Panda Patch Management

Reduza o risco e a complexidade da gestão de vulnerabilidades nos sistemas e aplicações de terceiros

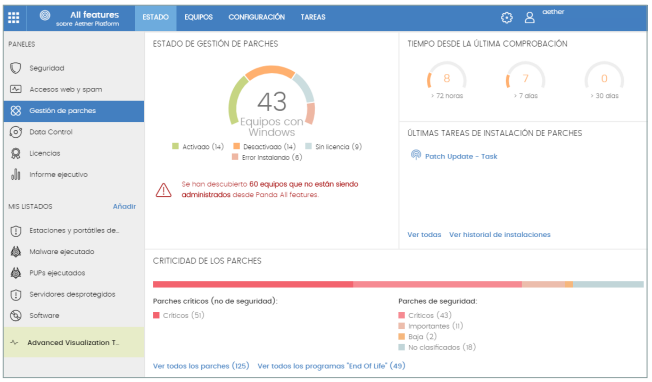
Actualmente, 99.96% das vulnerabilidades activas nos endpoints corporativos estão relacionadas com actualizações por realizar que, se fossem instaladas, iriam prevenir largamente o risco de segurança. Além disso, 86% dos endpoints corporativos não têm instalados patches críticos de aplicações de terceiros, tais como Java, Adobe, Mozilla Firefox, Chrome, Flash, Open Office, entre outros.[1]

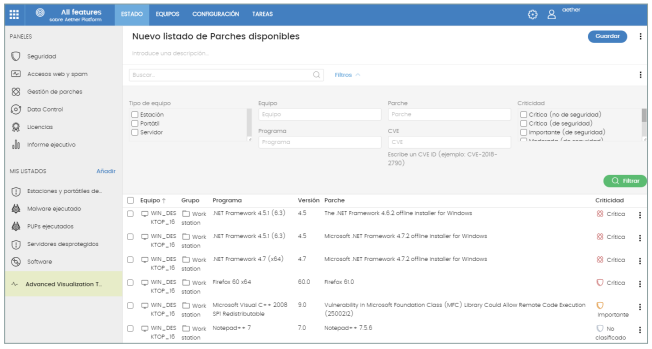
Caso esta tendência continue, em 2020, 99% das vulnerabilidades causadoras de incidentes de segurança serão exploits conhecidos que poderiam facilmente ter sido evitados se os patches tivessem sido aplicados antes do incidente.[2]

ESTÁ NA ALTURA DE INVERTER A TENDÊNCIA COM O PANDA PATCH MANAGEMENT

O Panda Patch Management é uma solução intuitiva de gestão das vulnerabilidades dos sistemas operativos e aplicações de terceiros, em postos de trabalho e servidores Windows. O resultado é uma reduçao da superfície de ataque, fortalecendo as capacidades preventivas e de contenção perante incidentes.

A solução não requer novos agentes ou uma consola de gestão própria, uma vez que está integrada nas soluções endpoint da Panda Security e proporciona visibilidade em tempo real e centralizada do estado das vulnerabilidades, patches, actualizações pendentes e software não suportado (EOL[3]), dentro ou fora da rede corporativa, bem como ferramentas de fácil utilização e em tempo real ao longo de todo o ciclo de vida da gestão de patches: desde a sua detecção e planeamento à instalação e monitorização.





VULNERABILIDADES: UM RISCO LATENTE

A maioria dos ataques e exploits aproveitam-se de **sistemas e aplicações de terceiros** não actualizados, explorando vulnerabilidades conhecidas e para as quais já existem patches disponíveis semanas ou até mesmo meses antes de se verificar a falha de segurança.

A divulgação massiva de vulnerabilidades, como as expostas pelo grupo Shadow Brokers ou a WikiLeaks, com instruções detalhadas sobre como comprometer sistemas e aplicações, permite a realização de ataques por um número crescente de cibercriminosos.

A transformação digital dificulta a tarefa de reduzir a superfície de ataque, devido ao crescimento exponencial do número de utilizadores, dispositivos, sistemas e aplicações de terceiros que requerem actualizações.

Pelo menos **cinco problemas comuns** frustam os programas de gestão de vulnerabilidades (VM):

- A **pesquisa por vulnerabilidades é um processo longo**. No entanto, se ocorrer um incidente a resposta deve ser **imediata**.
- As **empresas estão descentralizadas** e os trabalhadores não se ligam continuamente à rede corporativa. As **ferramentas on-premise** não cobrem esses cenários.
- A maioria das ferramentas VM necessitam que seja instalado **um agente específco** em endpoints que já se encontram sobrecarregados.
- As ferramentas de VM da Microsoft não permitem às empresas actualizar **aplicações de terceiros** de um modo centralizado e unificado.
- As outras soluções de segurança que oferecem patch management **não correlacionam detecção com endpoints vulneráveis** para acelerar a resposta e a mitigação do ataque.

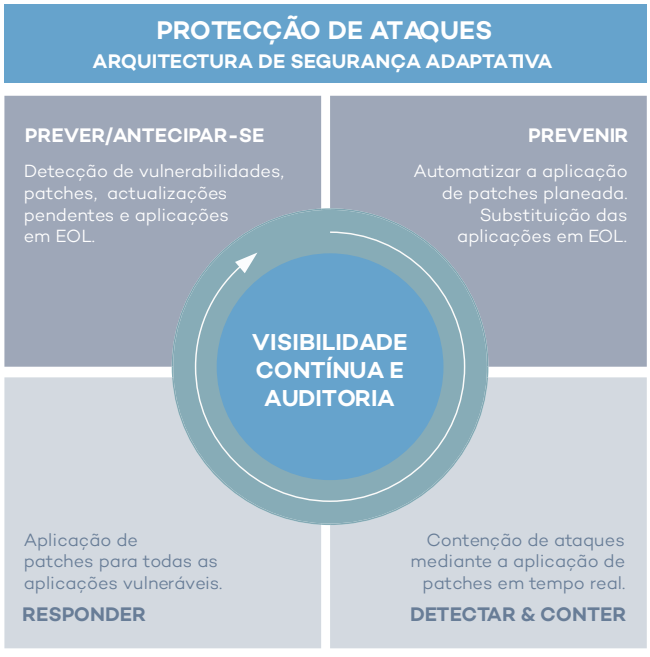
[1] Gartner, Focus on the Biggest Security Threats, Not the most Publicized. Publicação: 2 Novembro 2017As vulnerabilidades de dia-zero são apenas 0,4%, para as restantes , 99,96%, existem actualizações para as resolver. National Vulnerability Database. 86% das vulnerabilidades afectam aplicações de terceiros.
[2] Gartner, How to Respond to the 2018 Threat Landscape. Greg Young. Publicação: 28 Novembro 2017.
[3] EOL (End-of-Life): Um produto que está em fim de vida útil (do ponto de vista do fabricante), que poderá deixar de receber actualizações.

Panda Patch Management

BENEFÍCIOS

O Panda Patch Management permite, numa única **solução**:

- **Auditar, monitorizar e priorizar as actualizações dos sistemas operativos e aplicações.** Um único painel, actualizado em tempo real, permite visibilidade agregada ao estado dos patches e actualizações pendentes do sistema e de centenas de aplicações de terceiros.
- **Prevenir incidentes, reduzindo a superfície de ataque por vulnerabilidades.** A gestão de patches e actualizações com ferramentas de gestão, fáceis e intuitivas, permitem adiantar-se à exploração de vulnerabilidades.
- **Conter e mitigar ataques que exploram vulnerabilidades, aplicando imediatamente actualizações críticas a partir da consola Cloud.** A consola correlaciona detecções com vulnerabilidades, minimizando o tempo de resposta, contenção e remediação mediante a actualização necessária a partir da consola. Além disso, permite isolar da rede computadores afectados, mitigando assim a expansão do ataque.
- **Reduzir custos operativos**
  - **Não requer nem deployments nem actualizações de agente nos endpoints,** simplificando a gestão sem sobrecarregar os computadores e servidores.
  - **Minimiza o esforço das actualizações** remotas a partir da consola Cloud. Além disso, a aplicação de patches está optimizada para minimizar erros.
  - **Visibilidade imediata e não acompanhada** de todas as vulnerabilidades, actualizações e aplicações em EOL imediatamente após a activação.
- **Cumprir com o principio de responsabilidade activa,** requisito de muitas regulamentações (RGPD, HIPAA e PCI), que obriga as organizações a estabelecer todas as medidas que garantam a protecção de dados sensíveis das quais são responsáveis.



O Panda Patch Management multiplica as capacidades de prevenção e resposta das soluções de segurança endpoint da Panda Security, ao permitir uma implementação robusta da Arquitectura de Segurança Adaptativa[4].

PRINCIPAIS FUNCIONALIDADES

O Panda Patch Management fornece todas as ferramentas necessárias para gerir, a partir de uma única consola, a segurança e actualizações do sistema operativo e de aplicações de terceiros.

Detecção:

- Painel único de computadores vulneráveis, patches pendentes e aplicações em EOL[3], bem como o status de remediação.
- Informação detalhada sobre patches e actualizações pendentes, detalhes do boletim de segurança correspondente (CVE) com informação de máquinas e grupos, entre outros. Acções disponíveis:
  - Filtrar e pesquisar por criticidade, computador, aplicação, patch, CVE e estado.
  - Capacidade de realizar acções directamente nos computadores: reiniciar, instalar agora ou programar.
- Pesquisas de actualizações, em tempo real ou periódicas (3, 6, 12 ou 24 horas).
- Em detecções de exploits e programas maliciosos, notificações dos patches pendentes. A instalação pode ser efectuada de imediato ou programada a partir da consola, podendo isolar-se o computador se for necessário.

Planificação e instalação de patches e actualizações:

- Configuráveis por criticidade.
- Sobre grupos ou endpoints específicos.
- Imediatas ou programadas, uma única vez ou em intervalos regulares (data e hora).
- Gestão controlada dos reinícios e excepções.

Monitorização do estado dos endpoints e suas actualizações, mediante:

- Painel de controlo e listas de acções.
- Relatórios de alto nível e detalhados.
- Listagem de computadores actualizados, com actualizações pendentes ou com erros.

Gestão granular por grupos e perfis com permissões:

- Visibilidade de computadores vulneráveis, patches e actualizações pendentes, em função do perfil.
- Gestão por grupo ou computador, a partir da consola.

Compatível com as seguintes soluções em Plataforma Aether:

Panda Endpoint Protection | Panda Endpoint Protection Plus
Panda Adaptive Defense | Panda Adaptive Defense 360

Sistemas Operativos Suportados: Windows XP SP3 ou superior. Windows Server 2003 (32/64 bits y R2) SP2 ou superior.

Aplicações de terceiros suportadas:
https://www.pandasecurity.com/business/PatchManagementApp

Certificações e Reconhecimento

A Panda Security participa regularmente e é premiada devido à capacidade de protecção e performance pelos Virus Bulletin, AV- Comparative, AV-Test, NSSLabs.

O Panda Adaptive Defense conseguiu a certificação EAL2+ na avaliação feita pelo standard Common Criteria.

*Gartner reconheceu a Panda Security como Visionária no Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) em 2018
https://www.pandasecurity.com/gartner-magic-quadrant/

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