

Ivanti Device Control

Les fuites de données que provoque l'utilisation accidentelle (voire parfois malveillante) de périphériques et/ou supports amovibles atteignent un niveau inquiétant. Ivanti® Device Control applique des stratégies de sécurité à l'utilisation de périphériques amovibles et au chiffrement des données. La solution centralise la gestion des périphériques et des données via une approche de type liste blanche/« refus par défaut ». De plus, elle offre un niveau de protection supplémentaire contre les malwares introduits par des moyens physiques.

Protégez les données des pertes et des vols

Plus vos collaborateurs travaillent à distance, plus ils ont besoin d'un accès hors du réseau. Mais l'impact potentiel des pertes de données, accidentelles ou malveillantes, est vraiment préoccupant. Aujourd'hui, les supports/périphériques amovibles constituent le vecteur de fuites de données le plus courant : pas de limites aux copies de fichiers, pas de chiffrement, pas de pistes d'audit et pas de gestion centralisée. Ivanti Device Control vous permet d'utiliser ces outils qui améliorent la productivité tout en limitant leur potentiel de fuites de données (et l'impact associé).

Principales fonctions

Liste blanche / « Refus par défaut »

Attribuez des permissions d'accès aux périphériques et supports amovibles autorisés à des utilisateurs ou des groupes d'utilisateurs spécifiques. Par défaut, l'accès est refusé à tous les périphériques/supports et utilisateurs non explicitement autorisés.

Chiffrement par stratégie pour le stockage amovible

La solution chiffre de manière centralisée les périphériques (comme les lecteurs USB Flash) et les supports (DVD, CD, etc.) amovibles, et applique des stratégies de chiffrement à la copie de données vers ces périphériques/supports.

Restrictions de copie des données

La solution restreint la quantité quotidienne de données copiées vers les périphériques et supports amovibles, pour chaque utilisateur, et limite l'utilisation de ces périphériques/supports à certaines périodes ou à certains jours.

Filtrage des types de fichiers

La solution contrôle les types de fichiers dont le déplacement vers et depuis les périphériques/supports amovibles est autorisé, pour chaque utilisateur, ce qui limite la propagation des malwares.

Gestion centralisée / Rôles d'administrateur

La solution centralise la définition et la gestion de l'accès des utilisateurs, groupes d'utilisateurs, ordinateurs et groupes d'ordinateurs aux périphériques ou supports amovibles autorisés sur le réseau. Par défaut, l'accès est refusé à tous les périphériques/supports et utilisateurs non explicitement autorisés.

Accès temporaire/planifié

La solution accorde aux utilisateurs un accès temporaire/planifié aux périphériques et supports amovibles, ce qui permet d'autoriser l'accès « à l'avenir » sur une période limitée.

Permissions contextuelles

Les stratégies d'accès/d'utilisation restent en vigueur quel que soit l'état de la connexion, et vous pouvez les adapter selon que le poste client est connecté ou non au réseau.

Contrôle d'accès fondé sur les rôles

La solution affecte des permissions à des utilisateurs ou groupes d'utilisateurs en fonction de leur identité Windows Active Directory ou Novell eDirectory (les deux systèmes sont pris en charge).

Agent protégé contre les manipulations

La solution installe des agents sur chaque poste client du réseau. Ces agents sont protégés contre toute suppression non autorisée, même par des utilisateurs dotés de droits d'administrateur. Seuls les administrateurs Device Control peuvent désactiver cette protection.

Architecture flexible/évolutive

La solution permet un contrôle et une application des paramètres à l'échelle de l'entreprise, grâce à une architecture client-serveur évolutive dotée d'une base de données centrale optimisée pour de meilleures performances. Les configurations de serveur virtualisé sont prises en charge.



Fonctionnement d'Ivanti Device Control

- 1. Découvrez** tous les périphériques amovibles qui sont actuellement connectés (ou l'ont été par le passé) à vos postes client.
- 2. Évaluez** tous les périphériques Plug-and-play, par classe, groupe, modèle et/ou ID spécifique, et définissez des stratégies via une approche de listes blanches.
- 3. Mettez en place** des limitations de copie de fichiers, le filtrage des types de fichier et des stratégies de cryptage forcé pour les données déplacées vers des périphériques amovibles.
- 4. Surveillez** l'ensemble des changements de stratégie, des activités des administrateurs et des transferts de fichiers pour garantir une application constante des stratégies.
- 5. Générez des rapports** sur l'utilisation des périphériques et des données afin de prouver votre conformité aux stratégies de l'entreprise et/ou aux réglementations en vigueur.

« L'un des principaux avantages du déploiement d'Ivanti Device Control est sa fonction de listes blanches, qui garantit qu'aucun périphérique non autorisé ne peut être utilisé, quelle que soit la façon dont il est connecté. Les périphériques USB à mémoire Flash représentent un vrai risque, car ils peuvent servir à voler des données à l'entreprise ou à introduire des « malwares » susceptibles d'empêcher l'utilisation des ordinateurs et d'infecter rapidement d'autres PC sur le même réseau. Ivanti Device Control est un produit puissant et facile à utiliser, c'est pourquoi Barclays a choisi cette solution. »

*Paul Douglas
Responsable de l'équipe Construction du poste de travail ADIR
Barclays*

Découvrez les avantages d'Ivanti Device Control

- Protection des données contre la perte et le vol
- Sécurisation de l'exécution des outils de productivité
- Amélioration de l'application des stratégies de sécurité
- Contrôle précis, grâce aux limites d'accès
- Blocage de l'infiltration des malwares via des moyens physiques, et le mappage de structures de gestion centralisées et décentralisées
- Surveillance de tous les transferts de fichiers vers les imprimantes et les supports physiques



www.ivanti.fr



+33 (0)1 49 03 77 80



sales@ivanti.com