

APX Modules DLP

BÉNÉFICIEZ D'UNE VISIBILITÉ, D'UN CONTRÔLE ET D'UNE SÉCURITÉ SUR LES DONNÉES SENSIBLES ENTRANTES ET SORTANTES EN ÉTENDANT LES CAPACITÉS DE DLP DE L'ENTREPRISE À VOS CANAUX WEB ET DE MESSAGERIE ÉLECTRONIQUE

Entre une réputation ternie et des amendes et sanctions réglementaires, une violation de données peut avoir de fâcheuses conséquences pour votre société. En outre, comme la force de travail devient de plus en plus mobile, il est crucial de disposer d'une visibilité sur les données sensibles qui entrent et sortent de votre réseau.

Pour mettre un terme au vol de données, respecter les exigences de conformité et préserver votre marque et votre propriété intellectuelle, vos défenses informatiques doivent fonctionner en dehors de votre société. Vous devez sécuriser vos données sensibles au niveau du Web et de la messagerie électronique pour vos employés mobiles qui travaillent en dehors du réseau. En étendant les capacités complètes de DLP pour l'entreprise à vos défenses, vous avez la possibilité de sécuriser les canaux Web et de messagerie électronique, et bien plus encore.

POURQUOI CHOISIR LES MODULES DE DLP POUR LE WEB ET LA MESSAGERIE ÉLECTRONIQUE DE FORCEPOINT™?

Les Modules de DLP pour le Web et la messagerie électronique de Forcepoint reposent sur une technologie extrêmement précise et la meilleure du marché, afin de répondre rapidement et facilement aux exigences de conformité et réglementaires en étendant les capacités de DLP pour l'entreprise au Web et à la messagerie électronique. Ils confèrent une visibilité en temps réel et historique sur le transfert de données sensibles à tout moment. Avec un grand nombre de capacités uniques, comme la ROC (reconnaissance optique des caractères) et l'identification des chiffrements personnalisés, Forcepoint élève la DLP pour l'entreprise à un nouveau niveau.

- Une bibliothèque complète de modèles prêts à l'emploi, qui vous permet de configurer et de déployer rapidement des politiques pour identifier et stopper le vol de vos données critiques.
- Un assistant facile à utiliser pour déployer les modules de DLP pour le Web et la messagerie électronique avec votre personnel en toute facilité.
- Bénéficiez d'une visibilité sur les données entrantes et sortantes de votre réseau qui transitent via le Web et la messagerie électronique.
- Empêchez la « Drip DLP », qui désigne le vol lent et à faibles volumes de données comme des numéros de cartes de crédit ou d'autres archives.
- Neutralisez les menaces internes grâce à des analyses comportementales qui identifient et signalent les personnes pouvant présenter un risque envers votre entreprise.
- La ROC (reconnaissance optique des caractères) permet d'identifier le texte contenu dans une image pour éviter que des données ne filent en douce dans des captures d'écran, des photos et d'autres images.
- Avec la solution AP-EMAIL, appliquez les politiques de DLP au trafic d'Microsoft Office 365 pour sécuriser les données sensibles tout en adoptant les nouvelles technologies.
- Remédiez aux données sensibles, pour vous permettre de les auditer, de les bloquer, de les autoriser, de les alerter, de les informer, de les mettre en quarantaine* ou de les chiffrer* lorsqu'elles sont trouvées. (* s'applique uniquement au Module DLP pour la messagerie électronique).



UNE SOLUTION QUI SE DÉPLOIE ET QUI SÉCURISE RAPIDEMENT MES DONNÉES CRITIQUES, EN LES EMPÊCHANT DE QUITTER MON RÉSEAU VIA LE WEB OU LA MESSAGERIE ÉLECTRONIQUE

Avec une bibliothèque complète de modèles et de politiques prêts à l'emploi, Forcepoint vous permet de sécuriser rapidement vos données sensibles.

TENEZ-VOUS-EN AU PERSONNEL EXISTANT

L'architecture TRITON de Forcepoint est une architecture totalement intégrée qui regroupe des capacités de création de rapports, de gestion des données et de gestion des politiques dans une seule et même interface utilisateur pour vos solutions dédiées au Web, à la messagerie, aux données, au Cloud et aux appareils mobiles.

IDENTIFIEZ ET ÉDUQUEZ LES UTILISATEURS À RISQUE

Les analyses comportementales identifient et signalent les personnes pouvant présenter un risque envers l'entreprise, sur la base de mauvaises habitudes ou d'un certain mécontentement.

JE NE SAIS PAS QUELLES DONNÉES QUITTENT MA SOCIÉTÉ NI COMMENT

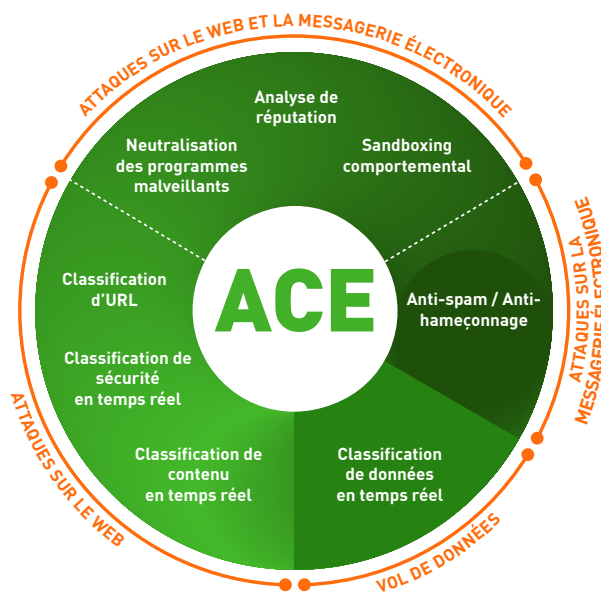
Bénéficiez d'une visibilité sur les données sensibles qui entrent et sortent via le Web et les courriels grâce à la DLP de Forcepoint pour le Web et la messagerie.

UNE VISIBILITÉ SUR LES DONNÉES SENSIBLES CONTENUES DANS LES IMAGES D'ANCIENS FICHIERS NUMÉRISÉS

La technologie de reconnaissance optique des caractères (ROC) de Forcepoint permet de visualiser le texte contenu dans les images et de faire appliquer les politiques pour empêcher les données sensibles identifiées dans les images numérisées de quitter votre réseau.

JE DOIS M'ASSURER QUE LES DONNÉES RÉGLEMENTÉES NE S'ÉCHAPPENT PAS DE MON RÉSEAU EN PETITES QUANTITÉS

Mettez un terme à la fuite de données lente et à faibles volumes grâce à la méthode « Drip DLP » de Forcepoint. En s'intéressant aux événements cumulés au fil du temps, cette technologie détecte le vol « goutte à goutte » d'une archive ou d'un numéro de carte de crédit à la fois.



LA DIFFÉRENCE DE FORCEPOINT:

Le Moteur ACE (Advanced Classification Engine)

Le moteur ACE de Forcepoint fournit une protection contextuelle en ligne et en temps réel pour le Web, la messagerie électronique, les données et la sécurité mobile et s'appuie sur une analyse prédictive et un calcul composite des risques pour offrir la sécurité la plus efficace du marché. Il sécurise les contenus en analysant les communications entrantes et sortantes à partir de la meilleure protection du marché basée sur les données pour éviter le vol de ces dernières. Des classificateurs conçus pour l'analyse de la sécurité, des données et du contenu en temps réel — le résultat d'années de recherche et de développement — permettent au moteur ACE de détecter chaque jour davantage de menaces que les moteurs antivirus traditionnels (la preuve est mise à jour quotidiennement sur le site <http://securitylabs.forcepoint.com>). Le moteur ACE est la principale défense intégrée dans les solutions TRITON® de Forcepoint, et est pris en charge par le réseau Forcepoint ThreatSeeker Intelligence Cloud

CONTACT

www.forcepoint.com/contact

SUR FORCEPOINT

Forcepoint™ est une marque de commerce de Forcepoint, LLC. SureView®, ThreatSeeker® et TRITON® sont des marques déposées de Forcepoint, LLC. Raytheon est une marque déposée de Raytheon Company. Toutes les autres marques ou marques déposées appartiennent à leurs propriétaires respectifs.

[DATASHEET_MODULE_DLP_FR]-100007FR.011416

FORCEPOINT
TRITON® APX

www.forcepoint.com