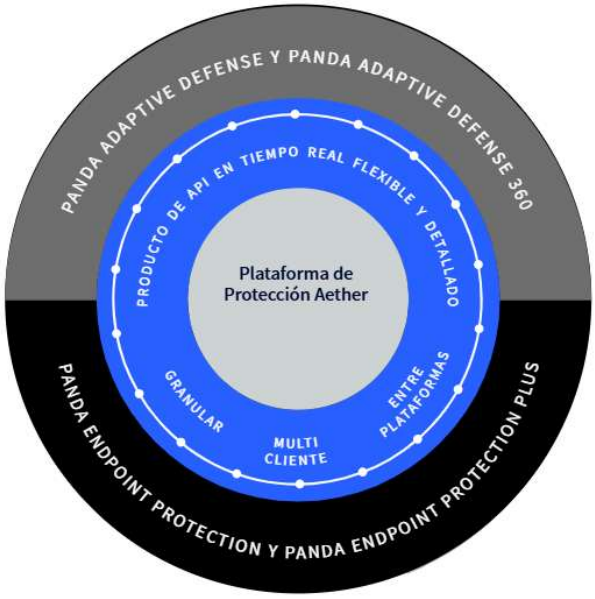


Figura 3: Plataforma de administración en la nube unificada: Aether

BENEFICIOS DE LA PLATAFORMA AETHER

Lograr Más Valor en Menos Tiempo Con Una Implementación Simple Que Provee Visibilidad Inmediata

- Implementación, instalación y configuración en minutos con valor agregado desde el primer día
- Agente ligero de múltiples productos y múltiples módulos que puede implementarse en todas las plataformas comunes (Windows, Mac, Linux, Android)
- Detección automática de endpoints desprotegidos e instalación remota
- Tecnología patentada de proxy, incluso en computadoras sin conexión web
- Optimización de tráfico, con tecnología propietaria/ tecnología caché

Fácil de Usar, Adaptable a Su Organización

- Consola basada en web intuitiva que brinda administración flexible y modular
- Roles predefinidos y personalizados
- Auditoría detallada de acciones en la consola
- Usuarios con visibilidad y permisos totales o restringidos
- Políticas de seguridad para grupos y endpoints
- Inventarios de hardware y software, y registro de cambios

Facilita la Supervisión que Acelera la Respuesta

- Indicadores clave de prioridades y paneles de control
- Alertas priorizadas y confirmadas en su flujo de trabajo
- Historial de incidentes completo y práctico: procesos relacionados, origen, tiempo de permanencia, prevalencia, etc.
- Actúe sobre los endpoints con un simple clic: reinicie, aísle, aplique parches y realice análisis para acelerar el tiempo de respuesta

PREMIOS Y CERTIFICACIONES

WatchGuard y Panda tienen el compromiso de someter sistemáticamente sus soluciones a pruebas y validaciones de terceros independientes. Nos enorgullece el reconocimiento que recibimos de organizaciones líderes de pruebas, como Virus Bulletin, AV-Comparatives, AV-Test y NSS Labs.

AV-Comparatives recomienda Adaptive Defense 360: "Debido a que esta solución clasifica todos los procesos ejecutados, no puede fallar en el registro de ningún malware".

Plataformas Compatibles y Requisitos de Sistema de Panda Adaptive Defense 360

Las plataformas compatibles están en continua evolución a fin de ofrecer la mayor cobertura posible para los sistemas operativos más nuevos. Puede acceder al soporte en línea para cada uno de nuestros productos a través de los siguientes enlaces:

Servidores y estaciones de trabajo de Windows: http://go.pandasecurity.com/endpoint-windows/requirements

Dispositivos con Mac OS: http://go.pandasecurity.com/endpoint-macos/requirements

Servidores y estaciones de trabajo de Linux: http://go.pandasecurity.com/endpoint-linux/requirements

Dispositivos móviles Android: http://go.pandasecurity.com/endpoint-android/requirements

Panda Patch Management: http://go.pandasecurity.com/patch-management/requirements

Panda Cloud Systems Management: http://go.pandasecurity.com/systems-management/requirements

SIEM Feeder: http://go.pandasecurity.com/siem-feeder/requirements

Advanced Reporting Tool: http://go.pandasecurity.com/reporting-tool/requirements

Panda Full Encryption: http://go.pandasecurity.com/full-encryption/requirements