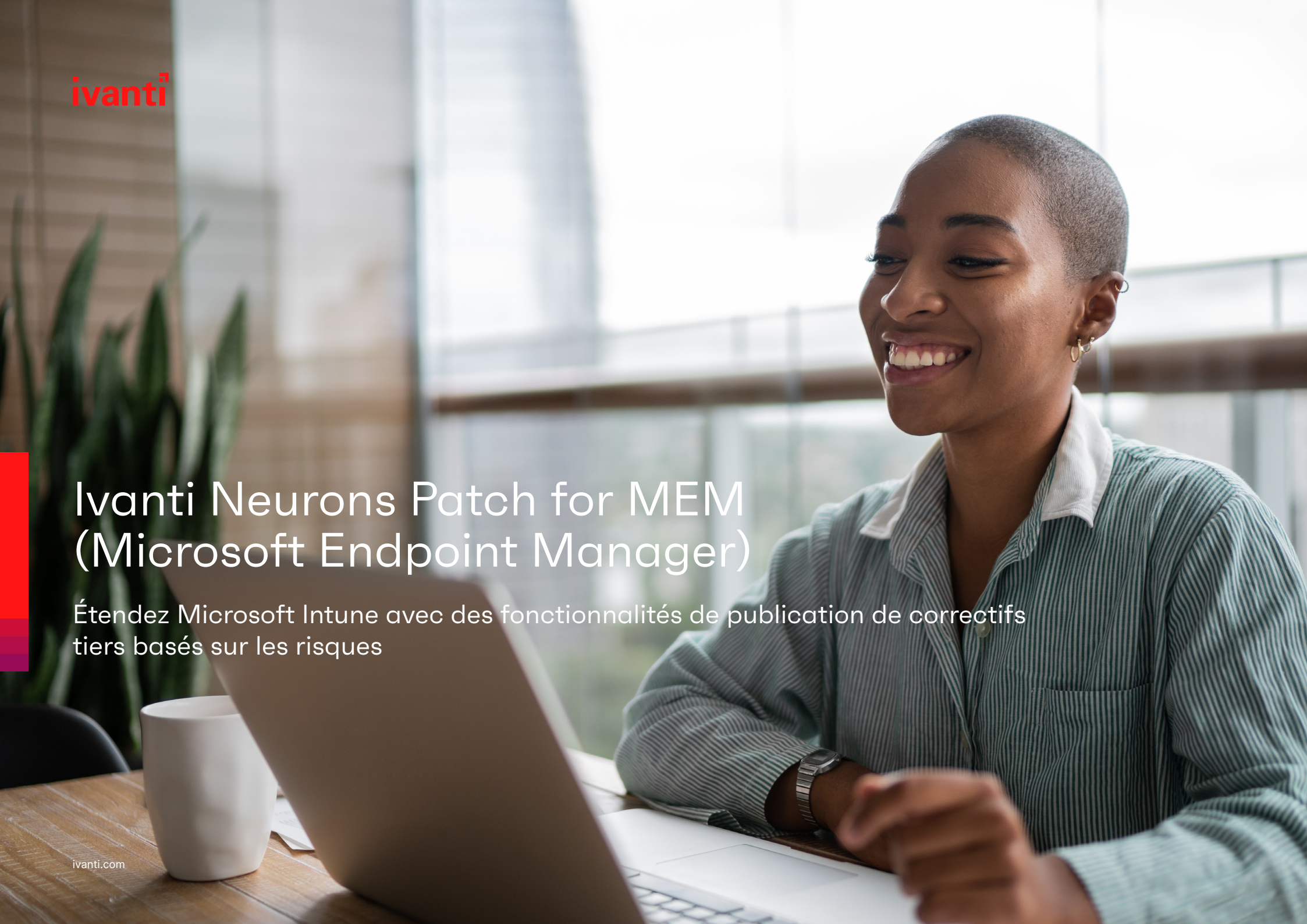


Ivanti Neurons Patch for MEM (Microsoft Endpoint Manager)

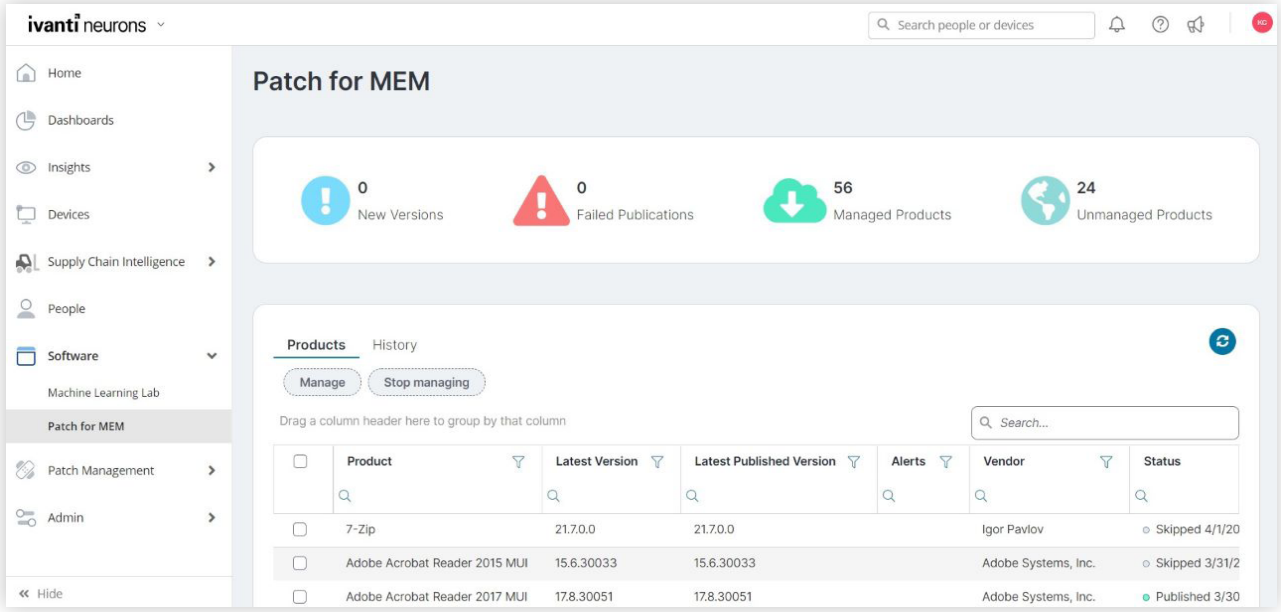
Étendez Microsoft Intune avec des fonctionnalités de publication de correctifs tiers basés sur les risques

Ivanti Neurons Patch for MEM étend les implémentations Microsoft Intune existantes pour inclure les mises à jour des applications tierces. Avec ses informations décisionnelles sur les correctifs et sa « threat intelligence », les entreprises sont en mesure de prioriser correctement la remédiation des vulnérabilités des logiciels tiers.

Mises à jour tierces dans Intune

Les fuites de données et les attaques par ransomware se multiplient chaque année. Parallèlement, le nombre d'applications déployées par les entreprises a augmenté de 24 % depuis 2016.[1] Il n'est donc pas surprenant que les applications tierces soient devenues le vecteur d'attaque préféré des cybercriminels. Malheureusement, les fuites de données dues aux vulnérabilités des applications tierces sont aussi les plus chères : une fuite de donnée coûte en moyenne 4,33 millions de dollars à une entreprise.[2]

Pour s'en prémunir, il convient d'appliquer le plus rapidement possible les mises à jour des applications tierces. Toutefois, le nombre toujours croissant d'applications concernées rend la tâche difficile. Pour compliquer les choses, il faut traquer toujours plus de vulnérabilités : aux États-Unis, la base de données nationale des vulnérabilités (NVD) en découvre en moyenne 61 par jour.[3]



La bonne nouvelle, c'est que 4 % seulement des CVE (Common Vulnerabilities and Exposures) ont été exploitées dans des attaques.[4] La mauvaise nouvelle, par contre, c'est qu'il est difficile d'identifier ces 4 % parmi les plus de 130 000 vulnérabilités répertoriées dans la NVD. Par exemple, une entreprise qui appliquerait l'ensemble des correctifs de vulnérabilités critiques en se basant sur le score CVSS (Common Vulnerability Scoring System) v3 ferait l'impasse sur 73,61 % des vulnérabilités de ransomwares.[3]

La situation est encore plus problématique pour les entreprises qui utilisent Microsoft Intune pour distribuer les applications et leurs mises à jour sur leurs périphériques. Même si Intune offre des fonctions complètes de gestion des correctifs pour les applications Microsoft, il ne possède aucune fonction native pour mettre à jour les applications tierces.

Présentation d'Ivanti Neurons Patch for MEM

Ivanti Neurons Patch for MEM étend les implémentations Microsoft Intune existantes pour inclure les mises à jour des applications tierces, sans nécessiter aucune infrastructure supplémentaire. Il fournit également de la « threat intelligence » et des insights sur la fiabilité des correctifs. L'équipe IT peut ainsi prioriser et corriger les vulnérabilités les plus dangereuses. Avec Ivanti Neurons Patch for MEM, vous bénéficiez d'une protection renforcée contre les fuites de données, les ransomwares et toute autre menace liée aux vulnérabilités des applications tierces.

Principales caractéristiques

Extension de Microsoft Intune avec la publication de correctifs tiers

Optimisez le retour sur investissement d'Intune tout en vous protégeant des menaces émanant des vulnérabilités des applications tierces. Ivanti Neurons Patch for MEM publie directement dans Intune les mises à jour d'applications tierces prétestées provenant de la plateforme Ivanti Neurons. Les équipes IT peuvent ainsi déployer les mises à jour des applications tierces en même temps que les mises à jour d'OS et d'applications Microsoft diffusées dans Intune, au sein de leurs workflows de gestion du cycle de vie des applications.

De plus, comme Ivanti Neurons Patch for MEM est une solution Cloud native, les clients Intune peuvent entièrement migrer le traitement des correctifs vers le Cloud, et s'aligner sur la vision de Microsoft : une gestion moderne sans infrastructure supplémentaire.

Protection proactive contre les exploitations actives

Priorisez vos actions de remédiation en fonction des risques encourus en vous appuyant sur des données sur les exploitations connues et sur le contexte des menaces des vulnérabilités, y compris leurs liens avec les ransomwares. Le score Ivanti VRR (Vulnerability Risk Rating) vous aide à prioriser vos actions en fonction des risques et vous arme mieux que le score CVSS. En effet, il tient compte des données les plus fiables sur les vulnérabilités et les menaces, mais aussi de la confirmation humaine des exploitations, fournie par des équipes qui effectuent des tests d'intrusion.

Garantie d'un déploiement réussi des correctifs

Gagnez du temps en réussissant vos déploiements de correctifs grâce aux mises à jour d'application prétestées et aux insights sur la fiabilité des correctifs. Ivanti teste soigneusement chaque package de correctif créé. Les tests sont menés au sein d'un environnement virtuel très étendu pour garantir le bon fonctionnement des packages pour un grand nombre de systèmes d'exploitation et de versions d'applications.

Pour encore plus de sérénité, des insights sur la fiabilité des correctifs vous permettent d'évaluer les mises à jour d'après leur fiabilité dans des environnements réels avant de les déployer. Ils émanent essentiellement de données de crowdsourcing sur le ressenti des utilisateurs et de données de télémétrie anonymisées sur le déploiement des correctifs.

Rationalisation des processus de gestion des correctifs

Améliorez votre efficacité opérationnelle grâce aux fonctionnalités d'optimisation d'Ivanti Neurons Patch for MEM :

- Publiez automatiquement les mises à jour d'applications tierces dans Intune au fur et à mesure qu'elles sont disponibles (autopublication facultative).
- Déployez vos correctifs avec succès en utilisant des mises à jour d'applications prétestées associées à des insights sur la fiabilité des correctifs.
- Priorisez efficacement le déploiement des correctifs en vous appuyant sur la « threat intelligence ». Vous pourrez ainsi vous concentrer sur les correctifs les plus importants.
- Facilitez la communication entre les équipes Sécurité et Opérations IT en encourageant les discussions sur les données et les risques, et en échangeant des insights sur les codes d'exploitation et les malwares.

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 actifs 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 www.ivanti.fr.

Copyright © 2022, Ivanti. Tous droits réservés. IVI-2671 07/22 JP

ivanti

www.ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr

1. Okta, « Business at Work 2022 Report », 2022. https://www.okta.com/report/businesses-at-work-2022/
2. IBM Security, « 2021 Cost of a Data Breach Report », 28 juillet 2021. https://www.ibm.com/security/data-breach
3. Cyber Security Works, Cyware, Ivanti, « 2022 Ransomware Spotlight Report », 26 janvier 2022. https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
4. Cybersecurity and Infrastructure Security Agency (CISA), « Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities », 3 novembre 2021. https://cyber.dhs.gov/bod/22-01/