DATASHEET

WATCHGUARD PATCH MANAGEMENT

Reduza o risco e a complexidade do gerenciamento de vulnerabilidades em sistemas operacionais e aplicativos de terceiros

De acordo com o Ponemon Institute,[1] 57% das vítimas de ciberataques disseram que a aplicação de um patch teria impedido o ocorrido. Além disso, 34% disseram que sabiam da vulnerabilidade antes do ataque.

Os ciberataques de ransomware, como Wanna Cry ou Petya, utilizaram a estratégia perfeita contra empresas com poucas políticas de gerenciamento de patches nos sistemas operacionais, mas não só isso. 86% das vulnerabilidades ocorrem devido a aplicativos de terceiros sem patch, como Java, Adobe, Firefox, Chrome, Flash e OpenOffice.

VULNERABILIDADES: UM RISCO LATENTE

Atualmente, a exploração de vulnerabilidades continua sendo a principal causa da maioria das violações de segurança. Casos famosos, como os ataques Wanna Cry, Petya e BlueKeep, fizeram estragos ao redor do mundo e ainda estão frescos na memória de todos.

Somente um pequeno número de ataques acontece em decorrência de vulnerabilidades realmente desconhecidas (ataques zero-day), já que a maioria deles é causada por vulnerabilidades conhecidas.

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

Pelo menos três problemas operacionais comuns prejudicam programas de gerenciamento de vulnerabilidades (VM):

- A descoberta de vulnerabilidades é um processo longo. No entanto, a resposta precisa ser imediata em casos de incidentes.
- As empresas estão descentralizadas, e os funcionários não estão continuamente conectados à rede corporativa. As ferramentas de VM no local não abrangem esses cenários.
- Outras soluções de segurança que oferecem gerenciamento de patches não correlacionam a detecção com endpoints vulneráveis, de modo a acelerar a resposta e a atenuação do ataque.

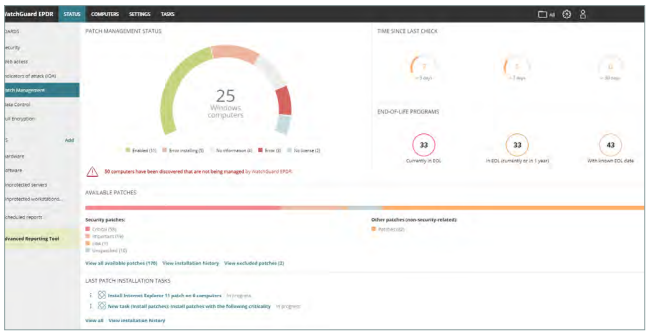

Figura 1: *Status de organização do Patch Management – painel principal*

WATCHGUARD PATCH MANAGEMENT

O WatchGuard Patch Management é uma solução fácil de usar criada para gerenciar vulnerabilidades em sistemas operacionais e aplicativos de terceiros usados em estações de trabalho e servidores do Windows. Ele reduz a superfície de ataque e, ao mesmo tempo, fortalece os recursos de prevenção e contenção da organização.

A solução não requer novos agentes de endpoint nem consoles de gerenciamento, pois está totalmente integrada a todas as soluções de endpoint da WatchGuard.

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)[2]. Além disso, oferece ferramentas para todo o ciclo de gerenciamento de patches, desde a descoberta e o planejamento até a instalação e o monitoramento.

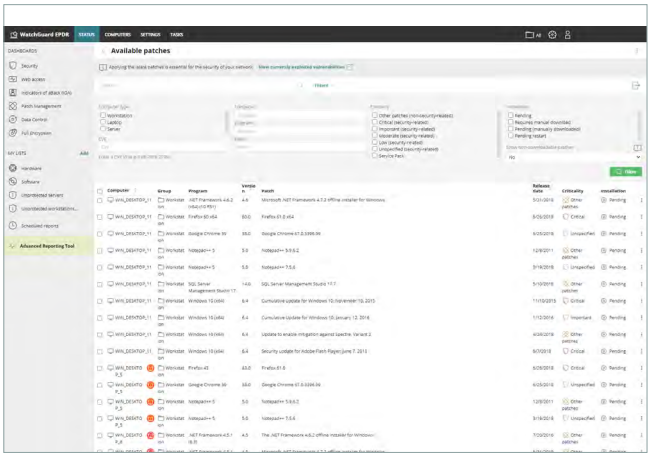

Figura 2: *Patches disponíveis – Patch Management*

[1] Estudo "Cost and consequences of gaps in vulnerability response" – Ponemon.

[2] Final de vida útil (EOL): um produto que está no final da vida útil e não recebe mais atualizações de segurança.

BENEFÍCIOS

Com uma solução fácil de usar, o WatchGuard Patch Management permite que você faça o seguinte:

- 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 quanto a vulnerabilidades, patches e atualizações pendentes de sistemas e de 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. Isso permite que as organizações se antecipem a ataques de exploração de vulnerabilidades.
- Contenha e corrija ataques de exploração de vulnerabilidades com o envio imediato de atualizações ou de patches via console da web. Os computadores afetados podem ser isolados do resto da rede, impedindo que o ataque se espalhe.
- Reduza o custo operacional:
  - A solução simplifica o gerenciamento, pois não é necessário implantar novos agentes de endpoint nem atualizar agentes existentes.
  - Minimiza os esforços da aplicação de patches à medida que as atualizações são lançadas remotamente do console baseado em nuvem.
  - Fornece visibilidade completa e imediata das vulnerabilidades, das atualizações pendentes e dos aplicativos EOL imediatamente após a ativação.
- Cumpra o princípio da prestação de contas, parte essencial de muitas regulamentações. Isso obriga as organizações a tomar as medidas técnicas e organizacionais adequadas para garantir a proteção apropriada de dados confidenciais.

WATCHGUARD PATCH MANAGEMENT
ARQUITETURA DE SEGURANÇA ADAPTATIVA

Estudo "Designing an Adaptive Security Architecture for Protection from Advanced Attacks" – Gartner.

PRINCIPAIS RECURSOS

Descoberta:

- Exibição em painel único com informações em tempo real de todos os computadores vulneráveis, patches pendentes e software sem suporte (EOL) com o status de correção.
- Informações detalhadas sobre patches e atualizações pendentes, bem como detalhes de boletins de segurança relevantes (CVE).
- Busca automática por patches disponíveis, em tempo real ou em intervalos periódicos (3, 6, 12 ou 24 horas).
- Notificação de patches pendentes em detecções de exploração.
- Capacidade de controlar o isolamento e aplicar patches em computadores e servidores.

Tarefas de planejamento e instalação de patches e atualizações:

- Possibilidade de configurar criticidade e software para aplicação de patches.
- Opção de programar para execução imediata, única ou repetida em intervalos regulares (data/hora).
- Controle de reinicializações do computador e definição de 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 de computadores, patches e pacotes de serviços vulneráveis.

Controle centralizado de 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).
- Cache de patches baixados.

Plataformas compatíveis e requisitos de sistema do WatchGuard Patch Management

Compatível com WatchGuard EPDR, WatchGuard EDR e WatchGuard EPP

Sistemas operacionais compatíveis: Windows

Lista de navegadores compatíveis: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera.

Patch Management para vulnerabilidades:
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

Aplicativos de terceiros compatíveis:
https://www.watchguard.com/wgrd-resource-center/patch-management

VENDAS NO BRASIL: +55 11 98586-8814 SUPORTE: +55 21 3956-0543 WEB: www.watchguard.com/br WatchGuard Technologies, Inc.

Número da peça WGCE67518_102921