Panda Patch Management

Reduzca los riesgos y la complejidad de administrar vulnerabilidades en sistemas y aplicaciones de terceros

panda
a WatchGuard brand

En la actualidad, **el 99,96% de las vulnerabilidades activas** en los endpoints corporativos se relacionan con la **falta de actualizaciones**.[1] Si estas actualizaciones se instalaran, contribuirían en gran medida a evitar los riesgos de seguridad. De hecho, según Ponemon Institute[2], **el 57% de las víctimas** de ataques informáticos afirmó que aplicar **un parche hubiera evitado** el ataque y el **34%** reconoció que conocía la vulnerabilidad antes del ataque.

Además, el **86% de las vulnerabilidades** se debe a **aplicaciones de terceros** sin parchear, como Java, Adobe, Firefox, Chrome, Flash y OpenOffice, entre otras.[1]

SIN DUDA, ES MOMENTO DE CAMBIAR ESTA TENDENCIA CON PANDA PATCH MANAGEMENT

Panda Patch Management es una **solución fácil de usar que sirve para administrar las vulnerabilidades de los sistemas operativos y las aplicaciones de terceros** en estaciones de trabajo y servidores de Windows. **Reduce la superficie de ataque y**, al mismo tiempo, fortalece las capacidades de prevención y contención de su organización.

La solución no requiere nuevos agentes de endpoint ni consolas de administración y se integra completamente con todas las soluciones de endpoint de Panda Security.

Además, **proporciona visibilidad centralizada y en tiempo real** del estado de seguridad de las **vulnerabilidades de software**, los parches **faltantes, las actualizaciones y el software (EOL[3])** no compatibles, dentro y fuera de la red corporativa, así como herramientas fáciles de usar y en tiempo real para todo el ciclo de administración de la revisión: desde la detección y la planificación hasta la instalación y la supervisión.

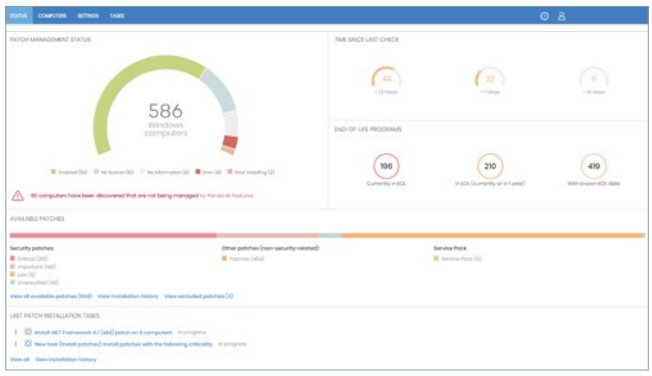


Figura 1: Estado de la organización con Patch Management: panel de control principal

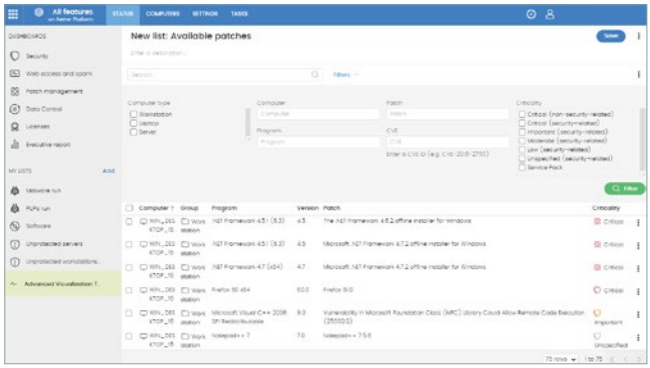


Figura 2: Parches disponibles: administración de Parches

VULNERABILIDADES: UN RIESGO LATENTE

Los **sistemas operativos y el software de terceros** sin parchear son el ambiente ideal para los ataques y las vulnerabilidades. Estas herramientas pueden aprovechar las vulnerabilidades para las cuales hay parches disponibles semanas o, incluso, meses antes de la vulneración.

La divulgación masiva de vulnerabilidades, como las expuestas por Shadow Brokers o WikiLeaks, con instrucciones detalladas sobre cómo poner en peligro sistemas y aplicaciones, permite que una mayor cantidad de criminales cibernéticos inicien ataques.

A causa de **la transformación digital**, es cada vez más difícil reducir la superficie de ataque, debido a la mayor cantidad de usuarios, dispositivos, sistemas y aplicaciones de terceros que requieren actualizaciones.

Como mínimo, **cinco problemas operativos comunes frustran los** programas de administración de vulnerabilidades (VM):

- **La detección de las vulnerabilidades es un proceso largo.** Sin embargo, el tiempo de respuesta frente a incidentes debe ser inmediato.
- **Las empresas están descentralizadas** y los empleados no están conectados continuamente a la red corporativa. **Las herramientas de VM en las instalaciones** no abarcan estos escenarios.
- La mayoría de las herramientas de VM requieren **otro agente específico** en los endpoints que ya están sobrecargados.
- La herramienta de VM de Microsoft no permite a las organizaciones realizar actualizaciones centralizadas y unificadas de **aplicaciones de terceros.**
- Otras soluciones de seguridad que ofrecen la administración de parches **no correlacionan la detección con endpoints vulnerables** para acelerar la respuesta y la mitigación del ataque.

Soluciones compatibles dentro de la PLATAFORMA AETHER:

- Panda Endpoint Protection
- Panda Endpoint Protection Plus
- Panda Adaptive Defense
- Panda Adaptive Defense 360

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

Aplicaciones de terceros compatibles:
www.pandasecurity.com/business/PatchManagementApp

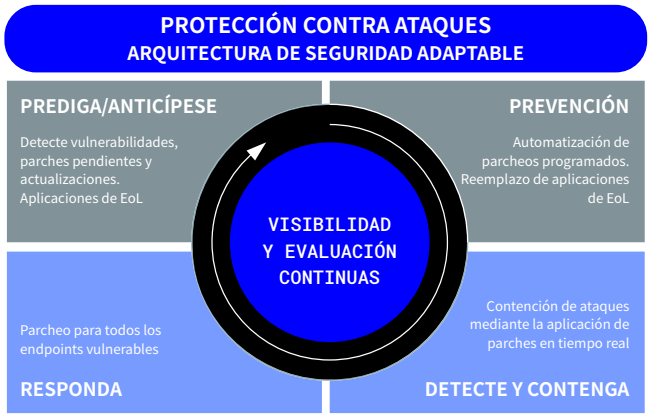
[1] **Gartner, Focus on the Biggest Security Threats, Not the most Publicized (Enfóquese en las Amenazas de Seguridad Más Importantes; no en las Más Publicitadas).** Publicado: 2 de noviembre de 2017. Las vulnerabilidades de día cero son solo el 0,4%; para el resto, el 99,96%, existen parches que las solucionan. Base de Datos Nacional de Vulnerabilidades. El 86% de las vulnerabilidades se encuentran en aplicaciones de terceros.
[2] **Costo y consecuencias de las brechas en la respuesta a las vulnerabilidades**, Ponemon.
[3] **EOL (Fin de Ciclo de Vida Útil): Un producto que está al final de su vida útil** (desde el punto de vista del proveedor), que es posible que ya no reciba actualizaciones de seguridad.

panda
a WatchGuard brand

BENEFICIOS

Con una **única solución fácil de usar,** Panda Patch Management le permite realizar lo siguiente:

- **Auditar, supervisar y priorizar las actualizaciones del sistema operativo y las aplicaciones.** La vista desde un solo panel ofrece visibilidad centralizada, actualizada y completa del estado de seguridad de la organización con respecto a las vulnerabilidades, los parches y las actualizaciones pendientes de los sistemas y cientos de aplicaciones.
- **Reducir sistemáticamente la superficie de ataque creada por las vulnerabilidades del software con el objetivo de evitar incidentes**. Esto se logra controlando los parches y las actualizaciones con herramientas de administración en tiempo real y fáciles de usar, que permiten a las organizaciones adelantarse a los ataques de aprovechamiento de vulnerabilidades.
- **Contener y mitigar los ataques de aprovechamiento de vulnerabilidades** con actualizaciones inmediatas. La consola de Panda Adaptive Defense 360, junto con Patch Management, permite a las organizaciones correlacionar las amenazas detectadas con las vulnerabilidades. El tiempo de respuesta se minimiza, lo que permite enviar parches de manera inmediata desde la consola web a fin de contener y corregir los ataques. Las computadoras afectadas pueden aislarse del resto de la red, lo que evita que el ataque se esparza.
- **Reducir el costo operativo:**
  - **Con Panda Patch Management, no es necesario implementar nuevos agentes de endpoint ni actualizar agentes existentes**, lo que simplifica la administración y evita la sobrecarga de la estación de trabajo y el servidor.
  - **Minimiza los esfuerzos de aplicación de parches, ya que las actualizaciones se inician de manera remota** desde la consola basada en la nube. Asimismo, la instalación se optimiza para minimizar errores.
  - **Proporciona visibilidad inmediata y completa de todas las vulnerabilidades**, las actualizaciones pendientes y las aplicaciones de EOL[3] instantáneamente después de la activación.
- **Cumplir con el principio de responsabilidad**, que forma parte de muchas regulaciones (GDPR, HIPAA y PCI). Esto obliga a las organizaciones a adoptar las medidas técnicas y organizativas correspondientes para garantizar la protección adecuada de los datos confidenciales bajo su control.



Panda Patch Management aumenta las capacidades de prevención, detección y respuesta de las soluciones de endpoint de Panda Security. Para ello, permite la implementación sólida de la arquitectura de seguridad adaptable.[4]

FUNCIONALIDADES CLAVE

Panda Patch Management proporciona todas las herramientas necesarias para administrar la seguridad y las actualizaciones del sistema operativo y las aplicaciones de terceros desde una única consola:

Detección:

- Vista desde un solo panel con información en tiempo real de todas las computadoras vulnerables, los parches pendientes y el software no compatible (EOL[3]), junto con su estado de corrección.
- Información detallada sobre parches y actualizaciones pendientes, detalles de boletines de seguridad relevantes (CVE), información sobre la computadora y grupos de computadoras y más. Acciones disponibles:
  - Filtre y busque parches según importancia, computadoras, grupos, aplicaciones, parche, CVE y estado.
  - Capacidad de tomar medidas directamente en las computadoras: reiniciar, instalar en el momento o programar.
- Análisis desatendido de actualizaciones pendientes, en tiempo real o en intervalos periódicos (3, 6, 12 o 24 horas).
- Notificación de parches pendientes en detecciones de vulnerabilidades. Capacidad de iniciar instalaciones de manera inmediata o programarlas desde la consola y asilar la computadora, si es necesario.

Planificación y tareas de instalación de parches y actualizaciones:

- Configurables según la importancia.
- En endpoints y grupos específicos.
- Inmediatas, programadas para una ejecución única o para una ejecución repetida en intervalos regulares (fecha/hora).
- Capacidad de controlar los reinicios de la computadora y configurar excepciones.
- Reversión para desinstalar un parche que pueda provocar un conflicto inesperado con una configuración existente.

Supervisión del estado de actualizaciones y el endpoint mediante:

- Panel de control y listas prácticas.
- Reportes de alto nivel y detallados.
- Listas de computadoras actualizadas y computadoras con actualizaciones pendientes con errores.

Administración granular basada en grupos y roles con diferentes permisos:

- Visibilidad basada en roles de las computadoras vulnerables, los parches y los paquetes de servicio.

Control centralizado de actualizaciones, parches y software:

- Capacidad de desactivar Windows Update y administrar las actualizaciones del sistema operativo de manera centralizada.
- Capacidad de excluir parches específicos por versión y tipo.
- Capacidad de excluir software (p. ej., Java).

[4] **Gartner: "Designing an Adaptive Security Architecture for Protection from Advanced Attacks"** ("Cómo diseñar una arquitectura de seguridad adaptable para la protección contra los ataques avanzados"), Neil MacDonald, Peter Firstbrook.

WatchGuard

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

No se proporcionan garantías expresas ni implícitas. Todas las especificaciones están sujetas a cambios y todos los productos, funcionalidades o características previstos para el futuro se suministrarán según su disponibilidad. ©2020 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, el logotipo de WatchGuard y Panda Security son marcas registradas o marcas comerciales registradas de WatchGuard Technologies, Inc. en los Estados Unidos y/o en otros países. Las demás marcas o nombres comerciales son propiedad de sus respectivos propietarios. N.º de pieza WGCE67359_091720