Cinq pièges courants à éviter en matière de sécurité des données

Apprenez à améliorer votre situation en matière de sécurité

IBM Security

Sommaire

Introduction

Cinq pièges courants en matière de sécurité des données

Conclusion

La sécurité des données devrait être une des grandes priorités des entreprises, et il y a une bonne raison à cela.

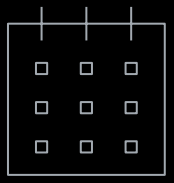
Bien que le paysage informatique soit de plus en plus décentralisé et complexe, il est important de comprendre que de nombreuses violations de sécurité peuvent être évitées. Si en matière de sécurité les problèmes et les objectifs peuvent différer d'une entreprise à une autre, les entreprises commettent souvent les mêmes erreurs courantes quand elles s'attaquent à la tâche de sécuriser leurs données. Qui plus est, de nombreux responsables d'entreprise considèrent souvent ces erreurs comme inévitables dans le cadre de pratiques normales.

Plusieurs facteurs internes et externes peuvent permettre à des cyberattaques d'aboutir :

- l'érosion des périmètres réseau
- le périmètre de vulnérabilité plus vaste qu'offrent les environnements informatiques plus complexes
- les risques croissants que les services cloud font peser sur les pratiques de sécurité existantes
- la sophistication croissante des cyberattaques
- le manque persistant de compétences en cybersécurité
- le manque de conscience de la part des employés des risques de sécurité qui pèsent sur les données

8,19 millions de $

coût moyen d'une atteinte à la protection des données aux États-Unis en 2019[1]



245 jours

temps moyen pour identifier une atteinte à la protection des données et contenir ses effets aux États-Unis[1]

Quelle est l'efficacité de vos pratiques de sécurisation des données ?

Étudions cinq des faux-pas en matière de sécurité des données les plus courants – et les plus évitables – qui rendent les entreprises vulnérables aux attaques potentielles, et la façon dont vous pouvez les éviter.

Accélérer la mise en conformité

Centraliser la sécurité

Établir la propriété

Évaluer les vulnérabilités

Prioriser les activités

Piège n° 1

Ne pas aller au-delà de la conformité

Conformité n'est pas forcément synonyme de sécurité. Les entreprises qui concentrent leurs ressources de sécurité afin de se conformer aux préconisations résultant d'un audit ou d'un examen de certification peuvent devenir complaisantes. De nombreuses atteintes à la protection des données ont concerné des entreprises qui respectaient pleinement la réglementation " du moins sur le papier. Les exemples suivants expliquent pourquoi se concentrer exclusivement sur la conformité peut réduire le niveau réel de sécurité :

Couverture incomplète
C'est souvent juste avant leur audit annuel que les entreprises s'occupent de corriger les problèmes liés à une mauvaise configuration de leurs bases de données et ceux découlant de politiques de contrôle d'accès périmées. Or l'évaluation des risques et des vulnérabilités doit être un processus continu.

Effort minimum
Beaucoup d'entreprises n'adoptent des solutions de sécurisation des données que pour répondre aux exigences légales ou à celles de leurs partenaires commerciaux. L'état d'esprit « prenons les mesures minimum et retournons à nos affaires » peut empêcher la mise en place de pratiques de sécurité adaptées. Sécuriser efficacement les données n'est pas un sprint mais un marathon.

Sentiment d'urgence décroissant
Les entreprises peuvent devenir complaisantes dans la gestion de leur contrôles lorsque les réglementations, telles que la loi Sarbanes-Oxley Act et le RGPD (règlement général sur la protection des données), sont en vigueur depuis un certain temps. Si, avec le temps, les responsables peuvent devenir moins attentifs à la confidentialité, la sécurité et la protection des données réglementées, les risques et les coûts associés à la non-conformité, quant à eux, restent les mêmes.

1,4

par jour

En dépit de la loi HIPAA (Health Insurance Portability and Accountability Act), on estime à 1,4 le nombre quotidien d'atteintes à la protection des données médicales en 2019[2].

Omission de données non réglementées
Certains actifs, tels que la propriété intellectuelle, peuvent faire courir des risques à votre entreprise s'ils sont perdus ou partagés avec des personnes non autorisées à y accéder. Se concentrer uniquement sur la conformité peut donc conduire les équipes chargées de la sécurité à négliger et sous-protéger des données précieuses.

Solution

Reconnaître et accepter que la conformité constitue un point de départ et non l’objectif à atteindre

Au lieu de se contenter de répondre aux exigences de conformité, les équipes chargées de la sécurité doivent élaborer des programmes stratégiques qui protègent de façon cohérente les données critiques de leur entreprise.

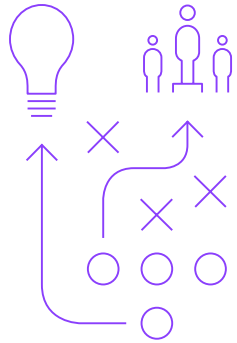
Les programmes de sécurisation et de protection des données doivent inclure les pratiques de base suivantes :

- **Découvrir et classer vos données** sensibles résidant sur site et dans vos magasins de données dans le cloud.
- **Évaluer les risques** grâce à des analyses et des informations contextuelles.
- **Protéger vos données** sensibles grâce au chiffrement et à des politiques d’accès flexibles.
- **Surveiller les schémas d’accès aux données** et d’utilisation de celles-ci afin de détecter rapidement les activités suspectes.
- **Réagir aux menaces** en temps réel.
- **Simplifier la conformité** et la production de rapports associée.

Ce dernier élément peut inclure les responsabilités juridiques associées à la conformité aux réglementations, les pertes qu’une entreprise peut subir, et le coût de ces pertes qui peut venir s’ajouter aux amendes pour non-conformité.

En fin de compte, vous devez réfléchir de façon holistique à la valeur des données que vous voulez sécuriser et aux risques qui pèsent sur elles.

Considérez la conformité comme une occasion d’innover et d’élever vos normes de sécurité pour soutenir votre entreprise.



Piège n° 2

Ne pas reconnaître la nécessité d'une sécurité des données centralisée

En l'absence d'obligations de conformité plus vastes couvrant la sécurité et la confidentialité des données, les chefs d'entreprise peuvent perdre de vue la nécessité d'une sécurité des données cohérente à l'échelle de l'entreprise.

Dans les entreprises utilisant des environnements multiclouds hybrides, lesquels évoluent et se développent constamment, de nouveaux types de sources de données peuvent faire leur apparition chaque semaine, voire chaque jour, et disperser fortement les données sensibles.

Les dirigeants des entreprises qui développent et étendent leurs infrastructures informatiques peuvent ne pas avoir conscience du risque que présente l'évolution de leur périmètre de vulnérabilité. Ils peuvent ne pas disposer de la visibilité et du contrôle appropriés lorsque leurs données sensibles se déplacent dans un environnement informatique de plus en plus complexe et hétérogène. Ne pas adopter des contrôles de bout en bout de la confidentialité, de la sécurité et de la protection des données – particulièrement dans les environnements complexes – peut se révéler une omission très coûteuse.

Utiliser des solutions de sécurité cloisonnées peut poser des problèmes supplémentaires. Par exemple, les entreprises qui possèdent un centre de contrôle des opérations de sécurité et une solution SIEM (security information and event management) peuvent négliger d'injecter dans ces systèmes les informations fournies par leur solution de sécurisation des données. De même, un manque d'interopérabilité entre le personnel, les processus et les outils de sécurité peut compromettre l'efficacité de n'importe quel programme de sécurité.

Le chiffrement, la gestion de la continuité des opérations, l'intégration de la sécurité dans le processus de développement de logiciels (DevSecOps) et le partage de renseignements sur les menaces peuvent contribuer à réduire le coût d'une atteinte à la protection des données[1].

Solution

Savoir où se trouvent vos données sensibles, aussi bien sur site que dans le cloud

La sécurisation des données sensibles doit aller de pair avec vos autres initiatives en matière de sécurité. En plus de comprendre où vos données sensibles sont stockées, vous devez savoir quand et comment elles font l'objet d'un accès – même si ces informations changent rapidement. En outre, vous devez vous efforcer d'intégrer vos informations et vos politiques de protection et de sécurisation des données dans votre programme de sécurité global, afin de permettre une communication étroitement alignée entre les technologies. Une solution de sécurisation des données fonctionnant dans des environnements et sur des plateformes hétérogènes peut faciliter ce processus.

Quand le moment est-il venu d'intégrer la sécurité des données et les autres contrôles de sécurité au sein d'une pratique de sécurité plus globale ? Voici quelques signes qui suggèrent que votre entreprise est peut-être prête à franchir cette nouvelles étape :

Risque de perte de données importantes
La valeur des données propres à votre entreprise et de ses données sensibles est si élevée que leur perte porterait un coup sévère à la viabilité de votre entreprise.

Implications réglementaires
Votre entreprise collecte et conserve des données réglementées, telles que des numéros de carte bancaire, d'autres informations de paiement ou des données personnelles.

La sécurisation des données sensibles doit aller de pair avec vos autres initiatives en matière de sécurité.

Manque de supervision de la sécurité
Votre entreprise s'est développée au point qu'il est devenu difficile de suivre et sécuriser tous les nœuds finaux de son réseau, y compris les instances cloud. Par exemple, savez-vous clairement où, quand et comment les données sont enregistrées, partagées et consultées dans vos magasins de données résidant sur site ou dans le cloud ?

Évaluation inadéquate
Votre entreprise a adopté une approche fragmentée qui l'empêche d'avoir une compréhension claire de ce qu'elle dépense exactement pour toutes ses activités liées à la sécurité. Par exemple, avez-vous mis en place des processus qui mesurent précisément le retour sur investissement des ressources affectées à la réduction des risques qui pèsent sur la sécurité de vos données ?

Si votre entreprise se trouve dans l'une de ces situations, vous devez envisager d'acquérir les compétences et les solutions qui vous permettront d'intégrer la sécurisation des données dans vos pratiques de sécurité globales.

Piège n° 3

Ne pas définir qui est responsable des données

Même quand elles sont conscientes de la nécessité de sécuriser leurs données, de nombreuses entreprises n'ont pas de responsable spécifiquement chargé de veiller à la protection des données sensibles. Souvent, ce problème devient apparent au cours d'un incident d'audit ou de sécurité, lorsque l'entreprise doit impérativement trouver le véritable responsable.

Les dirigeants peuvent alors s'adresser au directeur informatique, qui risque de leur répondre : « Notre travail est de veiller au bon fonctionnement des systèmes-clés. Adressez-vous à un membre de mon personnel informatique. » Ces employés du service informatique peuvent être responsables de plusieurs bases de données contenant des données sensibles mais ne pas disposer d'un budget consacré à la sécurité.

Généralement, les membres de l'équipe du directeur de la sécurité informatique ne sont pas directement responsables des données qui transitent dans l'entreprise. Ils peuvent conseiller les responsables des différents secteurs d'activité de l'entreprise, mais dans beaucoup d'entreprises personne n'est explicitement responsable des données proprement dit. Les données d'une entreprise sont l'un de ses actifs les plus précieux. Pourtant, si personne n'en est désigné comme propriétaire, il devient très difficile de sécuriser correctement les données sensibles.

74 %

des entreprises interrogées ont reconnu que le manque de compétences en cybersécurité a impacté leur fonctionnement[3].

« En 2018, 67,9 % des entreprises interrogées ont déclaré avoir un responsable des données. Toutefois, ce rôle reste mal défini. »[4]

Rapport de NewVantage intitulé « Big Data and AI Executive Survey 2019 », récapitulatif des conclusions destinés aux dirigeants

Lire l'étude →

Solution

Engager un responsable des données ou de la protection des données, qui veillera spécialement à la sécurité de vos données critiques et sensibles

Dans les environnements informatiques complexes, il est crucial de suivre les données :

partagées entre les unités commerciales

situées dans des infrastructures multiclouds hybrides

stockées sur des appareils mobiles

Un responsable des données ou de la protection des données peut se charger de cette tâche. D'ailleurs, le RGPD oblige les entreprises basées en Europe ou qui travaillent avec des citoyens de l'Union européenne à nommer un responsable de la protection des données. Cette obligation traduit le fait que les données sensibles – en l'occurrence les données personnelles – ont une valeur qui dépasse le cadre du secteur d'activité qui les utilise. En outre, elle impose aux entreprises de disposer d'un poste spécialement conçu pour être responsable des données. Pour choisir un responsable des données ou un responsable de la protection des données, tenez compte des objectifs et des responsabilités suivants :

Compétences techniques et sens des affaires
Évaluer les risques et rédiger une étude de rentabilité pratique des investissements de sécurité appropriés, compréhensible par les dirigeants non techniciens.

Mise en œuvre stratégique
Diriger au niveau technique un plan de mise en place de mesures de détection, de réponse et de contrôle de la sécurité des données afin de protéger ces dernières.

Leadership en matière de conformité
Comprendre les exigences de conformité et savoir comment y associer les contrôles de sécurité des données correspondants pour garder votre entreprise en conformité.

Surveillance et évaluation
Suivre l'évolution du contexte des menaces et mesurer l'efficacité de votre programme de sécurisation des données.

Flexibilité et mise à l'échelle
Savoir quand et comment ajuster la stratégie de sécurisation des données, par exemple en étendant aux nouveaux environnements les règles d'accès aux données et d'utilisation de celles-ci en adoptant des outils plus sophistiqués.

Répartition des tâches
Définir les attentes avec les fournisseurs de service de cloud en ce qui concerne les SLA et les responsabilités associées aux risques menaçant la sécurité des données et à la résolution des problèmes.

Plan de réponse à une atteinte à la protection des données
Être prêt à jouer un rôle-clé dans l'élaboration d'un plan stratégique de réponse aux violations et d'atténuation de leurs effets.

En fin de compte, le responsable des données ou de la protection des données doit jouer un rôle moteur pour favoriser la collaboration entre les équipes et dans toute l'entreprise dans le domaine de la sécurité des données, car tous les collaborateurs doivent travailler ensemble afin de sécuriser efficacement les données de l'entreprise. Cette collaboration peut aider le responsable des données ou de la protection des données à superviser les programmes et les protections dont votre entreprise a besoin pour mieux sécuriser ses données sensibles.

Piège n° 4

Ne pas éliminer les vulnérabilités connues

Dans les entreprises, les violations majeures sont souvent dues à des vulnérabilités connues qui n'ont pas été corrigées bien que des correctifs appropriés aient été publiés. Ne pas corriger rapidement les vulnérabilités connues met en danger les données de votre entreprise, car les cybercriminels recherchent activement ces points d'entrée faciles.

Toutefois, de nombreuses entreprises ont du mal à mettre en œuvre rapidement les correctifs car cette opération nécessite un haut degré de coordination entre les équipes chargées des outils informatiques, de la sécurité et de l'exploitation. En outre, les correctifs nécessitent souvent des tests pour s'assurer qu'ils ne perturbent pas le fonctionnement d'un processus ou n'introduisent pas une nouvelle vulnérabilité.

Et dans les environnements de cloud, il est parfois difficile de déterminer si un correctif doit être appliqué à un service fourni par un tiers ou à un composant d'application. Même si une vulnérabilité est détectée dans un service, les utilisateurs de ce service n'ont souvent aucun contrôle sur le processus de résolution en vigueur chez son fournisseur.

51 %

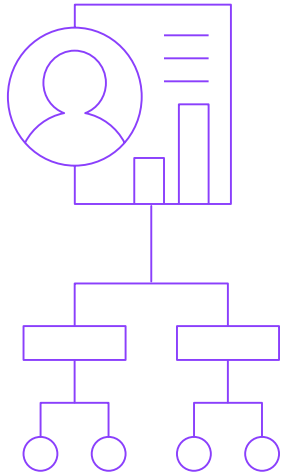
des violations enregistrées en 2019 sont dues à des attaques malveillantes. Ces attaques sont la cause de violations la plus fréquente et la plus coûteuse.

Solution

Établir un programme de gestion des vulnérabilités efficace et mettre en place la technologie adéquate pour soutenir son évolution

La gestion des vulnérabilités comprend généralement certaines des tâches suivantes :

- Tenir un inventaire précis de vos données et de leur état de référence.
- Procéder à une analyse et à une évaluation fréquentes des vulnérabilités dans toute votre infrastructure, y compris vos actifs hébergés dans le cloud.
- Prioriser la correction des vulnérabilités en fonction de la probabilité qu'elles soient exploitées et de l'impact que cette exploitation aurait sur votre entreprise.
- Inclure la gestion des vulnérabilités et la réactivité dans le SLA signé avec vos fournisseurs de services tiers.
- Brouiller les données sensibles ou personnelles chaque fois que possible. Le chiffrement, la « tokenization » et l'occultation sont trois moyens d'y parvenir.
- Gérer correctement les clés de chiffrement, en veillant à ce qu'elles soient stockées de façon sécurisée et renouvelées de manière adéquate afin de garder vos données chiffrées en sécurité.



Même en utilisant un programme de gestion des vulnérabilités mature, il est impossible de créer un système parfait. Par conséquent, puisque même les environnements les mieux protégés peuvent subir des intrusions, vos données ont besoin d'un niveau de protection supplémentaire. La bonne combinaison de compétences et de techniques de chiffrement des données peut vous aider à protéger vos données contre les menaces nouvelles ou émergentes.

Piège n° 5

Ne pas prioriser et exploiter la surveillance des activités liées aux données

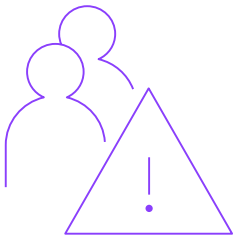
Surveiller l'accès aux données et leur utilisation est un aspect essentiel de toute stratégie de sécurisation des données. Tout dirigeant doit savoir qui accède aux données de l'entreprise, ainsi que quand et comment ces personnes y accèdent. Cette surveillance doit permettre de déterminer si ces personnes ont le droit d'accéder aux données, si leur niveau d'accès est correct et s'il induit une augmentation du risque pour l'entreprise.

Les ID utilisateur privilégiés sont des sources fréquentes de menaces internes. Un plan de protection des données doit inclure une surveillance en temps réel afin de détecter les comptes d'utilisateur privilégié utilisés pour des activités suspectes ou interdites. Afin d'empêcher toute activité malveillante, une solution doit pouvoir effectuer les opérations suivantes :

- Bloquer et mettre en quarantaine tout activité suspecte violant les règles définies.
- Interrompre ou fermer les sessions des utilisateurs ayant un comportement anormal.
- Utiliser des flux de travail prédéfinis adaptés à la réglementation dans les différents environnements de données.
- Envoyer des alertes exploitables aux systèmes de sécurité et d'exploitation informatiques.

Le coût moyen d'une menace interne est de

11,45 millions de $[6].



Tenir compte de la sécurité des données et des informations concernant la conformité et savoir quand et comment réagir aux menaces potentielles peut être difficile. Comme les utilisateurs autorisés accèdent à plusieurs sources de données telles que des bases de données, des systèmes de fichiers, des environnements de grand système et des environnements de cloud –, surveiller toutes ces interactions et enregistrer les informations correspondantes peut sembler une tâche insurmontable. Le défi consiste à surveiller, capturer, filtrer et traiter un volume énorme d'activités liées aux données – et à y répondre – de manière efficace. Si elle ne dispose pas d'un plan correct, votre entreprise peut être confrontée à davantage d'informations sur ces activités qu'elle ne peut raisonnablement en traiter, ce qui réduira l'intérêt de cette surveillance.

Solution

Élaborer une stratégie complète de détection et de protection des données

Pour ce faire, lorsque vous vous engagez dans un processus de sécurisation des données, vous devez dimensionner et délimiter vos efforts de surveillance afin de répondre correctement aux exigences et aux risques. Cela nécessite souvent d'adopter une approche par étapes qui permet de développer et mettre à l'échelle des bonnes pratiques dans toute votre entreprise. En outre, il est indispensable de consulter les parties prenantes clés de l'entreprise et de son service informatique dès le début du processus afin de comprendre les objectifs métier à court et long terme.

Ces consultations doivent aussi permettre de déterminer la technologie qui sera nécessaire pour soutenir les initiatives-clés. Par exemple, si l'entreprise projette d'ouvrir des bureaux dans une autre ville en utilisant des référentiels de données situés pour partie sur site et pour partie dans le cloud, votre stratégie de sécurisation des données doit évaluer l'impact de ce plan sur la situation de l'entreprise en matière de sécurité des données et de conformité. Il se peut, par exemple, que les données de l'entreprise soient désormais soumises à de nouvelles exigences concernant la sécurité et la conformité, telles que le RGPD, la loi California Consumer Privacy Act (CCPA), la loi brésilienne Lei Geral de Proteção de Dados (LGPD), etc.

Vous devez aussi vous concentrer en priorité sur une ou deux sources, celles qui sont les plus susceptibles de contenir les données les plus sensibles. Veillez à ce que vos politiques de sécurité soient claires et détaillées pour ces sources avant d'étendre ces pratiques au reste de votre infrastructure.

En 2019, le coût total moyen d'une atteinte à la protection des données était

95 % plus élevé

dans les entreprises non équipées d'une solution d'automatisation de la sécurité[1].

5,16 millions de $ **sans solution d'automatisation**[1].

2,65 millions de $ **avec une solution d'automatisation complètement déployée.**

Vous devez rechercher une solution automatique de surveillance des activités liées aux données ou aux fichiers, offrant également un outil d'analyse riche pouvant être focalisé sur les risques-clés et les comportements inhabituels des utilisateurs privilégiés. Bien qu'il soit essentiel que cette solution vous alerte automatiquement quand elle détecte un comportement anormal, elle doit aussi vous permettre d'agir rapidement lorsqu'elle détecte des anomalies ou des écarts par rapport à vos règles d'accès aux données. Les mesures de protection doivent inclure le blocage ou le masquage dynamique des données.

Lorsque vous développez vos plans de surveillance des activités liées aux données et de protection, il est souvent utile de réfléchir aux questions suivantes :

- Quelles sont mes deux principales sources de données les plus sensibles ?
- Quelles sont les 10 à 15 autres sources de données que je dois prioriser ensuite, en fonction de leur volume de données sensibles ?
- Certains nœuds finaux ou ressources cloud contiennent-ils des données présentant un risque plus élevé ?
- Mes environnements sur site, hybride et cloud échangent-ils librement des données sensibles ?
- Quels sont les utilisateurs qui doivent être autorisés à accéder à cette source de données et selon quelles conditions ?
- Quels sont les utilisateurs ou comptes privilégiés à haut risque qui doivent être désactivés ou qui nécessitent une surveillance renforcée ?
- Ma solution de sécurisation des données offre-t-elle des fonctionnalités de surveillance de l'activité en temps réel et de protection automatique des données ?
- Est-ce que je dispose d'une surveillance en temps réel pour suivre les données contenues dans des fichiers résidant dans des magasins de données, tels que des bases de données SQL (Structured Query Language), des distributions Hadoop, des plateformes Not only SQL (NoSQL), etc. ?
- Ma solution de surveillance tient-elle compte des magasins de données qui chevauchent plusieurs environnements multiclouds hybrides et me permet-elle de produire des rapports personnalisés qui seront transmis aux bonnes personnes au bon moment ?
- Est-ce que je dispose des fonctionnalités d'analyse des risques et de surveillance filtrée requises pour pouvoir prioriser efficacement les risques, les vulnérabilités et les efforts de résolution des problèmes ?

Plus vous serez précis dans la définition de vos priorités de surveillance et de vos besoins en matière de protection, plus vous utiliserez efficacement les ressources de détection et de réponse de la solution.

Étapes suivantes

Comment éviter ces pièges courants en matière de sécurité des données ?, tout particulièrement alors que les environnements multiclouds hybrides gagnent en popularité auprès des entreprises. Il convient tout d'abord de reconnaître l'existence du problème et de préparer votre entreprise à adopter une approche proactive et holistique de la sécurisation de ses données, quel que soit l'endroit où elles se trouvent.

Si votre entreprise possède un environnement informatique hybride complexe, vous ne pouvez pas vous permettre une approche cloisonnée de la sécurisation de ses données. Il vous faut des stratégies de protection des données qui englobent toute votre infrastructure de données et qui prennent en charge tous vos types de données.

Voici les mesures que vous pouvez prendre immédiatement pour protéger les données importantes de votre entreprise :

- Élaborer une stratégie de sécurisation des données qui soutient les objectifs métier et technologiques à court et long terme de votre entreprise.
- Mettre en œuvre cette stratégie avec les personnes, les processus et les outils appropriés.
- Planifier vos ressources de manière à ce que votre programme de sécurisation des données et de conformité puisse être efficacement redimensionné à mesure que votre entreprise adopte les technologies modernes.

La plateforme de protection des données IBM Security Guardium est conçue pour aider les entreprises à adopter une approche plus intelligente et plus souple de la protection de leurs données cruciales, où qu'elles se trouvent. Découvrez pourquoi elle peut représenter une bonne solution pour votre entreprise.

Pour en savoir plus, consultez la page web ibm.com/guardium.

>4 semaines

La plupart des entreprises reconnaissent la valeur de Guardium en moins d'un mois[7].

Pourquoi choisir IBM Security ?

IBM Security propose l'un des portefeuilles de produits et de services de sécurité d'entreprise parmi les plus sophistiqués et les plus intégrés du marché. Ce portefeuille, qui bénéficie de la collaboration d'IBM X-Force®, une équipe de recherche et de développement de renommée mondiale, fournit des renseignements de sécurité afin d'aider les entreprises à protéger globalement leur personnel, leurs infrastructures, leurs données et leurs applications. Il propose des solutions dans les domaines suivants : gestion des identités et des accès, sécurité des bases de données, gestion des applications, gestion des risques, gestion des points de terminaison, sécurité réseau, et bien d'autres. Ces solutions permettent aux entreprises de gérer efficacement le risque et de mettre en œuvre une sécurité intégrée pour les architectures mobile, cloud et de réseaux sociaux, ainsi que d'autres architectures métier d'entreprise.

IBM est l'une des plus grandes entreprises au monde de recherche, de développement et de distribution de solutions de sécurité. Elle surveille plus de

60 milliards

d'événements de sécurité par jour dans plus de 130 pays.

IBM détient plus de 3 700 brevets dans le domaine de la sécurité.

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

La page d'accueil d'IBM est accessible à l'adresse suivante : **ibm.com**

Le présent document contient des informations en vigueur à la date de la première publication et susceptibles d'être modifiées par IBM à tout moment. Toutes les offres mentionnées ne sont pas distribuées dans tous les pays où IBM exerce son activité.

Les données de performances et les exemples de clients ne sont présentés qu'à des fins d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation spécifiques. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même le fonctionnement des produits ou logiciels non IBM avec les produits ou logiciels IBM. LES INFORMATIONS DU PRÉSENT DOCUMENT SONT FOURNIES « EN L'ÉTAT » ET SANS GARANTIE EXPLICITE OU IMPLICITE D'AUCUNE SORTE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE À CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE À L'EXÉCUTION D'UN TRAVAIL DONNÉ. Les produits IBM sont garantis conformément aux dispositions des contrats au titre desquels ils sont fournis.

Chaque client est tenu de s'assurer qu'il respecte la réglementation applicable. IBM ne donne aucun avis juridique et ne garantit pas que ses services ou produits sont conformes aux lois applicables.

Déclaration de bonnes pratiques de sécurité : la sécurité du système IT englobe la protection des systèmes et des informations grâce à la prévention, la détection et la réponse en cas d'accès internes et externes non autorisés. Un accès non autorisé peut entraîner la modification, la destruction, le détournement ou l'utilisation impropre des informations, ou une détérioration ou une utilisation impropre de vos systèmes, notamment en vue de les utiliser pour attaquer autrui. Aucun système ou produit IT ne doit être considéré comme entièrement sécurisé, et aucun produit, service ou dispositif de sécurité ne peut être entièrement efficace pour empêcher une utilisation ou un accès inappropriés. Les systèmes, produits et services d'IBM sont conçus pour fonctionner dans le cadre d'une stratégie de sécurité globale et conforme à la loi qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent nécessiter des performances maximales des autres systèmes, produits et services. IBM NE GARANTIT PAS QUE LES SYSTÈMES, PRODUITS OU SERVICES SONT PROTÉGÉS CONTRE LES AGISSEMENTS MALVEILLANTS OU ILLÉGAUX D'UN TIERS OU QU'ILS PROTÉGERONT VOTRE ENTREPRISE CONTRE DE TELS AGISSEMENTS.

1 « Cost of a Data Rreach report 2019 ». *IBM Security.* databreachcalculator.mybluemix.net/executive-summary

2 « Healthcare Data Breach Statistics ». *Journal de l'HIPAA. www.hipaajournal.com/healthcare-data-breach-statistics*

3 Jon Oltsik. « The Life and Times of Cybersecurity Professionals 2018 ». *Enterprise Strategy Group and Information Systems Security Association International*, avril 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 NewVantage Report, « Big Data and AI Executive Survey 2019 Executive Summary of Findings ». *NewVantage Partners,* 2019. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. « Why Privileged Account Management Is Key to Preventing Insider Threats ». *Security Intelligence,* 20 juin 2018. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 "Cost of Insider Threats: Global Report 2020". *Ponemon Institute*, 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 "Rapport Ponemon : Client Insights on Data Protection with Guardium." *Ponemon Institute,* août 2019. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

60031860-FRFR-00