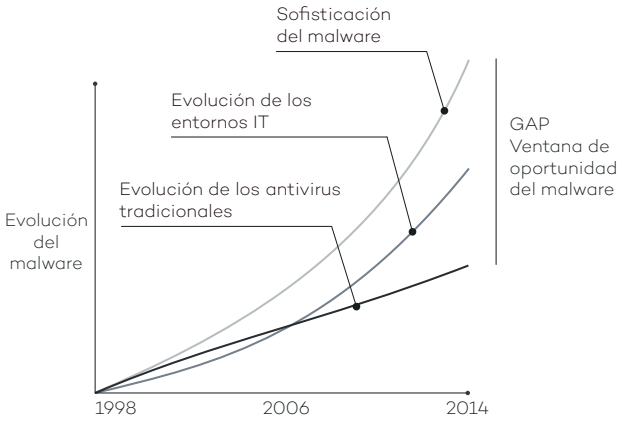
Adaptive Defense

Visibilidad sin Límites, Control Absoluto

Cierra la ventana de oportunidad de las nuevas amenazas avanzadas

¿CREES QUE TU ORGANIZACIÓN ESTÁ PROTEGIDA CONTRA ATAQUES DIRIGIDOS O ZERO-DAY?

El panorama del malware y la seguridad informática ha sufrido un cambio fundamental en volumen y en sofisticación.En volumen con un incremento exponencial de los virus en circulación (cerca de 300.000 nuevas muestras aparecen cada día) y en sofisticación, con nuevas técnicas de penetración y ocultación que les permite establecerse en las redes de las empresas durante largos periodos de tiempo.



Al mismo tiempo, los entornos IT han aumentado significativamente en complejidad, dificultando su gestión y aumentando su vulnerabilidad.

Sin embargo, los antivirus tradicionales se han quedado atrás. Su evolución lineal implica continuar utilizando las antiguas técnicas de detección basadas en ficheros de firmas y algoritmos heurísticos. Esto implica resultados poco precisos, es decir, malware sin detectar y generación de falsos positivos.

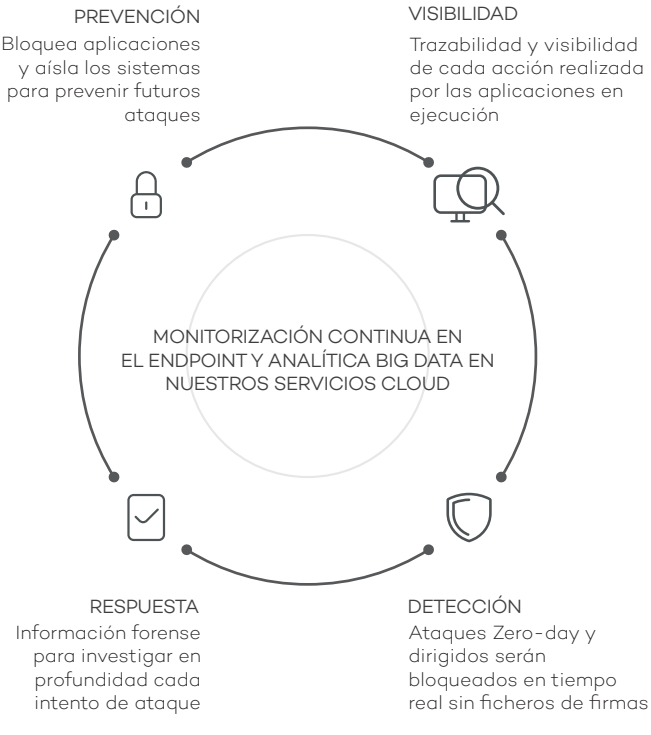
Esta discrepancia ha generado lo que denominamos **"ventana de oportunidad del malware"**: el lapso de tiempo entre la aparición de un nuevo virus y su neutralización por parte de los proveedores de seguridad. Un tiempo cada vez mayor, aprovechado por los hackers para introducir virus, ransomware, troyanos 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.

Gobiernos, bancos y otras grandes empresas están sufriendo ya este tipo de ataques que los antivirus tradicionales no son capaces de detectar a tiempo.

Según mediciones realizadas por nuestro departamento de Research con millones de muestras de virus y los mejores antivirus del mercado, el 18% del malware nuevo no es detectado en las 24 primeras horas e incluso al cabo de 3 meses, los antivirus tradicionales siguen sin detectar un 2% del malware.

La solución a estos problemas es **Adaptive Defense**: nuestro servicio capaz de clasificar cada aplicación de tu organización de forma precisa, permitiendo ejecutar únicamente lo que es lícito.

Para conseguirlo, hemos trabajado durante los últimos 5 años en un **nuevo 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.



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

GARANTÍA DE PROTECCIÓN ROBUSTA Y COMPLETA

Panda Adaptive Defense ofrece dos modos de operación:

- 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** únicamente permite 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 la red.

COMPATIBILIDAD CON SOLUCIONES DE ANTIVIRUS TRADICIONALES

Adaptive Defense puede coexistir con antivirus tradicionales convirtiéndose en la **herramienta corporativa definitiva para bloquear todo tipo de malware, incluyendo ataques dirigidos y de zero-day** que las soluciones tradicionales de seguridad no son capaces de detectar.

PROTECCIÓN ANTE SISTEMAS OPERATIVOS Y APLICACIONES VULNERABLES

Debido a la ausencia de actualizaciones, sistemas no soportados por su proveedor original (como Windows XP) se convierten en blanco automático de ataques zero-day 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 utiliza reglas contextuales y de comportamiento, permitiendo a las empresas trabajar en un entorno seguro aunque dispongan de sistemas operativos o aplicaciones no actualizadas.

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, máquinas infectadas y acciones realizadas por el malware.
- Recibe informes por e-mail con la actividad diaria del servicio.

MÓDULO SIEM DISPONIBLE

Adaptive Defense 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 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 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)