

# ManageEngine

La gestion informatique  
simplifiée

Solution de gestion informatique en temps réel

# ManageEngine

Division des solutions de gestion informatique d'entreprise de Zoho Corporation

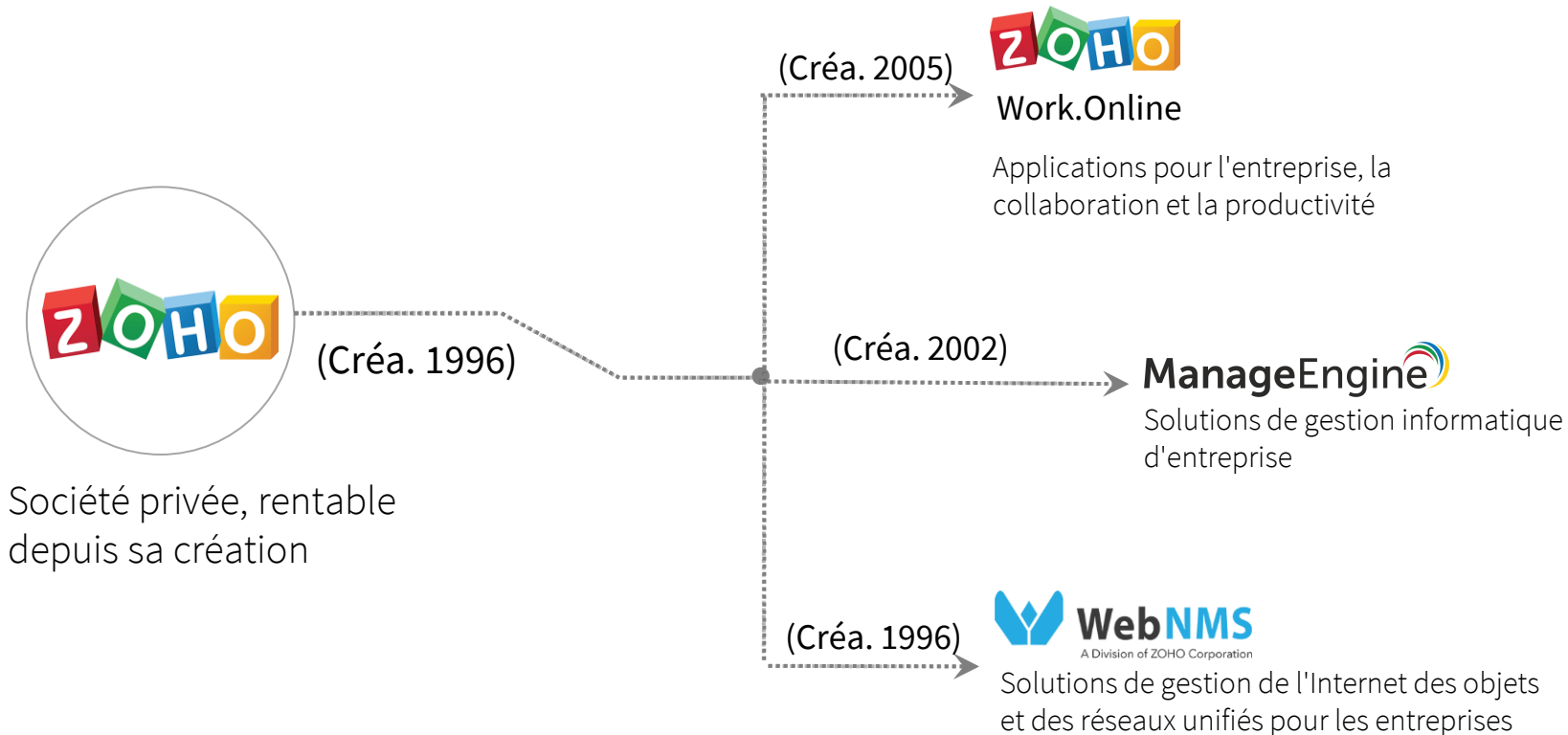
Fondée en 1996 sous le nom d'AdventNet

Entreprise privée, fournisseur et partenaire solide

Siège social à Pleasanton, en Californie

Des millions de clients dans tous les secteurs d'activité

# ManageEngine - la division de gestion informatique d'entreprise de ZOH O Corporation



# Solutions ManageEngine



## Gestion Active Directory

Active Directory  
Serveur Exchange  
Portail libre-service  
Restauration et sauvegarde



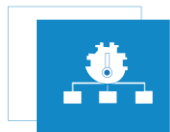
## Gestion des terminaux

Gestion des postes de travail  
Gestion des appareils mobiles  
Déploiement de systèmes d'exploitation  
Gestion des correctifs  
Gestion des navigateurs  
Gestion des vulnérabilités



## Gestion des services informatiques

Centre d'assistance  
Cycle de vie des actifs  
CMDB et ITIL  
Support client



## Gestion des opérations informatiques

- Performance du réseau
- Performance des applications
- Expérience de l'utilisateur final
- Changement et configuration du réseau
- Infrastructure convergente
- Infrastructure de stockage
- Bande passante et trafic
- Supervision du serveur SQL



## Sur-Demande

- Performance des applications
- Logiciel de centre d'assistance
- Récupération et sauvegarde d'Active Directory
- Gestion des appareils mobiles
- Gestion des correctifs
- Gestion des journaux



## Sécurité informatique

- Gestion des journaux
- Analyse des pare-feu
- Analyse des vulnérabilités
- Mot de passe privilégié
- Détection d'anomalies sur le réseau

# 2 millions d'utilisateurs

---

3 des 5 entreprises du  
**Fortune 100** sont clientes de  
ManageEngine

Standard  
Chartered 



 **BARCLAYS**

L'ORÉAL

  
**SAINT-GOBAIN**

JPMORGAN CHASE & CO.

 **AT&T**

**ManageEngine** 

# Device Control Plus

Solution automatisée pour le contrôle centralisé des appareils et la gestion de la sécurité des fichiers

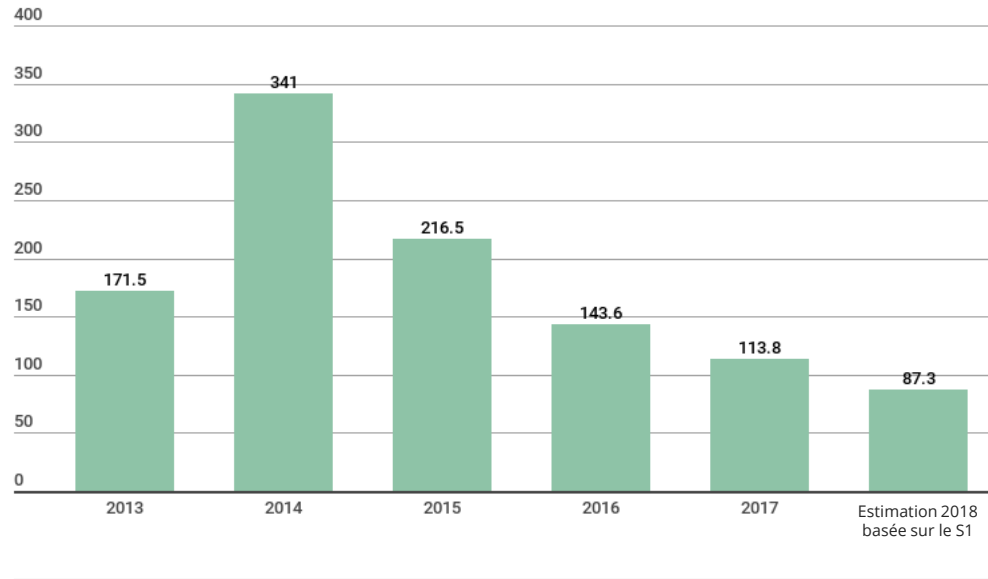
# Qu'est-ce que Device Control Plus?

**Device Control Plus** est une solution complète de contrôle des périphériques et de gestion des mouvements de fichiers qui prend en charge la détection et la gestion basée sur la confiance zéro de divers périphériques intégrés et externes. Les capacités de sécurité de l'information de ce produit aident les organisations à sécuriser le périmètre de leur réseau et à limiter efficacement les pertes de données.

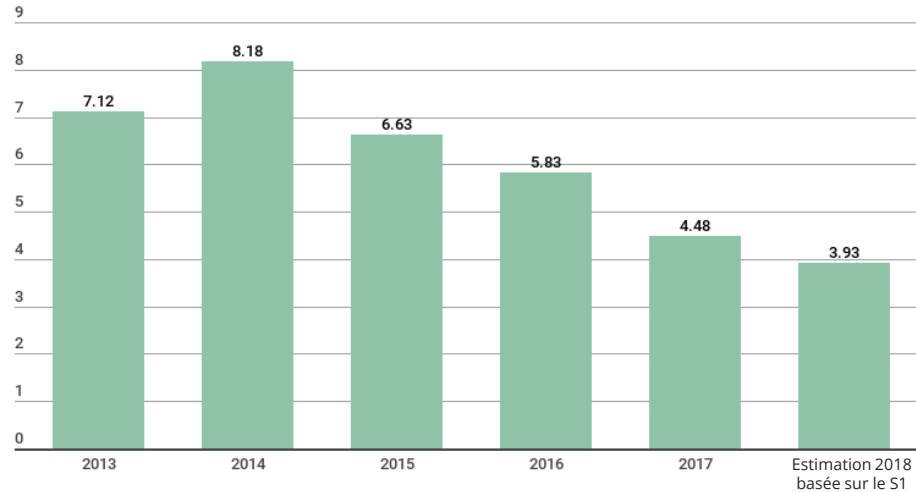
# Pourquoi le contrôle des périphériques est-il important pour votre entreprise?



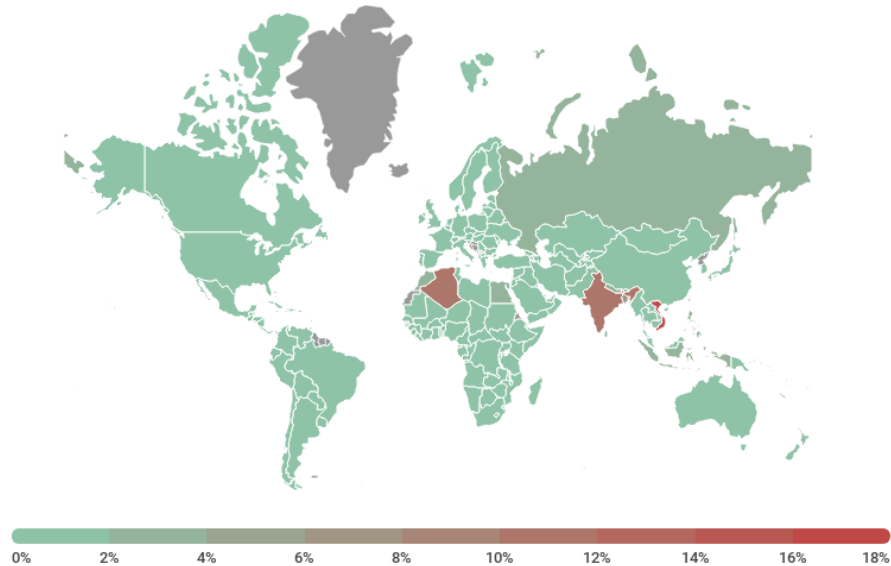
## Nombre total (en millions) d'infections de logiciels malveillants par des supports amovibles 2013 - 2018.



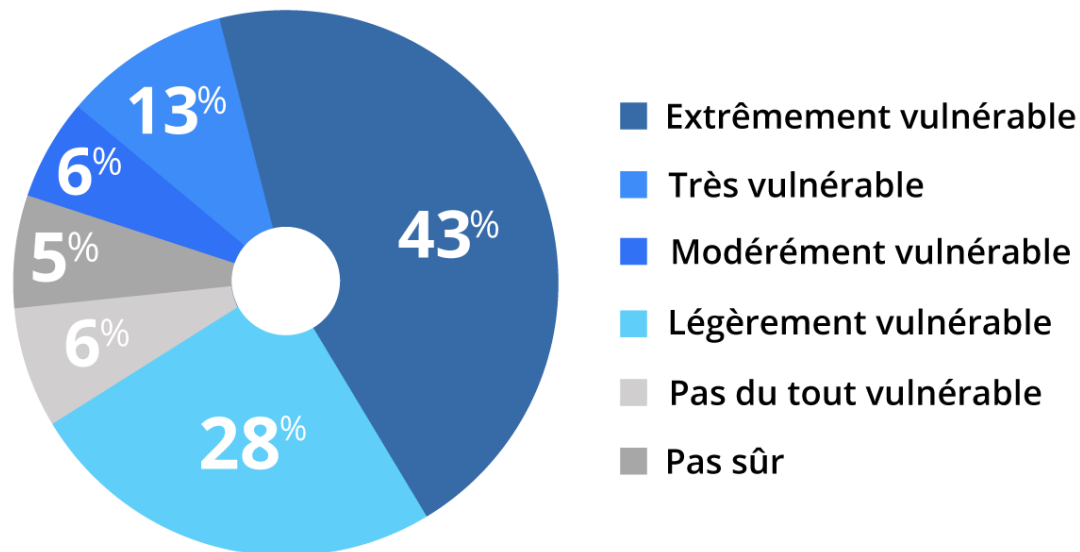
## Nombre d'utilisateurs uniques (en millions) touchés par des infections de logiciels malveillants par des supports amovibles 2013 - 2018.



## Proportion d'utilisateurs affectés par un exploit particulier via un support amovible, 2018.



Les capacités traditionnelles de contrôle des périphériques laissent toujours les organisations avec des quantités massives **de fichiers non protégés**.  
**Une solution logicielle robuste est nécessaire pour prévenir la perte de données.**



De nombreuses entreprises de différents secteurs sont menacées par des attaques internes ou des pertes de données dues à une mauvaise utilisation des appareils.  
La vôtre pourrait être l'une d'entre elles.

## Qui est exposé au risque ?



Services financiers



Télécommunications



Services techniques



Organisation industrielle



Secteur de santé



Gouvernement

## Obstacles à un contrôle efficace des dispositifs

- De nombreuses connexions de périphériques se produisent chaque jour, ce qui peut être difficile à suivre sans détection automatique.
- Les différents utilisateurs/rôles nécessitent différents niveaux d'accès, ce qui peut prendre beaucoup de temps pour attribuer manuellement les autorisations d'accès à chaque fois.
- Un contrôle d'accès rudimentaire, tel que l'autorisation ou le blocage complet, peut être trop restrictif, contre-productif et/ou dangereux.
- Les restrictions de transfert de données peuvent être difficiles à appliquer sans politiques granulaires.

# Une solution polyvalente pour la sécurité des appareils et des données

- Le contrôle des périphériques est l'une des mesures de sécurité les plus fondamentales parmi l'ensemble des protocoles de prévention des pertes de données.
- Avec Device Control Plus, sécurisez votre réseau et évitez toutes les attaques internes et les acteurs malveillants en détectant et en gérant rapidement les nombreux périphériques connectés à votre réseau.
- En outre, protégez toutes les données critiques de l'entreprise et, le cas échéant, facilitez le transfert sécurisé des données grâce à des fonctionnalités telles que le contrôle de l'accès et du transfert des fichiers, le traçage et le suivi des fichiers et l'octroi d'un accès temporaire aux périphériques.

# Mettez en place un contrôle complet des périphériques en 3 étapes

- Sélectionnez un type de périphérique et choisissez des périphériques spécifiques.
- Configurez une politique en fonction de vos besoins opérationnels spécifiques.
- Associez la politique à des groupes d'ordinateurs personnalisés.

# Aperçu des fonctionnalités

- Découverte automatique des périphériques
- Contrôle de l'accès aux fichiers
- Contrôle du transfert de fichiers
- Traçage des fichiers
- Réplication des fichiers
- Accès temporaire
- Rapports détaillés

# Découverte automatique des dispositifs

- Détectez automatiquement plus de 17 types de périphériques intégrés et externes.
- Classez chaque périphérique découvert comme étant de confiance, autorisé ou bloqué.
- Créez une liste de "dispositifs de confiance" comprenant des dispositifs sur liste blanche appartenant à des personnes hautement autorisées sur la base du chemin d'accès de l'instance du dispositif ou d'un modèle de caractères génériques.
- Empêchez les périphériques non autorisés de pénétrer dans votre réseau ou d'y mener des activités illicites.

# Contrôle d'accès aux fichiers

- Assurez une sécurité basée sur les rôles en attribuant des autorisations aux utilisateurs en fonction de leur titre et de leur description de poste.
- Déléguez différents niveaux d'accès pour un contrôle optimal : Lecture seule, copie et modification de fichiers sur les périphériques, déplacement de fichiers des périphériques vers l'ordinateur.
- Comme mesure de précaution supplémentaire, n'autorisez l'accès aux fichiers que pour les dispositifs qui sont chiffrés par BitLocker.

# Contrôle du transfert de fichiers

- Limitez le transfert de données en fonction des types d'extensions de fichiers, de sorte que les utilisateurs ne puissent obtenir que les données pertinentes pour leurs tâches.
- Imposez des règles concernant la quantité d'informations pouvant être transférées afin de garantir que les utilisateurs reçoivent les données nécessaires à leurs tâches actuelles.
- Veillez à ce que seules les informations nécessaires soient transférées par l'organisation et par les utilisateurs autorisés

# Traçage des fichiers

- Obtenez immédiatement les journaux de toutes les activités de transfert de fichiers qui ont lieu au sein de votre organisation.
- Analysez tous les détails saillants concernant ces opérations de transfert de fichiers, notamment :
  - ✓ Les noms, les extensions et la taille des fichiers
  - ✓ Emplacement initial d'où il a été déplacé
  - ✓ Les appareils utilisés pour transférer les données
  - ✓ Ordinateurs auxquels les dispositifs étaient connectés
  - ✓ Les utilisateurs qui ont initié l'opération



# Réplication de fichiers

- La réplication de fichiers (shadowing) est une meilleure pratique de sécurité des données pour garder les fichiers critiques à portée de main.
- Lorsqu'un fichier est transféré ou modifié sur un dispositif USB, le contenu du fichier est répliqué exactement.
- Les copies résultantes sont conservées dans un partage réseau protégé par un mot de passe.
- Les types de fichiers qui sont copiés peuvent être choisis en fonction de leur extension et de leur taille.

# Autorisations d'accès temporaires

- Les utilisateurs peuvent demander un accès temporaire via le portail libre-service de l'agent tray pour un maximum de commodité. Ils seront invités à inclure les détails du dispositif et la raison de leur demande.
- Les administrateurs informatiques peuvent examiner la demande et accorder l'accès par le biais de la console elle-même ou en envoyant un e-mail avec le code/script d'accès temporaire unique.
- Les autorisations peuvent être désignées de manière flexible sur la base d'un calendrier spécifique ou d'une durée que l'utilisateur peut activer au moment de son choix.

# Rapports détaillés

- Obtenez des journaux détaillés de toutes les activités de transfert de dispositifs et de fichiers qui ont lieu au sein de l'organisation.
- Utilisez un filtre intelligent pour faciliter l'analyse
- Identifiez facilement toute perturbation des politiques.
- Obtenez des informations sur la façon de modifier les politiques afin de répondre à la fois à la sécurité du réseau et aux besoins des utilisateurs.
- Consultez les graphiques d'information du tableau de bord pour avoir une vue d'ensemble des tendances liées aux périphériques et aux fichiers.

# Quels sont les avantages de Device Control Plus pour votre organisation?

- Maintenir une cyberhygiène optimale en empêchant toutes les intrusions non autorisées de dispositifs et en éliminant les exploits potentiels basés sur des fichiers.
- Empêchez l'élévation des privilèges et toutes les attaques d'initiés.
- Assurez une récupération rapide en cas d'urgence liée à la sécurité des données.
- Favorisez la collaboration en autorisant l'accès temporaire aux appareils pour les utilisateurs tiers tels que les consultants et les stagiaires.
- Soyez toujours informé des modèles d'accès aux appareils et aux fichiers pour créer des politiques efficaces et améliorer la visibilité du réseau.

# Éditions

Fonctionnalités	Professionnelle	Gratuite
Adapté pour	Adapté au contrôle des postes de travail en réseau local	Petites entreprises avec jusqu'à 25 appareils dans le réseau local
Systèmes d'exploitation pris en charge	Windows	Windows

**Demandez une démonstration :**

> [Demande de démo](#)

**Pour en savoir plus sur Device Control Plus :**

<https://www.pgsoftware.fr/uems/device-control-plus>