LA RECONNAISSANCE DE L'INDUSTRIE

Neuf fois leader* dans le Gartner Magic Quadrant portant sur « Enterprise Data Loss Prevention ».
* Gartner MQ pour la prévention des pertes de données d'entreprise, 16 février 2017. Anciennement Websense dans le Gartner MQ pour la prévention des pertes de données comme dans le Gartner MQ des rapports de surveillance de contenu, de filtrage et de prévention de pertes de données. Gartner ne recommande aucunement les fournisseurs, produits ou services décrits dans ses publications de recherche et ne conseille pas aux utilisateurs de technologie de choisir uniquement les fournisseurs les mieux classés. Les études de Gartner reflètent les opinions de l'organisation de recherche Gartner et ne doivent pas être interprétées comme des exposés de faits. Gartner exclut toute garantie, expresse ou implicite, concernant cette recherche, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.

FORCEPOINT

L'AVANTAGE FORCEPOINT

À PROPOS DE FORCEPOINT

Forcepoint transforme la cybersécurité en se concentrant sur ce qui est le plus important : comprendre les intentions des individus qui interagissent avec les données critiques et les propriétés intellectuelles, où qu'elles se trouvent. Grâce à nos systèmes sans concession, les entreprises peuvent accorder à leurs employés un accès sans restriction aux données confidentielles, tout en assurant la protection de la propriété intellectuelle et la simplification de la conformité. Basé à Austin, au Texas, Forcepoint apporte ses services à plus de 20 000 organisations à travers le monde.Pour plus d'informations sur Forcepoint, consultez le site www.forcepoint.com et suivez-nous sur Twitter : @ForcepointSec

CONTACT

Pour plus d'informations, visitez www.forcepoint.com.

[BROCHURE_CORPORATE_OVERVIEW_FR] 400019FR.052418

LES DÉFIS ACTUELS EN CYBERSÉCURITÉ

Dans une ère de transformation numérique, les entreprises les plus performantes du monde choisissent de monétiser leurs données et propriétés intellectuelles. La protection de ces données et propriétés intellectuelles des vols ou de la corruption est critique, les pertes pouvant dévaster les profits et les réputations durement gagnés par les marques. Les RSSI et les autres cadres dirigeants chargés de la sécurité comprennent ces enjeux, mais leur travail est plus difficile que jamais, à une époque où les nouveaux modèles opérationnels de l'IT adoptent les clouds publics, le BYOD et la mobilité.

IDC prévoit que 60 % de l'IT des entreprises sera hors site et dans le cloud d'ici 2018[1].

Les données sont maintenant partout, et peuvent être exploitées depuis n'importe où. En conséquence, les surfaces d'attaque ont grandi de façon exponentielle, tout comme le nombre des nouvelles menaces en évolution constante. Quel que soit le type d'attaque, les failles d'aujourd'hui ont pour source l'utilisateur final, de simples erreurs de manipulation jusqu'aux actions malveillantes.

Les enjeux ont clairement changé, et l'approche doit faire de même. Forcepoint se pose en pionnier de la sécurité orientée sur le facteur humain, un nouveau paradigme qui se centre sur le lieu, le moment et la façon dont les personnes interagissent avec les données. En détectant les tendances normales et anormales des utilisateurs avec les données, nous pouvons identifier et anticiper les risques, réduire la complexité et nous concentrer sur les événements qui sont vraiment importants.

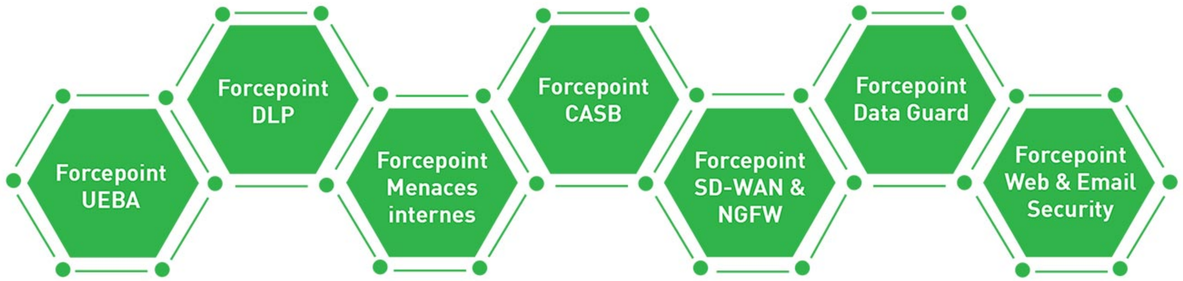
"Les leaders en sécurité et gestion des risques doivent adopter une approche stratégique permanente et dynamique d'estimation des risques et de la confiance (continuous adaptive risk and trust assessment, CARTA). Cela est vital pour autoriser en toute sécurité les initiatives commerciales numériques dans un monde d'attaques avancées et ciblées. Cela activera la prise de décisions en temps réel, basées sur le risque et la confiance, pour des interventions adaptées à la situation.[2]"
— Gartner Research, Top 10 Tendances stratégiques en technologie pour 2018

1 https://www.idc.com/getdoc.jsp?containerId=US41883016
2 Gartner, Top 10 Tendances stratégiques en technologie pour 2018, par David W Cearley et autres auteurs, 3 octobre 2017.

LE SYSTÈME «HUMAN POINT» DE FORCEPOINT

Le système centré sur l' humain de Forcepoint réunit un vaste ensemble de capacités qui corrige et comprend le rythme des personnes et le flux de vos données. Le système a été conçu pour que chaque élément soit le meilleur de sa catégorie et puisse fonctionner seul ou s'intégrer dans votre environnement existant. Pour consolider plus encore votre infrastructure, commencez par n'importe quel produit et intégrez les autres quand vous êtes prêt. Notre politique unifiée, nos analyses et nos coordinations communes allègent la gestion.

Le système Human Point comprend :



Forcepoint UEBA
Analyse comportementale des utilisateurs et entités pour un monde à zéro périmètre. Le leader en connaissances exploitables basées sur un score s'adaptant au risque.

Forcepoint DLP
Découverte et protection pour respecter la conformité des réglementations et de l'industrie.

Forcepoint Menaces internes
Visibilité des utilisateurs et contexte de l'incident pour les données sensibles. La compréhension la plus complète des intentions de l'utilisateur, sur plus d'un million de terminaux.

Forcepoint CASB
Visibilité et contrôle sur tout votre environnement cloud. La prise en charge la plus large des applications cloud avec une estimation unique et personnalisée des risques, basée sur le comportement de l'utilisateur et la classification de l'accès aux données.

Forcepoint SD-WAN & Firewall nouvelle génération NGFW
Sécurité réseau hautement sécurisée, efficace et disponible. NGFW réduit les dépenses réseau de 50 %, diminue de 86 % les cyberattaques et réduit le temps d'intervention des incidents jusqu'à 73 %.

Forcepoint Data Guard
Collaboration et partage d'informations sécurisés pour les agences gouvernementales. Élimine les longs et coûteux transferts manuels des données hautement réglementées et sensibles.

Sécurité du Web et de la messagerie électronique Forcepoint
Protection unifiée contre les menaces avancées n'importe où, sur n'importe quel appareil. Détection 100 % de menaces sans faux positifs.

LE FACTEUR HUMAIN

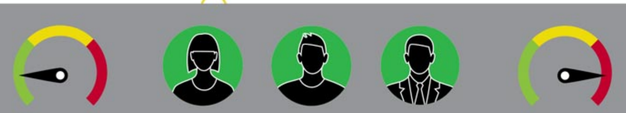
QUI EST FORCEPOINT ?

Forcepoint a été fondé avec l'objectif de fournir des solutions de cybersécurité de nouvelle génération :

- C'est l'une des plus grandes entreprises privées de cybersécurité dans le monde, avec des milliers d'entreprises et d'entités gouvernementales comme clients, dans plus de 150 pays.
- C'est un acteur majeur de la communauté du Renseignement et de cyber missions à forte confiance.
- L'un des portfolios de produits de sécurité les plus complets de l'industrie.

En vous éloignant d'une approche cybersécuritaire basée sur les menaces, vous pouvez concentrer votre attention sur les deux seules constantes en matière de sécurité –– les personnes et les données.

Protéger du facteur humain signifie sécuriser l'intersection où se croisent les personnes, les données critiques et les propriétés intellectuelles, et cela commence par la compréhension du rythme des personnes et le flux de vos données. Cela permet de savoir à quoi ressemble l'activité d'un employé normal et productif, et de voir toutes les interactions uniques des personnes avec les données. Parallèlement, cela vous permet de savoir où se trouvent et comment transitent vos données, dans votre entreprise et en dehors. En protégeant du facteur humain, vous gagnez une meilleure visibilité, une politique unique à travers des systèmes distribués, une application rapide et une meilleure conformité pour le monde actuel, sans périmètre.



Forcepoint Dynamic Data Protection est la première solution DLP nouvelle génération qui propose une sécurité qui s'adapte au risque. Elle réunit le produit DLP leader de son secteur avec un noyau d'analyse centré sur le comportement, pour protéger contre l'exfiltration de données. Dynamic Data Protection détermine une ligne "normale" de comportement utilisateur et applique une vaste gamme de contre-mesures de sécurité automatisées selon les fluctuations du score de risque de l'utilisateur, le tout sans intervention de l'administrateur.

LES APPROCHES TRADITIONNELLES ATTEIGNENT UN POINT DE RUPTURE

L'approche traditionnelle en cybersécurité dépend de l'utilisation de produits standards qui n'interagissent pas entre eux. Des technologies disparates fonctionnent au cas par cas, mais le manque d'intégration entre elles a pour résultat la génération d'un nombre écrasant d'alertes. Les équipes de sécurité sont mises au défi de distinguer les menaces réelles parmi des milliers de fausses alertes. Le temps qu'ils les trouvent, des dégâts substantiels peuvent avoir lieu.

La surcharge d'alertes est le symptôme d'un problème plus important : la dépendance en une approche binaire, centrée sur les menaces, où les "bonnes" et "mauvaises" activités peuvent être traitées via des politiques statiques. Mais l'intention motivant la vaste majorité des événements survenant entre les deux extrémités de ce spectre reste inconnue. Comme elles n'ont pas la compréhension du contexte de l'activité, les équipes de sécurité doivent examiner manuellement chacune d'elles. Choisir une approche centrée sur les menaces conduit à un scénario sans victoire possible.

Qui plus est, les équipes de cybersécurité semblent destinées à échouer. On estime que plus de 80 % des incidents de sécurité exploitent des vulnérabilités bien connues.[5]La façon dont nous travaillons aujourd'hui ne fonctionnera pas dans le futur, tout simplement.

3 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4 Ponemon Institute, Étude des coûts des failles de sécurité 2017
5 SANS Institute, Cyber Security Trends: Viser au-delà de la cible pour augmenter la sécurité en 2017

POURQUOI UNE CYBERSÉCURITÉ CENTRÉE SUR L'HUMAIN ?

Plus de quatre-vingts pour cent des incidents de sécurité dus au hacking tirent parti d'identifiants compromis. De simples services d'identification et d'authentification d'utilisateur et d'appareil ne peuvent pas surveiller le comportement et n'imposent aucune limite aux données une fois l'accès accordé. Avec les méthodes traditionnelles de cybersécurité, il est également impossible de se défendre contre des hackers quand ils ont compromis des bons utilisateurs en "possédant" illicitement leurs systèmes.

En outre, les employés peuvent faire des erreurs, causant sans le vouloir des fuites de données. Parfois il arrive que des employés mécontents n'aient pas de bonnes intentions.

Plutôt que d'essayer de sécuriser totalement des réseaux possédés et gérés par des tiers, ce qui bloque divers points d'accès et génère un nombre écrasant d'événements de sécurité, il est primordial de comprendre le cybercomportement de tous les utilisateurs – les employés, les clients et les partenaires – alors qu'ils interagissent avec les données et les systèmes, pour évaluer proactivement les risques posés par leur activité.

UNE SÉCURITÉ ADAPTÉE AU RISQUE

La traditionnelle approche de la sécurité centrée sur les événements n'a plus aucun sens dans le complexe cyberpaysage actuel. La sécurité la plus efficace est celle qui s'adapte au risque, donnant le contexte nécessaire pour appliquer dynamiquement les politiques pertinentes, jusqu'au niveau individuel. Et c'est seulement via le contexte que l'on peut comprendre si le comportement d'un utilisateur ou d'une entité est normal, suspicieux ou malveillant.

S'adaptant au risque, l'approche de Forcepoint détecte, analyse et applique des règles : elle protège vos utilisateurs, données et réseaux en temps réel, et augmente l'efficacité de vos investissements en sécurité.

À la différence d'autres systèmes, notre solution ne submerge pas votre SIEM d'alertes nécessitant une intervention manuelle.
Cela permet de savoir à quoi ressemble l'activité d'un employé normal et productif, et de voir toutes les interactions uniques s entre les personnes et les données, appliquant automatiquement les politiques adaptées à leur profil de risque.

Parallèlement, cela vous permet de savoir où se trouvent et comment transitent vos données, dans votre entreprise et en dehors. Notre modèle s'adaptant aux risques fournit une plus grande visibilité, une politique unique à travers des systèmes distribués, une application rapide et une meilleure conformité.