Panda Patch Management

Reduza o risco e a complexidade das vulnerabilidades em sistemas e aplicativos de terceiros

panda
a WatchGuard brand

Hoje, **99,96% das vulnerabilidades ativas** nos endpoints corporativos estão relacionadas a **atualizações não realizadas**.[1] Se essas atualizações fossem instaladas, elas contribuiriam muito para evitar riscos à segurança. De fato, de acordo com o Instituto Ponemon,[2] **57% das vítimas** de ataques cibernéticos disseram que a aplicação de **um patch teria impedido** essa ação, e **34%** disseram que sabiam da vulnerabilidade antes do ataque.

Além disso, 86% das vulnerabilidades ocorrem devido a **aplicativos de terceiros** não reparados, como Java, Adobe, Firefox, Chrome, Flash e OpenOffice, entre outros.[1]

CHEGOU A HORA DE MUDAR ESSA TENDÊNCIA COM O PANDA PATCH MANAGEMENT

O Panda Patch Management é uma **solução fácil de usar criada para gerenciar vulnerabilidades dos sistemas operacionais e aplicativos de terceiros em** estações de trabalho e servidores do Windows. Ela **reduz a superfície de ataque**, ao mesmo tempo em que fortalece as capacidades de prevenção e contenção da sua organização.

A solução não requer novos agentes de endpoint nem consoles de gerenciamento porque está totalmente integrada a todas as soluções de endpoint da Panda Security.

A tecnologia também **fornece visibilidade centralizada e em tempo real** sobre o status de segurança das **vulnerabilidades de software**, patches ausentes, atualizações e software sem suporte (EOL[3]**), dentro e fora da rede corporativa. Além disso, oferece ferramentas fáceis de usar e em tempo real para todo o ciclo de gerenciamento de patches: desde a descoberta e o planejamento até a instalação e o monitoramento.**

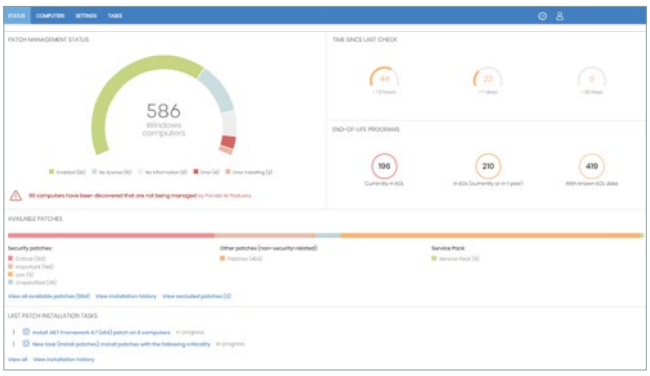


Figura 1: Status da organização de gerenciamento de patches – painel principal

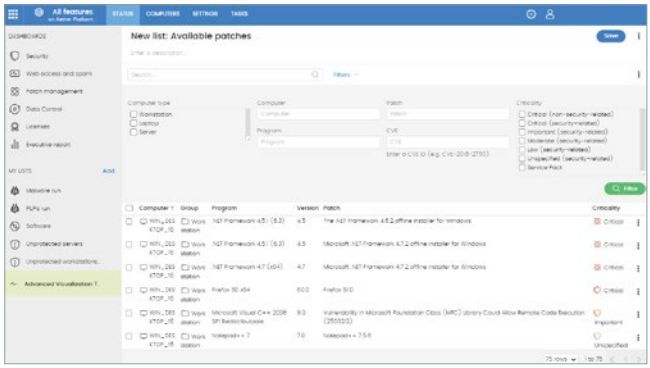


Figura 2: Patches disponíveis – Gerenciamento de patches

VULNERABILIDADES: UM RISCO LATENTE

Sistemas operacionais não reparados e softwares de terceiros fornecem o local perfeito para reprodução de invasores e explorações. Essas ameaças podem tirar proveito de vulnerabilidades dos patches por semanas ou até meses antes da violação.

A divulgação massiva de vulnerabilidades, como as expostas pelos Shadow Brokers ou WikiLeaks, com instruções detalhadas sobre como comprometer sistemas e aplicativos, permite que um número crescente de hackers lance ataques.

A transformação digital está tornando cada vez mais difícil reduzir a superfície de ataque, devido ao crescente número de usuários, dispositivos, sistemas e aplicativos de terceiros que requerem atualizações.

Pelo menos **cinco problemas operacionais comuns frustram** programas de gerenciamento de vulnerabilidades (VM):

- **A descoberta de vulnerabilidades é um processo longo.** No entanto, a resposta deve ser imediata no caso de um incidente.
- **As empresas estão descentralizadas**, e os funcionários não estão continuamente conectados à rede corporativa. **As ferramentas de VM no** local não cobrem esses cenários.
- A maioria das ferramentas de VM requer **outro agente específico** em endpoints que já estão sobrecarregados.
- A ferramenta de VM da Microsoft não permite que as organizações realizem atualizações unificadas e centralizadas de **aplicativos de terceiros.**
- Outras soluções de segurança que oferecem gerenciamento de patches **não correlacionam a detecção com endpoints vulneráveis** para acelerar a resposta e mitigação do ataque.

Soluções compatíveis da PLATAFORMA AETHER:

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

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

Aplicativos de terceiros compatíveis:
www.pandasecurity.com/business/PatchManagementApp

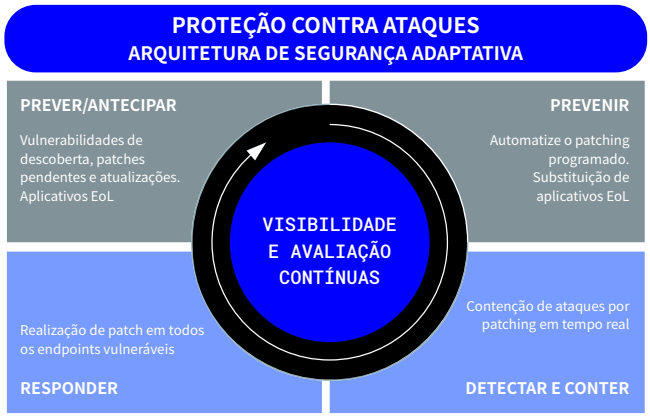
[1] **Gartner, foca nas maiores ameaças de Segurança, não nas mais divulgadas.** Publicado em: 2 de novembro de 2017. As vulnerabilidades de zero-day são apenas 0,4% e, para as outras 99,96%, há patches de correção. Banco de Dados de Vulnerabilidades Nacionais. 86% das vulnerabilidades são encontradas em aplicativos de terceiros.
[2] **Custo e consequências de lacunas na resposta à vulnerabilidade**–Ponemon
[3] **EOL (Fim da Vida): Um produto que está no final da vida útil** (do ponto de vista do fornecedor), que talvez não receba mais atualizações de segurança

panda
a WatchGuard brand

BENEFÍCIOS

Com uma **única solução fácil de usar,** o Panda Patch Management permite que você realize as seguintes ações:

- **Audite, monitore e priorize as atualizações do sistema operacional e dos aplicativos.** A exibição de um painel único oferece visibilidade centralizada, atualizada e agregada sobre o status de segurança da organização em relação a vulnerabilidades, patches e atualizações pendentes de sistemas e centenas de aplicativos.
- **Previna incidentes, reduzindo sistematicamente a superfície de ataque criada por vulnerabilidades de software**. Controle patches e atualizações com ferramentas de gerenciamento fáceis de usar e em tempo real que permitem que as organizações se antecipem a ataques de exploração de vulnerabilidades.
- **Contenha e atenue ataques de exploração de** vulnerabilidades com atualizações imediatas. O console do Panda Adaptive Defense 360, em conjunto com o Patch Management, permite que as organizações correlacionem ameaças detectadas e explorações com vulnerabilidades. O tempo de resposta é minimizado, com a contenção e correção de ataques, eliminando imediatamente patches do console da web. Os computadores afetados podem ser isolados do resto da rede, impedindo que o ataque se espalhe.
- **Reduza o custo operacional:**
  - **O Panda Patch Management não exige que você implante novos agentes de endpoint nem atualize quaisquer agentes existentes,** simplificando o gerenciamento e evitando sobrecarga de estações de trabalho e do servidor.
  - **Minimiza os esforços dos patches à medida que as atualizações são lançadas** remotamente a partir do console baseado em nuvem. Além disso, a instalação é otimizada para minimizar erros.
  - **Fornece visibilidade completa e imediata de todas as vulnerabilidades**, atualizações pendentes e aplicativos EOL[3] imediatamente após a ativação.
- **Esteja em conformidade com o princípio da prestação de contas**, que é parte essencial de muitas regulamentações (GDPR, HIPAA e PCI). Isso obriga as organizações a tomar as medidas técnicas e organizacionais adequadas para garantir a proteção apropriada de dados confidenciais.



O Panda Patch Management aumenta os recursos preventivos, de detecção e resposta das soluções de endpoint da Panda Security, permitindo uma implementação robusta da Arquitetura de Segurança Adaptativa.[4]

PRINCIPAIS RECURSOS

O Panda Patch Management fornece todas as ferramentas necessárias para gerenciar a segurança e as atualizações do sistema operacional e aplicativos de terceiros a partir de um único console:

Descoberta:

- Exibição em painel único com informações em tempo real de todos os computadores vulneráveis, patches pendentes e software sem suporte (EOL[3]), com o status de correção.
- Informações detalhadas sobre patches e atualizações pendentes, detalhes de boletins de segurança relevantes (CVE), bem como informações de computadores e grupos de computadores e muito mais. Ações disponíveis:
  - Filtrar e procurar patches com base na criticidade, no computador, no grupo, no aplicativo, no patch, no CVE e no status.
  - Capacidade de tomar ações diretamente nos computadores: reiniciar, instalar agora ou agendar.
- Varredura autônoma para atualizações pendentes, em tempo real ou usando intervalos periódicos (3, 6, 12 ou 24 horas).
- Notificação de patches pendentes em detecções de exploração. Capacidade de iniciar instalações imediatamente ou programá-las a partir do console, isolando o computador, se necessário.

Tarefas de planejamento e instalação de patches e atualizações:

- Configuração pela criticidade.
- Em endpoints e grupos específicos.
- Imediato, agendado para execução única ou para execução repetida em intervalos regulares (data/hora).
- Capacidade de controlar reinicializações do computador e definir exceções.
- Reversão para desinstalar um patch que pode causar um conflito inesperado com uma configuração existente.

Endpoint e monitoramento de status de atualização via:

- Painéis e listas acionáveis.
- Relatórios de alto nível e detalhados.
- Listas de computadores atualizados, computadores com atualizações pendentes com erros.

Gerenciamento granular baseado em grupos e funções com diferentes permissões:

- Visibilidade baseada em funções em computadores, patches e service packs vulneráveis.

Controle centralizado sobre atualizações, patches e software:

- Capacidade de desativar o Windows Update e gerenciar centralmente atualizações do sistema operacional.
- Possibilidade de excluir patches específicos por versão e por tipo.
- Capacidade de excluir software (por exemplo, Java).

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

WatchGuard

VENDAS NOS EUA 1.800.734.9905 VENDAS INTERNACIONAIS +1.206.613.0895 www.watchguard.com | pandasecurity.com