Panda Adaptive Defense

Detección y Respuesta en Endpoints

panda
a WatchGuard brand

SEGURIDAD CIBERNÉTICA DE LA ORGANIZACIÓN

La movilidad, el procesamiento y el almacenamiento en la nube han revolucionado el entorno empresarial. **Las estaciones de trabajo son el objetivo principal de la mayoría de los ataques cibernéticos.** 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. **Un administrador típico de seguridad cibernética** dedica **dos tercios de su tiempo a la administración de alertas de malware**.[1]

LA SOFISTICACIÓN DE LOS ATAQUES INFORMÁTICOS

Ciber-Defensa Contra Amenazas Avanzadas

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

Frente a este panorama, las plataformas de protección tradicionales no alcanzan. Esto se debe a que no proporcionan suficiente visibilidad detallada de los procesos y aplicaciones que se ejecutan en las redes corporativas.

Además, **algunas soluciones de EDR**, lejos de ofrecer soluciones, **crean 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 amenazas **manualmente**.

PANDA ADAPTIVE DEFENSE

La Solución de EDR: Detección y Respuesta en el Endpoint

Panda Adaptive Defense es una solución de seguridad cibernética innovadora para computadoras, computadoras portátiles y servidores que se entrega desde la nube. **Automatiza la prevención, la detección, la contención y la 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.

Panda Adaptive Defense combina la más amplia variedad de **capacidades automatizadas de EDR**. También cuenta con **dos servicios administrados por expertos de Panda Security, que se entregan como una funcionalidad de la solución:**

- **Servicio de Aplicaciones de Confianza Cero**
- **Servicios de Búsqueda de Amenazas**

Gracias a su arquitectura en la nube, el agente es liviano y tiene poco impacto en el rendimiento del dispositivo, que se administra a través de una arquitectura de nube única, incluso cuando está aislado.

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

BENEFICIOS

Simplifica y Minimiza los Costos de Seguridad

- Sus innovadores servicios reducen los costos destinados a personal experto. No hay falsas alertas para administrar ni se delega responsabilidad.
- Los servicios aprenden de las amenazas automáticamente. No se pierde tiempo en configuraciones manuales.
- Se brinda máxima prevención en el endpoint. 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 (por 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 omitieron 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).
- Capacidad de rastrear cada acción; funcionalidades prácticas de visibilidad 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.

[1] El costo de la contención del malware según Ponemon Institute. También citado por Swimlane: https://swimlane.com/blog/cybersecurity-statistics-2017 y en otros estudios de terceros.

SEGURIDAD AVANZADA Y AUTOMATIZADA DE ENDPOINTS

Las técnicas de protección tradicional son medidas de bajo costo enfocadas en la prevención que resultan válidas para amenazas y comportamiento malicioso conocidos, pero son insuficientes. Para defender una organización y lograr que las amenazas cibernéticas lleguen a su fin, es necesario alejarse de la prevención tradicional y virar hacia la prevención, la detección y la respuesta continuas, asumiendo en todo momento que la organización está en peligro
y que todos los endpoints están constantemente bajo amenaza de atacantes.

Panda Adaptive Defense integra tecnologías preventivas tradicionales con capacidades innovadoras y adaptativas de prevención, detección y respuesta en una solución única a fin de lidiar con las amenazas cibernéticas avanzadas, tanto presentes como futuras:

- Tecnologías Preventivas Tradicionales
- Antimalware permanente multivectorial y análisis a pedido
- Listas negras/blancas administradas
- Inteligencia Colectiva
- Heurística previa a la ejecución
- Protección contra alteraciones
- Corrección y reversión
- Tecnologías de Seguridad Avanzadas
- EDR: supervisión continua 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 en entornos reales
- Análisis del comportamiento y detección de indicadores de ataques (IoA), como scripts, macros, etc.
- Búsqueda de amenazas y análisis forense

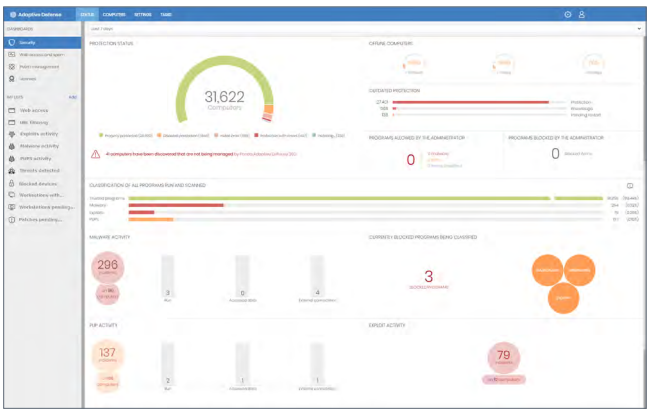

Figura 1: Panel de Control Principal de Panda Adaptive Defense.

SERVICIO DE CONFIANZA CERO DE APLICACIONES

Un servicio innovador que clasifica el 100% de los procesos, supervisa la actividad del endpoint y bloquea la ejecución de aplicaciones y procesos maliciosos. Para cada ejecución, se envía un veredicto de clasificación en tiempo real de "malicioso" o "legítimo", sin incertidumbre y sin la delegación 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 big data** y técnicas de **aprendizaje automático** multinivel, como el **aprendizaje profundo**, los resultados de la supervisión continua y la automatización de la experiencia y del conocimiento acumulados por el equipo de seguridad y amenazas de Panda Security.

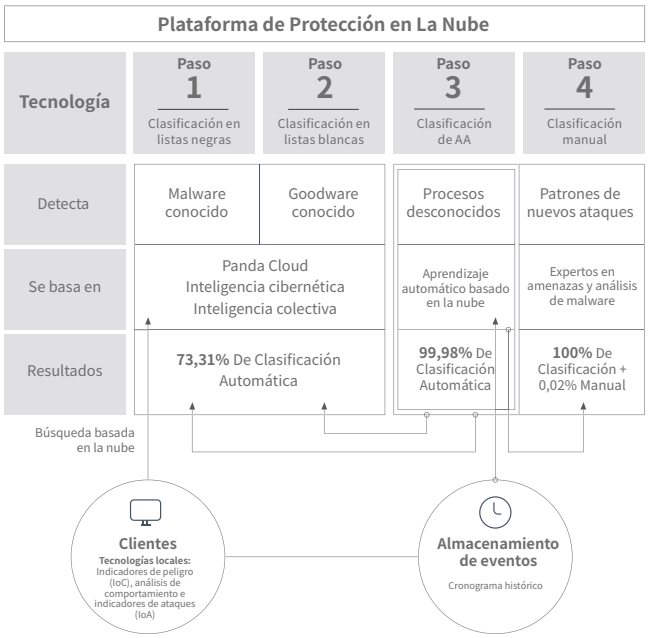

Figura 2: Secuencia de servicio de clasificación de la nube.

El servicio de búsqueda de amenazas 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

Sistemas operativos compatibles: Windows (Intel & ARM), macOS y Linux. Las capacidades de EDR están disponibles en Windows, macOS y Linux; Windows es la plataforma que proporciona todas las capacidades en su totalidad.

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

VENTAS EN EE. UU.: 1.800.734.9905 VENTAS INTERNACIONALES: +1.206.613.0895 www.watchguard.com | pandasecurity.com