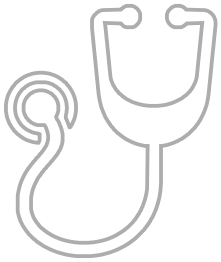
SAFEND DPS POUR LES ETABLISSEMENTS DE SANTÉ

Livre Blanc



safend
a SuperCom company

POURQUOI NE PAS PROTÉGER LES DONNÉES SENSIBLES MET VOTRE ETABLISSEMENT DE SANTÉ EN DANGER

Changeant le visage des soins de santé, les technologies de communication d'aujourd'hui apportent de nouveaux risques et défis liés aux données, à leur sensibilité, à leur utilisation et à leur sécurité. Afin de protéger les informations sensibles, ces changements sont dus notamment à des réglementations et des normes strictes comme la nouvelle régulation Européenne GDPR, ce qui apporte des exigences supplémentaires sur les établissements de santé.

Quelles sont les informations sensibles dans les établissements de santé?

- Les renseignements personnels sur les patients
- Les renseignements personnels sur le personnel
- Les antécédents médicaux du patient
- L'historique financier du patient et du personnel
- Les informations sur la gestion des établissements de

Quels sont les principaux risques sur les données dans les établissements de santé

- Le vol interne de données, intentionnel ou involontaire
- Les fuites de données sensibles via des points d'extrémité: ports et périphériques de stockage USB, périphériques externes tels que CD, DVD et imprimantes
- Les accès non autorisés à des données non protégées
- Les accès non autorisés à des données protégées
- L'envoi d'informations classifiées aux mauvaises personnes

Comment ces risques peuvent-ils affecter un établissement de santé?

- Les actions judiciaires menées par les patients ou leurs représentants à la suite d'un mauvais usage de leurs informations sensibles
- Les amendes éventuelles après avoir manqué aux normes locales ou pour sanctionner une cyber-attaque réussie
- La perte d'intégrité et de réputation
- La perte de main-d'œuvre et d'heures de travail pour traiter les plaintes des patients
- De lourdes pertes financières résultant de vols de données réussies

Quelques faits et chiffres en 2016

- Groupe hospitalier privé de l'Artois, France : Plusieurs fichiers PDF retrouvés sur le web et contenant les identités, résultats sanguins, informations personnelles, allergies et penchants pour l'alcool de patients. La fuite était due à pare-feu maladroitement suspendu et à des données non chiffrées.

- Hôpital du Nouveau-Mexique, Albuquerque, USA: un problème technique lié aux systèmes de facturation des hôpitaux a causé l'envoi de renseignements médicaux de plus de 2 800 patients à des adresses incorrectes

- UnityPoint Health-Allen Hospital, Iowa, USA: violation de données sur le vol d'informations personnelles, y compris les numéros de sécurité sociale de 1 620 personnes

- Keck Medicin, Los Angeles, USA: les fichiers de données sur deux serveurs ont été rendus inaccessibles aux employés après avoir été compromis par un Ransomware. L'hôpital n'a pas voulu payer l'argent de la rançon

QUELS SONT LES DÉFIS DE LA PROTECTION DES

Fournir une solide solution technologique à la protection des données et rester conforme aux réglementations et aux normes requises sans pour autant affecter l'efficacité de l'utilisateur final.
D'autres défis majeurs incluent le contrôle de l'accès aux fichiers et aux dossiers de données sensibles, le chiffrement des données et la façon dont les informations sont sauvegardées et téléchargées. Les autres exigences sont la sécurisation des dispositifs externes ainsi que la mise en place d'alertes et d'analyses en continu.

Etre à jour avec les normes telles que la régulation GDPR

- Se mettre et rester en conformité avec les standards de sécurité tels que le GDPR
- Comprendre et respecter les normes locales et internationales

Où les données sensibles sont-elles les plus exposées à la menace?

- Sur les postes clients tels que les ordinateurs, les ordinateurs portables et les appareils mobiles
- Sur les supports externes tels que les clés de stockage USB, les disques durs externes ou les CD/DVD
- Lors des transferts de données

Savoir où les données sensibles sont à tout moment

- Pour définir une forte politique des autorisations d'accès
- Pour empêcher les bonnes personnes de faire de mauvaises choses
- Pour empêcher les mauvaises personnes de faire de mauvaises choses

Comment éviter l'utilisation de données volées

- Définir quelles sont les informations accessibles et par qui
- Chiffrer les informations sensibles
- Chiffrer les données des ordinateurs portables et des périphériques externes de

COMMENT SAFEND DPS PROTÈGE VOS DONNÉES

Un fonctionnement silencieux sans perturber les activités quotidiennes

La solution Safend DPS Data Protection pour les institutions financières est basée sur les modules Protector et Encryptor qui équilibrent la productivité et la performance sans interférer avec les activités quotidiennes.
Lors de l'installation de Safend DPS sur un réseau, une analyse précise des exigences en matière de protection des données est évaluée. Cela permet de créer des stratégies et leurs exceptions, de créer des profils et d'ajouter des autorisations utilisateur / machine concernant l'utilisation des ports et des médias de stockage externes.
En tant que suite granulaire, qui surveille et contrôle les flux d'informations sur les postes clients de votre établissement, Safend DPS applique des politiques d'autorisations et d'exceptions car il protège, chiffre, inspecte et génère des rapports sur l'utilisation des ports et des périphériques.
Par exemple, Protector peut bloquer l'utilisation de tous les périphériques externes tout en autorisant la copie des fichiers Excel sur un modèle de clé USB spécifique.

Rentabilité et adaptabilité

L'intégration de Safend DPS dans le réseau de données de votre organisation contribue à réduire les coûts associés aux fuites de données via les postes clients non protégés.
Safend DPS a actuellement la capacité de prendre en charge plus de 250 000 terminaux via un seul environnement.

Compréhension des exigences de conformité

Safend DPS Protector propose déjà une solution pour répondre à la norme GDPR de l'UE et, en tant que solution personnalisable, elle peut être modifiée pour s'adapter à tous les cas de figure. Safend DPS peut également répondre à d'autres exigences de conformité majeures telles que SOX, HIPAA, PCI, FISMA ou d'autres normes spécifiques.

Surmonter les problèmes d'intégration

Safend DPS est conçu pour une installation complète et peut être installé par les experts certifiés Safend ou par l'administrateur système de votre société. En fonction des besoins de la solution, l'ensemble du processus d'intégration est simple et ne prend que très peu de temps.

Les profils, les politiques et les exceptions de Safend DPS

Avant l'installation du serveur, Safend DPS peut identifier l'utilisation des connexions USB, FireWire, PCMCIA, PCI, stockage interne et WiFi dans votre établissement.
L'utilisation de ces informations fournit aux administrateurs les connaissances dont ils ont besoin pour créer des politiques, des autorisations et des exceptions préventives à l'échelle de l'entreprise.
Cela peut inclure le blocage de tous les périphériques externes, puis l'attribution d'exceptions à différents utilisateurs / périphériques ou que des informations spécifiques puissent uniquement être téléchargées sur un périphérique externe.

Plus de faits et de chiffres

- Vista Research: 70% des fuites de données proviennent de l'entreprise
- Forrester: 52% des grandes entreprises nord-américaines ont perdu des données confidentielles via des supports amovibles comme les clés USB
- IDC: plus de 60% de données confidentielles résident sur les postes clients
- Ponemon Institute: plus de 16 000 ordinateurs portables sont perdus chaque semaine dans les aéroports par des hommes et des femmes en transit aux Etats-Unis, en Europe et aux Emirats Arabes Unis

Safend DPS propose les options suivantes:

- Bloquer / permettre le transfert de données
- Bloquer le transfert de données et recueillir des informations
- Bloquer le transfert de données sans recueillir d'informations
- Permettre le transfert de données et recueillir des informations
- Permettre le transfert de données sans recueillir d'informations

Un serveur et un agent de protection des données

Construit en tant que suite de modules de protection des données, Safend DPS protège vos informations en les contrôlant, les chiffrant, les surveillant et les mettant à jour au cours de leur cycle de vie.

Les modules Safend Data Protection Suite

- Protector: contrôle des ports (physiques et sans fil) des postes clients, contrôle et chiffrement des médias de stockage
- Encryptor: chiffrement transparent des données sur les ordinateurs portables et les PC
- Auditor: détection immédiate des risques sur les ports / périphériques WiFi connectés aux postes du réseau

Protector, contrôle des points ports et des périphériques

Solution souple et intuitive, dotée de puissantes fonctionnalités de chiffrement des fichiers basées sur des règles, Protector évite les échanges de données inappropriées avec les smartphones, les appareils photo numériques ou les cartes mémoires. Protector permet la création de stratégies de sécurité hautement granulaires et personnalisables qui détectent, autorisent ou restreignent automatiquement les transferts de fichiers en fonction des autorisations de chaque utilisateur et du type, du modèle et du numéro de série des périphériques utilisés.

Encryptor, chiffrement complet des données

Solution de chiffrement complète, spécialement pour les informations financières, Encryptor bloque l'accès inapproprié ou le transfert d'informations. Comme il sécurise les données des postes clients, Encryptor avertit immédiatement l'administration de tous les incidents de fuite de données intentionnels ou non. Avec toujours une longueur d'avance sur les technologies de piratage de données existantes et nouvelles, Encryptor protège les données au repos et peut couvrir jusqu'à 250 000 postes à partir d'un seul serveur.

Auditor, détection immédiate des risques

Ayant la capacité de fonctionner sur jusqu'à 60.000 ordinateurs, Auditor fonctionne avec ou sans le serveur DPS et permet de connaitre l'utilisation des ports USB, FireWire, PCMCIA, PCI, des stockages internes et des connexions WiFi des postes connectés sur votre réseau. Auditor recherche les informations sur vos postes selon l'architecture Microsoft Active Directory, la plage IP ou le nom de l'ordinateur et peut s'intégrer simplement à Safend Protector.

COMMENT SAFEND DPS PROTÈGE LES DONNÉES DE VOS POSTES

En comprenant les défis de sécurité et en introduisant des solutions éprouvées, Safend DPS protège les données de vos postes clients en les surveillant et les protégeant et vous informe si elles sont utilisées et par qui.
Safend DPS est très stable, s'adapte à tous les environnements et, une fois intégré à votre réseau, il s'exécute automatiquement sans interrompre les activités quotidiennes.
Conçu comme une solution robuste pour le contrôle des ports et des périphériques, équipé également d'un mécanisme anti-sabotage, Safend DPS intègre même des règles prédéfinies de mise en conformité telles que GDPR, PCI, HIPAA et SOX.
Safend est déjà utilisé comme une solution de protection des données par de nombreux établissements de santé qui l'ont intégrée dans leur réseau pour protéger leurs informations sensibles.