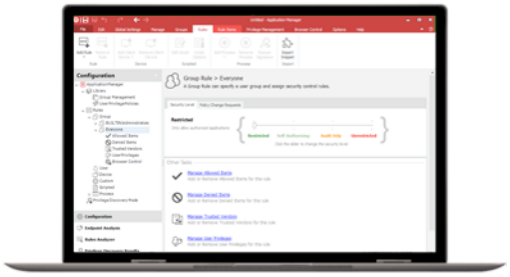
Contrôle des applications

Renforcez la sécurité des postes client, allégez la charge de travail du département IT et réduisez les coûts.



Ivanti® Application Control offre au département IT un contrôle sans précédent des postes client. La solution élimine les risques de sécurité tout en fournissant à l'utilisateur une expérience de qualité dans les environnements Windows les plus récents. Outre le contrôle contextuel des applications, la solution permet une gestion sécurisée des privilèges Windows, qui vous permet de supprimer les droits administrateurs afin de bloquer tout exécutable non autorisé, comme les malwares, les ransomwares, les logiciels sans licence et autres applications inconnues : ils ne peuvent être ni installés ni exécutés. Application Control permet également à votre équipe IT de gérer l'accès aux applications et les privilèges utilisateur de manière efficace dans l'ensemble de votre parc de postes de travail et de serveurs.

Prise en charge complète de Windows Server 2016 et prise en charge étendue de Windows 10

Application Control 10.1 assure une prise en charge complète de Windows Server 2016 et une prise en charge étendue de Windows 10, ce qui renforce sa capacité à bloquer les ransomwares et les malwares. Cette nouvelle version offre également aux administrateurs IT un contrôle amélioré et plus détaillé des utilisateurs finaux, qui renforce la sécurité du poste client et la personnalisation par l'utilisateur.

Trusted Ownership™ (Propriétaire de confiance)

Application Control utilise la fonction de propriétaire de confiance (Trusted Ownership), qui contrôle la sécurité du poste client dès l'installation. Elle repose sur l'examen du propriétaire NTFS d'une application. Lorsqu'une application est introduite (et possédée) par un propriétaire qui n'est pas de confiance, comme un utilisateur standard, le système interdit instantanément à l'application de s'exécuter.

Cependant, si l'application est introduite et possédée par un « propriétaire de confiance », à savoir un administrateur ou un système de déploiement de logiciels comme Microsoft SCCM, tous les utilisateurs peuvent exécuter cette application, sauf mesure contraire. Cela épargne au département IT la charge constante de maintenance des listes blanches typiques des autres solutions de contrôle des applications, lorsque le contenu d'application ou de système d'exploitation est mis à jour.

Signatures numériques

Vous pouvez attribuer aux applications et aux fichiers des signatures numériques SHA-1, SHA-256 ou ADLER32 afin de garantir l'intégrité des applications, et d'interdire l'exécution des applications modifiées ou avec usurpation d'identité.

Listes blanches et listes noires

Le département IT peut combiner des configurations de listes blanches et noires avec Trusted Ownership, afin de contrôler les applications connues qui réussissent le test de propriétaire NTFS. Les applications auxquelles les

utilisateurs ne doivent pas accéder, notamment les outils dont l'administrateur est propriétaire, comme cmd.exe ou ftp.exe, sont automatiquement bloquées. Il est également possible de créer des listes blanches pour garantir que seules les applications de confiance connues peuvent s'exécuter sur un système.

Gestion des privilèges Windows

En fournissant aux utilisateurs des droits administrateurs complets, vous rendez de fait vos postes client vulnérables, vous augmentez considérablement les coûts liés à la gestion et à la sécurité, vos utilisateurs perdent en productivité, vous engendrez des problèmes légaux et de responsabilité juridique, et la mise en conformité devient compliquée. En supprimant les droits administrateurs et en attribuant aux utilisateurs des privilèges de niveau plus élevé, et ceci uniquement pour les applications ou tâches dont ils ont besoin, vous simplifiez la sécurité du poste client, limitez le nombre d'appels au support et réduisez le coût total de possession (TCO).

Demandes de changement à la demande

Les utilisateurs mobiles et ceux qui travaillent beaucoup hors connexion peuvent avoir besoin d'accéder à des applications non approuvées. Si vous interdisez l'accès à ces applications, vous nuisez à la productivité et à la qualité de l'expérience utilisateur. La fonction de demandes de changement à la demande permet aux utilisateurs finaux de demander une élévation en urgence de leurs privilèges ou un accès d'urgence à l'application concernée, lorsque leur productivité est affectée par la non-disponibilité des applications.

Redirection d'URL

Si un utilisateur laisse un navigateur Web ouvert sur une page Web ou une application spécifique, puis qu'il se reconnecte depuis un autre périphérique ou à un autre emplacement, son navigateur peut être redirigé vers une adresse sûre prédéfinie.

Archivage des applications

L'application copie automatiquement les fichiers interdits que les utilisateurs ont tenté d'exécuter et les stocke dans un référentiel sécurisé pour les analyser en toute sécurité.

Gestion des licences

Application Control est plébiscité par Microsoft pour l'application du contrôle des licences logicielles. En contrôlant les utilisateurs ou les périphériques qui ont la permission d'exécuter des applications nommées, il est possible de définir des limites concernant le nombre d'instances de chaque application, les périphériques ou utilisateurs autorisés à exécuter l'application, le moment où les utilisateurs peuvent exécuter un programme et la durée d'exécution.

www.ivanti.fr

+33 (0)1 49 03 77 80

sales@ivanti.com