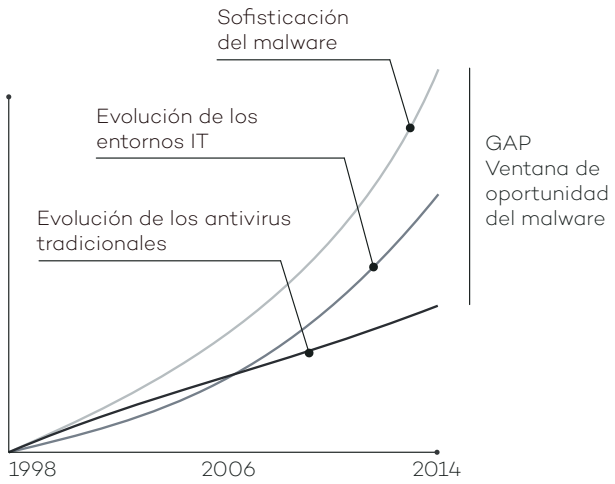
Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

DEFENSA AVANZADA PARA ENDPOINTS: PROTECCIÓN, DETECCIÓN, RESPUESTA Y REMEDIACIÓN EN UNA ÚNICA SOLUCIÓN

Defender tus dispositivos de un ataque no es sencillo. Tu protección debe incluir una amplia gama de mecanismos de defensa que incluya un antivirus/anti-malware tradicional, firewall personal, filtrado Web y de correo, y control de dispositivos. Además, toda protección debe proporcionar defensas adicionales contra amenazas difíciles de detectar, como ataques dirigidos y de día cero. Hasta ahora, las organizaciones informáticas tenían que recurrir a la compra y mantenimiento de productos distintos de diferentes proveedores para defender sus equipos.

Adaptive Defense 360 es el primer y único producto que combina funciones de protección (EPP) y detección y respuesta en el endpoint (EDR) en una única solución. **Adaptive Defense 360** automatiza tareas y funcionalidades, reduciendo la carga de trabajo del departamento informático. **Adaptive Defense 360** integra la solución EPP líder de Panda, que ofrece seguridad sencilla y centralizada, acciones de remediación, monitorización e informes en tiempo real, protección por perfiles, control centralizado de dispositivos, así como filtrado y monitorización Web.



Sin embargo, eso es sólo el principio. El panorama del malware y la seguridad informática ha sufrido un cambio fundamental en volumen y en sofisticación. La aparición de más de 200.000 nuevos virus cada día y la sofisticación de las técnicas de penetración y ocultación de malware ha hecho que las redes empresariales sean más vulnerables que nunca a los ataques dirigidos y de día cero.

Las soluciones tradicionales para la protección de dispositivos resultan eficaces a la hora de bloquear malware conocido mediante el uso de técnicas de detección basadas en ficheros de firmas y algoritmos heurísticos. Sin embargo, no resultan efectivas contra los ataques dirigidos y de día cero, capaces de aprovechar la 'ventana de oportunidad del malware': el tiempo que transcurre entre la aparición de un nuevo virus y su neutralización por parte de los proveedores de seguridad. Un tiempo cada vez mayor, aprovechado por los hackers para introducir virus, ransomware, troyanos y otros tipos de malware avanzado en las empresas. Estas amenazas, cada vez más habituales, podrían encriptar todos tus documentos confidenciales y pedirte una compensación monetaria como chantaje, o simplemente recoger información sensible para espionaje industrial.

Adaptive Defense es la solución de Panda a este tipo de ataques. Adaptive Defense ofrece un servicio de detección y respuesta en el endpoint capaz de clasificar cada aplicación de tu organización de forma precisa, permitiendo ejecutar únicamente lo que es lícito. Las funcionalidades EDR de Panda Adaptive Defense 360 se fundamentan en un modelo de seguridad basado en 3 principios: continua monitorización de las aplicaciones de los puestos y servidores de la empresa, clasificación automática mediante técnicas de Machine Learning en nuestra plataforma Big Data en la nube y, por último, la opción de que técnicos expertos analicen aquellas aplicaciones no clasificadas automáticamente, con el fin de conocer el comportamiento de todo aquello que se ejecuta en tu organización.

Estas funcionalidades se combinan ahora con la solución EPP líder de Panda, cerrando el ciclo de la **protección adaptiva contra el malware, que incluye prevención, detección, análisis forense y remediación automatizadas**.

La única solución que garantiza la seguridad de todas las aplicaciones ejecutadas

GARANTÍA DE PROTECCIÓN ROBUSTA Y COMPLETA

Panda Adaptive Defense 360 ofrece dos modos:

- **El Modo Estándar** permite la ejecución de las aplicaciones catalogadas como goodware, y de las aplicaciones todavía no catalogadas por los sistemas automatizados y Panda Security..
- **El Modo Extendido** permite únicamente la ejecución de aplicaciones goodware. El bloqueo extendido es la solución perfecta para empresas con objetivos de seguridad de tipo "riesgo cero".

INFORMACIÓN FORENSE

- **Visualiza mediante grafos de ejecución los eventos** desencadenados por el malware.
- Obtén información visual del destino de las comunicaciones del malware, los ficheros creados y mucho más con los Mapas de Calor.
- Localiza el software con vulnerabilidades conocidas instalado en tu red.

PROTECCIÓN ANTE SISTEMAS OPERATIVOS Y APLICACIONES VULNERABLES

La ausencia de actualizaciones hace que los sistemas no soportados por su proveedor original (como Windows XP), se conviertan en blanco automático de ataques de día cero y de nueva generación que aprovechan las vulnerabilidades del sistema.

Por otro lado, las vulnerabilidades de aplicaciones como Java, Adobe, Microsoft Office y navegadores son aprovechadas por el 90% del malware.

El módulo de protección contra vulnerabilidades incluido en Adaptive Defense 360 emplea reglas contextuales y de comportamiento, permitiendo a las empresas trabajar en un entorno seguro aunque dispongan de sistemas operativos o aplicaciones no actualizadas.

COMPLETA FUNCIONALIDAD EPP

Adaptive Defense 360 integra la solución EPP líder de Panda, que ofrece las siguientes características:

- Acciones de remediación
- Control centralizado de dispositivos, que previene la entrada de malware y la fuga de información mediante el bloqueo de distintos tipos de dispositivos
- Filtrado y monitorización Web
- Antivirus y anti-spam para Exchange Server
- Firewall en el endpoint, y mucho más...

INFORMACIÓN CONTINUADA DEL ESTADO DE LA RED

Recibe alertas inmediatas en el momento en que se identifique malware en la red, con un informe completo detallando su localización, las máquinas infectadas y las acciones realizadas por el malware.

Recibe informes por email con la actividad diaria del servicio.

MÓDULO SIEM DISPONIBLE

Adaptive Defense 360 se integra con soluciones SIEM, agregando información detallada sobre la actividad de todas las aplicaciones ejecutadas en los puestos.

Para aquellos clientes que no dispongan de un SIEM, Adaptive Defense 360 incorpora su propio sistema de almacenamiento y gestión de eventos de seguridad para el análisis en tiempo real de toda la información recabada.

SERVICIO 100% GESTIONADO

Olvídate de invertir recursos en personal técnico para gestionar cuarentenas, ficheros sospechosos o desinfecciones y reinstalaciones de los equipos infectados Adaptive Defense 360 clasifica todas las aplicaciones de forma automática mediante técnicas de Machine Learning en nuestros entornos Big Data bajo la continua supervisión de los técnicos especializados de PandaLabs, que controlan en todo momento el proceso.

REQUISITOS TÉCNICOS

Consola Web

- Conexión a Internet
- Internet Explorer 10
- Microsoft Edge
- Firefox (última versión)
- Google Chrome (última versión)

Agente

- Sistemas operativos (estaciones): Windows XP SP2 o superior (Vista, Windows 7, 8, 8.1 y 10)
- Sistemas operativos (servidores): Windows Server 2003 / 2008 / 2012 / 2016
- Conexión a Internet (directa o mediante proxy)

Soporte parcial (sólo EPP):

- Linux, MAC OS X y Android