Panda Adaptive Defense 360

Seguridad Automatizada y Avanzada
Ponga fin a las amenazas informáticas

panda
a WatchGuard brand

DESAFÍOS DE SEGURIDAD CIBERNÉTICA DE LA ORGANIZACIÓN

Los endpoints son el principal objetivo de la mayoría de los ataques cibernéticos y a medida que la infraestructura de la tecnología se vuelve más compleja, las organizaciones se esfuerzan por conseguir los conocimientos y los recursos necesarios para supervisar y administrar los riesgos de seguridad de endpoints. Entonces, ¿qué tipos de desafíos enfrentan las empresas cuando adoptan soluciones de seguridad para los endpoint?

- **Numerosas alertas:** 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.
- **Complejidad:** Demasiadas herramientas de seguridad cibernética, desconectadas entre si, pueden ser difíciles de administrar para por los profesionales de la seguridad, debido a la cantidad de tecnologías habilitadoras, la falta de habilidades internas y el tiempo requerido para identificar amenazas.
- **Rendimiento deficiente:** Con frecuencia las soluciones de seguridad para endpoints requieren la instalación y la administración de múltiples agentes en cada computadora de escritorio, servidor y computadora portátil supervisada, lo que genera errores graves, rendimiento deficiente y alto consumo de recursos.

Las técnicas tradicionales de protección de endpoints, enfocadas en la prevención, son válidas para amenazas conocidas y comportamientos maliciosos, pero no son suficientes contra las amenazas cibernéticas avanzadas. Desde los vectores de compromiso comunes hasta las nuevas amenazas, los atacantes siempre buscan maneras de liberarse de los avisos de TI, evadir las medidas de defensa y aprovechar las nuevas debilidades.

DE LA PREVENCIÓN A LA RESPUESTA – SEGURIDAD DE ENDPOINTS AUTOMATIZADA

Panda Adaptive Defense 360 es una solución de seguridad cibernética innovadora 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 cualquier amenaza avanzada, malware de día cero, ransomware, suplantación de identidad, vulnerabilidad en la memoria o ataque sin malware y sin archivo, dentro y fuera de la red corporativa.

A diferencia de otras soluciones, combina la más amplia variedad de tecnologías de protección de endpoints (EPP) con capacidades automatizadas de detección y respuesta (EDR). También cuenta con dos servicios administrados por expertos de Panda Security, que se brindan como una funcionalidad de la solución:

- **Zero-Trust Application Service:** clasificación del 100% de las aplicaciones
- **Threat Hunting Service:** detección de hackers e intrusos

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

Panda Adaptive Defense 360 integra tecnologías de endpoint tradicionales con protección innovadora y adaptable y tecnologías de EDR en una solución única, que permite a los profesionales de TI hacer frente a las amenazas informáticas avanzadas:

Tecnologías Preventivas Tradicionales

- Firewall personal o administrado (IDS)
- Control de dispositivos
- Inteligencia colectiva
- Lista de rechazos / lista de permisos
- Antimalware permanente multivectorial y análisis a pedido
- Heurística previa a la ejecución
- Filtrado de URL y navegación web
- Protección contra suplantación de identidad (Anti-phishing)
- Protección contra alteraciones
- Corrección automática y capacidad de reversión
- Recupere archivos cifrados con Shadow copies

Tecnologías de Seguridad Avanzadas

- Supervisión continua de endpoints con EDR
- Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.)
- Sandboxing en entornos reales
- Protección antiexploit
- Threat hunting, incluido el análisis del comportamiento y la detección de IoA (indicadores de ataques), para detectar ataques LotL (Living-off-the-Land).
- Indicadores de ataques asociados al marco de MITRE ATT&CK
- Detección y prevención de ataques de RDP
- Capacidades de contención y corrección, como el aislamiento de computadoras y el bloqueo de programas por hash o nombre del programa

Plataformas compatibles y requisitos de sistema de Panda Adaptive Defense 360

Sistemas operativos compatibles: Windows (Intel & ARM), macOS, Linux, iOS 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.

BENEFICIOS

Simplifica y Maximiza la Seguridad

- Sus servicios automatizados reducen los costos de personal especializado. No hay necesidad de administrar falsas alertas, no se pierde tiempo en configuraciones manuales y no se delegan responsabilidades.
- 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 en arquitectura nativa de la nube.

Fácil de Usar y Mantener

- El portafolio de seguridad de endpoints maneja todas las necesidades de protección de sus endpoints con una notable simplicidad desde una consola web única.
- Fácil de configurar. Plataforma cruzada de administración de endpoints desde una vista unificada.
- Ofrece un diseño de interfaz de usuario nuevo y visible que puede dominarse rápidamente.mastered.

Funcionalidades de EDR Automatizadas

- Detecta y bloquea técnicas, tácticas y procedimientos de ataques informáticos y la actividad maliciosa en la memoria (exploits) antes de que puedan causar daño.
- 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.

MODELO ZERO-TRUST: UNA PROTECCIÓN EN CAPAS

La plataforma de seguridad de endpoints de Panda Security no utiliza una única tecnología. Implementamos varias tecnologías juntas para reducir las posibilidades de que una amenaza se convierta en un ataque. Al trabajar de manera conjunta, estas tecnologías utilizan recursos del endpoint para minimizar el riesgo de una vulneración.

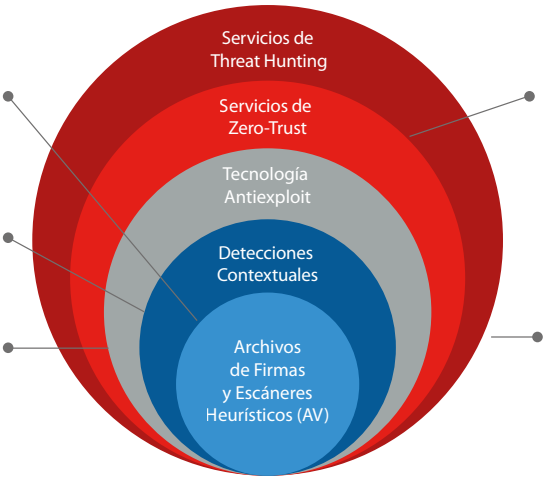
Modelo Zero-Trust: una protección en capas

CAPAS PARA ENDPOINTS:

Capa 1 - Archivos de Firmas y Tecnologías Heurísticas
Tecnología efectiva y optimizada para detectar ataques conocidos

Capa 2 - Detecciones Contextuales
Nos permiten detectar ataques sin malware y sin archivos

Capa 3 - Tecnología Antiexploit
Nos permite detectar ataques sin archivos diseñados para aprovechar vulnerabilidades



CAPAS NATIVAS DE LA NUBE

Capa 4 - Servicio de Zero-Trust de Aplicaciones
Ofrece detección en caso de que una capa anterior sea una vulnerabilidad, detiene los ataques a computadoras ya infectadas y los ataques de movimiento lateral dentro de la red

Capa 5 - Servicio de Threat Hunting
Nos permite detectar endpoints comprometidos, ataques en etapas iniciales, actividades sospechosas y la detección de IoA

Los archivos de firmas y tecnologías heurísticas, conocidas como protección de endpoint tradicional (EPP), conforman una capa de tecnología de antivirus de última generación que ha probado ser efectiva contra muchas amenazas comunes de bajo nivel y bloqueos de URL maliciosos.

La detección contextual es muy eficaz contra ataques basados en scripts, ataques con uso de herramientas de sistema operativo de goodware, como PowerShell, WMI, etc.; vulnerabilidades de navegadores web, y otras aplicaciones a las que se dirigen los ataques con frecuencia, como Java, Adobe, entre otras.

La tecnología Antiexploit permite buscar y detectar comportamientos anómalos. Cumple una función crítica en endpoints sin revisión o con revisiones por implementar y en endpoints con sistemas operativos que ya no son compatibles.

El Servicio de Zero-Trust Application clasifica el 100% de los procesos y prohíbe de manera predeterminada cualquier ejecución hasta que esté certificada como confiable. No hay necesidad de clasificar manualmente las amenazas ni de delegarlas a administradores de seguridad..

El Servicio de Threat Hunting se basa en un conjunto de reglas de búsqueda de amenazas, creado por especialistas en ciberseguridad, que se procesan de manera automática en todos los datos recolectados a partir de la telemetría, lo que identifica indicadores de ataque (IoA) que minimizan el tiempo de detección y respuesta (MTTD y el MTTR).

WatchGuard

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