Le Guide complet de la protection des données

Forcepoint

Brochure

Vue d'ensemble

D'une certaine manière, la relation entre la sécurité des données et la performance en entreprise est une histoire aussi vieille que le monde des affaires. Après tout, la forme la plus simple d'avantage concurrentiel est la capacité d'une entreprise à pouvoir garder son « secret dans la sauce » - qu'il s'agisse d'un procédé breveté, d'une propriété intellectuelle essentielle ou même une véritable recette de cuisine.

Mais aujourd'hui, ce problème est infiniment plus complexe. On estime que 90 % des données mondiales ont été créées en seulement deux ans.[1] Cet effet a été amplifié : prolifération des appareils mobiles, clients et contractants éloignés, employés à domicile ou itinérants, et bien d'autres facteurs. Cela signifie que les données sont stockées et consultées dans plus d'emplacements, par plus de personnes – à tout moment.

Dans la foulée de cette évolution du rôle des données sur le lieu de travail, des incidents de vols de données très médiatisés ont contribué à faire de la sécurité des données un nouvel atout commercial majeur. L'impact financier est un facteur important : le coût moyen d'un vol de données est de 3,26 millions de dollars.[2] Néanmoins, les incidents liés à la sécurité des données peuvent aussi nuire gravement à l'image d'une entreprise et éroder la confiance que lui donnent ses clients.

Les secteurs fortement réglementés tels que les services de santé et les services financiers sont depuis longtemps soumis à un mandat légal de sécurisation des données sensibles. Récemment, cependant, l'attention accrue du public et la sensibilisation à la sécurité des données ont contribué à stimuler une nouvelle législation ciblant la manière dont les entreprises peuvent collecter, traiter et stocker des données. La loi malaisienne sur la protection des données personnelles, le règlement général sur la protection des données européen (RGPD), les principes australiens de protection de la vie privée, la loi californienne sur la protection des consommateurs – la liste est longue. Et c'est suffisant pour que toute organisation, qu'elle soit soumise à la réglementation en vigueur ou non, réfléchisse de manière critique à la protection des données.

3,26 millions de dollars

Coût moyen d'un incident de compromission des données[2]

2 600-10 000

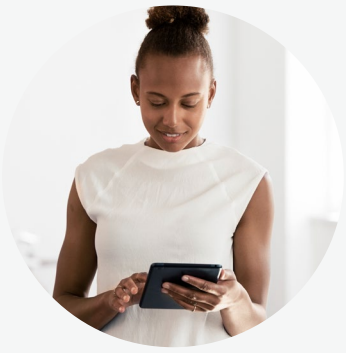
Nombre de documents sensibles perdus lors d'une violation moyenne[2]

68%

Pourcentage de vols de données qui restent non découverts pendant des mois

Au milieu de tout cela, une chose est devenue claire : Permettre aux entreprises et aux employés les moyens d'être performants dans l'environnement commercial actuel exige un changement dans notre façon d'envisager la sécurité des données. Dans l'état de changement constant qui est devenu notre nouvelle norme, les politiques réactives ne suffisent plus à assurer notre sécurité. Examinons comment faire pour adopter une position proactive en matière de protection des données, et pourquoi c'est le choix le plus sûr pour les entreprises aujourd'hui.

On estime que 90 % des données mondiales ont été créées en seulement deux ans.[1]



Relever le rôle de la sécurité des données

Pour de nombreuses équipes de sécurité des données, les journées consistent en des cycles de réception d'une alerte, d'enquête et de réparation des dommages. Et cela, en boucle. Problème : Des politiques rigides signalent souvent des activités à faible risque, ce qui donne lieu à des alertes de type “Faux positifs”. Enquêter sur ces problèmes représente un fardeau immense pour les équipes chargées de la sécurité des données, car elles ont déjà plus de tâches et de responsabilités à accomplir que de bande passante à leur disposition.

Une technologie de protection des données qui peut lire le contexte de la cyberactivité peut alléger ce fardeau pour les équipes de sécurité, en les aidant à concentrer leurs enquêtes sur les incidents vraiment menaçants et à filtrer ceux qui ne présentent pas un risque réel pour l'activité. En lui permettant d'employer plus judicieusement son temps, une équipe de sécurité peut faire évoluer son rôle au sein d'une entreprise, passant d'une simple application des règles à une conduite proactive de l'entreprise vers un avenir plus sûr et plus efficace.

Dynamiser votre croissance professionnelle

Des experts en sécurité des données qui ne sont pas submergés par des notifications peuvent avoir le temps d'encadrer et de former d'autres employés, contribuant ainsi à leur développement professionnel et à leur plan de carrière.

Dynamiser votre croissance commerciale

Des professionnels en sécurité capables de trouver des gains d'efficacité dans leur propre charge de travail peuvent aider à identifier les opportunités de croissance de l'entreprise, grâce à une utilisation optimisée des données. (Ou alerter sur les comportements à risques pour les données qui peuvent entraver la croissance commerciale).

Dynamiser votre transformation numérique

Harmoniser les enquêtes en les basant sur la compréhension du contexte de l'incident donne aux équipes le temps d'optimiser leurs politiques et procédures pour s'adapter à la culture des données dans le cloud – permettant une transformation numérique plus rapide tout en apportant un avantage concurrentiel à l'entreprise.

Protéger les données partout où l'on travaille

L'approche traditionnelle de prévention de la perte des données protège vos données sur trois points d'accès : sur votre réseau, sur les terminaux, et, de plus en plus fréquemment, dans le cloud. Et cela pourrait suffire, tant que les personnes qui accèdent à ces données restent à l'intérieur de ces périmètres. Mais ce n'est pas le cas, de plus en plus fréquemment, et dès qu'un périmètre est franchi, les politiques de protection des données se brisent. Cela signifie qu'il faut envisager différemment la solution. Examinons ce qui peut être fait pour trouver une solution.

Ce qu'implique la Transformation cloud

Migrer dans le cloud n'est pas de savoir "si" on va le faire. Mais plutôt "quand" cela va être fait. Les exigences du personnel travaillant à distance, des clients et des partenaires stratégiques éloignés ne font qu'accélérer le calendrier, poussant à une adoption plus rapide du cloud. Un exemple ? Aujourd'hui, 87 % des entreprises comptent sur leurs employés pour accéder aux applications professionnelles mobiles à partir de leur smartphone personnel[3], appelé "bring-your-own-device" ou « BYOD » ou PAP (Prenez votre Appareil Personnel). En outre, près d'un quart de personnel de la Génération Y déclare avoir téléchargé des fichiers d'entreprise sur ces appareils et avoir installé des applications tierces dans le cloud (bring-your-own-cloud ou BYOC) sans en avertir le service informatique ou la direction. Ces comportements créent ce que l'on appelle la Shadow IT, ou informatique fantôme. Cela démontre qu'une entreprise ne contrôle pas toujours quand et comment elle passe dans le cloud. Mais quel que soit le rythme, des politiques de sécurité bien ancrées ont du mal à suivre et à s'adapter aux nouvelles demandes.

L'une des raisons est que les fournisseurs d'applications cloud ont tendance à privilégier la portabilité, l'accessibilité et la facilité d'utilisation – mais pas nécessairement la sécurité de données qui sont rendues portables, accessibles, ou faciles à utiliser. Ils se concentrent sur un modèle de responsabilité partagée,dans lequel ils sécurisent l'infrastructure, mais laissent aux clients le soin d'assurer la sécurité des données partagées dans l'infrastructure. Cela signifie que, compte tenu de la nature transitoire et mobile du travail aujourd'hui, il vous incombe de mettre en place une protection des données qui s'applique partout où les personnes travaillent.

Le Nouveau Périmètre est Humain

Comment pouvez-vous assurer la sécurité de vos données quand les personnes les utilisent au-delà de votre ligne de défense ? Cela demande la prise en compte d'un nouveau périmètre : le périmètre Humain.

La protection des données centrée sur le facteur humain permet de conserver les données dans un environnement sécurisé, dans lequel tout le monde peut accéder, quel que soit le lieu de travail. De plus, le fait de lier la sécurité des données à l'identité d'une personne permet de mettre en place des politiques qui tiennent compte du niveau de risque personnel, en donnant un aperçu des intentions. Par exemple, un incident impliquant un employé de longue date en qui on a confiance peut être beaucoup moins préoccupant qu'un incident impliquant un prestataire suspect ou un ex-employé mécontent. Enfin, la surveillance de la sécurité des données au niveau humain permet de voir comment ces données sont utilisées sur différents dispositifs et applications, en fournissant un contexte qui peut aider les équipes de sécurité à mieux identifier les menaces et à en tirer des enseignements.

La Protection des données : Un nouvel Atout commercial

Protéger les données en tenant compte du facteur humain est adapté à la réalité dynamique du monde commercial d'aujourd'hui – Mais quelle est sa valeur dans votre monde ? Pour répondre à cette question, démystifions la légende urbaine qui frappe les équipes de sécurité des données partout dans le monde : la protection est l'ennemi de la productivité. Avec les bons outils et processus, chacun peut transmettre ses énergies à l'autre.

Des réponses précises

Les tactiques traditionnelles de prévention des pertes de données peuvent simplement bloquer les actions risquées - par exemple, l'enregistrement d'un fichier d'entreprise sensible sur une clé USB personnelle. Et, si une telle action a été entreprise par un ex-employé mécontent ou un contractant à court terme, ce genre de tactique est logique. Le plus souvent, cependant, ce n'est pas le cas ; il peut s'agir d'un cadre de l'entreprise qui essaie simplement de sauvegarder un fichier important ou de le déplacer vers un nouvel ordinateur. Mais les politiques traditionnelles de sécurité ne peuvent pas faire la différence, aussi bloquent-elles régulièrement des cyberactivités totalement inoffensives, entravant ainsi la productivité.

La détection des risques au niveau humain permet d'examiner le contexte et l'intention derrière une action, ce qui permet de réagir de façon spécifique, et non générale. Cela permet non seulement de réduire les interruptions dans le travail du personnel, mais aussi d'alléger la charge d'enquête des équipes de sécurité, en leur permettant d'aider le progrès plutôt que de le bloquer.

Réduction des vulnérabilités

Même des employés qui n'ont aucune mauvaise intention peuvent être frustrés par des couches de sécurité qui l'empêchent de faire son travail. Ainsi, sans avoir de mauvaises intentions, ils peuvent essayer de trouver une solution de rechange, en contournant légèrement les règles afin de pouvoir passer le barrage posé par la sécurité. Dans le dernier exemple, peut-être qu'ils fractionneraient le fichier en petites parties, puis les enverraient par courriel vers un ordinateur personnel, pour que le fichier puisse finalement être enregistré sur le disque.

Cela crée deux problèmes. Premièrement, cette séquence d'actions peut déclencher une alarme encore plus urgente qu'une tentative d'enregistrement d'un fichier sur un disque amovible, car elle indique qu'une personne tente de passer outre les mesures de sécurité. Elle devra probablement faire l'objet d'une inspection, ce qui demande du temps et des ressources. Mais ce qui est plus inquiétant, c'est que de telles solutions de contournement, aussi innocentes soient-elles, peuvent introduire de nouvelles vulnérabilités qui sapent les politiques de sécurité qui les ont motivées. Une protection des données centrée sur le facteur humain permettrait d'adopter des politiques plus souples et plus appropriées, en arrêtant cette spirale descendante avant qu'elle ne s'enclenche.

Posture proactive

Comme tout enseignant, propriétaire d'animal de compagnie ou professionnel de la sécurité des données peut en témoigner, il est beaucoup plus efficace de prévenir un mauvais départ que d'avoir à réparer après coup.

Grâce aux indices contextuels et aux connaissances comportementales que fournissent les données centrées sur l'être humain, il est possible de stopper les véritables menaces avant qu'elles n'infligent des dommages, tout en permettant à l'entreprise d'être performante au plus haut niveau. Le personnel peut vaquer à ses occupations sans trébucher sur des politiques de sécurité inflexibles. Les équipes chargées de la sécurité des données peuvent trier avec précision les alertes et se concentrer sur la résolution des incidents qui présentent un risque réel. Il s'agit de la sécurité des données, sans compromis.

Le nouveau standard de la protection des données

La nature évolutive des menaces pour la sécurité signifie que nous devons adapter notre mentalité pour assurer la sécurité des données - et cela implique d'accepter que le changement est, et sera toujours, constant.C'est pourquoi nos principes fondamentaux en matière de protection des données sont bâtis en gardant à l'esprit les besoins de demain :

1. Une culture de sécurité des données préventive, et non punitive

Le rôle des équipes de sécurité des données passera de l'application rétroactive des politiques de sécurité à la conduite de leurs entreprises de leurs collègues vers des comportements plus sûrs d'utilisation des données.

2. Estimation des risques basée sur le facteur humain

L'utilisation de données mobiles et dynamiques exige une sécurité qui prenne en compte la seule constante : l'utilisateur. Cela permet une sécurité souple qui s'adapte aux changements de comportement et du niveau de risque d'une personne.

3. Vue globale des données

Le maintien d'une visibilité totale des données l orsqu'elles se déplacent en dehors de votre réseau, entre les terminaux ou dans le cloud donne des indices contextuels sur les intentions, ce qui permet d'apporter des réponses adaptées en matière de sécurité.

4. Des politiques homogènes, quel que soit l'environnement

Établir votre périmètre de sécurité au niveau humain permet de s'assurer que les données sont protégées, où qu'elles soient stockées ou accédées.

Êtes-vous prêt à découvrir l'étape suivante de votre sécurité de données proactive ?

› **Consultez notre infographie** Les 9 étapes pour réussir la protection des données

1. IBM Marketing Cloud, "10 Key Marketing Trends for 2017"
2. Ponemon Institute, "U.S. Cost of a Data Breach Study," 2017
3. Syntonic, "BYOD Usage in the Enterprise," 2016

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données, dont l'objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Les solutions personnalisées de Forcepoint s'adaptent en temps réel à la façon dont les personnes interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables pour des milliers de clients dans le monde entier.