DATASHEET

WATCHGUARD PATCH MANAGEMENT

Riduci i rischi e la complessità della gestione delle vulnerabilità in sistemi operativi e applicazioni di terze parti

Secondo il Ponemon Institute,[1] il 57% delle vittime di attacchi informatici ha affermato che l'applicazione di una patch avrebbe impedito l'attacco e il 34% ha dichiarato di essere a conoscenza della vulnerabilità già prima dell'attacco.

Gli attacchi informatici ransomware, come WannaCry o Petya, sono stati una vera bufera per le aziende che avevano adottato policy inadeguate di gestione delle patch per i sistemi operativi, ma non solo. L'86% delle vulnerabilità è dovuto alla mancata applicazione di patch ad applicazioni di terze parti, ad esempio, Java, Adobe, Firefox, Chrome, Flash e OpenOffice.

VULNERABILITÀ: UN RISCHIO LATENTE

Lo sfruttamento delle vulnerabilità è ancora oggi la causa principale della maggior parte delle violazioni della sicurezza. Casi tristemente noti come WannaCry, Petya e BlueKeep, che hanno causato il caos in tutto il mondo, sono ancora un vivo ricordo nella mente di tutti.

Solo un ridotto numero di attacchi avviene a seguito di vulnerabilità veramente sconosciute (attacchi zero-day), poiché la maggior parte è causata da vulnerabilità note.

La trasformazione digitale rende sempre più difficile ridurre la superficie di attacco, dato il numero crescente di utenti, dispositivi, sistemi e applicazioni di terze parti da aggiornare.

Vi sono almeno tre problemi operativi diffusi che ostacolano i programmi di gestione delle vulnerabilità:

- L'individuazione delle vulnerabilità richiede tempo. Tuttavia, in caso di incidente la risposta deve essere immediata.
- Le aziende sono decentralizzate e i dipendenti non sempre connessi alla rete aziendale. Gli strumenti di gestione delle vulnerabilità in sede non coprono tutte le situazioni possibili.
- Altre soluzioni di sicurezza con funzioni di gestione delle patch non sono in grado di stabilire una correlazione tra il rilevamento e gli endpoint vulnerabili per velocizzare la risposta e mitigare gli attacchi.

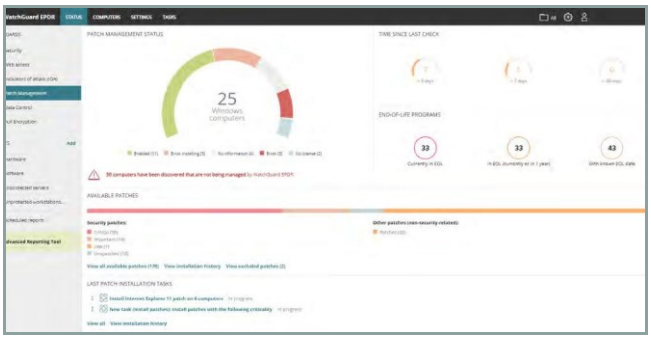

Figura 1: *Stato di organizzazione della gestione delle patch - dashboard principale*

WATCHGUARD PATCH MANAGEMENT

WatchGuard Patch Management è una soluzione intuitiva per gestire le vulnerabilità dei sistemi operativi e delle applicazioni di terze parti su postazioni di lavoro e server Windows. Riduce la superficie di attacco e allo stesso tempo rafforza le capacità di prevenzione e contenimento dell'azienda.

Inoltre, poiché è completamente integrato con tutte le soluzioni endpoint di WatchGuard. non richiede l'implementazione di nuovi agenti né console di gestione.

Offre altresì una visibilità centralizzata in tempo reale dello stato di sicurezza delle vulnerabilità del software, delle patch mancanti, degli aggiornamenti e dei software non supportati (fuori produzione, EOL[2]), oltre a strumenti per tutto il ciclo di gestione delle patch: dal rilevamento alla pianificazione, dall'installazione al monitoraggio.

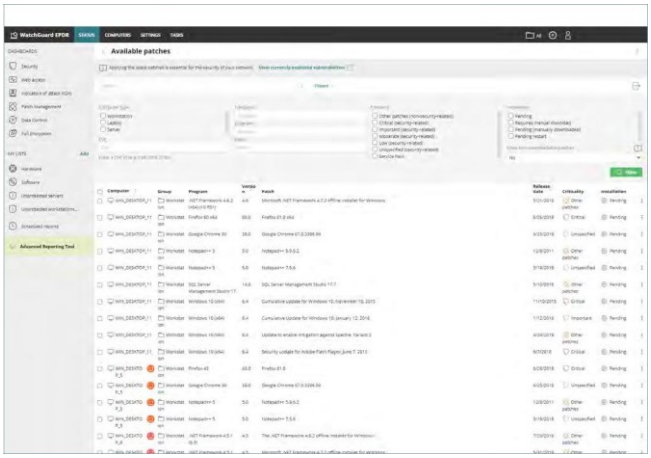

Figura 2: *Patch disponibili - Gestione delle patch*

[1] Costi e conseguenze delle lacune nella risposta alle vulnerabilità - Ponemon.

[2] EOL (End-of-Life: fuori produzione): Prodotti che sono giunti al termine della loro vita utile, per i quali non vengono più forniti aggiornamenti di sicurezza

VANTAGGI

WatchGuard Patch Management, in un'unica soluzione semplice da utilizzare, offre:

- Verifica, monitoraggio e assegnazione di priorità agli aggiornamenti del sistema operativo e delle applicazioni. Vista a pannello unico per una visione centralizzata, aggregata e aggiornata dello stato di sicurezza dell'azienda, in materia di vulnerabilità, patch e aggiornamenti in sospeso per i sistemi e centinaia di applicazioni.
- Prevenzione degli incidenti grazie alla riduzione sistematica della superficie d'attacco creata dalle vulnerabilità del software. Gestione di patch e aggiornamenti con strumenti in tempo reale semplici da usare, che permettono di evitare gli attacchi che sfruttano vulnerabilità.
- Contenimento e risoluzione di attacchi che sfruttano le vulnerabilità grazie all'installazione immediata di aggiornamenti o patch dalla console web. I computer interessati possono essere isolati dal resto della rete, per impedire la diffusione dell'attacco.
- Riduzione dei costi operativi:
  - Gestione semplificata: non richiede l'implementazione di nuovi agenti endpoint o l'aggiornamento di quelli esistenti.
  - Semplifica gli interventi relativi alle patch: gli aggiornamenti vengono avviati da remoto dalla console Cloud.
  - Fornisce una visibilità completa e immediata di tutte le vulnerabilità, gli aggiornamenti in sospeso e le applicazioni EOL subito dopo l'attivazione.
- Conformità ai principi di responsabilità richiesti da vari regolamenti. Le aziende sono obbligate ad adottare misure tecniche e organizzative appropriate, per garantire una protezione adeguata dei dati sensibili in loro possesso.

"Progettiamo un'architettura di sicurezza adattiva per la protezione dagli attacchi avanzati" - Gartner

CARATTERISTICHE PRINCIPALI

Inventario:

- Vista a pannello unico con informazioni in tempo reale riguardanti tutti i computer vulnerabili, le patch in sospeso e il software non supportato (EOL), con il relativo stato di risoluzione.
- Informazioni dettagliate sulle patch e gli aggiornamenti in sospeso, con i relativi bollettini di sicurezza (CVE).
- Ricerca automatica delle patch disponibili, in tempo reale o a intervalli periodici (3, 6, 12 o 24 ore).
- Notifica delle patch in sospeso nel rilevamento degli exploit.
- Capacità di isolare, applicare patch e reintegrare computer e server.

Pianificazione delle patch e degli aggiornamenti e attività di installazione:

- Configurazione di per criticità e software da aggiornare
- Programmazione di una sola esecuzione immediata o di esecuzioni ripetute a intervalli regolari (data/ora).
- Controllo del riavvio dei computer e impostazione delle eccezioni.
- Ripristino per disinstallare una patch che potrebbe causare un conflitto imprevisto con una configurazione esistente.

Monitoraggio dello stato degli endpoint e degli aggiornamenti tramite:

- Dashboard ed elenchi utili. Report di alto livello e dettagliati.
- Elenco di computer aggiornati e computer con aggiornamenti in sospeso ed errori.

Gestione granulare in base ai gruppi e ai ruoli con autorizzazioni diverse:

- Visibilità basata su ruoli per i computer vulnerabili, le patch e i service pack.

Controllo centralizzato degli aggiornamenti, delle patch e del software:

- Possibilità di disabilitare Windows Update e gestire centralmente gli aggiornamenti del sistema operativo.
- Possibilità di escludere patch specifiche in base alla versione e al tipo.
- Capacità di escludere software (es. Java).
- Salvataggio in cache delle patch scaricate.

Piattaforme supportate e requisiti di sistema di WatchGuard Patch Management

Compatibile con WatchGuard EPDR, WatchGuard EDR e WatchGuard EPP

Sistemi operativi supportati: Windows

Elenco dei browser compatibili: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera.

Gestione delle patch per le vulnerabilità:
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

Applicazioni di terze parti supportate:
https://www.watchguard.com/wgrd-resource-center/patch-management

Per informazioni contata SOPHIANET SRL – commerciale@sophianet.it