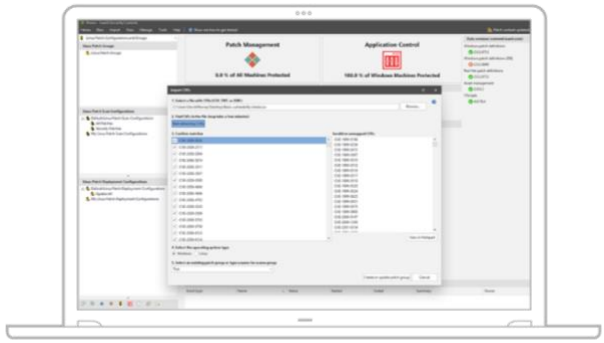
Ivanti Security Controls

Les équipes IT passent trop de temps à gérer la sécurité de périphériques toujours plus nombreux ; par ailleurs, les équipes Sécurité souffrent d'un manque de main-d'œuvre avéré. C'est pourquoi Ivanti simplifie la gestion de la sécurité IT à l'aide d'une solution unifiée qui cible les vecteurs d'attaque les plus fréquents. Ivanti Security Controls (anciennement Ivanti Patch pour Windows) regroupe des outils de sécurité dont les experts mondiaux s'accordent à penser qu'ils créent les barrières les plus solides contre les cyberattaques modernes : découverte des logiciels autorisés et non autorisés dans votre environnement pour vous protéger et vous défendre, gestion des correctifs pour votre environnement OS et applicatifs hétérogène, création de listes blanches dynamiques et gestion granulaire des privilèges. La solution comprend également des outils supplémentaires qui aident les départements IT et Sécurité à mieux collaborer pour mieux protéger l'entreprise.

Correctifs pour Windows et Linux

Ivanti Security Controls est une solution unique de gestion automatisée des correctifs qui s'applique non seulement aux serveurs Windows physiques et virtuels, mais aussi aux postes de travail. Nous avons, par ailleurs, ajouté la prise en charge des correctifs Red Hat Enterprise Linux à la solution d'application de correctifs leader du marché.

- **Appliquez des correctifs à vos serveurs virtuels.** Trouvez les postes de travail et serveurs en ligne et hors ligne, recherchez les correctifs manquants et déployez-les. Appliquez ensuite les correctifs à tout votre environnement, des OS aux applications en passant par les machines virtuelles (VM) et même l'hyperviseur ESXi, grâce à l'intégration étroite du produit avec VMware. Il est possible de maintenir même les images virtuelles hors ligne pour qu'elles soient constamment prêtes au déploiement. Vous ne voulez pas suivre les deux étapes du processus de création d'une VM et devoir lui appliquer des correctifs. En tenant vos modèles hors ligne à jour à tout moment, vous pouvez déployer une VM sans avoir à vous inquiéter de savoir si elle est bien à jour.



- **Appliquez des correctifs sans agent.** La technologie sans agent vous permet d'évaluer des correctifs et de les déployer sur les postes de travail et serveurs connectés à votre réseau, tout en limitant l'impact sur votre équipe et sur la charge de traitement du système. Sinon, vous pouvez utiliser l'agent pour créer autant de stratégies d'agent différentes que nécessaire pour gérer votre réseau, ce qui offre une extrême flexibilité pour les correctifs. L'agent assure aussi un meilleur suivi des correctifs dans les environnements où les périphériques ne sont pas constamment connectés au réseau. Attribuez une configuration d'agent différente à chaque périphérique de votre entreprise.
- **Appliquez des correctifs à vos machines Windows et Linux.** Vous devez intégrer à votre ensemble de solutions de gestion, un logiciel de gestion des correctifs capable de gérer les environnements hétérogènes d'aujourd'hui. Il est

indispensable d'étendre l'application des correctifs au-delà de Windows. En procédant de manière efficace, avec une seule interface et un outil automatisé, non seulement vous allégez la charge de travail du département IT, mais vous limitez les risques d'erreur humaine tout en renforçant vos défenses.

- **Appliquez des correctifs à vos applications.** Les applications tierces comme Adobe Acrobat Flash et Reader, Google Chrome, Mozilla Firefox et Oracle Java sont les applications et extensions de navigateur le plus souvent ciblées par les pirates.

  Notre catalogue de correctifs est le plus riche du marché et notre équipe Contenu fait passer toute une série de tests de qualification et de validation à chacun de ces correctifs pour vous éviter de le faire vous-même. Vous et votre équipe gagnez ainsi du temps, pour vous consacrer aux principaux objectifs de l'entreprise.

Une gestion pertinente des listes blanches et des privilèges

Ivanti Security Controls inclut aussi une fonction de gestion dynamique des listes blanches. Elle utilise des modèles de confiance à la place des listes, ce qui réduit les délais de formation, les coûts de possession une fois le système opérationnel et l'impact sur les performances, tout en assurant un niveau de sécurité très élevé en bloquant toutes les attaques de type « zero day ». Cela permet aussi au département IT de retirer aux utilisateurs leurs droits Admin, tout en les autorisant à effectuer leurs opérations respectives. De plus, cela facilite le processus d'ajout de permissions supplémentaires en cas de besoin.

- **Simplification des listes blanches.** La solution permet un accès autorisé aux applications, services et composants sans que le département IT ait besoin de gérer manuellement de très longues listes et sans contrainte pour les utilisateurs. La fonction Trusted Ownership™, par exemple, permet d'utiliser la notion de propriétaire NTFS d'un fichier afin de simplifier le processus de listes blanches.

  L'utilisation de plusieurs comptes de confiance pour définir les propriétaires des fichiers de confiance facilite l'implémentation d'une liste blanche, ainsi que l'ajout et la mise à jour permanents des applications via vos systèmes de gestion, étant donné que les propriétaires de confiance sont les comptes qui effectuent l'installation et les opérations de mise à jour/à niveau.

- Prenez le contrôle des clés du royaume. Il existe de nombreuses vulnérabilités, lesquelles si elles sont exploitées, donnent au pirate des permissions identiques à celles de l'utilisateur actuel. Les pirates peuvent utiliser des références d'authentification volées et les droits Admin de l'utilisateur concerné afin d'avoir un accès complet aux informations et systèmes, et s'infiltrer encore plus loin sur votre réseau. L'attribution de droits Admin sur un serveur présente aussi d'autres risques, notamment la possibilité de démarrer ou d'arrêter des services et d'installer ou de supprimer un logiciel par erreur.
- Certaines entreprises appliquent encore une stratégie de verrouillage total des permissions utilisateur, mais les utilisateurs ont généralement besoin de certaines fonctions qui exigent inévitablement qu'on leur attribue des privilèges d'administration sur leur système. Microsoft n'offre que deux niveaux de contrôle : Utilisateur ou Admin (Accès complet). Il existe quelques variantes entre les deux, mais pas assez pour assurer une bonne expérience à l'utilisateur ou à l'administrateur.
- Notre solution fournit des fonctions JEA (Just Enough Administration) et de JIT (Just-in-Time Administration), ce qui vous permet de retirer aux utilisateurs leurs droits administrateurs, tout en les autorisant quand même à effectuer les opérations dont ils ont besoin, notamment grâce à l'élévation et l'ajout facile de privilèges en cas de besoin. Désormais, vous avez le choix. Vous pouvez basculer un administrateur avec droits complets au niveau d'un utilisateur standard et autoriser l'élévation des privilèges quand cela s'avère nécessaire. L'utilisateur pourra ainsi installer des applications, une imprimante, il pourra utiliser PowerShell ou tout autre produit dont il a besoin, mais il ne disposera pas de plus de privilèges que ceux qu'il doit posséder.
- Vous pouvez également modifier le compte de cet administrateur à droits complets pour éliminer les éléments auxquels il ne doit pas avoir accès. Bloquez PowerShell, par exemple, ou l'accès à des fonctions spécifiques. Limitez les privilèges d'administration à des consoles, à des applications, à des services et commandes spécifiques pour limiter les risques qu'un administrateur introduise des malwares, stoppe des services essentiels ou affecte les performances de services indispensables.

Plus d'outils pour gagner du temps et de l'argent

Ivanti Security Controls inclut également les fonctions suivantes, simplifiant ainsi encore plus aux départements Sécurité et Opérations IT leur tâche de sécurisation de l'entreprise.

- **Intégration et automatization au-delà d'Ivanti** Les API REST de correctifs permettent à Security Controls de s'intégrer à d'autres produits, d'automatiser les processus partagés, et d'assurer l'accès à distance et le contrôle à distance de la console.
- **Comblez le fossé entre Sécurité et Opérations IT en utilisant des CVE pour la création de listes de correctifs.** Ivanti Security Controls peut effectuer une évaluation des vulnérabilités de tous les fournisseurs utilisés dans l'entreprise, découvrir les correctifs qui concernent les vulnérabilités CVE (Common Vulnerabilities and Exposures) et constituer un groupe de mises à jour de correctifs, qui peut rapidement être approuvé en vue de son déploiement dans l'environnement. C'est un gain de temps énorme, qui remplace le processus manuel actuel.

En savoir plus

www.ivanti.fr
+33 (0)1 49 03 77 80
contact@ivanti.fr