

safend

Solutions de protection contre les fuites d'informations par les postes de travail

Protégez vos IP d'entreprise, vos secrets commerciaux, ainsi que les données sensibles de vos clients et de vos employés



Maintenez un équilibre optimal entre la productivité et la sécurité des informations

Conformez-vous aux règles de sécurité des données et aux normes de confidentialité

La protection efficace des informations commence sur les postes de travail

Les solutions de Safend vous protègent contre les fuites de données par les postes de travail. En proposant une visibilité et un contrôle granulaires sur les ports et les périphériques des utilisateurs, Safend permet la protection des données sensibles, qu'elles soient ou non en mouvement, sans nuire à la productivité.

Fuites d'informations par les postes de travail | la menace

Au cours de la décennie qui a suivi la prise de pouvoir des technologies VPN et de pare-feu, les grands investissements dans des solutions pour passerelles ont démontré leur inefficacité face aux employés malintentionnés ou négligents munis d'un simple périphérique de stockage amovible.

La survie et le succès de l'activité reposent sur la sécurité des informations. Les entreprises sont tributaires de la sécurité de leurs données. Ces dernières peuvent être des informations concernant la propriété intellectuelle de plans et de secrets commerciaux, ou des renseignements confidentiels concernant la clientèle, comme des données sanitaires, des informations financières et des numéros de sécurité sociale. En outre, les régulateurs demandent la garantie que les données confidentielles resteront accessibles aux seuls utilisateurs autorisés.

Les statistiques industrielles démontrent régulièrement que les menaces sécuritaires les plus réelles pour les entreprises sont internes. Comme plus de 60 % des données des entreprises sont stockées sur les postes de travail, les solutions pour passerelles et les politiques de sécurité ne sont pas suffisantes pour atténuer les risques.

Le nombre croissant de périphériques de stockage amovibles, d'interfaces (physiques et sans fil), et d'utilisateurs ayant accès à des informations sensibles, contribuent à faire des fuites d'informations - qu'elles soient accidentelles ou malintentionnées - une menace très réelle. Il est simplement trop aisé pour quiconque de connecter un lecteur de MP3, un appareil numérique ou une clé USB sur un point d'accès en entreprise, et de repartir avec des données sensibles. Selon Forrester, la perte de données par les postes de travail est désormais un problème de sécurité majeur - devant les programmes nocifs, les espions et autres menaces.

Sécurité des postes de travail | un impératif financier

Avec l'apparition de brèches fortement médiatisées dans la sécurité des données, les entreprises sont confrontées à un fort préjudice pour leur image de marque et à des pertes monétaires très déstabilisantes. Pour y répondre, les responsables de l'informatique et de la sécurité des entreprises doivent adopter des stratégies de prévention contre les fuites d'informations (ILP) sur les postes de travail. Dans les faits, Aberdeen estime que, sans une solide solution de protection des données sur les postes de travail, les sociétés peuvent perdre des millions de dollars pour cause de vols d'IP ou d'emploi non approuvé de données précieuses.

Sécurité des postes de travail | un impératif réglementaire

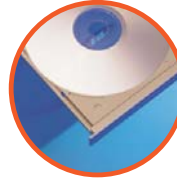
Les initiatives de réglementation de la sécurité, telles que Sarbanes Oxley (SOX), HIPAA, FISMA, BASEL II, et le DPA (UK Data Protection Act) imposent aux sociétés de préserver une visibilité constante de l'activité des postes de travail. Dans le climat actuel très sensible aux réglementations, les sociétés sont censées faire preuve d'une compréhension totale de toutes les activités de transfert des données. Elles doivent identifier et limiter toutes les formes et les sources possibles de fuites tout en remédiant immédiatement aux failles sécuritaires détectées, rapport d'audit d'utilisation des ressources à l'appui. Sans la mise en place d'une solution efficace visant à sécuriser et contrôler les postes de travail, il est difficile de se mettre en

Les menaces pour les postes de travail en chiffres

- 52% des sociétés étudiées ont subi des pertes de données via des lecteurs USB ou autres supports amovibles - *Forrester Report 2007*
- Plus de 70% des failles sécuritaires et des vols de données sont d'origine interne - *Vista Research*

Le coût des fuites de données

- Le coût moyen par incident lié à des pertes de données était de 5 millions de \$ en 2006, et sa croissance annuelle est de 30% - *Ponemon Institute*
- Les fuites d'informations déclenchent, en moyenne, une baisse de 5 % du prix des actions des sociétés.
- Il faut presque un an pour revenir au niveau antérieur à l'incident.
-- *EMA Research*



Le défi | une prévention efficace contre les fuites de données par les postes de travail

Malgré le danger clair et présent de fuites d'informations, la mise en place d'une stratégie ILP efficace reste un obstacle difficile à gravir pour la plupart des sociétés.

Les périphériques externes modernes - lecteurs flash, adaptateurs de communication, téléphones intelligents et bien d'autres - augmentent considérablement la productivité. Ils permettent aux employés de rester en contact et connectés, et aident à créer un avantage compétitif. La sécurisation des postes de travail sans impact sur la productivité nécessite une solution très souple, capable de prendre en compte les dynamiques des environnements de travail du monde réel.

Comme la plupart des utilisateurs considèrent les périphériques externes comme étant personnels et privés - contrecarrant et contournant souvent les solutions de sécurité imposées - les solutions d'ILP modernes doivent être transparentes. Par ailleurs, les compromis ne sont pas acceptables. Tous les points de fuite possibles des données doivent être protégés par une sécurité puissante, applicable de force et à l'épreuve des sabotages.

Il est clair qu'il est primordial pour la sécurité des données d'identifier les données sensibles ou les activités suspectes. Les sociétés ont besoin d'une visibilité en profondeur sur les activités en cours et passées des postes de travail, et elles mettent en place des solutions de sécurité des postes de travail qui retracent les transferts de données en se basant sur les politiques de sécurité des données de l'entreprise.

La combinaison ultime de visibilité et de contrôle

Safend crée des solutions conçues pour assurer une protection ILP complète depuis la base. Elles offrent aux administrateurs de la sécurité la puissance d'une visibilité granulaire sur chaque fuite potentielle par un point d'accès, des capacités sophistiquées de création de politique, et des fonctions d'application.

Avec leur mise en œuvre aisée, leur entretien en douceur pour les administrateurs, et leur transparence maximum pour les utilisateurs, les solutions de Safend permettent aux sociétés de profiter pleinement des avantages de l'informatique mobile en termes de productivité, sans compromis pour la sécurité.

Safend élimine les fuites d'informations sur des milliers de postes de travail, proposant une visibilité et un contrôle complets sur tous les points de circulation des données sensibles.

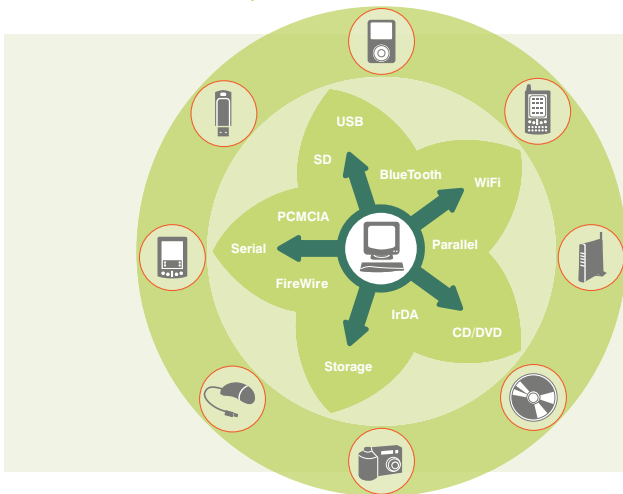
Visibilité

Seule la visibilité détaillée de l'activité des postes de travail - en cours et passée - peut permettre aux administrateurs de la sécurité d'espérer contrôler et appliquer des politiques de sécurité en harmonie avec les usages du monde réel. Safend offre aux sociétés la capacité d'interroger, de manière rapide et transparente, tous les postes de travail organisationnels, tout en localisant et en répertoriant tous les périphériques qui sont ou ont été connectés localement.

Contrôle

Sans capacité d'application absolue, les meilleures politiques de sécurité des postes de travail ne fonctionnent pas. Le contrôle granulaire de l'activité des postes de travail et du contenu est crucial pour la sécurité. Safend contrôle le trafic en temps réel et applique des politiques de sécurité personnalisées sur toutes les interfaces physiques et sans fil, ainsi que sur les périphériques de stockage. Safend détecte, consigne et restreint les transferts de données non approuvés depuis chaque ordinateur de l'entreprise. Chaque ordinateur est protégé en permanence, même lorsqu'il n'est pas connecté au réseau. En ajoutant une protection contre les accès indésirables aux données provenant du côté extérieur du pare-feu, Safend assure encore plus la sécurité des utilisateurs mobiles et de leurs données en cryptant les informations écrites sur les périphériques de stockage amovibles ou en forçant l'emploi unique de lecteurs flash à cryptage physique.

Effective Endpoint ILP



Safend propose :

- La visibilité du contenu de chaque point d'accès
- Un contrôle granulaire sur la totalité des interfaces physiques/sans fil, ainsi que les périphériques de stockage
- Une protection embarquée des données sensibles stockées sur chaque ordinateur de l'entreprise

Pourquoi Safend ?

- Sécuriser et contrôler intelligemment chaque point d'accès
- Protéger la propriété intellectuelle de la société et les données confidentielles de l'entreprise
- Protéger les informations sensibles sur les clients et les employés
- Maintenir la conformité avec les règles de sécurité des données
- Empêcher les atteintes à la réputation et aux revenus résultant de failles sécuritaires
- Équilibrer la demande de mobilité et le besoin de sécurité

CITATIONS

"Le simple fait de dire à plus de 500 personnes de ne pas se servir de leurs ports USB n'était pas une solution réaliste... Safend nous offre les outils dont nous avons besoin pour préserver la confidentialité et l'intégrité des informations de nos clients. "

- Bill Liston, Technicien de solutions informatiques, ConnectiCare

"Les produits de Safend sont bien pensés et, en réalité, ils ont dépassé nos attentes. Le produit est robuste et il nous aide dans notre quête proactive d'identification des problèmes potentiels. "

- Alan Pomerantz, Responsable de la sécurité de la Bourse de Philadelphie

"L'installation de Safend nous a permis de gérer et contrôler facilement l'activité de tous les périphériques de notre entreprise... Le déploiement s'est déroulé en douceur - aucune erreur, aucun souci... Nous avons gagné du temps et évité les efforts inutiles."

- Michael Apt, Responsable de l'informatique et de la sécurité, SCD

À propos de Safend

Safend est un distributeur majeur de solutions préventives contre les fuites des données par les postes de travail, protégeant l'entreprise contre les pertes de données par les ports physiques, sans fil et des supports amovibles, tout en assurant la conformité avec les réglementations de sécurité des données et les normes de confidentialité. Les solutions de Safend, disponibles dans le monde entier, sont mises en œuvre au sein d'entreprises internationales, d'agences gouvernementales et de petites et moyennes entreprises. Fondée en 2003, Safend est une société privée dont le siège est basé à Tel Aviv. Elle a des bureaux à Philadelphie. Pour tout renseignement, visitez le site : www.safend.com.



www.safend.com

Safend Ltd. 32 Habarzel Street, Tel-Aviv 69710, Israel Tél: +972.3.6442662, Fax: +972.3.6486146

Safend Inc. 2 Penn Center, Suite 301, Philadelphia, PA 19102, USA Tél: +1.215.496.9646, Fax: +1.215.496.0251

Gratuit depuis les U.S.A. (vers les U.S.A. et Israël): 1.888.225.9193, info@safend.com

Copyright © 2007, Safend Ltd. Les informations contenues dans ce document sont exactes au moment de la publication. Elles peuvent être modifiées sans notification préalable. 06/07 001