DATA SHEET

FICHE TECHNIQUE DE TOTAL DEFENSE ENDPOINT ET DE CLOUD SECURITY

Pourquoi ai-je besoin de Endpoint et de Cloud security ?

PAYSAGE DES LOGICIELS MALVEILLANTS/MENACES CHANGEANT RAPIDEMENT :

La gamme et la complexité des menaces jour J se sont rapidement développées. Les logiciels malveillants peuvent attaquer votre entreprise de nombreuses manières y compris en se servant du Web et des e-mails.

Le contenu de la plupart des sites Internet Web 2.0 de nos jours, comme YouTube, Facebook et Twitter est dynamique et influencé par des millions d'utilisateurs Internet. Les entreprises ne peuvent plus se contenter de supposer que les sites Internet légitimes soient sûrs et ne contiennent aucun logiciel malveillant. Plus de 80% des infections par des virus malveillants d'aujourd'hui ont lieu sur des sites Internet légitimes compromis par des pirates.

L'e-mail est également devenu un outil dangereux. Les courriers indésirables sont passés du simple inconvénient à une véritable épidémie et à un vecteur de menace majeure quant aux logiciels et contenus malveillants, faisant de ces derniers un risque sérieux pour la sécurité des entreprises.

MAIN D'ŒUVRE À DISTANCE :

La tentative de résolution des problèmes de sécurité TI d'entreprise complexes de plus en plus importants et de prise en charge d'une main d'œuvre dont la demande d'accès à diverses ressources Web ne cesse d'augmenter et voulant avoir les moyens de travailler à distance est - jusqu'à présent - décourageante. Total Defense offre une protection complète et illimitée mêmes aux utilisateurs à distance grâce à une solution Endpoint & Cloud Security qui permet également de réduire les coûts.

SÉCURITÉ MULTICOUCHE :

Vu le nombre, variété et complexité des menaces jour J en constante augmentation, la tâche de protection des données et des actifs de l'entreprise est très lourde pour les administrateurs TI. Les vecteurs d'attaque se sont développés et incluent votre navigateur Web, messagerie électronique, interface USB ou connectivité Wi-Fi. Avec plusieurs vecteurs d'attaque, une approche de sécurité multicouche est nécessaire à la couverture de toutes vos bases.

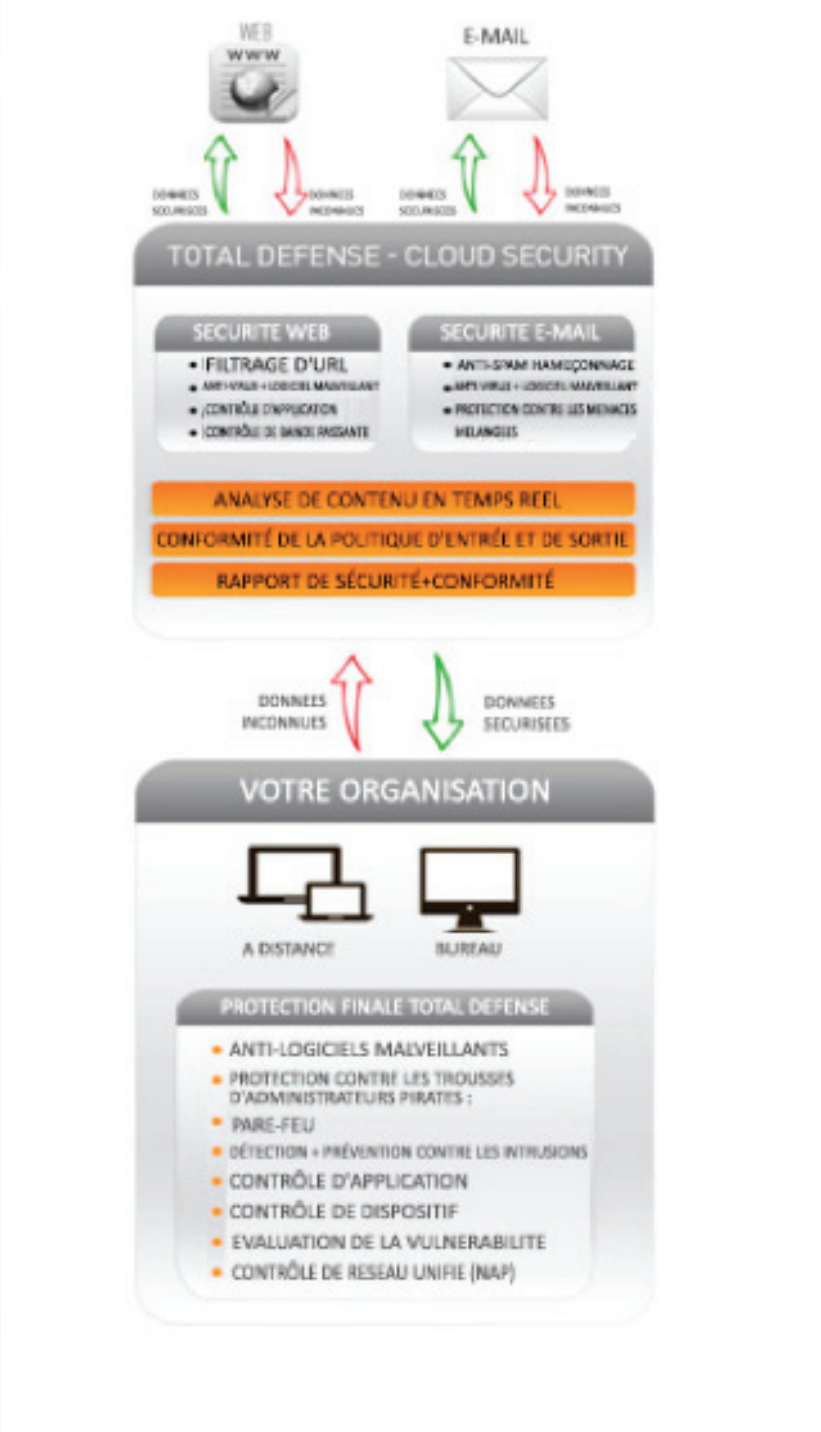
La Suite Total Defense Endpoint Suite protège vos utilisateurs finaux contre les menaces de dispositifs USB non autorisés, cartes SD, CD/BluRay et autres supports physiques ou dispositifs connectés.

Total Defense Cloud Security protège vos utilisateurs finaux contre les menaces Web et e-mail incluant des téléchargements ou des pièces jointes d'e-mail infectés, des exploitations de navigateurs et des codes malveillants actifs.

Ensemble, Total Defense Endpoint et Cloud Security offre une protection complète contre tous les vecteurs d'attaque et garantit à vos utilisateurs et données une sécurité même lorsque les points finaux sont en-dehors de votre réseau.

POURQUOI CHOISIR LA PROTECTION TOTAL DEFENSE ENDPOINT ET CLOUD ?

Total Defense Endpoint & Cloud Security offre une protection complète, multicouche et illimitée aux points finaux, serveurs et machines à distance contre les intrusions, programmes et logiciels malveillants.



TOTAL DEFENSE™
Beyond Protection

FONCTION	AVANTAGE
PROTECTION FINALE :	
Moteur anti-logiciels malveillants robuste	Protection complète contre les virus, chevaux de Troie, vers, logiciels espions et bots
Protection contre les trousses d'administrateurs pirates	Détection et nettoyage de trousses d'administrateurs pirates intégrées
Prévention contre les intrusions hébergée et pare-feu de bureau à états	Protection des points finaux contre les intrusions même lorsque vous êtes déconnecté du réseau
Contrôle d'applications	Offre une protection contre les applications malveillantes, une contrôle de la bande passante et de la productivité en vous permettant de bloquer et d'autoriser de manière sélective les applications exécutées sur les points finaux de votre environnement
Contrôle de dispositif	Surveillance et contrôle de l'utilisation des dispositifs de stockage amovibles
Console de gestion Web	Gestion centrale et surveillance des points finaux, politiques, concessions de licences, événements et rapports à partir d'une seule console
Évaluation de la vulnérabilité	Vous permet de mettre en place des politiques et de se conformer aux normes de sécurité
Politiques prédéfinies	Fournit les paramètres recommandés et permet un déploiement plus rapide/facile
Listes d'exclusions	Réduit les charges indirectes en permettant aux administrateurs de mettre en place une liste de données critiques et d'applications intensives qui pourraient être exclues des balayages en temps réel
Découverte de points finaux	Vous fournit plusieurs options - Balayage de réseau, balayage Active Directory, balayage de plage IP et découverte rapide pour simplifier le processus de configuration
Rapport complet	Meilleur suivi du statut de la protection et des logiciels malveillants aux points finaux avec vues résumées et détaillées
Contrôle de réseau unifié (NAP)	S'assure que seuls les systèmes conformes aux paramètres de sécurité de l'entreprise puissent accéder aux ressources de réseau
CLOUD SECURITY :	
FONCTIONS WEB :	
Filtrage d'URL	Gestion des accès Web et protection contre les attaques de logiciels malveillants
Contrôle d'applications (Cloud Security)	Prise de contrôle sur les applications sur les bureaux des utilisateurs accédant à Internet, assurant productivité et protection contre les menaces des applications Web 2.0 (ex. diffusion multimédia, messagerie Web, etc.)
Contrôle de bande passante	Surveillance et contrôle de la consommation de la bande passante pour veiller à ce que la bande passante de votre entreprise ne soit utilisée qu'à des fins professionnelles
FONCTIONS E-MAIL :	
Anti-spam et anti-phishing	Détection et blocage des courriers indésirables dans le cloud, avant que votre passerelle e-mail ne les reçoive
Protection contre les menaces mélangées	Détection et blocage de pièces jointes infectées, de liens d'URL malveillantes d'e-mails garantissant à votre entreprise en protection complète contre une gamme complète de menaces
FONCTIONS CLOUD COMMUNES :	
Anti-virus et protection contre les logiciels malveillants	Protection contre les virus, logiciels espions, botnets, exploitations de navigateurs et autres menaces Web 2.0
Conformité de la politique d'entrée/sortie	Garantie d'une utilisation appropriée des ressources, blocage de contenus Web/e-mail inappropriés et création d'un lieu de travail sûr et productif pour vos employés
Rapport de conformité	Suivi d'événements spécifiques et de l'activité de l'utilisateur et contrôle total de l'Internet de votre entreprise - trafic HTTP et SMTP
Synchronisation de répertoires	Configuration simplifiée et gains de temps avec la synchronisation automatique. Total Defense prend en charge tous les formats de répertoires communs incluant Active Directory et le LDAP

TOTAL DEFENSE™
Beyond Protection

PROTECTION FINALE - COMPATIBILITÉ DU SYSTÈME :

CONFIGURATION REQUISE POUR LES SITES PETITS À MÉDIUM (<1000 POINTS FINAUX) :

Composant	Processeur	RAM	Disque dur
Serveur de gestion minimum	1,80 GHz Pentium 4*	1GO**	40GO
Serveur de gestion recommandé	2,80 GHz Intel Core 2 Duo	2GO	100GO
Microsoft SQL Server	2,80 GHz Intel Core 2 Duo	2GO	100GO

* Les UC avec des particularités inférieures n'ont pas été testées, elles pourraient fonctionner si leur vitesse/modèle est proche de celles susmentionnées.
**Un serveur de gestion avec 1 GO de RAM prend en charge un maximum de 250 points finaux et une partition. Il ne devrait être utilisé que pour les tâches basiques, comme la visualisation du Tableau de bord, et ne prend pas en charge la création, la gestion ou le déploiement de politiques de Protection proactive. Ces restrictions disparaissent si vous mettez à niveau le Serveur de gestion à 2 GO ou plus.

PROTECTION FINALE - SYSTÈME D'EXPLOITATION COMPATIBLE

SERVEUR	CLIENT
Windows 2003 Server – SP2 ou supérieur	Windows XP Professional
Windows 2003 Server R2 – SP2 ou supérieur	Windows 2000 Professional
Windows 2008 Server – SP2 ou supérieur	Windows 2000 Server Standard
Windows 2008 Server R2 – SP1 ou supérieur	Windows 2003 Server
Windows Small Business Server (2003, 2008, 2011)	Windows 2003 Server R2
Windows 7 – SP1 ou supérieur	Windows Vista
	Windows 2008 Server
	Windows 2008 Server R2
	Windows Small Business Server (2003, 2008, 2011)
	Windows 7