FICHE TECHNIQUE

WATCHGUARD PATCH MANAGEMENT

Réduisez le risque et la complexité de la gestion des vulnérabilités dans les systèmes d'exploitation et les applications tierces.

Selon l'institut Ponemon,[1] 57 % des victimes de cyberattaques ont affirmé que l'application d'un correctif aurait empêché l'attaque, et 34 % ont même déclaré qu'elles avaient connaissance de la vulnérabilité avant l'attaque.

Les cyberattaques de ransomware comme WannaCry ou Petya ont déclenché une véritable tempête contre les entreprises ayant une mauvaise stratégie de gestion des correctifs de leur système d'exploitation, mais elles ne sont pas les seules. 86 % des vulnérabilités sont dues à des applications tierces auxquelles aucun correctif n'a été appliqué telles que Java, Adobe, Firefox, Chrome, Flash et OpenOffice.

LES VULNÉRABILITÉS : UN RISQUE LATENT

L'exploitation des vulnérabilités reste aujourd'hui encore la première cause de failles de sécurité. Des exemples célèbres tels que WannaCry, Petya et BlueKeep, qui ont causé des ravages dans le monde entier, sont encore dans toutes les mémoires.

Les attaques de type « Zero Day », qui découlent de vulnérabilités totalement inconnues, sont rares. La plupart des menaces sont liées à des vulnérabilités connues.

La transformation numérique rend de plus en plus difficile la réduction de la surface d'attaque, en raison du nombre croissant d'utilisateurs, d'appareils, de systèmes et d'applications tierces qui nécessitent des mises à jour.

Au moins trois problèmes opérationnels courants entravent les programmes de gestion des vulnérabilités (VM) :

- La découverte des vulnérabilités est un long processus. Cependant, la réponse doit être immédiate en cas d'incident.
- Les unités légales sont décentralisées, les employés ne sont pas connectés en permanence au réseau de l'entreprise. Les outils VM on-premise ne couvrent pas ces scénarios.
- D'autres solutions de sécurité qui proposent une gestion des correctifs n'établissent pas de corrélation entre la détection et les postes de travail vulnérables pour accélérer la réponse et atténuer l'attaque.

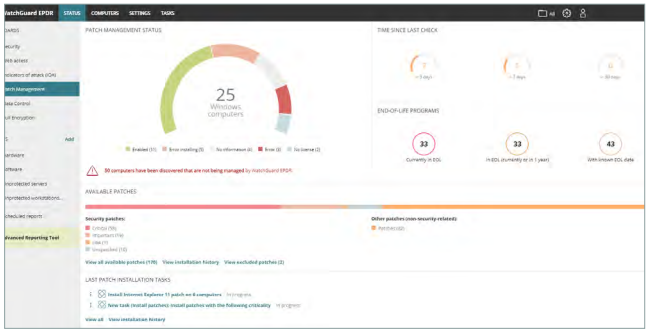


Figure 1 : Statut de l'entreprise vu par Patch Management – tableau de bord principal

WATCHGUARD PATCH MANAGEMENT

WatchGuard Patch Management est une solution conviviale de gestion des vulnérabilités des systèmes d'exploitation et des applications tierces sur les postes de travail et les serveurs Windows. Elle réduit la surface d'attaque, tout en renforçant les capacités de prévention et de confinement de votre entreprise.

La solution ne requiert pas de nouveaux agents des postes de travail ou de nouvelles consoles de gestion, car elle est entièrement intégrée à toutes les solutions pour endpoints de WatchGuard.

Elle assure également une visibilité centralisée et en temps réel sur le statut de sécurité des vulnérabilités logicielles, les correctifs manquants et les mises à jour en attente et des logiciels non pris en charge (fin de vie)[2], ainsi que des outils pour l'ensemble du cycle de gestion des correctifs : de la découverte et de la planification à l'installation et à la surveillance.

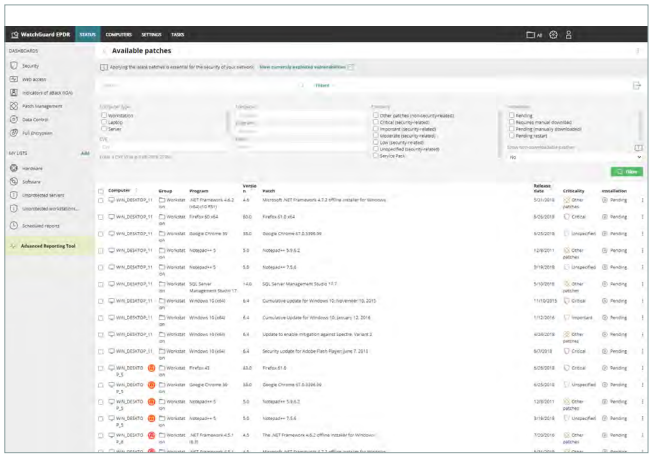


Figure 2 : Correctifs disponibles – Patch Management

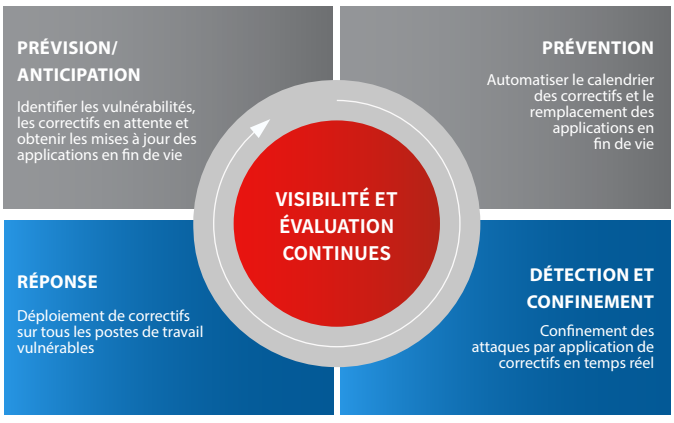
[1] Cost and consequences of gaps in vulnerability response – Ponemon.
[2] EOL (fin de vie) : Un produit en fin de vie qui ne reçoit plus de mises à jour de sécurité

AVANTAGES

Au sein d'une seule et même solution conviviale, WatchGuard Patch Management vous permet de :

- Vérifier, surveiller et prioriser les mises à jour des systèmes d'exploitation et des applications. Un tableau unique centralise des informations en temps réel et agrégées sur la sécurité de l'entreprise et donne de la visibilité sur les failles, les correctifs et les mises à jour en attente, pour le système et des centaines d'applications.
- Prévenir les incidents pour réduire de façon systématique la surface d'attaque générée par les failles des logiciels. Gestion des correctifs et des mises à jour grâce à des outils de gestion en temps réel simples d'utilisation, qui permettent à l'entreprise d'anticiper les attaques par exploitation des failles.
- Contenir et remédier aux attaques par exploitation des vulnérabilités en publiant immédiatement des mises à jour ou des correctifs depuis la console Web. En outre, les ordinateurs infectés peuvent être isolés du reste du réseau pour éviter la propagation de l'attaque.
- Réduire les coûts opérationnels :
  - Simplifie la gestion, car il n'est pas nécessaire de déployer de nouveaux agents pour les postes de travail ou de mettre à jour les agents existants.
  - Facilite l'application des correctifs car les mises à jour sont lancées à distance depuis la console dans le Cloud.
  - Confère une visibilité complète et immédiate sur toutes les vulnérabilités, les mises à jour en attente et les applications en fin de vie dès leur activation.
- Conforme aux principes comptables, inhérent à de nombreuses réglementations. Contraint les entreprises à prendre les mesures techniques et organisationnelles adéquates pour garantir la bonne protection des données sensibles sous leur responsabilité.

WATCHGUARD PATCH MANAGEMENT
ARCHITECTURE DE SÉCURITÉ ADAPTATIVE



« Designing an Adaptive Security Architecture for Protection from Advanced Attacks » – Gartner

FONCTIONS CLÉS

Découverte :

- Une vue d'ensemble avec des informations en temps réel sur tous les ordinateurs vulnérables, les correctifs en attente et les logiciels non pris en charge (fin de vie), avec le statut de leur remédiation.
- Informations détaillées sur les correctifs et mises à jour en attente, détails des bulletins de sécurité pertinents (CVE).
- Recherche automatique des correctifs disponibles en temps réel ou à intervalles périodiques (3, 6, 12 ou 24 heures).
- Notification des correctifs en attente pour les détections d'exploits.
- Capacité à appliquer des correctifs et à contrôler l'isolation des ordinateurs et des serveurs.

Tâches de planification et d'installation des correctifs et des mises à jour :

- Configurer la criticité et le logiciel auquel appliquer un correctif.
- Planifier l'exécution immédiate, en une seule fois, ou l'exécution répétée à intervalles réguliers (date/heure).
- Contrôler les redémarrages de l'ordinateur et définition des exceptions.
- Restauration afin de désinstaller un correctif qui peut causer un conflit inattendu avec une configuration existante.

Surveillance de l'état des postes de travail et des mises à jour via :

- Un tableau de bord et des listes d'actions. Des rapports globaux et détaillés.
- Des listes des ordinateurs mis à jour et des ordinateurs en attente de mise à jour avec des erreurs.

Gestion détaillée basée sur des groupes et des rôles avec différentes permissions :

- Visibilité, basée sur les rôles, des ordinateurs vulnérables, des correctifs et des service packs.

Contrôle centralisé des mises à jour, des correctifs et des logiciels :

- Aptitude à désactiver Windows Update et à gérer de manière centralisée les mises à jour du système d'exploitation.
- Aptitude à exclure des correctifs spécifiques par version et par type.
- Capacité à exclure des logiciels (p. ex., Java).
- Mise en cache des correctifs téléchargés.

Plateformes prises en charge et configuration système requise pour WatchGuard Patch Management

Compatible avec WatchGuard EPDR, WatchGuard EDR et WatchGuard EPP

Systèmes d'exploitation pris en charge : Windows

Liste des navigateurs compatibles : Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge et Opera.

Gestion des correctifs pour les vulnérabilités :
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

Applications tierces prises en charge :
https://www.watchguard.com/wgrd-resource-center/patch-management

SERVICE COMMERCIAL FRANCE +33 97 755 4336 ADRESSE EMAIL france@watchguard.com SITE INTERNET www.watchguard.com/fr WatchGuard Technologies, Inc.