ivanti neurons

Ivanti Neurons for Patch Management

Réduisez les risques et l'exposition aux menaces en priorisant et en éliminant les vulnérabilités

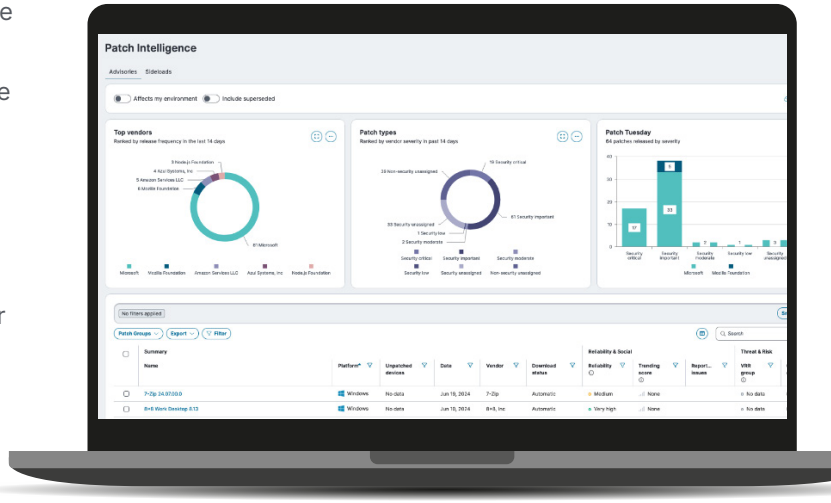
Ivanti Neurons for Patch Management est une solution Cloud native qui fournit une intelligence décisionnelle sur les risques liés aux périphériques pour les applications Windows, macOS, Linux et tierces. Priorisez et corrigez les vulnérabilités grâce à des insights sur votre exposition aux risques actifs, sur la fiabilité des correctifs et sur la conformité des périphériques. Protégez-vous de toute une variété de menaces, y compris les ransomwares.

Gestion des correctifs basée sur les risques

Les attaques par ransomware deviennent chaque année plus fréquentes et plus graves, avec un impact dévastateur sur les entreprises. Une étude montre que le coût moyen d'une fuite de données atteint 4,88 millions de dollars, soit 10 % de plus qu'en 2023, la plus forte augmentation depuis la pandémie.[1]

Les attaques vont devenir plus fréquentes et plus graves à mesure que la technologie et l'IA progresseront. Le ransomware en tant que service (RaaS) permet à pratiquement n'importe qui de lancer une attaque : aucune connaissance de la sécurité ni expertise en codage n'est nécessaire. La multiplication des vulnérabilités accroît les risques ; l'exploitation des vulnérabilités a augmenté de 180 % par rapport à l'an dernier.[2] Une étude de Google révèle que les exploitations Zero Day ont augmenté de 50 % en un an.[3] Pire encore, nous sommes désormais à l'ère du piratage par IA. Des chercheurs de l'Université de l'Illinois ont formé des agents d'IA à pirater de manière autonome des sites Web pour découvrir et exploiter les vulnérabilités Zero Day.[4]

L'un des meilleurs moyens de contrer les attaques par ransomware est d'appliquer des correctifs remédiant aux vulnérabilités et expositions. Malheureusement, 71 % des professionnels IT et de sécurité trouvent que l'application des correctifs est trop complexe et prend trop de temps.[5] C'est certainement en raison du volume effarant de vulnérabilités. Aux États-Unis, la base de données nationale des vulnérabilités (NVD) répertorie plus de 230 000 vulnérabilités.[6] Bien que seul un faible pourcentage soit lié aux ransomwares, 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.



Ivanti Neurons for Patch Management fournit des insights sur les menaces et sur la fiabilité des correctifs tout en apportant une visibilité étendue sur les risques courus par les périphériques pour les applications Windows, macOS, Linux et tierces. Ces informations cruciales permettent aux équipes IT de prioriser et de 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

Priorisation basée sur les risques

Ivanti Neurons for Patch Management applique une stratégie de priorisation basée sur les risques pour cibler en premier les correctifs correspondant aux vulnérabilités critiques, surtout celles liées aux ransomwares. En se concentrant sur les correctifs qui éliminent les risques les plus sévères, les équipes IT peuvent allouer des ressources à d'autres priorités stratégiques, rationaliser le processus de gestion des correctifs et rendre leur sécurité plus efficace. En traitant immédiatement les vulnérabilités les plus graves, cette approche limite sensiblement les risques de ransomwares et autres failles de sécurité, afin d'assurer une défense solide dans un environnement de menaces complexe.

Contexte de menaces actives

Renforcez votre sécurité IT en priorisant les vulnérabilités critiques à l'aide du score VRR (risque de la vulnérabilité). Cette notation surpasse les scores CVSS traditionnels, car elle intègre des évaluations de risques basées sur des situations réelles. Notre système VRR classe les correctifs à partir d'insights détaillés sur les risques adverses, notamment des informations sur les exploitations et les vulnérabilités liées aux ransomwares. Renforcé par des données de haute qualité et validé par les experts en tests d'intrusion, le système VRR oriente efficacement les efforts de remédiation, ce qui booste considérablement vos défenses contre les menaces actives et potentielles.

Déploiement par risque

À mesure que les vulnérabilités sont découvertes, les éditeurs de logiciels publient des mises à jour pour y remédier. C'est essentiel pour atténuer les risques, notamment en cas d'exploitation Zero Day ou de divulgation publique. Cependant, intégrer ces mises à jour publiées en continu relève du défi, d'autant que le planning de maintenance est souvent établi sur une base mensuelle. C'est pourquoi des failles de sécurité restent parfois des semaines sans correction.

La fonction de déploiement basé sur les risques prend en charge plusieurs tâches de déploiement en parallèle : maintenance mensuelle standard, mises à jour prioritaires hebdomadaires et application immédiate des correctifs Zero Day. Les mises à jour sont ainsi gérées automatiquement, garantissant que les systèmes sont à jour et intègrent les correctifs les plus récents, quelle que soit leur date de publication.

> « 63 % des professionnels IT et de sécurité disent que les silos de données ralentissent le temps de réponse des équipes Sécurité. »[7]

Élimination des obstacles entre IT et Sécurité

En fournissant à vos équipes IT et Sécurité un accès égal à des informations cruciales telles que le suivi des SLA et l'intelligence basée sur les risques, vous créez les conditions d'une collaboration équitable et favorisez une vision globale et un langage commun entre les deux équipes, avec à la clé des actions transversales plus rapides et efficaces. Cette approche unifiée réduit les conflits et permet de donner une réponse coordonnée aux parties prenantes. En partageant des insights sur la fiabilité des correctifs, obtenus à partir de données de crowdsourcing et de télémétrie de déploiement, vous réalisez des évaluations proactives et évitez les échecs de déploiement (vous garantissez surtout la conformité de vos SLA). Cette stratégie améliore la coordination entre les équipes et renforce la posture de sécurité de l'entreprise.

Transition du On-premise au Cloud

Entamez votre migration vers le Cloud en passant d'une gestion des correctifs On-premise à une gestion Cloud avec Ivanti Neurons for Patch Management. Notre solution Cloud native vous permet d'effectuer cette transition à votre propre rythme sans avoir à tout changer. L'expérience de migration d'Ivanti assure une transition progressive en fournissant à la fois une visibilité sur les périphériques gérés dans le Cloud et ceux gérés par les solutions On-premise d'Ivanti.

Fiabilité des correctifs

La fiabilité des correctifs est indispensable pour l'intégrité et la sécurité des systèmes. Pour évaluer l'efficacité et la sécurité des correctifs avant leur déploiement Ivanti exploite des informations de ressenti issues du crowdsourcing (communautés d'utilisateurs), des données de déploiement anonymisées et des tests avancés. L'agent Ivanti Neurons configure de façon autonome les correctifs testés et les distribue rapidement à des milliers de périphériques, identifiant très tôt les problèmes potentiels. Les équipes IT sont en mesure de prendre des décisions éclairées sur les correctifs, ce qui limite les risques d'erreurs et améliore la stabilité et les performances de l'environnement IT. Cette méthode limite les interruptions de service et garantit une protection continue contre les vulnérabilités.

Hétérogénéité garantie grâce à une plateforme unique

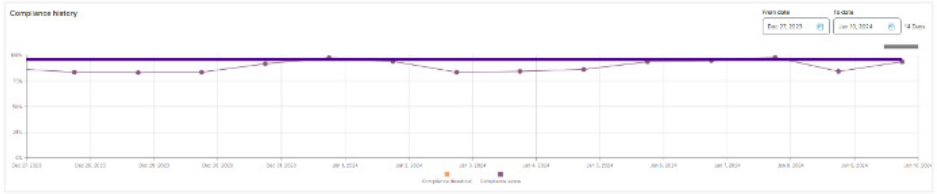
Une plateforme hétérogène est essentielle pour maintenir des normes de sécurité solides dans des environnements IT variés. C'est l'assurance d'une gestion efficace et proactive des risques de sécurité IT. Ivanti Neurons for Patch Management prend en charge les applications Windows, MacOS, Linux et tierces avec une expérience de gestion unifiée qui simplifie la surveillance des différents systèmes et booste la productivité.

Une plateforme unique permet de mettre en oeuvre des stratégies de sécurité cohérentes. Elle améliore également l'efficacité opérationnelle en évitant de basculer entre différentes solutions de gestion des correctifs. En réduisant la complexité et les risques d'oubli, vous garantissez une protection et une visibilité complètes de tous les postes client. Grâce à l'identification rapide des vulnérabilités et des incohérences, cette approche exhaustive évite les fuites de données, limite les interruptions de service et les coûts de récupération, tout en protégeant les actifs de l'entreprise.

Un nouveau mode de mesure : la durée d'exposition

La course aux chiffres :

il est impossible de suivre les mises à jour publiées chaque jour, et par conséquent d'être en conformité.



La mesure de l'essentiel :

Un KPI basé sur les risques permet aux équipes de se concentrer sur les risques réels et de se mettre en conformité.

Rapports de conformité

En matière de gestion des correctifs, les rapports de conformité sont essentiels. Le système automatisé d'Ivanti se concentre sur des KPI basés sur les risques qui reflètent les risques sur le terrain. Cela garantit que tous les correctifs sont documentés et respectent les normes réglementaires, réduisant ainsi considérablement la non-conformité. Le système aligne la gestion des correctifs sur les exigences de sécurité. Les SLA sont définis en tenant compte de la date de publication des mises à jour plutôt qu'en se basant sur les délais opérationnels IT habituels. Pour les équipes de sécurité confrontées aux difficultés des cycles contenus d'application des correctifs, cet aspect est primordial. En recalibrant les SLA sous l'angle de l'exposition aux vulnérabilités, le département IT peut mieux répondre aux exigences de sécurité tout en gérant les demandes opérationnelles : le cadre de sécurité global de l'entreprise est ainsi renforcé.

À propos d'Ivanti

Ivanti améliore et sécurise l'Everywhere Work pour favoriser la réussite des entreprises et l'efficacité des collaborateurs. Nous mettons la technologie au service des gens, et pas l'inverse. Aujourd'hui, les collaborateurs utilisent une multitude de périphériques personnels et professionnels pour accéder aux données et applications IT sur plusieurs réseaux, afin de rester productifs où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Ivanti est l'une des rares entreprises technologiques capable de détecter, de gérer et de protéger tous les actifs IT et postes client d'une entreprise. Plus de 40 000 clients, dont 85 entreprises Fortune 100, ont choisi Ivanti pour fournir une expérience numérique d'excellence aux collaborateurs, et améliorer la productivité et l'efficacité de leurs équipes IT et Sécurité. Chez Ivanti, nous nous efforçons de créer un environnement où tous les points de vue sont écoutés, respectés et valorisés. Nous nous engageons aussi pour un avenir plus durable pour nos clients, nos partenaires, nos collaborateurs et la planète. Pour en savoir plus ou pour contacter Ivanti, visitez le site ivanti.com.

ivanti neurons

Pour en savoir plus ou pour contacter Ivanti, visitez le site ivanti.com.

1. IBM, « Cost of a Data Breach Report 2024 », 2024. https://www.ibm.com/reports/data-breach
2. Verizon, « 2024 Data Breach Investigations Report », 2024.. https://www.verizon.com/business/resources/reports/dbir/
3. Google, « A Year in Review of Zero-Days Exploited In-the- Wild in 2023 », mar 2024. https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends
4. Richard Fang, Rohan Bindu, Akul Gupta, Qiusi Zhan, Daniel Kang, « Teams of LLM Agents can Exploit Zero-Day Vulnerabilities », 2 juin 2024. https://arxiv.org/abs/2406.01637.
5. Ivanti, « Les défis de la gestion des correctifs : Résultats d'enquête et informations, alors que les entreprises passent à l'Everywhere Workplace », 7 octobre 2021. https://www.ivanti.com/fr/resources/v/doc/ivi/2634/5318feb0a0ff.
6. Securin, « Ransomware Report 2023 Year in Review »,
7. 2024. https://www.securin.io/ransomware-report-2023-year-in-review-download/.
8. Ivanti, « 2024 État de la cybersécurité », 2024. https://www.ivanti.com/fr/resources/research-reports/state-of-cybersecurity-report