Ivanti Neurons for Patch Management

Priorisation et correction efficaces des vulnérabilités

Ivanti Neurons for Patch Management est une solution cloud native de gestion des correctifs, qui fournit de l'information décisionnelle sur l'exposition active aux risques, la fiabilité des correctifs, la conformité des périphériques ainsi que l'état de santé et les risques de votre infrastructure IT. Elle aide les entreprises à mieux se protéger contre les menaces, y compris les ransomwares.

Gestion des correctifs basée sur les risques

Les attaques par ransomware deviennent chaque année plus fréquentes et plus violentes. Leur impact sur les entreprises est terrible. Des études montrent que le coût moyen d'une attaque par ransomware est de 4,62 millions de dollars (en plus du montant de la rançon).[1]

Il y a fort à craindre que la situation n'empire. En effet, le ransomware en tant que service (RaaS) permet aujourd'hui à pratiquement n'importe qui de lancer une attaque : aucune connaissance de la sécurité ni expertise en codage n'est nécessaire. En outre, le nombre des CVE (Common Vulnerabilities and Exposures - la liste publique des vulnérabilités et failles de sécurité) a pratiquement quadruplé en 2020.[2] Pire encore, les pirates qui utilisent des ransomwares visent de plus en plus souvent des PME pour éviter l'attention que les médias accordent aux attaques sur les grandes entreprises.[3]

L'un des meilleurs moyens de contrer les attaques par ransomware est d'appliquer les correctifs corrigeant les CVE. Malheureusement, 71 % des professionnels de l'IT et de la sécurité trouvent que l'application des correctifs est trop complexe et prend trop de temps.[4] C'est certainement en raison du volume effarant de vulnérabilités que l'on connaît. Aux États-Unis, la base de données nationale des vulnérabilités (NVD)

répertorie plus de 100 000 vulnérabilités. Bien que seul un faible pourcentage de ces vulnérabilités soit lié au ransomware, et que le pourcentage d'exploitations actives soit encore plus faible, il est parfois difficile pour une entreprise d'identifier les menaces les plus dangereuses. Sur 2018-2020, d'après les scores CVSS v3, les entreprises ayant uniquement appliqué les correctifs de vulnérabilités « critiques » n'étaient protégées que contre 35 % des ransomwares.[2]

Ivanti Neurons for Patch Management fournit des analyses sur les menaces, des informations sur la fiabilité des correctifs, et apporte une visibilité sur les risques courus par les périphériques. L'équipe IT peut ainsi prioriser et corriger les vulnérabilités les plus dangereuses. Outre les gains d'efficacité et de productivité générés, Ivanti Neurons for Patch Management renforce la protection des entreprises contre les fuites de données, les ransomwares et les menaces liées aux vulnérabilités logicielles.

Principales fonctionnalités

Meilleure protection contre les exploitations actives grâce à l'application proactive des correctifs

Appuyez-vous sur les analyses et les informations à votre disposition pour prioriser la correction des vulnérabilités en fonction des risques encourus, des exploitations connues et du contexte de menace de ces vulnérabilités, y compris leurs liens avec les ransomwares. Le score VRR (risque de la vulnérabilité) Ivanti vous aide à prendre des actions en ayant une meilleure connaissance des risques. Il vous donne de meilleures armes que le score CVSS, car il tient compte des données les plus fiables sur les vulnérabilités et les menaces, mais aussi des signalements humains sur les exploitations tirés des tests d'intrusion.

Réalisation plus rapide des SLA grâce aux données sur la fiabilité des correctifs et sur les tendances

Gagnez du temps et assurez la bonne réussite des déploiements de correctifs grâce aux informations sur leur fiabilité. Elles proviennent de données sur le ressenti général des utilisateurs, collectées en crowdsourcing (sur les sites de communautés d'utilisateurs), ainsi que de données télémétriques de déploiement des correctifs, collectées en mode anonyme. Ces informations vous permettent d'évaluer les correctifs en fonction de leur fiabilité dans des applications réelles, avant de les déployer. De plus, le suivi des SLA (accords de niveau de service), qui fournit une bonne visibilité sur les périphériques inclus dans vos SLA, vous permet d'agir sur ces périphériques avant qu'ils ne soient plus conformes.

Transition d'une gestion des correctifs sur site (on-premise) à une gestion dans le Cloud

Entamez votre migration vers le Cloud en vous reposant sur les technologies Ivanti de gestion de correctifs. Ivanti Neurons for Patch Management est une solution native Cloud qui vous permet de passer d'une gestion des correctifs on-premise à une gestion dans le Cloud, à votre propre rythme. Pour une transition progressive, la solution offre une expérience centralisée, qui vous apporte une visibilité sur l'ensemble des périphériques en incluant ceux gérés dans le Cloud et ceux gérés par des solutions on-premise.

Rationalisation des processus de gestion des correctifs

Améliorez votre efficacité opérationnelle en éliminant les solutions en silos : plus besoin de passer d'une solution de gestion des correctifs à l'autre. Avec Ivanti Neurons for Patch Management, vous bénéficiez d'une visibilité sur l'ensemble des terminaux de votre environnement via une vue centralisée. Les « insights » sur les vulnérabilités et les informations décisionnelles sur les correctifs vous permettent de prioriser efficacement les déploiements pour vous concentrer sur les plus importants. Enfin, lorsqu'il est temps d'appliquer les correctifs, quelques minutes suffisent pour déployer les configurations sur les périphériques via l'agent Ivanti Neurons.

À propos d'Ivanti

Ivanti rend possible l'Everywhere Workplace. Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux données et aux applications du département IT sur différents réseaux, afin de rester productifs en travaillant de partout. La plateforme d'automatisation Ivanti Neurons connecte les solutions Ivanti de gestion unifiée des terminaux (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin de créer une plateforme IT unifiée permettant l'autoréparation et l'autosécurisation des périphériques, et le self-service aux utilisateurs. Plus de 40 000 clients, dont 96 des entreprises Fortune 100, ont choisi Ivanti pour découvrir, gérer, sécuriser et servir leurs biens IT, du Cloud à la périphérie, ainsi que pour fournir une expérience utilisateur d'excellence aux collaborateurs, où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Pour en savoir plus, visitez le site ivanti.com.fr

ivanti neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com

1. IBM Security, « 2021 Cost of a Data Breach Report », 28 juillet 2021. https://www.ibm.com/downloads/cas/OJDVQGRY
2. RiskSense, Cyber Security Works, « Ransomware Through the Lens of Threat and Vulnerability Management », 9 novembre 2021. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw
3. Coveware, « Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021 », 21 octobre 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
4. Ivanti, « Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere », 7 octobre 2021. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges