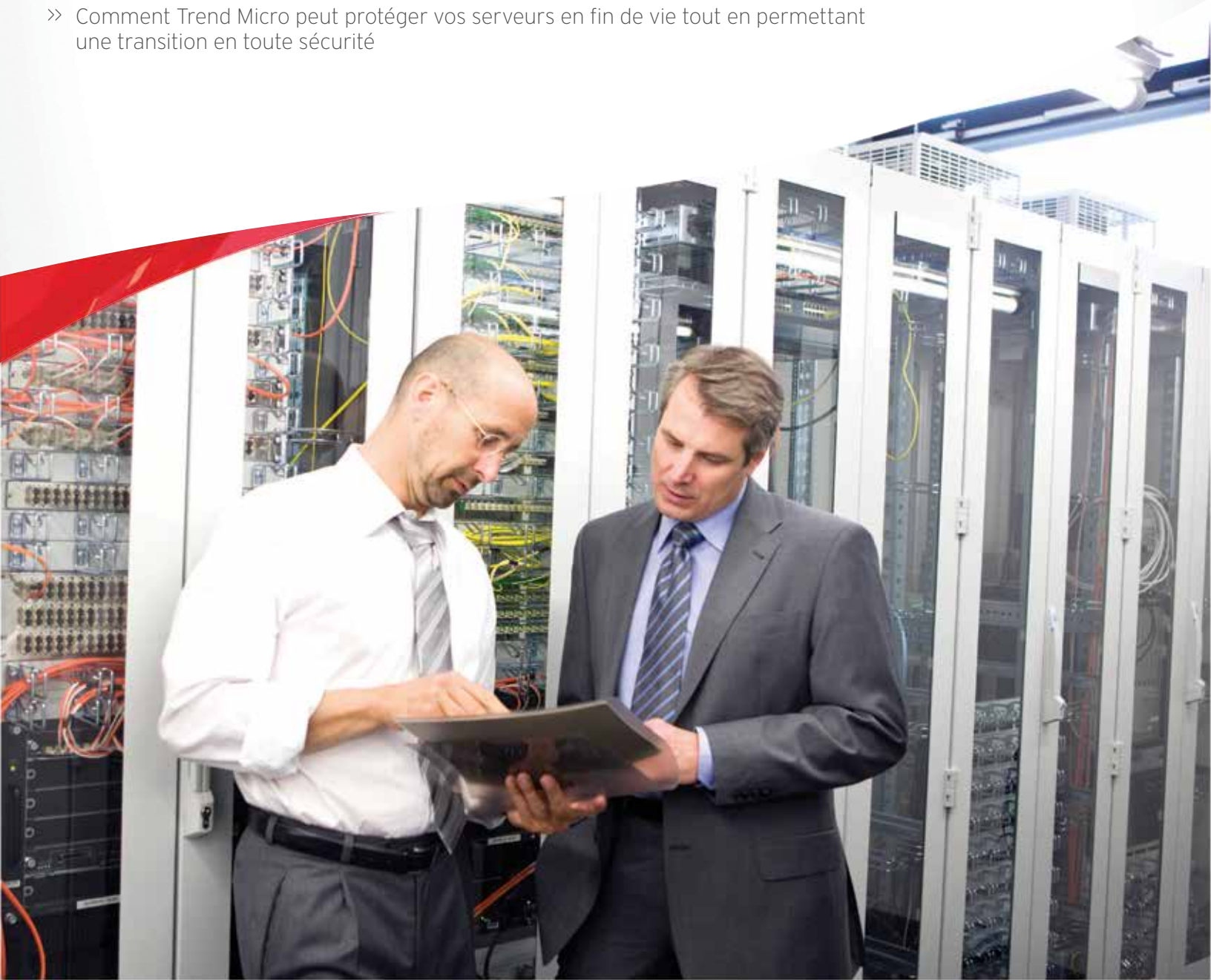




Securing Your Journey to the Cloud

Le Temps Presse pour le support Windows Server 2003

» Comment Trend Micro peut protéger vos serveurs en fin de vie tout en permettant une transition en toute sécurité



Sommaire

Introduction	3
Connaître les risques liés aux systèmes en fin de vie	4
Rester protégé avant, pendant et après la migration	4
Poursuite de l'utilisation de Windows Server 2003 : que faire ?.....	5
La meilleure des approches : une solution de sécurité qui a fait ses preuves.....	6
Ce que fait Deep Security et pourquoi cela est-il important	7
Comment la solution Deep Security fonctionne-t-elle ?	9
Pourquoi Trend Micro	11
Conclusion : Le temps presse mais une solution existe	12

Introduction

Juillet 2015 marquera la fin du support de Microsoft Windows Server 2003, ce qui menacera les serveurs de millions d'entreprises. Selon une étude récemment menée par le cabinet d'analyse de premier plan Enterprise Strategy Group (ESG), « Plus de 80 % des entreprises et des organisations du marché intermédiaire continuent d'utiliser Windows Server 2003 dans une certaine mesure ». Si votre entreprise utilise Microsoft Server 2003, la fin du support introduira de graves risques de sécurité, sauf si vous êtes prêt à migrer vers une nouvelle plateforme ou à mettre en place des mécanismes de contrôle pour compenser. Les pirates informatiques savent que Microsoft ne reconnaîtra ou ne créera plus de correctifs pour les vulnérabilités, ces serveurs vont donc rapidement devenir les cibles favorites des attaques. Les risques liés à l'utilisation de Windows Server 2003 après la fin du support s'accroîtront dans le temps, étant donné que le nombre de problèmes augmentera et qu'ils ne seront pas corrigés.

Ce livre blanc étudie les risques auxquels les entreprises qui utilisent des plateformes en fin de vie comme Windows Server 2003 s'exposent, ainsi que les options disponibles pour remédier à ces risques. Il s'intéresse tout particulièrement à la façon dont Deep Security™ de Trend Micro™ peut protéger les plateformes dont le support a pris fin. Fournie par le leader du marché de la sécurité des serveurs², Deep Security offre une plateforme complète de contrôles de sécurité qui permettent de protéger des plateformes en fin de vie telles que Windows 2003, ce qui permet aux entreprises de planifier et d'effectuer une transition solide pour l'entreprise. La plateforme permet aux entreprises d'éviter de subir le coût élevé de la conclusion de contrats de support personnalisés pour des correctifs de sécurité Microsoft, et de prolonger la durée de vie des systèmes et applications hérités. Deep Security fournit en outre une procédure de migration simple pour sécuriser les systèmes au-delà de Windows 2003, dont Windows 2012, Microsoft Azure et d'autres fournisseurs Cloud leaders comme Amazon Web Services (AWS).

¹ Enterprise Strategy Group, Microsoft Windows Server 2003: the End is Nigh, Feb. 2015

² IDC Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares, Figure 2, doc #250210, August 2014

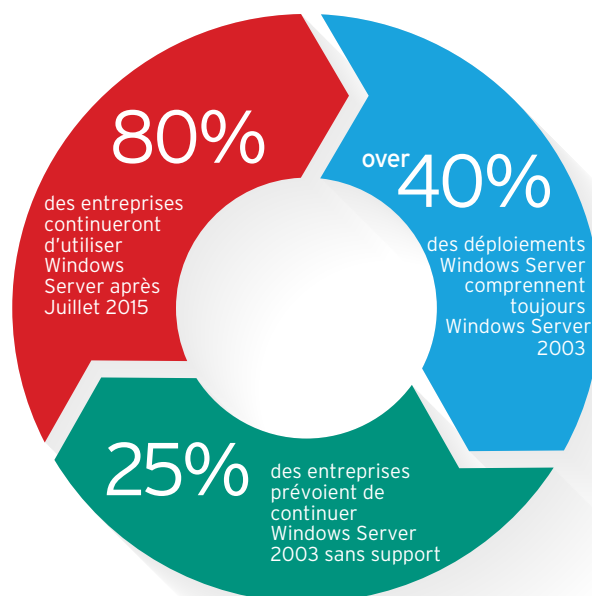
Connaître les risques liés aux systèmes en fin de vie

Malgré une procédure de fin de support organisée par Microsoft, il semble qu'un grand nombre d'entreprises continuent d'utiliser Windows Server 2003 dans leurs infrastructures. Que cela soit dû à un manque de temps et de ressources, ou à des applications métier cruciales impossibles à migrer dans un avenir proche, il est clair que beaucoup d'entreprises seront en situation de danger après le 14 juillet 2015.

Le fait d'ignorer les défis associés au fait de continuer à utiliser des systèmes sans support entraîne une multitude de risques, notamment en raison du fait qu'une partie du code des plateformes plus récentes et bénéficiant d'un support est souvent partagée avec les plateformes précédentes.

Un nouveau programme malveillant d'une plateforme avec un support (Windows 2012 par exemple) peut également affecter un système plus ancien sans support avec lequel elle partage du code. Sans mises à jour pour les systèmes en fin de vie comme Windows Server 2003, il existe désormais clairement un vecteur d'attaque pour les pirates informatiques.

En plus, l'exécution de systèmes sans support et non protégés génère des risques allant au-delà de cette plateforme. Un serveur compromis peut rendre l'ensemble du réseau vulnérable aux attaques, aux pertes de données et aux programmes malveillants. Il sera également impossible d'assurer le respect de réglementations comme la norme PCI DSS 3.0 ou autres sans plan d'action.



* Enterprise Strategy Group, Microsoft Windows Server 2003: the End is Nigh, Feb. 2015

Rester protégé avant, pendant et après la migration

Dans l'idéal, les entreprises devraient planifier la fin des systèmes Microsoft Server 2003, mais en réalité, les plans sont souvent confrontés à des contraintes budgétaires ou techniques. Les entreprises doivent être en mesure de quitter les systèmes sans support selon leur calendrier, tout en préservant la sécurité de ces systèmes en fin de vie de façon économique. Que vous prévoyiez de migrer vers Windows Server 2012 R2, Microsoft Azure ou d'autres environnements Cloud de premier plan comme Amazon Web Services (AWS), vous devez protéger non seulement Windows Server 2003, mais aussi les environnements plus récents. Lors de l'étude des options, cela doit être un élément clé du point de vue opérationnel et de la sécurité.

Poursuite de l'utilisation de Windows Server 2003 : que faire ?

Plusieurs choix s'offriront aux entreprises une fois la date de fin du support de Windows Server 2003 arrivée. Comme pour la plupart des options, des aspects positifs et négatifs sont à prendre en compte lors du processus de planification. Bien que les entreprises doivent étudier les risques et les coûts associés à chacune des options, certaines arrivent clairement en tête de liste.

1. STATUS QUO : LAISSER LES DÉPLOIEMENTS WINDOWS SERVER 2003 EN L'ÉTAT

Il est toujours possible de ne rien faire face à toutes les analyses de risques, ce qui n'engendrerait aucune augmentation des coûts associés à la migration ou à la mise en place de contrôles de sécurité supplémentaires. Les risques générés pour une entreprise par un système sans correctif seraient toutefois impossibles à gérer. Windows Server 2003 deviendra une cible naturelle pour les pirates et une fois compromis, il pourra constituer un moyen pour les attaquants de causer des dommages considérables à une entreprise. Cette option a été incluse dans un souci d'exhaustivité, cependant, avec les approches immédiatement disponibles qui sont à la fois sécurisées et rentables, celle-ci n'est pas recommandée.

2. CONTRATS DE SUPPORT PERSONNALISÉ DE MICROSOFT

Il est possible que Microsoft propose des contrats de support personnalisé et étendu pour Windows Server 2003, qui permettront aux clients d'appliquer des correctifs de sécurité d'urgence. Cependant, ce type de contrat est généralement très coûteux (souvent plus de 200 000 \$ par an³), ce qui amène les clients à rechercher d'autres alternatives pour réduire les risques ou, dans certains cas, à accepter le risque d'une éventuelle compromission. En plus, pour pouvoir souscrire un contrat de support client, Microsoft exige qu'un client ait un plan de migration clair en place, ce qui n'est parfois pas possible à court terme pour beaucoup d'entreprises.

3. ISOLEMENT

L'une des approches de gestion des risques associés aux logiciels sans support comme Windows Server 2003 consiste à rendre ces systèmes difficiles à atteindre pour les pirates informatiques. L'isolement de ces systèmes sur d'autres réseaux ou VLAN, ou leur segmentation à l'aide du réseau ou de pare-feu basés sur un hôte ajoute un niveau de difficulté, qui amènera peut-être les pirates à décider que la tâche est simplement trop difficile. L'isolement du réseau ne sera cependant pas pratique pour les systèmes essentiels de l'entreprise. Rendre les systèmes sans support difficiles à atteindre ajoute un niveau de sécurité mais les empêche aussi d'être utilisés de manière efficace, ce qui rend le motif de leur conservation caduc. Bien que cette solution puisse fonctionner pour un petit pourcentage de serveurs déployés, il ne s'agira probablement pas d'une solution pratique pour la plupart des entreprises.

4. RENFORCEMENT DU SYSTÈME

Le renforcement des systèmes Windows 2003 (par exemple, suppression des services et comptes utilisateur inutiles) est un bon moyen de réduire les risques. Les utilisateurs autorisés pourront cependant toujours accéder à ces systèmes, la restriction seule des comptes utilisateur ne sera donc peut-être pas pratique pour des raisons professionnelles.

Les entreprises devraient tirer parti des stratégies de restriction logicielles intégrées à Windows Server 2003 déployées par le biais de la stratégie globale afin de réduire les risques liés à l'exécution de commandes erronées par les applications. Bien qu'elle ne soit pas simple, il s'agit d'une bonne approche qui permet d'empêcher la compromission des serveurs par le biais d'une application, dans la mesure où elle est appliquée en plus d'autres mesures de protection.

Il est à noter que le renforcement par la suppression des services et ports inutiles n'est pas simple, notamment lorsque les applications métier sont conçues pour fonctionner sur des systèmes d'exploitation généralistes avec une multitude de services d'application et de ports (par exemple, ports RPC, services Web). Il est tout à fait possible que le renforcement « casse » l'application. La restriction des ports des applications peut également rendre les pare-feu de filtrage de paquets inefficaces, car un grand nombre d'applications allouent les ports de façon dynamique lorsque cela est nécessaire.

³ Trend Micro Customer Interviews, 2014

5. DEPLOIEMENT DE CONTRÔLES DE SÉCURITÉ SUPPLÉMENTAIRES

Afin de remédier aux éventuelles vulnérabilités de Windows Server 2003, il est possible de mettre en place des contrôles de sécurité supplémentaires afin de détecter les attaques et de s'en protéger. Les solutions basées sur un hôte sont l'idéal, car les solutions à périmètre ne peuvent pas fournir un ensemble de mécanismes de protection efficaces pour chaque serveur individuel. Les contrôles clés basés sur un hôte à prendre en compte sont notamment :

- la détection et la préventions afin de se protéger contre les vecteurs d'attaque du réseau ;
- la surveillance de l'intégrité des fichiers systèmes, des paramètres du registre et autres fichiers d'applications critiques afin d'assurer de la détection des changements imprévus ou suspects ;
- une solution anti-programmes malveillants afin de se protéger contre les nouvelles formes de programmes malveillants.

Étant donné le nombre de contrôles nécessaires, il est recommandé de déployer une solution capable de tous les gérer sur une seule et même plateforme. Veillez en outre à ce que cette même plateforme puisse être utilisée pour des déploiements plus récents, indépendamment de l'environnement serveur (Windows ou Linux) et de l'approche de déploiement (physique, virtuel et/ou Cloud).

La meilleure des approches : une solution de sécurité qui a fait ses preuves

Bien que la mise en place de certains aspects du renforcement du serveur, dont notamment les stratégies de restriction logicielle intégrées à Windows, aidera à résoudre les problèmes, il est évident que sans l'aide de Microsoft pour détecter les vulnérabilités et fournir des correctifs pour Windows Server 2003, les entreprises qui continuent d'utiliser la plateforme dont le support a pris fin doivent déployer des contrôles de sécurité supplémentaires. Sans correctif de Microsoft pour Windows Server 2003, il est absolument primordial de continuer à gérer les vulnérabilités. Deep Security de Trend Micro peut vous apporter cette protection. Deep Security fournit une plateforme complète de contrôles de sécurité utilisés par des milliers d'entreprises du monde entier et qui protègent les serveurs physiques, virtuels et Cloud, dont les plateformes en fin de vie comme Windows XP et Windows 2000 Server. Elle peut fournir les fonctionnalités cruciales nécessaires pour garantir une transition en toute sécurité pour l'entreprise, laissant ainsi cette dernière décider du moment et de la façon dont la migration depuis Windows Server 2003 se produira, sans risque ni coûts inutiles.

Deep Security DE TREND MICRO

Deep Security est une plateforme de sécurité complète, qui permet de protéger tous les serveurs des environnements physiques, virtuels et Cloud. Elle peut être déployée en tant qu'agent individuel sur des serveurs physiques, virtuels ou Cloud, ou en tant qu'appliance virtuelle sur un serveur VMware ESX afin de protéger les machines virtuelles invitées par une sécurité sans agent. Il est possible d'appliquer la stratégie de façon automatique, avec des systèmes de recherche des changements qui pourront éventuellement nécessiter des mesures de protection supplémentaires et leur application aux serveurs vulnérables.

Deep Security comprend des contrôles de sécurité du réseau qui ont fait leurs preuves et qui peuvent appliquer des correctifs virtuels aux systèmes critiques, les protégeant ainsi des vulnérabilités jusqu'à ce qu'un correctif soit disponible et déployé, ou en guise de protection avant et pendant la migration si le support du système a cessé, comme c'est le cas de Windows Server 2003.

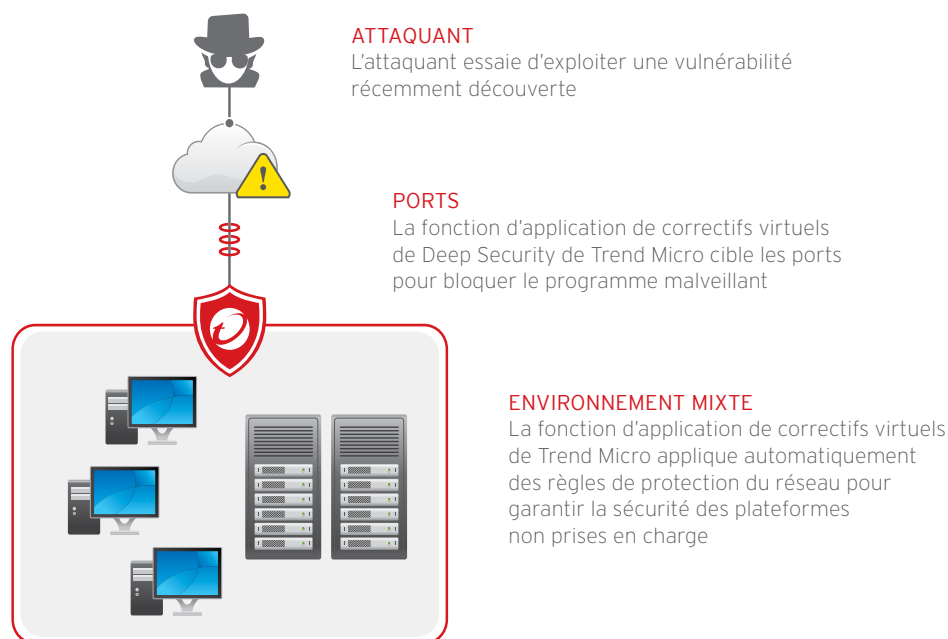
Pour vous protéger des changements survenant dans un système qui n'est plus mis à jour par Microsoft, Deep Security comprend également des fonctionnalités de sécurité du système, avec notamment la surveillance de l'intégrité et des fichiers journaux, ce qui permet de détecter les changements là où il ne devrait plus y en avoir. Enfin, afin de s'assurer de la protection complète des serveurs, la plateforme comprend des fonctionnalités anti-programmes malveillants qui détectent et remédient aux attaques des programmes malveillants.

Ce que fait Deep Security et pourquoi cela est-il important

Deep Security est une plateforme basée sur un hôte qui fournit une multitude de contrôles de sécurité par le biais d'un agent individuel. Comme cela est recommandé, elle comporte des fonctionnalités clés pour protéger les serveurs bientôt en fin de vie (comme Windows Server 2003) et, pendant la migration de l'entreprise, comprend des fonctionnalités importantes qui réduisent les risques et les coûts opérationnels sur les serveurs physiques, virtuels et Cloud. Deep Security fournit également des fonctions de sécurité supplémentaires qui permettent de sécuriser les serveurs sur le centre de données et le Cloud.

SÉCURITÉ DE RÉSEAU : DÉTECTION ET PRÉVENTION DES INTRUSIONS (IDS/IPS)

Les fonctions de détection et de prévention des intrusions (IDS / IPS) de Deep Security protègent les serveurs de l'exploitation des vulnérabilités connues ou non ([Shellshock](#) et [Heartbleed](#) par exemple). Le moteur Deep Packet Inspection (DPI) utilise des milliers de règles éprouvées qui s'appliquent au trafic du réseau dans les couches 2 à 7. Ces règles peuvent être appliquées automatiquement sur la base d'un environnement de déploiement (par exemple, Windows Server 2003) afin de protéger les ressources systèmes réseau et applications d'entreprise auxquelles aucun correctif n'est appliqué.



Deep Security comprend une protection contre les vulnérabilités prête à l'emploi pour des centaines d'applications, dont les bases de données, le Web, la messagerie électronique et les serveurs FTP. La plateforme offre également une protection immédiate contre les vulnérabilités connues pour lesquelles aucun correctif n'a été créé et contre les vulnérabilités inconnues, à l'aide de règles intelligentes qui ont recours à l'analyse comportementale et à l'apprentissage automatique pour bloquer les nouvelles menaces.

Les règles de protection des applications Web de Deep Security défendent le système contre les attaques Web les plus courantes, dont l'injection SQL, le cross-site scripting et les autres vulnérabilités des applications Web - [les protégeant de ces vulnérabilités](#) jusqu'à ce des correctifs soient créés. Les règles de sécurité appliquent la conformité du protocole et utilisent des analyses heuristiques pour identifier les activités malveillantes.

Deep Security utilise son pare-feu professionnel bidirectionnel et dynamique intégré pour accompagner l'application de ces règles IPS. Le pare-feu permet également de contrôler les communications sur les ports et les protocoles nécessaires pour corriger les opérations du serveur, et pour bloquer tous les autres ports et protocoles. Cela permet de réduire d'autant plus le risque d'accès non autorisé à un déploiement Windows Server 2003.

SÉCURITÉ DU SYSTÈME : SURVEILLANCE DE L'INTÉGRITÉ

Grâce à la fonction de surveillance de l'intégrité de Deep Security, les entreprises sont alertées en temps réel en cas de changements inattendus au niveau du système d'exploitation et des fichiers des applications, y compris les points d'attaque clé comme les fichiers hôtes, les répertoires et les valeurs de clé de registre. En outre, pour les déploiements virtualisés sur VMware, la solution utilise la technologie Intel TPM/TXT pour entreprendre une surveillance de l'intégrité de l'hyperviseur pour tous les changements au niveau de l'hyperviseur, ce qui étend la sécurité et la conformité à la couche de l'hyperviseur. Deep Security permet aussi de simplifier l'administration en réduisant grandement le nombre de bons événements connus grâce à la mise sur liste blanche Cloud automatique à partir du Certified Safe Software Service de Trend Micro™.



Central dashboard gives instant notification of malicious changes to sensitive files and applications

Lorsque le support d'un système a pris fin, différentes zones du système d'exploitation et des applications ne sont plus modifiées. Grâce à la surveillance de l'intégrité, les entreprises voient rapidement ce qui a changé et comment. Elles peuvent ainsi prendre immédiatement des mesures en cas de problème. Enfin, le balisage fiable des événements qui réplique automatiquement les actions en cas d'événement similaire sur l'ensemble du centre de données permet également de réduire les frais administratifs.

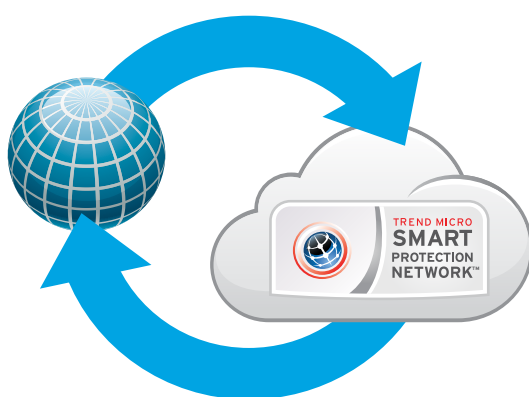
SOLUTION ANTI-PROGRAMMES MALVEILLANTS AVEC RÉPUTATION WEB

Un agent anti-programmes malveillants fournit une protection contre les programmes malveillants dont les virus, les logiciels espions, les vers et les chevaux de Troie sur les serveurs physiques, virtuels et Cloud. L'intégration à la solution mondiale de renseignement sur les menaces Smart Protection Network™ de Trend Micro™ pour les fonctions de réputation Web renforce la protection des serveurs et des bureaux virtuels.

Deep Security peut être configurée à l'aide de stratégies pour analyser automatiquement les systèmes et déployer des règles, ou simplement prévenir les administrateurs des règles recommandées pour les systèmes vulnérables. L'analyse des recommandations rationalise la gestion des mises à jour de sécurité en recommandant automatiquement les règles à déployer pour protéger un système donné. Deep Security analyse le système afin d'identifier les règles IDS / IPS à appliquer parmi des milliers afin d'optimiser la protection en fonction de la version du système d'exploitation, du service pack, du niveau des correctifs et des applications installées. Les stratégies peuvent être utilisées pour analyser régulièrement les systèmes (chaque semaine par exemple) afin de rechercher les éventuelles nouvelles vulnérabilités et d'appliquer automatiquement une protection adaptée. Lorsqu'une règle est activée, notamment pour les nouvelles vulnérabilités telles que Shellshock et Heartbleed, elle est déployée de façon transparente où cela est nécessaire. Elle protège ainsi les systèmes concernés et supprime le besoin immédiat d'appliquer un correctif contre la vulnérabilité. En cas de systèmes en fin de vie comme Windows Server 2003, pour lesquels aucun correctif ne va paraître, ce mécanisme de protection est primordial.

PROTECTION INTELLIGENT

Les mises à jour de sécurité sont fournies par une équipe dédiée composée d'experts en sécurité qui surveillent les menaces 24h/24 et 7j/7 afin de garantir la meilleure protection possible aux clients Deep Security. Cette équipe surveille continuellement plusieurs sources d'informations de divulgation des vulnérabilités, dont plus de 100 sources telles que SANS, CERT, Bugtraq, VulnWatch, Packet Storm et SecuriTeam. Elle collecte également des informations à partir de plus de 150 millions de points de terminaison du Smart Protection Network™ de Trend Micro. Ces informations sont utilisées pour identifier et mettre en corrélation de nouvelles menaces et vulnérabilités, et ensuite pour créer les règles associées qui permettront de protéger les systèmes menacés. Par exemple, Trend Micro a fourni une protection contre Heartbleed et Shellshock dans les 24 heures suivant leur divulgation publique, ce qui a permis de protéger immédiatement les serveurs utilisant Deep Security.



Réseau de capteurs mondial

Collecte plus d'informations à plus d'endroits

- Des centaines de millions de capteurs
- 16 milliards de requêtes liées à des menaces chaque jour

Renseignement sur les menaces mondial

Analyse et identifie précisément les menaces plus vite

- Identifie les nouvelles menaces 50 fois plus vite que la moyenne (laboratoires NSS)
- Surveillance 24h/24 et 7j/7

Protection proactive

Bloque les menaces réelles plus tôt

- Des centaines de règles de protection fournies chaque année, dont plus de 900 propres à Microsoft
- Réaction rapide face aux nouvelles menaces comme Heartbleed et Shellshock
- 500 000 nouvelles menaces identifiées et 250 millions bloquées chaque jour

En ce qui concerne la protection contre les vulnérabilités, l'équipe de recherche se concentre sur les risques pour le serveur et les logiciels de bureau qui sont susceptibles d'exister dans un environnement client. Cela comprend les systèmes d'exploitation (Microsoft Windows, Linux et UNIX), mais aussi des logiciels d'entreprise comme des navigateurs Web, des serveurs Web, des serveurs d'applications, des logiciels de sauvegarde et des bases de données.

Comment Deep Security fonctionne-t-elle ?

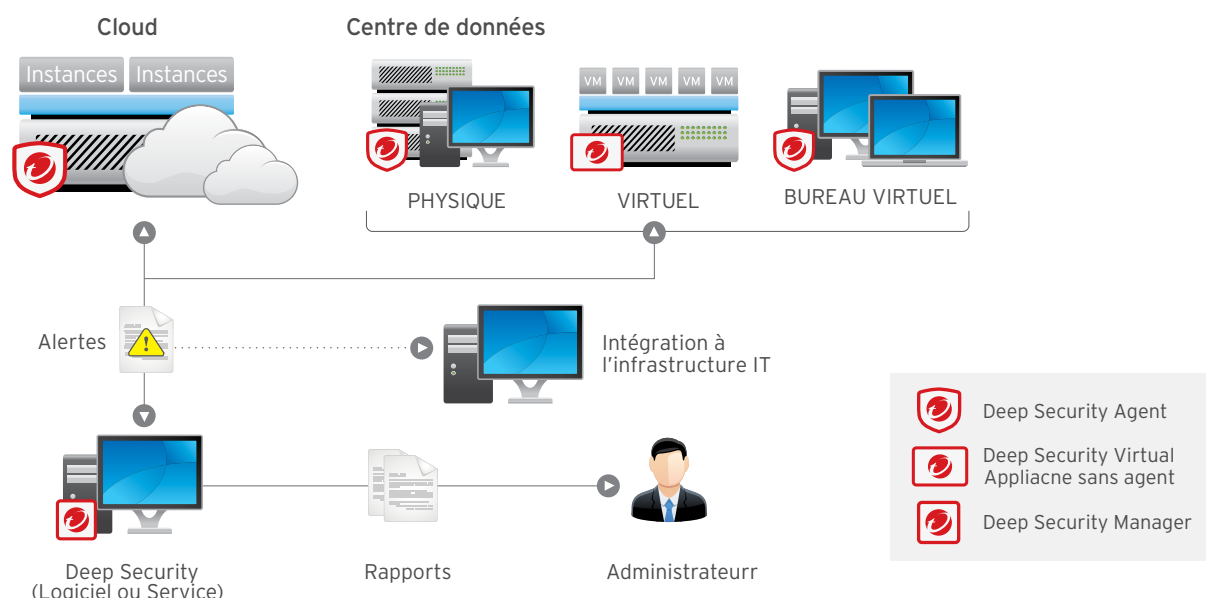
Deep Security fournit des fonctions de sécurité cruciales pour protéger les serveurs vulnérables, dont l'application de correctifs virtuels par le biais de solutions IDS / IPS, la surveillance de l'intégrité et un logiciel anti-programmes malveillants. Il s'agit d'une plateforme de sécurité basée sur un hôte qui garantit la sécurité des serveurs, applications et données sur les serveurs physiques, virtuels et Cloud. Elle protège également les entreprises des violations et des perturbations des opérations sans appliquer de correctif d'urgence. En ce qui concerne les plateformes pour lesquelles le support a pris fin et aucun nouveau correctif ne sera créé, elle constitue une fonction cruciale pour protéger les applications métier sensibles.

Contrairement aux approches de sécurité à périmètre héritées, l'adoption d'une approche basée sur un hôte permet à Deep Security de protéger les serveurs du trafic « Nord-Sud » traditionnel d'un centre de données, ainsi que du trafic « Est-Ouest » qui s'accroît en raison des modifications des déploiements informatiques qui utilisent la virtualisation et les technologies Cloud. Le fait de disposer d'une sécurité au niveau de l'hôte permet

aux entreprises de protéger chaque environnement serveur spécifique, ce qui est primordial pour les systèmes d'exploitation sans support, pour lesquels aucun nouveau correctif ne sera créé. Cela permet aussi de protéger les systèmes des attaques provenant d'autres serveurs compromis se trouvant dans le réseau, qui ne seraient pas arrêtées par la sécurité à périmètre. En ce qui concerne les déploiements Cloud élastiques, la possibilité de faire évoluer horizontalement et instantanément la solution est mieux soutenue par la sécurisation automatique de chaque instance de serveur virtuel au fur et à mesure de sa venue en ligne, et non en forçant tout le trafic à passer par un goulet d'étranglement qui sera limité dans sa capacité à réagir et à évoluer.

La solution comprend Deep Security Manager et Deep Security Agent. Pour les déploiements VMware, il existe également Deep Security Virtual Appliance, qui s'intègre facilement à VMware ESX et NSX et qui permet d'automatiser le déploiement de la sécurité sur un SDDC (software-defined data center, centre de données défini par logiciel).

CONTRÔLE LA SÉCURITÉ SUR LES SERVEURS PHYSIQUES, VIRTUELS ET CLOUD



Deep Security MANAGER

Deep Security Manager permet aux administrateurs de créer des profils de sécurité et de les appliquer aux serveurs sur des déploiements physiques, virtuels et Cloud. Il présente une console centralisée pour surveiller les alertes et les mesures préventives entreprises en réponse aux menaces, et peut être configuré de sorte à automatiser ou distribuer des mises à jour de sécurité aux serveurs sur demande. Manager peut être utilisé afin de générer des rapports pour mieux cerner les activités et respecter les exigences en termes de conformité. La fonctionnalité de balisage des événements rationalise la gestion des événements à volume élevé et permet de créer un flux de travail des réponses aux incidents.

DEEP SECURITY APPLIANCE (SÉCURITÉ SANS AGENT)

Pour les déploiements VMware, il existe un composant au niveau de l'hyperviseur nommé Deep Security Appliance, qui permet de déployer la sécurité sans agent pour les serveurs hébergés sur un hôte ESX. Lorsque les entreprises ont choisi de déployer VMware NSX, elles peuvent utiliser la plateforme Deep Security conjointement aux fonctionnalités de microsegmentation fournies par un SDN (Software Defined Networking, réseau défini par logiciel) afin d'obtenir un centre de données virtualisé sécurisé.

DEEP SECURITY AGENT

Deep Security Agent est un petit composant logiciel intelligent déployé sur le serveur ou la machine virtuelle protégée et qui applique la stratégie de sécurité. Il s'agit d'un agent de sécurité unique qui s'intègre à tous les modules Deep Security utilisés, ce qui rationalise le déploiement et la gestion. En ce qui concerne l'application de correctifs virtuels, Deep Security Agent s'intègre au pilote réseau (pile) du système afin d'évaluer les paquets réseau par rapport aux règles de Deep Security. Si le moteur de règles identifie un programme malveillant, la connexion au réseau est interrompue afin de mettre fin et d'empêcher l'attaque. L'agent peut être déployé automatiquement par le biais d'une stratégie et d'outils d'orchestration et ne déploie que les composants de contrôle de sécurité dictés par la stratégie, ce qui rationalise la taille de l'agent.



Pourquoi Trend Micro

Comme nous l'avons indiqué dans ce livre blanc, Trend Micro propose une plateforme de sécurité complète qui permet de protéger les systèmes dont le support a pris fin, comme Windows Server 2003 par exemple. Deep Security peut en outre être utilisée dans tous les environnements de serveurs, qu'ils soient physiques, virtuels ou Cloud, afin de rationaliser la gestion et d'assurer la cohérence de la sécurité pendant la migration de l'entreprise. L'approche basée sur un hôte de Deep Security répond aux besoins des centres de données modernes et du Cloud, car elle protège les serveurs en fonction de leurs configurations spécifiques, partout où ils sont déployés.

Des entreprises du monde entier font confiance à Trend Micro pour protéger leurs environnements sans support grâce à nos fonctions uniques d'application de correctifs virtuels qui protègent leurs systèmes vulnérables et sans correctif, dont Windows XP et les déploiements de Windows 2000 Server. Windows Server 2003 sera protégé de la même façon, avec un support dédié jusqu'à fin 2020, ce qui permet de réaliser une migration sans heurt.

“Application de correctifs virtuels de Deep Security nous protège des vulnérabilités du système hérité, sur lesquelles il est impossible d'appliquer un correctif ou que le fournisseur ne corrigera jamais. Deep Security découvre les failles et nous protège jusqu'à ce que nous puissions remplacer ces vieux,”

Jeremy Mello
Network Systems Specialist
City of Fresno

Cela fait en outre cinq ans qu'IDC désigne Trend Micro comme étant le leader mondial du marché de la sécurité des serveurs⁴, ce qui montre que de plus en plus d'entreprises font confiance à Trend Micro pour sécuriser leurs infrastructures informatiques sensibles. Deep Security est la seule solution intégrant autant de fonctionnalités de sécurité des serveurs sur une seule et même plateforme, ce qui permet de coordonner plusieurs technologies de sécurité, pour une solution de sécurité des serveurs hautement efficace pour Windows Server 2003 et au-delà.

Conclusion: Le temps presse mais une solution existe

Si vous utilisez Windows Server 2003 aujourd'hui, la date du 14 juillet 2015, qui marquera la fin du support de la solution, approche. Avec plus de 80 % des entreprises qui continueront d'utiliser une partie des systèmes Windows Server 2003 après cette date, il est évident que vous ne serez pas seul. Étant donné la complexité de la protection des plateformes serveur des entreprises, ces dernières devraient envisager d'adopter une approche à plusieurs volets afin de protéger les déploiements de Windows Server 2003, avec notamment l'utilisation des stratégies de restriction logicielles intégrées de Microsoft et le déploiement de contrôles de sécurité supplémentaires.

Si vous utilisez Windows Server 2003, Deep Security de Trend Micro est la solution idéale pour protéger l'ensemble de vos serveurs avant, pendant et après la migration. Elle offre les contrôles de sécurité clés nécessaires pour protéger les déploiements Windows Server 2003, dont la sécurité du réseau pour l'application de correctifs virtuels, la sécurité du système par le biais de la surveillance de l'intégrité des ressources serveur sensibles et un logiciel pour la protection contre les derniers programmes malveillants. La plateforme permet aux opérations informatiques de mieux gérer les systèmes et d'améliorer la conformité, en protégeant les systèmes vulnérables jusqu'à ce qu'un correctif puisse être appliqué. Pour les systèmes sans support comme Windows Server 2003, Deep Security peut les protéger des dernières vulnérabilités, ce qui évite les violations de données et garantit la continuité des opérations, tout en permettant le respect de normes et réglementations importantes (PCI DSS, FISMA, HIPAA).

Adoptée par des milliers de clients pour protéger des millions de serveurs dans le monde entier, la plateforme Deep Security est la solution qui a fait de Trend Micro le leader sur le marché de la sécurité des serveurs. Si votre entreprise utilise Windows Server 2003, Deep Security peut vous aider à vous assurer que votre entreprise est protégée de façon rapide et rentable, aujourd'hui, et demain.

DÉCOUVREZ EN PLUS

sur la façon dont Trend Micro peut vous protéger lors de la fin du support de Windows Server 2003

Contactez-nous au 01 76 68 65 00 ou rendez-vous sur www.trendmicro.com/server2003

⁴ IDC Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares, Figure 2, doc no 250210, août 2014

Trend Micro, un leader mondial des logiciels et solutions de sécurité, a pour mission de sécuriser les échanges d'informations numériques. Se fondant sur 26 ans d'expérience, nos solutions à destination du grand public, des professionnels et des institutions gouvernementales déploient une sécurité multicouche des données pour protéger les informations sur les équipements mobiles, les Endpoints, les passerelles, les serveurs et le Cloud. Trend Micro concrétise une protection évoluée des données, grâce à des technologies innovantes, simples à déployer et à gérer, et qui s'adaptent à un environnement évolutif. Toutes nos solutions sont optimisées par le Smart Protection Network™, l'infrastructure de sécurité et de veille de Trend Micro basée sur le Cloud, et sont prises en charge par plus de 1200 chercheurs en sécurité à travers le monde.

© 2015, Trend Micro, Incorporated. Tous droits réservés. Trend Micro et le logo t-ball Trend Micro sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou déposées de leurs propriétaires respectifs.
www.trendmicro.com et blog.trendmicro.fr

• **TREND MICRO FRANCE SA**
• 85, Avenue Albert 1^{er}
• 92500 RUEIL-MALMAISON
• Tél : 01 76 68 65 00
• www.trendmicro.fr