Kaspersky Vulnerability and Patch Management

Plus de simplicité et de sécurité grâce aux outils de gestion informatique centralisée

Points forts

- Détection et hiérarchisation automatisées des vulnérabilités
- Distribution automatisée des correctifs et des mises à jour pour plus de 150 applications
- Prise en charge du mode d'essai des correctifs
- Distribution programmée des correctifs
- Optimisation du trafic
- Surveillance des résultats et génération de rapports
- Outils complets de gestion client
- Installation logicielle et prise de contrôle à distance, y compris pour les sites distants
- Déploiement des systèmes d'exploitation

Les vulnérabilités non corrigées dans les applications largement utilisées représentent l'une des plus grandes menaces pour la sécurité informatique des entreprises. Mais le problème ne vient pas seulement des vulnérabilités de type « zero-day ». Du fait même de la complexification de l'informatique actuelle, il est toujours plus difficile de remédier aux insuffisances des logiciels vulnérables : si vous ne savez pas exactement ce qui est installé, comment sécuriser le tout ?

Les services informatiques sont confrontés à des tâches importantes, difficiles et impliquant la mobilisation de ressources considérables. La gestion et l'administration des mises à jour logicielles, ainsi que la surveillance continue des vulnérabilités potentielles, en font partie. Grâce à la centralisation et à l'automatisation des principales tâches de sécurité, de configuration et de gestion, telles que l'évaluation des vulnérabilités, la distribution des correctifs et des mises à jour, la gestion des inventaires et le déploiement d'applications, Kaspersky Vulnerability and Patch Management permet non seulement de gagner du temps, mais également de renforcer la sécurité.

Une visibilité complète

Grâce à une visibilité complète sur le réseau depuis une console unique, les administrateurs sont totalement au fait de chaque application et appareil entrant sur le réseau, y compris des appareils appartenant aux visiteurs. Cette visibilité permet un contrôle centralisé de l'accès aux données et aux applications de l'entreprise par utilisateur ou appareil, conformément aux politiques informatiques de l'entreprise et aux exigences de conformité réglementaires.

Sécurité renforcée

Renforcez la sécurité informatique et réduisez les charges de travail des tâches courantes grâce à des correctifs et mises à jour distribués automatiquement et au bon moment.

Kaspersky Vulnerability and Patch Management offre une visibilité complète et met à votre disposition toutes les informations nécessaires pour préserver la sécurité de votre entreprise. L'ensemble du cycle d'évaluation des vulnérabilités et de gestion des correctifs est automatisé : détection et hiérarchisation des vulnérabilités, téléchargement, test et distribution des correctifs et des mises à jour, surveillance des résultats et génération de rapports. Vous gagnez ainsi en efficacité tout en réduisant sensiblement l'impact sur les ressources.

Rationalisation des tâches informatiques

Kaspersky Vulnerability and Patch Management intègre divers outils de gestion permettant d'automatiser de nombreuses fonctions d'administration informatique. Distribution automatisée des applications avec accès à distance vérifié et dépannage pour réduire au minimum le temps et les ressources nécessaires à la mise en service de nouveaux postes de travail ou au déploiement de nouvelles applications.

Administrer de manière centralisée

Kaspersky Vulnerability and Patch Management est un composant géré de la console Kaspersky Security Center. Il est possible d'utiliser et de gérer chaque fonction à partir de cette console centrale à l'aide de commandes et d'interfaces homogènes et intuitives, la finalité étant d'automatiser les tâches informatiques courantes.

Évaluation des vulnérabilités et gestion des correctifs

ANALYSEZ VOTRE RÉSEAU POUR GÉNÉRER DES INVENTAIRES MATÉRIELS ET LOGICIELS.

La détection automatique et le suivi de l'équipement matériel et logiciel permettent aux administrateurs de connaître exactement les ressources présentes sur le réseau de l'entreprise. L'analyse automatisée des logiciels permet une détection rapide des logiciels obsolètes susceptibles de représenter un risque de sécurité et ayant besoin d'être mis à jour.

DÉTECTION ET HIÉRARCHISATION DES VULNÉRABILITÉS

L'analyse automatisée des vulnérabilités permet une détection, une hiérarchisation et une correction rapides des vulnérabilités. L'analyse des vulnérabilités peut s'exécuter automatiquement ou être programmée en fonction des exigences de l'administrateur. La gestion flexible des politiques facilite la distribution de logiciels mis à jour et compatibles, ainsi que la création d'exceptions.

TÉLÉCHARGEMENT, TEST ET DISTRIBUTION DES CORRECTIFS ET DES MISES À JOUR

Les mises à jour et les correctifs peuvent être téléchargés automatiquement depuis les serveurs de Kaspersky Lab. Vous pouvez les tester avant distribution afin d'éviter tout impact négatif sur les performances des systèmes et l'efficacité des employés. Les correctifs et les mises à jour peuvent être immédiatement distribués tandis que le déploiement des correctifs peut être différé.

SURVEILLANCE DES RÉSULTATS ET GÉNÉRATION DE RAPPORTS

Kaspersky Vulnerability and Patch Management indique aux administrateurs informatiques l'état d'installation des correctifs et leur permet de générer des rapports d'analyse, de rechercher d'éventuelles points faibles, de faire le suivi des modifications et d'évaluer la sécurité informatique de l'entreprise, au niveau du réseau comme de chaque appareil et système.

DISTRIBUTION LOGICIELLE RAPIDE ET EFFICACE

Déploiement/mise à jour à distance, depuis une seule console. Plus de 150 applications parmi les plus répandues, identifiées via Kaspersky Security Network, peuvent être automatiquement installées, après les heures de bureau si vous le souhaitez. Trafic réduit vers les sites distants grâce à la technologie Multicast pour la distribution logicielle en local.

Outils de gestion

DÉPANNAGE À DISTANCE

Pour bénéficier de temps de réponse réduits, d'une plus grande efficacité et d'une meilleure assistance pour les sites distants, Kaspersky Security Center utilise RDP et la technologie de partage de bureau Windows (via l'assistance à distance Windows). La connexion à distance aux ordinateurs client via l'agent d'administration assure aux administrateurs un accès intégral aux données et aux applications sur le client, même lorsque les ports TCP et UDP sont fermés. Un mécanisme d'autorisation empêche l'accès à distance par les personnes non autorisées et, pour des raisons de traçabilité et de vérification, toutes les activités effectuées au cours d'une session d'accès à distance sont enregistrées dans un journal.

DÉPLOIEMENT DU SYSTÈME D'EXPLOITATION

Kaspersky Vulnerability and Patch Management automatise et centralise la création, le stockage et le clonage d'images système sécurisées, et permet le déploiement de systèmes d'exploitation sur de nouvelles machines, ainsi que les réinstallations. Toutes les images sont conservées dans un inventaire spécial, immédiatement accessible pendant le déploiement. Les images des stations de travail client peuvent être déployées soit par le biais de serveurs PXE (Preboot eXecution Environment, qui peuvent également servir pour les nouvelles machines sans système d'exploitation), soit par le biais de tâches Kaspersky Vulnerability and Patch Management (déploiement d'images de système d'exploitation sur des machines client gérées).

En envoyant des signaux Wake-on-LAN aux ordinateurs, vous pouvez distribuer automatiquement les images après les heures de bureau normales. UEFI est également pris en charge.

Comment acheter

Kaspersky Vulnerability and Patch Management est disponible :

- En tant que composant de Kaspersky Endpoint Security for Business Advanced
- En tant que composant de Kaspersky Total Security for Business
- En tant que module complémentaire pour Kaspersky Endpoint Security for Business Select
- En tant que solution à la carte

www.kaspersky.fr
#truecybersecurity