Panda Patch Management

Reduce el riesgo y la complejidad de las vulnerabilidades en los sistemas y aplicaciones de terceros

A día de hoy, el **99,96% de las vulnerabilidades** activas en los entornos corporativos **tienen actualizaciones pendientes**, que, de aplicarse, se prevendría en gran medida el riesgo de seguridad. Asimismo, el **86%** de las **vulnerabilidades** se deben a **actualizaciones** no realizadas en **aplicaciones de terceros** como Java, Adobe, Mozilla, Firefox, Chrome, Flash, OpenOffice, entre otras[1].

De seguir con esta tendencia, en el 2.020, el 99% de las **vulnerabilidades causante de incidentes de seguridad**, serán conocidas y **podrían haberse evitado** si se hubieran actualizado antes del incidente[2].

ES HORA DE CAMBIAR ESTA TENDENCIA CON PANDA PATCH MANAGEMENT

Panda Patch Management, es una **solución intuitiva de gestión de las vulnerabilidades** de los sistemas operativos y aplicaciones de terceros, en estaciones y servidores Windows.
El resultado es una **reducción de la superficie de ataque**, fortaleciendo las capacidades preventivas, y de **contención ante incidentes**.

La solución, que no requiere de nuevos agentes ni consola de gestión propia, al estar **integrada en las soluciones endpoint** de Panda Security, proporciona **visibilidad en tiempo real** y centralizada del estado de las **vulnerabilidades**, **parches**, **actualizaciones** pendientes, y software no soportado (en EoL[3]), dentro o fuera de la red corporativa.

Sus herramientas de gestión automatizadas y en tiempo-real cubren desde el descubrimiento y planificación hasta la instalación y monitorización de parches y actualizaciones.

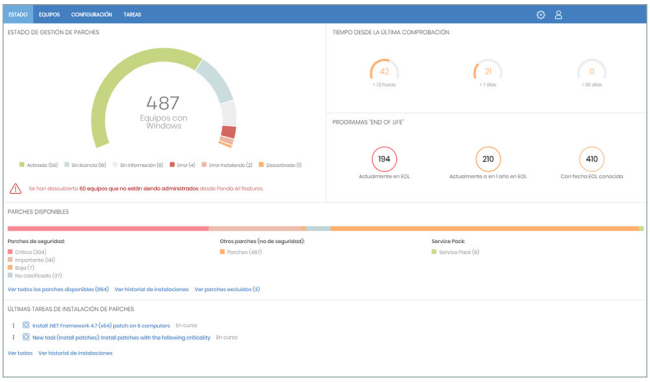

Figura 1: Panel principal del estado de la gestión de parches en el parque: parches disponibles, programas EoL, tareas de instalación, etc...

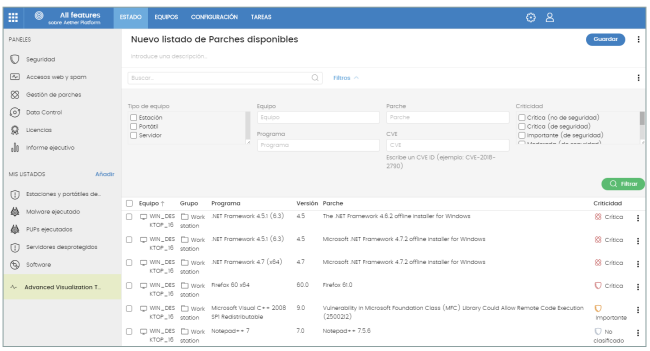

Figura 2: Listado de parches disponibles de los equipos en el parque.

LAS VULNERABILIDADES: UN RIESGO LATENTE

La mayoría de los ataques y exploits se aprovechan de los **sistemas y aplicaciones de terceros no actualizados**, explotando vulnerabilidades conocidas, para las que se dispone de una actualización semanas, incluso meses antes de la brecha.

La divulgación masiva de vulnerabilidades, como las conocidas del grupo Shadow Brokers o los WikiLeaks de ciber-inteligencia explicando cómo comprometer los sistemas, permite el acceso masivo de ciber-atacantes profesionalizados, y en continuo crecimiento, a información crítica de seguridad.

La Transformación Digital dificulta la tarea de reducir la superficie de ataque, debido al crecimiento exponencialmente de usuarios, dispositivos, sistemas y aplicaciones de terceros que requieren ser actualizados.

Al menos **cinco problemas comunes frustran** los programas de gestión de vulnerabilidades (VM):

- La **búsqueda de vulnerabilidades lleva horas**, pero ante un incidente, la **respuesta** para mitigar el daño debe de ser **inmediata**.
- Las **empresas están descentralizadas**, los empleados no se conectan a la red corporativa. Las **herramientas on-premise** de gestión de vulnerabilidades no cubre estos escenarios.
- La mayoría de las herramientas de VM requieren de **otro agente** a instalar y gestionar sobre equipos y servidores que ya están sobrecargados.
- La herramienta on-premise de VM de Microsoft **no cubren** la problemática de la actualización de **aplicaciones de terceros**, necesitando otra aplicación con una gestión no unificada.
- Otras soluciones de seguridad que incluyen gestión de vulnerabilidades, **no correlacionan detección** con endpoints **vulnerables** para acelerar la respuesta y frenar el ataque.

[1] Gartner, Focus on the Biggest Security Threats, Not the most Publicized. Published: 2 Noviembre 2017. Las vulnerabilidades latentes son de día cero son en el 0,4%, para el resto, 99,96%, existen actualizaciones para resolverlas. National Vulnerability Database. El 86% de las vulnerabilidades afectan a aplicaciones de terceros.
[2] Gartner, How to Respond to the 2018 Threat Landscape. Greg Young. Published: 28 Noviembre 2017.
[3] Aplicaciones en su fase de "fin de vida" (End of Life), vulnerables por defecto, al limitarse o terminar su soporte o corrección.

Panda Patch Management

BENEFICIOS

Panda Patch Management permite en una única **solución**:

- **Auditar, monitorizar y priorizar las actualizaciones de los sistemas operativos y aplicaciones.** Un panel único en la consola centraliza, actualizado en tiempo real, permite una visibilidad agregada del estado de los parches y actualizaciones pendientes del sistema y cientos de aplicaciones de terceros.
- **Prevenir incidentes, reduciendo sistemáticamente la superficie de ataque por vulnerabilidades**. La gestión de parches y actualizaciones con herramientas de gestión, fáciles e intuitivas, permiten adelantarse a la explotación de vulnerabilidades.
- **Contener y mitigar ataques que explotan vulnerabilidades,** aplicando inmediatamente las actualizaciones críticas desde la consola Cloud. La consola correlaciona detecciones con vulnerabilidades, minimizando así el tiempo de respuesta, contención y remediación mediante la actualización necesaria desde la consola. Adicionalmente, permite aislar de la red los equipos afectados, mitigando así la expansión al ataque.
- **Reducir los costes operativos.**
  - **No requiere ni despliegues ni actualizaciones de agente en los endpoints**, simplificando la gestión son sobrecargar los equipos y servidores.
  - **Minimiza el esfuerzo de las actualizaciones** remotas desde la consola Cloud. Además, la aplicación de parches está optimizada para minimizar errores.
  - **Visibilidad inmediata y desatendida** de las vulnerabilidades, actualizaciones y aplicaciones en EoL[3], tras la activación.
- **Cumplir con el principio de responsabilidad activa**, requisito en muchas regulaciones (GDPR, HIPAA y PCI), que obliga a las organizaciones a establecer todas las medidas que garanticen la protección de datos sensibles bajo su responsabilidad.

Panda Patch Management multiplica las capacidades preventivas, de detección y respuesta de las soluciones de seguridad endpoint de Panda Security, al permitir una implementación robusta de la Arquitectura Adaptativa de Seguridad[4]

[4] Gartner: "Designing an Adaptive Security Architecture for Protection from Advanced Attacks", Neil MacDonald, Peter Firstbrook

FUNCIONALIDADES CLAVE

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

Descubrimiento:

- Panel único de equipos vulnerables, parches pendientes y aplicaciones en EoL[3] junto con el estado de su remediación, en tiempo real.
- Desglose de parches y actualizaciones pendientes y detalles del boletín de seguridad correspondiente (CVE) con información de máquinas y grupos, entre otros. Sobre ellos se puede:
  - Filtrar y buscar por criticidad, equipo, grupo, aplicación, parche, CVE y estado.
  - Tomar acciones directamente en los equipos: reiniciar, instalar ahora o programar.
- Búsquedas de actualizaciones pendientes, en tiempo-real o periódica (3, 6, 12 o 24 horas).
- En detecciones de exploits y programas maliciosos, se notifica de los parches pendientes. La instalación se lanza inmediatamente o se programa desde la consola, aislando el equipo si es necesario.

Tareas de planificación e instalación de parches y actualizaciones:

- Configurables por criticidad.
- Sobre grupos o endpoints específicos.
- Inmediatas o programadas una vez o cíclicamente en una fecha y hora.
- Con gestión controlada de los reinicios y excepciones.
- Rollback para la desinstalación de parches que podrían haber causado conflictos inesperados en la configuración.

Monitorización del estado de los endpoints y sus actualizaciones, mediante:

- Panel de control y listado accionables.
- Informes de alto nivel y detallados.
- Lista de equipos actualizados, con actualizaciones pendientes o en error.

Gestión granular por grupos y roles con permisos:

- Visibilidad de equipos vulnerables, parches y actualizaciones pendientes en función del rol.

Control centralizado de actualizaciones, parches y software:

- Posibilidad de deshabilitar Windows Update y gestionar las actualizaciones del sistema operativo de manera centralizada.
- Posibilidad de excluir parches específicos tanto por versiones como por familias.
- Capacidad de excluir software (por ejemplo: Java).

Soluciones compatibles sobre 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/requisitos

Aplicaciones de terceros soportadas:
https://www.pandasecurity.com/business/PatchManagementApp