SYMANTEC™ DATA CENTER SECURITY CAS D'UTILISATION

Assurer une sécurité maximale du serveur et de l'infrastructure sur les environnements physiques, virtuels et embarqués

Symantec™

PROTECTION COMPLÈTE POUR LES SERVEURS, LES INFRASTRUCTURES ÉVOLUTIVES DE DATA CENTERS, ET LES SYSTÈMES EMBARQUÉS ET INDUSTRIELS

Assurer la sécurité dans les banques de serveurs, les systèmes embarqués et industriels et le monde des data centers est une préoccupation majeure et constante. Les menaces évoluent, les data centers changent rapidement (notamment avec la virtualisation et les architectures software-defined), les périphériques contraints, qui se connectent à Internet avec des ressources limitées (communément appelés l'Internet des objets), sont de plus en plus nombreux, et les exigences en matière de gouvernance sont de plus en plus strictes. Pour toutes ces raisons, les entreprises peuvent trouver leurs solutions de sécurité traditionnelles insuffisantes.

« Les solutions de sécurité traditionnelles peuvent fournir d'utiles couches de protection au niveau des systèmes individuels mais ne peuvent répondre aux besoins de confidentialité, d'intégrité et de disponibilité qui caractérisent les serveurs et périphériques contraints, essentiellement hétérogènes, ni même les charges de travail qu'ils génèrent. »

L'enjeu est de taille, car les entreprises virtualisent toujours plus de serveurs au sein du data center ou cherchent à protéger des systèmes industriels et embarqués.

[1] Verizon Data Breach Investigation Report, 2014 (www.verizonenterprise.com/DBIR/)
[2] Symantec Internet Security Threat Report, 2014 (www.symantec.com/security_response/publications/threatreport.jsp)
[3] Symantec Attacks on Point of Sales (POS) Systems, 2014 (www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf)
[4] CISCO (www.newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342)

10 RAISONS POUR LESQUELLES LA SÉCURISATION DES SERVEURS ET INFRASTRUCTURES CRITIQUES EST NÉCESSAIRE

- Les serveurs sont l'infrastructure présentant le plus de violations en 2013[1]
- Le piratage est maintenant la principale méthode d'attaque[1]
- Augmentation de 62 % du nombre de failles de sécurité en 2013[2]
- Le ciblage des employés et les menaces avancées sont chose commune
- Il est nécessaire de protéger les serveurs contre les activités malveillantes et de garantir la visibilité des changements de configuration
- Il est indispensable de prendre en charge le workflow et/ou les applications critiques en proposant une haute disponibilité
- Les serveurs sont les composants centraux critiques du réseau et des infrastructures informatiques
- Les systèmes de points de vente et distributeurs de billets comptent parmi les plus grandes sources de vol de cartes bancaires[3]
- 50 milliards d'appareils seront connectés à Internet d'ici 2020[4]
- Il faut à la fois sécuriser les plates-formes physiques et les environnements virtuels

SECTEURS QUE NOUS PROTÉGEONS

- Commerce de détail
- Administration
- Finance
- Industrie et fabrication
- Distribution d'énergie

POURQUOI CHOISIR SYMANTEC ?

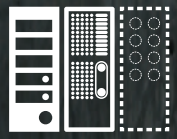
- Solutions éprouvées de sécurisation des serveurs
- Sans compromis contre les attaques*
- Solutions matures utilisées dans des environnements OEM
- Prise en charge de plus de 40 systèmes d'exploitation et périphériques contraints, embarqués et connectés
- Solutions complètes
- Protection basée sur des politiques

Pour relever ces défis, Symantec Data Center Security a été conçu pour protéger les infrastructures dynamiques virtuelles, physiques, industrielles et embarquées : des périphériques IoT, équipements de points de vente et systèmes de contrôle industriel (type SCADA) jusqu'au data center le plus complexe et aux environnements combinés de cloud public-privé. En surveillant et en protégeant les serveurs et les périphériques à l'aide de contrôles granulaires basés sur des politiques, votre entreprise peut assurer une protection proactive des environnements systèmes hétérogènes et des informations qu'ils contiennent.

* Dans un concours parrainé par Symantec à la conférence Black Hat 2014, plus de 50 hackers chevronnés ont échoué à capturer des « drapeaux » qui étaient cachés dans des systèmes Linux et Windows non-patchés mais protégés par le logiciel de Symantec.

SOLUTIONS SYMANTEC DATA CENTER SECURITY

DATA CENTER SECURITY: SERVER ADVANCED (DCS:SA)



Protection avancée de la sécurité du serveur pour les serveurs hétérogènes et les systèmes industriels critiques

DATA CENTER SECURITY SERVER (DCS:S)

Système de sécurité de pointe pour les infrastructures de data centers virtuels

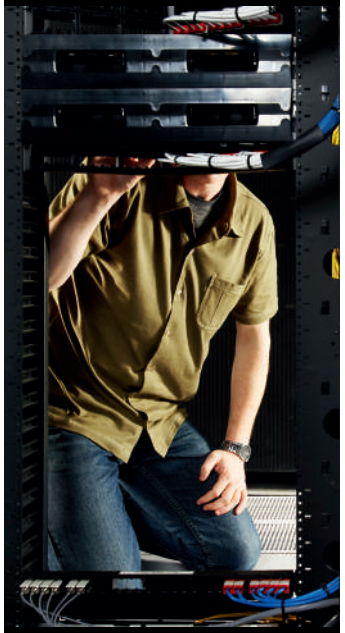
SYMANTEC EMBEDDED SECURITY: CRITICAL SYSTEM PROTECTION (SES:CSP)

Système de sécurité avancé pour les systèmes embarqués et contraints (IoT)

DÉCOUVREZ LES APPLICATIONS STRATÉGIQUES DE LA SÉCURITÉ DU DATA CENTER ET IDENTIFIEZ CELLES QUI PEUVENT AIDER VOTRE ENTREPRISE À ATTEINDRE SES OBJECTIFS

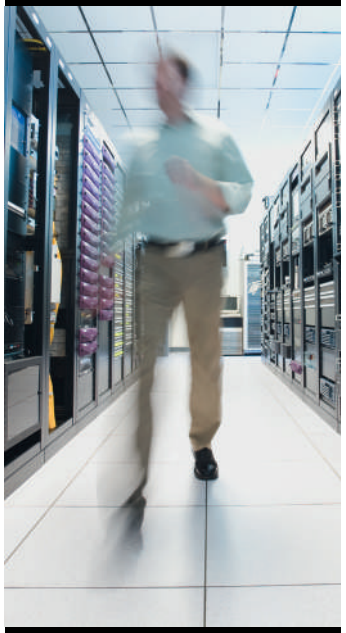
CAS D'UTILISATION 1 :

Sécuriser les plates-formes existantes et les systèmes en fin de vie (EOL) ou en fin de support (EOS) et réduire les coûts de support



CAS D'UTILISATION 2 :

Améliorer la fiabilité opérationnelle grâce à une limitation des correctifs et à une application effective du contrôle des changements



CAS D'UTILISATION 3 :

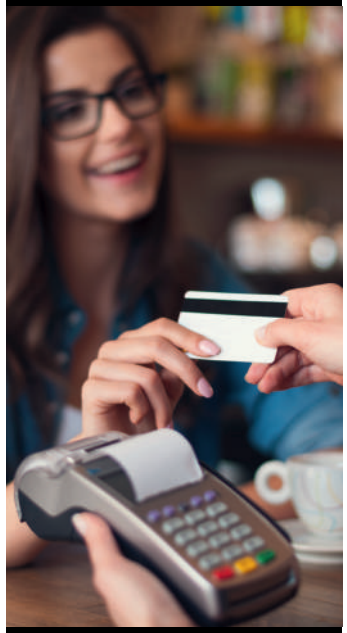
Protéger les périphériques industriels, embarqués et IoT contre les attaques ciblées

CAS D'UTILISATION 4 :

Durcissement du système et protection des infrastructures physiques et virtualisées

CAS D'UTILISATION 5 :

Répondre aux exigences de conformité et de risque, telles que Payment Card Industry Data Security Standard (PCI DSS)



CAS D'UTILISATION 1 :

Sécuriser les plates-formes existantes et les systèmes en fin de vie (EOL) ou en fin de support (EOS) et réduire les coûts de support

Le 14 Juillet 2015, le support de Microsoft® Windows® Server 2003 (Win2K3) ne sera plus assuré. Cela signifie qu'il n'y aura plus de correctifs de sécurité pour cette plate-forme. Pour beaucoup, les obstacles seront importants : manque de praticité et coûts prohibitifs ou simple manque de temps pour migrer vers de nouvelles plates-formes prises en charge. Ceci est aussi vrai pour les plates-formes plus anciennes telles que Windows 2000 et Windows NT.

POURQUOI EST-CE IMPORTANT ?

Les implications de ce scénario sont profondes. Sans correctifs de sécurité critiques, de nombreuses questions pouvant affecter le niveau de service pourront se présenter, telles que la perte complète du service, les violations de données, et même des cyber-attaques systémiques. Plusieurs options s'offrent à vous. Vous pouvez choisir de ne rien faire, mais cela mettra l'entreprise en grand danger, surtout si ces systèmes hébergent des services métiers critiques. Microsoft peut proposer des forfaits de support personnalisé, mais ceux-ci coûtent souvent beaucoup plus cher que les programmes de support standard, sans résoudre la question de la migration qui deviendra incontournable à long terme.
Vous pouvez également choisir de verrouiller et durcir votre système critique en fin de support avec une solution de sécurité puissante, atténuant ainsi la nécessité de migrer vers une autre plate-forme ou de payer de coûteux contrats de support personnalisé.

CAS D'UTILISATION 1 :

Sécuriser les plates-formes existantes et les systèmes en fin de vie (EOL) ou en fin de support (EOS) et réduire les coûts de support

SOLUTION SYMANTEC

Symantec Data Security Center: Advanced Server (DCS:SA) est la solution qui peut sécuriser et durcir les systèmes sans nécessiter de migration vers une autre plate-forme compatible et dégager de substantielles économies par rapport aux contrats de support personnalisés.

TÉMOIGNAGE CLIENT

Un grand distributeur avait besoin d'assurer la prise en charge et la protection d'anciens systèmes Windows NT et 2000. Au lieu de payer Microsoft pour une prise en charge étendue, il a utilisé DCS:SA pour verrouiller les systèmes et en prévenir toute mauvaise utilisation, ce qui lui a permis de réduire les risques pour un coût nettement inférieur.

AVANTAGES CLÉS

- Pas besoin de migrer le système existant en fin de vie
- Aucun besoin de payer de coûteux contrats de support de fin de vie
- Empêcher l'exploitation des vulnérabilités connues et inconnues aux cyber-attaques avancées
- Gagner en visibilité sur la sécurité du système critique
- Éviter de coûteuses périodes d'interruption
- Appliquer une séparation des tâches et supprimer les privilèges administrateur ou racine

FONCTIONNEMENT

- Sécurisation renforcée du système d'exploitation et prévention de l'exploitation des vulnérabilités connues avec des politiques de prévention d'intrusion prêtes à l'emploi spécialement adaptées à la plate-forme d'exploitation concernée
- Limitation des actions des applications et des systèmes d'exploitation avec des contrôles granulaires basés sur des politiques et par l'intermédiaire d'une solution sandbox
- Prévention de l'exploitation d'applications via des attaques consistant à provoquer un débordement de la mémoire tampon sur les systèmes Windows 32 et 64 bits
- Utilisation d'un large éventail de plates-formes physiques et virtuelles grâce à la prise en charge des cinq principales plates-formes (Windows, Linux,® AIX,® Solaris,™ et HP-UX®)

CAS D'UTILISATION 2 :

Améliorer la fiabilité opérationnelle grâce à une limitation des correctifs et à une application effective du contrôle des changements

En règle générale, les besoins de correctifs continus sur les serveurs coûtent en ressources, en argent et sont difficiles à gérer. Symantec Data Security Center: Advanced Server (DCS:SA) peut réduire les cycles de correctifs, faire appliquer des procédures de contrôle des changements et libérer des ressources au profit d'activités plus efficaces de gestion de serveur, tout en réduisant les coûts.

POURQUOI EST-CE IMPORTANT ?

Les avantages de l'application effective du contrôle des changements sont doubles.

Tout d'abord, grâce à une application effective du contrôle des changements, vous disposez d'un système entièrement protégé, stable et fiable, et ne risquez aucun changement de configuration entre les cycles de correctifs, même par les administrateurs. Cela permet d'avoir des cycles de correctifs moins fréquents, vous libérant du temps afin de vous concentrer sur les mises à jour critiques des cycles trimestriels ou semestriels tout en vous libérant du temps et des ressources pour vous concentrer sur des activités de gestion de serveur plus stratégiques.

Deuxièmement, les plates-formes et applications qui ne peuvent se voir appliquer de correctifs (comme les plates-formes en fin de support) peuvent être protégées par le durcissement du système, le sandboxing de processus, et la protection de la mémoire, ainsi que l'application de listes blanches ou la ségrégation réseau pour une tranquillité d'esprit supplémentaire.

CAS D'UTILISATION 2 :

Améliorer la fiabilité opérationnelle grâce à une limitation des correctifs et à une application effective du contrôle des changements

SOLUTION SYMANTEC

Symantec Data Security Center: Advanced Server (DCS:SA) est la solution qui peut sécuriser et durcir les systèmes sans nécessiter de migration vers une autre plate-forme compatible et dégager de substantielles économies par rapport aux contrats de support personnalisés.

TÉMOIGNAGE CLIENT

Un organisme bancaire devait réduire ses coûts et trouver des moyens de limiter le temps passé par ses équipes de gestion de serveur intervenant sur des activités de correctifs fréquentes et exigeantes. Grâce à Symantec DCS:SA, l'entreprise a réussi à réduire la fréquence du cycle de correctif, à concentrer ses équipes de gestion de serveur sur les activités les plus critiques, et à réduire les coûts tout en ayant l'assurance que leur banque de serveurs était sécurisée, même entre les mises à jour.

AVANTAGES CLÉS

- Sécuriser les systèmes entre les fenêtres de correctifs et faire respecter le contrôle des changements
- Réduire les coûts opérationnels de l'informatique en réduisant les cycles de correctifs
- Améliorer la sécurité des plates-formes et des applications existantes grâce au durcissement des systèmes
- La détection d'intrusion donne une visibilité sur les changements de configuration et les activités malveillantes
- La prévention des intrusions permet une protection proactive
- Appliquer une séparation des tâches et supprimer les privilèges administrateur ou racine

FONCTIONNEMENT

- Le durcissement des systèmes d'exploitation et des applications assure qu'aucun composant de l'OS ni aucune application critique ne peuvent être modifiés
- Limiter les privilèges d'administrateur et d'utilisateur racine en dehors des fenêtres de contrôle des changements
- Mettre en place une liste blanche sur les systèmes mono-rôle (FTP/HTTP)
- Utiliser des politiques de détection d'intrusion prêtes à l'emploi pour surveiller toute activité suspecte et dommageable
- Appliquer des politiques de prévention d'intrusion pour bloquer les exploits en temps réel
- Utiliser la ségrégation des réseaux basée sur l'hôte pour isoler les applications et les services sur les réseaux WAN et LAN

CAS D'UTILISATION 3 :

Protection des périphériques industriels, embarqués et IoT contre les attaques ciblées

Comment arrêter les attaques avancées sur les machines de points de vente, bornes interactives, guichets automatiques, serveurs de système de contrôle industriel ou périphériques IoT sans avoir besoin de mises à jour continues de signature ? Comment contrôlez-vous l'installation d'applications non autorisées sur les systèmes intégrés ? Comment vous assurez-vous que votre système de contrôle industriel ou votre système de gestion d'atelier est protégé contre les attaques ciblées ?

POURQUOI EST-CE IMPORTANT ?

Les systèmes de points de vente, bornes interactives, distributeurs automatiques de billets et serveurs des systèmes de contrôle industriel sont des équipements stratégiques pour de nombreuses entreprises. Toutefois, ces systèmes sont souvent peu protégés contre les menaces multiples actuelles telles que les attaques ciblées, l'exécution d'applications non autorisées et le vol de cartes de crédit. Les entreprises peuvent avoir recours aux logiciels antivirus traditionnels, mais ces solutions sont susceptibles d'avoir un impact négatif sur les performances des systèmes en raison de la mise à jour permanente des signatures.

CAS D'UTILISATION 3 :

Protection des périphériques industriels, embarqués et IoT contre les attaques ciblées

SOLUTION SYMANTEC

Symantec Embedded Security: Critical System Protection (SES:CSP) peut verrouiller et sécuriser les systèmes intégrés afin de les protéger contre les applications non autorisées et les programmes malveillants avec une solution de sécurité à la fois légère et complète basée sur des politiques de sécurité ainsi que sur un verrouillage des actions, et non sur la recherche permanente de nouvelles signatures antivirus.

WINCOR NIXDORF

« Avec SES:CEP, Symantec fournit la meilleure base de protection contre les intrusions actuellement disponible sur le marché. La collaboration avec un partenaire de confiance tel que Symantec permet à Wincor Nixdorf de renforcer encore son portefeuille de solutions de sécurité sur le long terme. »

- BERND REDECKER, RESPONSABLE DES SOLUTIONS DE SÉCURITÉ POUR LE SECTEUR BANCAIRE, WINCOR NIXDORF

AVANTAGES CLÉS

- Blocage des programmes malveillants via une protection avancée contre les menaces pour sécuriser les systèmes intégrés
- Réduction des coûts associés aux cycles d'installation de correctifs et à la mise à jour des signatures
- Utilisation d'une solution de sécurité légère fonctionnant de manière transparente, qui ne sature pas les ressources et ne requiert pas une actualisation constante des signatures, comme le font les solutions traditionnelles
- Respect des exigences de conformité
- Facilité de surveillance et de gestion des systèmes intégrés et dispersés

FONCTIONNEMENT

- Verrouillage des paramètres de configuration, des systèmes et de l'utilisation de supports amovibles avec un contrôle au niveau des applications et des systèmes
- Surveillance, contrôle et reporting permanents des modifications apportées aux fichiers de configuration avec surveillance de l'intégrité des fichiers
- Utilisation d'un agent léger pour minimiser l'impact sur les performances
- Limitation de l'accès des applications et du réseau aux systèmes avec un contrôle d'accès régi par des politiques reposant sur le principe du moindre privilège ou par l'intermédiaire d'une solution sandbox
- Gestion autonome des politiques de périphériques via des protocoles OTA

CAS D'UTILISATION 4 :

Durcissement du système et protection des infrastructures physiques et virtualisées

Appliquez-vous les recommandations de durcissement de VMware ? Comment limitez-vous les accès non autorisés à votre environnement virtuel ? Comment protégez-vous le serveur de gestion, l'hyperviseur et les machines virtuelles invitées ?

C'est possible grâce à Symantec Data Security Center: Server (DCS:S) et Data Center Security: Advanced Server (DCS:SA)

POURQUOI EST-CE IMPORTANT ?

Les technologies de sécurité morcelées telles que les antivirus et la création de listes blanches ne peuvent pas suffisamment protéger les serveurs virtuels en raison des besoins de confidentialité variable, d'intégrité et de disponibilité. Sans protection de chaque couche de la structure virtuelle, les serveurs et les applications et informations qu'ils contiennent seront exposés à un risque accru de failles de sécurité et d'interruptions des services ou des opérations stratégiques.

CAS D'UTILISATION 4 :

Durcissement du système et protection des infrastructures physiques et virtualisées

SOLUTION SYMANTEC

Symantec DCS:S sécurise vos environnements VMware NSX en combinant un service antivirus sans agent et des politiques de surveillance de la détection des intrusions d'hôte (HIDS) et de durcissement de la prévention de ces intrusions (HIPS) basées sur les dernières recommandations de durcissement VMware.

Sealed Air Corporation

« Sealed Air a l'intention de déployer DCS:SA sur plus de 1 000 serveurs de data center physiques et virtuels. Les fonctionnalités de détection et de prévention des intrusions d'hôte de DCS:SA associées à davantage de contrôles granulaires basés sur des politiques renforceront la sécurisation des terminaux pour notre environnement de data center. »

-CLAY BOSWELL, RESPONSABLE DE L'ASSURANCE DE L'INFORMATION, SEALED AIR CORPORATION.

AVANTAGES CLÉS

- Durcissement, protection et surveillance des serveurs vCenter exécutés sous Windows afin de les préserver des accès non autorisés, des attaques Zero Day et des attaques ciblées
- Analyse antivirus sans agent des charges de travail dynamiques
- Protection prête à l'emploi avec la détection et la prévention d'intrusion d'hôte
- Sécurisation des hôtes pour les partenaires de support des VM
- Déploiement des IDS et IPS au sein de modèles de provisionnement serveur

FONCTIONNEMENT

- Service antivirus grâce à une appliance de sécurité virtuelle sur la plate-forme NSX
- Sécurisation renforcée de vSphere par la sécurisation du serveur vCenter et de la pile d'applications avec un agent installé sur le serveur Windows
- Surveillance et sécurisation des hôtes de gestion des VM et des stations de travail
- Durcissement du système et protection de la charge de travail de chaque serveur virtuel avec des agents sur les différentes machines virtuelles invitées
- Exploitation de rapports personnalisés prêts à l'emploi pour votre environnement VMware

CAS D'UTILISATION 5 :

Respect des exigences de conformité et de risque, telles que Payment Card Industry Data Security Standard (PCI DSS)

Comment faites-vous pour détecter et empêcher les changements de configuration ? Comment faites-vous pour que les exigences de conformité de la norme PCI DSS soient toujours respectées sur vos serveurs ? Comment faites-vous pour protéger les données des titulaires de carte et maintenir la conformité à la norme PCI DSS ?

POURQUOI EST-CE IMPORTANT ?

Pour respecter la norme PCI DSS, les entreprises doivent constamment surveiller leur environnement afin de détecter les violations de politique tout en appliquant des contrôles compensatoires pour les exceptions au respect des obligations de la norme.

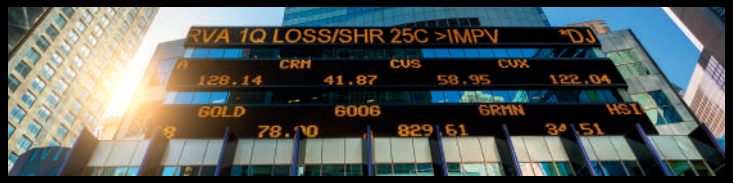
CAS D'UTILISATION 5 :

Répondre aux exigences de conformité et de risque, telles que Payment Card Industry Data Security Standard (PCI DSS)

SOLUTION SYMANTEC

Symantec Data Center Security: Server Advanced (DCS:SA) effectue une surveillance en temps réel, consolide les journaux d'événements pour le reporting et l'analyse, empêche les violations de politique et les falsifications de configuration et fournit des contrôles compensatoires pour certaines obligations de la norme PCI DSS. Pour tout cela, vous n'avez besoin que d'une seule solution.

TÉMOIGNAGE CLIENT



Un grand établissement financier souhaitait une solution de sécurité basée sur le comportement et une protection basée sur des politiques pouvant l'aider à se conformer aux règles FIM, PCI et SOX. Grâce à DCS:SA, il est en mesure d'assurer les contrôles FIM sans configuration préalable et il peut déployer rapidement des politiques pour répondre à leurs besoins croissants. Il a amélioré le niveau de sécurité dans sa DMZ, maintenu une conformité permanente aux règles PCI DSS, identifié des problèmes liés à des applications mal configurées et acquis une visibilité sur des problématiques de gestion de la configuration jusqu'alors totalement inconnues.

AVANTAGES CLÉS

- Protection des données PCI et des serveurs contre les attaques
- Respect permanent des exigences de la norme PCI DSS (en particulier des obligations 1.3, 5, 7, 10 et 11)
- Réduction des risques grâce à la détection en temps réel des comportements non autorisés
- Justification des contrôles compensatoires lors des audits par exportation des politiques
- Possibilité d'effectuer rapidement des recherches pour déterminer la meilleure ligne de conduite
- Séparation effective des tâches pour le personnel administratif et opérationnel

FONCTIONNEMENT

- Surveillance, contrôle et reporting permanents des changements avec surveillance de l'intégrité des fichiers
- Détection de l'apparition de différences par rapport à la configuration souhaitée avec des politiques de détection prêtes à l'emploi
- Limitation de l'accès des applications utilisateur et administrateur et du réseau aux périphériques et ressources PCI avec un contrôle d'accès régi par des politiques reposant sur le principe du moindre privilège
- Alertes en temps réel permettent d'enquêter sur les incidents avec une journalisation consolidée des événements
- Verrouillage de la configuration, des paramètres et des fichiers avec prévention des falsifications de fichiers et de systèmes

INFORMATIONS COMPLÉMENTAIRES

VISITEZ LE SITE WEB :
symantec.com/datacentersecurity

POUR CONTACTER UN SPÉCIALISTE PRODUIT EN EMEA
Composez le +44 (0) 870 243 1080

À PROPOS DE SYMANTEC
Symantec protège les informations échangées à travers le monde et se positionne comme leader mondial des solutions de sécurité, sauvegarde et disponibilité. Nos produits et services innovants protègent les individus et les informations dans n'importe quel environnement, du plus petit appareil mobile aux data centers et systèmes dans le cloud. Notre expertise inégalée en matière de protection des données, identités et interactions donne confiance à nos clients dans le monde interconnecté actuel. Pour plus d'informations, rendez-vous sur www.symantec.com ou rejoignez Symantec sur go.symantec.com/socialmedia

Symantec™