Le défi actuel

Les employés d'une entreprise utilisent souvent des périphériques de stockage amovibles pour transporter des données vitales et sensibles. Bien que ces derniers soient pratiques, ils peuvent également constituer une menace pour la sécurité de l'information s'ils sont exploités ou mal utilisés. La meilleure pratique consiste à surveiller et à gérer étroitement les actions et les déplacements de ces périphériques.

Comment Device Control Plus s'intègre dans votre environnement informatique

Device Control Plus peut être utilisé par les administrateurs informatiques pour obtenir un contrôle complet sur les nombreux périphériques de leurs réseaux. Cette solution logicielle robuste comprend un ensemble distinct de fonctionnalités qui permettent de créer des politiques d'accès aux fichiers flexibles et de contrôle des transferts. Ainsi, en attribuant le niveau approprié d'autorisations aux périphériques, tous les transferts de données effectuées via des périphériques intégrés et externes peuvent être minutieusement suivis et réglementés.

Points forts

- Auto-détection et gestion de plus de 17 types de périphériques et surveillance continue des ports de réseau.
- De nombreux paramètres évolutifs pour les politiques de protection de fichiers.
- Recherche méticuleuse de l'emplacement des fichiers, des utilisateurs et des points terminaux impliqués dans les opérations de transfert de données.
- Des dispositions temporaires d'accès pour encourager une collaboration à court terme avec des utilisateurs tiers
- Des rapports détaillés et des alertes rapides qui permettent une meilleure visibilité sur les appareils et les actions des fichiers.

Device Control Plus est essentiel pour éviter la perte de données par supports USB et amovibles, et est conçu pour que des mesures préventives et réparatrices puissent être mises en œuvre efficacement. Cet outil de prévention des fuites de données comporte des fonctionnalités telles que la mise sur liste noire et le blocage de l'accès aux données, qui sont deux de ses nombreuses méthodes pour dissuader les attaques basées sur des fichiers. En cas d'urgence, des protocoles hors normes tels que le traçage et la copie miroir des fichiers peuvent également être adoptés pour garantir la préservation de l'intégrité du réseau et la conservation de la valeur de la marque.

Fonctionnalités

Gestion des périphériques et des ports

Gérez efficacement plus de 17 types de périphériques à partir d'une seule console. Découvrez automatiquement les ports actifs de votre réseau et détecter quels sont les périphériques connectés à vos ordinateurs. Prenez des mesures proactives pour prévenir les injections de logiciels malveillants et la perte de données par inadvertance en désactivant l'exécution automatique sur tous les appareils douteux.

Contrôle d'accès aux fichiers

Créez et affinez les politiques de contrôle d'accès aux fichiers en fonction des services spécifiques et des fonctions des employés au sein de votre entreprise. Le protocole de contrôle d'accès basé sur les rôles garantit que tous les utilisateurs aient un accès suffisant aux informations de l'entreprise, relatives à leurs rôles, tandis que les autres données sans rapport avec leurs tâches sont maintenues hors limites. Des dispositions telles que les autorisations en lecture seule minimisent également la perte de données car les informations critiques pour l'entreprise peuvent être limitées à certains utilisateurs.

Copie de fichiers

Créez automatiquement des copies miroirs des fichiers transférés à partir d'un périphérique particulier. Les copies sont ensuite sauvegardées dans un dossier partagé, protégé par un mot de passe. En cas d'urgence, cette mesure de précaution permet d'identifier le contenu exact des fichiers transférés et aide à l'élaboration de stratégies de remédiation précises.

Contrôle des transferts de fichiers

Réglementez le nombre et le type de données transférées par des périphériques. En limitant le nombre d'octets, seules les informations vitales pour la tâche à accomplir sont transférées. En limitant le type d'extensions de fichier qui peuvent être copiées, les fichiers sensibles comme par exemple le code source, ou les documents financiers qui comportent des extensions .xml et/ou .xls, peuvent être bloqués pour les utilisateurs non autorisés.

Autorisations

Appliquez une politique de confiance zéro dans votre entreprise en bloquant par défaut tous les périphériques, à l'exception de quelques périphériques de confiance qui sont couramment utilisés par le personnel de base. Pour une sécurité accrue, l'option permettant de n'autoriser que les périphériques cryptés par BitLocker est également disponible. Pour chaque groupe ou ordinateur personnalisé, il est possible de créer des politiques concernant uniquement les périphériques de confiance. Ceci est avantageux car des privilèges plus élevés peuvent être attribués uniquement pour les périphériques utilisés uniquement par les employés clés ou pour des tâches spéciales.

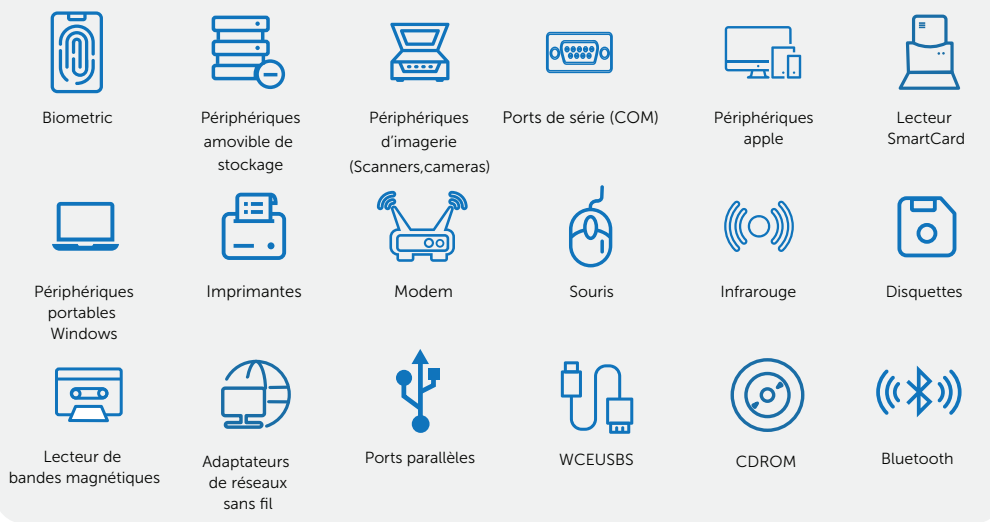
Accès provisoire

Dans les cas où des périphériques sur liste grise ou bloqués requièrent l'accès à des ordinateurs pour des tâches spécifiques, vous pouvez attribuer des autorisations en toute sécurité afin que les périphériques puissent obtenir les informations nécessaires sans compromettre la cyberhygiène. Lorsque des utilisateurs tiers ou des employés de niveau inférieur se voient accorder un accès à court terme, assurez-vous que les sessions et les actions sur les fichiers soient étroitement surveillées.

Rapports et audits

Générez des rapports détaillés, disponibles facilement, pour toutes les opérations de transfert de périphériques et de fichiers. Les audits peuvent être analysés de près afin de détecter toute intrusion indésirable ou tout écart par rapport à la politique d'accès. Les journaux offrent également un aperçu des habitudes des utilisateurs et des périphériques, de sorte que les politiques existantes peuvent être modifiées ou que de nouvelles politiques peuvent être créées pour renforcer le réseau.

Périphériques pris en charge



Configuration matérielle requise pour les serveurs Device Control Plus

Nb d'ordinateurs	Informations processeurs	Taille de RAM	Espace disque dur
1 jusqu'à 250	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MO cache	2 GO	5 GO
251 jusqu'à 500	Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MO cache	4 GO	10 GO
501 jusqu'à 1000	Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MO cache	4 GO	20 GO
1 001 jusqu'à 3000	Intel Core i5 (4 core/4 thread) 2.3 GHz. 6 MO cache	8 GO	30 GO
3 001 jusqu'à 5000	Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MO cache	8 GO	40 GO
5 001 jusqu'à 10 000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 20 MO cache	16 GO	60 GO
10 001 jusqu'à 20 000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 40 MO cache	32 GO	120 GO

OS pris en charge pour les serveurs Device Control Plus

Windows 7	Windows 8	Windows 8.1	Windows 10
Windows Server 2003	Windows Server 2003 R2	Windows Server 2008*	Windows Server 2008 R2*
Windows Server 2012	Windows Server 2012 R2*	Windows Server 2016*	Windows Server 2019*

OS pris en charge pour les agents Device Control Plus

Windows OS	Windows Server OS
Windows 10	Windows server 2016
Windows 8.1	Windows server 2012 R2
Windows 8	Windows server 2012
Windows 7	Windows server 2008 R2
	Windows server 2003

Navigateurs supportés

Vous devez installer l'un des navigateurs suivants sur votre ordinateur pour accéder à la console Device control Plus :

- Microsoft Edge
- Microsoft Internet Explorer 11
- Mozilla Firefox 44 et versions ultérieures
- Google Chrome 47 et versions ultérieures

PG Software EUROPE

Pour plus de détails

- www.manageengine.fr/device-control-plus
- commercial@pgsoftware.fr
- 0 805 296 540 Service & appel gratuits

ManageEngine
IT Management, Simplified