HEXATRUST

CYBERSECURITY & DIGITAL TRUST

PREVENTION DE LA FUITE DE DONNEES

La fuite de données, un risque à plusieurs millions de dollars contre lequel l'analyse comportementale est la solution optimale

Une intrusion coûte en moyenne 3,8 millions de dollars (*source : Ponemon, 2015*), mais les attaques sur Sony ou Target montrent que ce montant peut être encore bien plus élevé. La fuite de données constitue donc la plus importante menace actuelle. Elle menace l'ensemble du système d'information, mais aussi les activités métier de l'entreprise. Elle dépend aussi fortement de l'impact des actions humaines. L'information étant la matière première de l'entreprise, l'intégrité des données concerne l'ensemble du système d'information et de ses utilisateurs. Elle est donc de plus en plus assujettie à des obligations réglementaires.

VISION PAC

A CXP GROUP COMPANY

Sur le front de la Cyber Sécurité, les dénis de services et les atteintes à l'image-ont laissé place aux cyber criminels et cyber espions : le **vol d'informations importantes**. La fuite de données particulièrement attrayante dans une économie basée sur l'innovation et de plus en plus digitale.

Les architectures *« Big data »*, qui centralisent les données, et les solutions *« Cloud »*, qui les externalisent, rendent la sécurisation des données sensibles de plus en plus difficile.

La **fuite de données** est ainsi en passe de devenir le principal sujet de préoccupation des entreprises.

- Selon une enquête de PAC en France réalisée en 2015, le vol de données est le **premier risque** auquel font face les entreprises et un de ses avatars, l'espionnage, est le troisième.
- C'est un marché comprenant de nombreux acronymes comme Data Loss Prevention (DLP) et Mobile Data Protection (MDP). PAC évalue ce marché à 43 M€ en France, avec une croissance annuelle proche de 10%.

La fuite de données est en lien direct avec les activités et les actifs de l'entreprise ainsi que ceux de ses partenaires et de ses clients.

La fuite de données ne met pas seulement en danger l'activité de l'entreprise ou de l'organisation concernée. Elle touche également tout son écosystème et l'expose à une mise en cause de sa **responsabilité**.

Les **réglementations**, tant sectorielles que nationales ou internationales, sont la principale raison d'investissement dans ce type de protection, selon une enquête PAC en 2015.

Les vulnérabilités induites par la fuite de données sont **diverses** car les données étant la matière première de l'informatique, la protection contre leur fuite concerne un très grand nombre de systèmes dans l'entreprise. C'est aussi un concept qui reste proche d'autres segments clés de la Cyber Sécurité, comme l'authentification ou le cryptage.

Les principales menaces sont les **négligences,** les **malversations internes**, les **fraudes** et les **attaques** qui organisent la fuite de données à partir des systèmes internes.

La fuite de données est donc une préoccupation essentielle pour les entreprises et les administrations. Cependant, du fait de sa diversité, de l'aspect pervasif des informations et de l'étendue des actions humaines à prendre en compte, les solutions sont le plus souvent complexes, rigides, lourdes à mettre en place et insuffisamment précises.

RÉPONSE D'HEXATRUST

HEXATRUST
CYBERSECURITY & DIGITAL TRUST

Pour résoudre cette problématique complexe, les membres d'**HEXATRUST** proposent une approche reposant sur le tryptique **« Prévention - Détection - Correction »** qui doit être appliquée à plusieurs niveaux : applications manipulées, terminaux, flux entrants, flux sortants, gestion des accès et des usages.

Les solutions proposées par les membres d'**HEXATRUST** permettent ainsi de résoudre les problèmes clés liés aux fuites de données :

- Vol et perte de terminal
- Compromission de poste (APT, etc.)
- Usurpation d'identité
  - Utilisateurs à privilèges
  - Récupération de mot de passe
- Gouvernance des données et des accès
  - Légitimité des accès/identités
  - Classification des données (sensibilité)
- Comportement anormal d'un utilisateur et ou d'une application (volontaire ou involontaire)
  - Récupération
  - Fraude
- Erreur humaine (ex : partage excessif dans les applications cloud)

Les solutions des membres d'**HEXATRUST** intègrent aussi des fonctions essentielles de découverte des actifs à surveiller ainsi qu'une offre complète de chiffrement.

POSITIONNEMENT ET AVANTAGE D'HEXATRUST

La fuite de données est généralement couverte par les offres regroupées sous la bannière **DLP** ou **« Data Loss Prevention »**. Cette DLP « classique » fonctionne mal, car elle doit gérer un aspect humain, comportemental, qui est crucial pour se protéger.

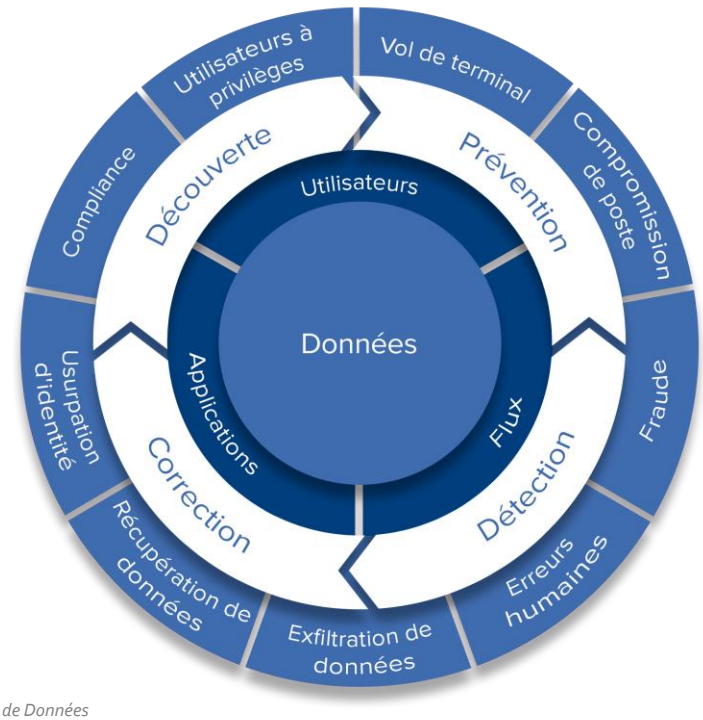
Les solutions actuelles sont, en outre, basées sur des systèmes de règles appliquées aux données, qui présentent **plusieurs inconvénients** comme la complexité de mise en œuvre, le nombre élevé de fausses alertes ou, à l'inverse, de *« faux positifs »*, sans compter la baisse de productivité, ou même le mécontentement des utilisateurs. Enfin, ces solutions s'adaptent mal aux changements fréquents que requièrent les activités des entreprises, en particulier dans le digital.

Pour se protéger de la perte de données, un domaine où le comportement humain est crucial, l'**analyse comportementale**, une des principales forces des solutions proposées par les membres d'**HEXATRUST**, est le concept le plus adapté et le plus efficace. Cette analyse cible les **comportements déviants** des utilisateurs, des terminaux et des applications qui manipulent les données. Les solutions d'analyse comportementale des membres d'**HEXATRUST** sont, par ailleurs, dotées de nombreuses **fonctionnalités innovantes** pour la gestion de la fuite des données :

- **Classification** et **déduction** automatique de la sensibilité des données
- **Analyse** des canaux et des applications qui les utilisent sur le terminal
- **Evaluation** du comportement des applications mobiles
- **Contrôle des flux** sortants et de leur conformité aux règles et réglementations (détection de fraude applicative, ségrégation des tâches)
- **Cartographie** et **analyse** du comportement des accès et des usages
- Analyse du **comportement des utilisateurs**

En étant plus proche de l'humain, les solutions des membres d'**HEXATRUST** se distinguent par leur approche novatrice. Elles sont capables de réaliser ce que les DLP *«classiques»* ne peuvent pas faire : gérer **l'impact des comportements humains** dans la fuite des données.
L'analyse comportementale constitue donc la **réponse du futur** à la fuite de données. Plutôt que d'infantiliser l'utilisateur avec des règles strictes et étendues, elle le **responsabilise** par le biais de règles essentielles.

PRÉVENTION DE LA FUITE DE DONNÉES



L'Association HEXATRUST : HEXATRUST est née de la volonté commune de PME et ETI françaises, acteurs complémentaires experts de la sécurité des systèmes d'information, de la cyber sécurité et de la confiance numérique.

10 bis avenue Ampère
78180 Montigny-le-Bretonneux – France
Tél : +33 1 39 30 62 50
www.bertin-it.com
luc.renouil@bertin.fr

Basées sur son hyperviseur certifié EAL 5+, les solutions de Bertin IT empêchent les fuites d'information, intentionnelles ou accidentelles, grâce au cloisonnement fort : entre réseaux interconnectés (passerelle de confiance, CrossinG®), entre données de différents niveaux accessibles au sein d'une même machine (poste multi-domaine, OneStation®), et entre périphérique USB et système hôte (station de neutralisation des menaces USB, WhiteN®).

38-42 rue Galliéni
92600 Asnières-sur-Seine – France
Tél : +33 1 84 19 04 10
www.brainwave.fr
jean-yves.pronier@brainwave.fr

Brainwave est un éditeur de logiciel focalisé sur l'Identity Analytics and intelligence. Notre mission est d'aider les entreprises à lutter contre la fraude, la fuite de données et les cyber risques, avec des solutions GRC analytiques novatrices. Brainwave renforce la sécurité informatique et la conformité par une analyse préventive des risques auxquels l'entreprise est exposée, que les applications et les données soient en interne ou dans le cloud.

6 avenue de la Cristallerie
92310 Sèvres – France
Tél : +33 1 46 20 96 00
www.denyall.fr
sdesaintalbin@denyall.com

DenyAll est un expert en sécurité applicative. DenyAll Web Application Firewall prévient la fuit de données en protégeant les applications web contre les attaques courantes, tels qu'injections SQL et cross-site scripting, qui permettent aux attaquants de capturer de gros volumes de données. DenyAll Web Services Firewall fait le même travail pour le trafic XML les applications orientées services (SOA). DenyAll Vulnerability Manager permet d'identifier et réduire les vulnérabilités que les hackers tentent d'exploiter pour attaquer votre infrastructure IT.

55 l'Occitane
31670 Labège – France
Tél : +33 5 67 34 67 80
www.itrust.fr
mgodefroy@itrust.fr

La solution Reveelium de ITrust permet la détection : de l'extraction anormale de données au sein du SI d'une entreprise ainsi que la détection du vol de données. Les logs analysés issus des proxys, des mails et des domaines permettent d'identifier un comportement anormal visant à voler ou extraire de l'information stratégique. Il est ainsi facile de bloquer l'extraction ou le vol en amont de la malveillance.

4 rue de Ventadour
75001 Paris – France
Tél : +33 9 69 39 09 99
www.olfeo.com
asouille@olfeo.com

Olfeo est la première solution de proxy et de filtrage de contenus multi-local. Olfeo offre un haut niveau de gestion des accès et de gestion des usages utilisateurs grâce une multitude de méthodes d'authentification afin d'identifier les comportements à risques. La haute technicité de la solution Olfeo permet de prévenir en amont toutes fuites de données grâce à son filtrage applicatif, à la gestion des droits Web 2.0 et la détection des attaques localisées.

Les Portes d'Antigone – Bât. B
71 place Vauban
34000 Montpellier – France
Tél : +33 4 67 20 99 11
www.pradeo.net
renaud.gruchet@pradeo.net

Pradeo analyse le comportement des applications mobiles pour révéler leurs actions cachées. Les comportements non conformes aux règles de sécurité sont détectés automatiquement pour protéger les terminaux mobiles. Cette approche constitue une réponse innovante face à la menace de fuites de données sur les mobiles et les objets connectés, partout où « Apps et Store » se déploient à grande échelle.

3 avenue Antoine Pinay
Parc d'activité des 4 Vents
59510 Hem – France
Tél : +33 3 28 32 88 88
www.vade-retro.com
gregoire.lepoutre@vade-retro.com

Vade Retro protège 235 millions de mailbox dans 76 pays sur les marchés des FAI/Hébergeurs, OEM, et Entreprises. Les USP de Vade Retro sont Advanced Antiphishing Program permettant d'explorer les liens au moment du click de l'utilisateur, la lutte contre les malware polymorphe au niveau du content filtering, ainsi que la gestion des mails non-prioritaires (classement + désinscription mails publicitaires). Vade Retro est numéro 1 en France en nombre de mailbox protégées (60M).

118 rue de Tocqueville
75017 Paris – France
Tél : +33 1 53 42 12 90
www.wallix.com
sales@wallix.com

Wallix AdminBastion Suite permet de limiter drastiquement les risques de fuite de données via la possibilité de définir - pour tout accès à un serveur ou un applicatif contenant des données sensibles – si l'utilisateur a le droit ou non d'effectuer des transferts de fichiers en « upload » et/ou en « download ».