# SAFEND DPS POUR LES MUNICIPALITÉS

Livre Blanc

safend
a SuperCom company

## SÉCURISER LES DONNÉES PUBLIQUES

Tout en offrant aux habitants une vie urbaine agréable, les municipalités d'aujourd'hui sont devenues une mine d'informations publiques et privées et des cibles parfaites pour le vol ou les fuites de données. L'augmentation des moyens de communication, le partage d'informations entre les infrastructures municipales, les services, les employés inter-bureaux et les résidents, ont également présenté des menaces supplémentaires et plus avancées sur les données municipales.
Ces menaces ont engendré des réglementations internes plus strictes ainsi que des exigences pour se conformer à des normes majeures telles que le GDPR.
En prenant cela en considération, lors de la recherche de solutions de protection des données, un besoin majeur est de savoir exactement quelles données sont à risque et où les fuites peuvent se produire.

**Exemples de données à risque**

- Les données personnelles des résidents et des employés, par exemple des services de bien-être, de santé, d'éducation, d'application de la loi ou de ressources humaines
- L'aménagement urbain, y compris les autorisations de planification, les appels d'offres, les développements futurs ou les actions en justice
- Les informations financières concernant les employés, les résidents ou les projets municipaux comme les méthodes de paiement ou les numéros de carte de crédit

**Quelles sont les principales menaces?**

- Les accès non autorisé aux données protégées et non protégées
- La fourniture innocente d'informations par manque de connaissance ou par négligence
- L'extorsion ou le transfert forcé d'informations sensibles
- Les fuites accidentelles ou intentionnelles de données via les terminaux: ports et périphériques de stockage USB, enregistreurs de clés, BYOD et autres périphériques externes tels que CD, DVD et imprimantes
- L'introduction de virus, de chevaux de Troie ou de vers via des terminaux comme les clés USB, les keyloggers ou via Internet
- Le trafic et l'utilisation externe de données sensibles volées

**Quelles peuvent être les répercussions?**

- Une menace pour la sécurité d'un pays et de ses habitants
- Le contrôle malveillant des réseaux de données classés, secrets et top-secrets
- La possession et l'utilisation de données et d'informations personnelles civiles
- Des dommages irréparables à l'intégrité et à l'image d'un pays
- Le trafic et la réutilisation d'informations volées / modifiées
- La perte de temps et d'argent pour gérer les attaques réussies
- Des amendes et des sanctions (GDPR)

## DÉFIS DE DONNÉES PUBLIQUES, PRIVÉES ET PERSONNELLES

Contenant les informations passées, présentes et futures d'une ville, les bases de données municipales sont extrêmement intéressantes pour les pirates informatiques, les groupes organisés et les internautes qui cherchent ce dont ils ont besoin. Souvent en plein essor, les technologies de vol de données posent de plus en plus de défis aux fournisseurs de solutions de protection des données dans leurs efforts pour demeurer en avance. Cela comprend le respect des normes, 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 et les standards**

- Comprendre et respecter les normes municipales internes
- Comprendre et respecter les normes locales et internationale

**Quelques faits et chiffres pour 2016**

- Medfield, Massachusetts, États-Unis: rançon payée après la fermeture des réseaux de données municipaux pendant une semaine. Exposition de renseignements personnels appartenant à 14 200 employés actuels et anciens du Comté de Salt Lak, Utah
- eThekwini Municipalité de Johannesburg: e-services arrêtés après l'exposition de données personnelles après qu'un hacker ait altéré l'URL du site.
- Ottawa, Canada: divulgation accidentelle de renseignements personnels de près de 2000 retraités lors d'une entrevue. Cette erreur est passée inaperçue jusqu'à ce que le journaliste informe la municipalité.
- Utrecht Pays-Bas: fuites de milliers de données personnelles des résidents via l'intranet municipal

**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 sont les données sensibles 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

## Les Dilemmes de la Protection des Données

- Trouver une solution qui fonctionne et qui ne perturbe pas les activités quotidiennes
- Trouver une solution efficace et granulaire
- Comprendre les normes de sécurité définies par les municipalités
- Répondre aux exigences de conformité telles que le GDPR
- Surmonter les problèmes d'intégration
- Définir simplement les profils, les politiques de sécurité et les exceptions

**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

**Un fonctionnement silencieux sans perturber les activités quotidiennes**

La solution Safend DPS Data Protection pour les Municipalités 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.

**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.