Comment créer une stratégie durable de cybersécurité

Comment une approche centrée sur es données peut accroître l'agilité et renforcer la préparation aux failles de sécurité

Contents

Introduction

Alors que les organisations adoptent la transformation numérique, les entreprises collectent, traitent et stockent des quantités de données plus importantes que jamais.

En conséquence, une croissance commerciale efficace et durable doit désormais s’appuyer sur une gouvernance des données complète et multi-cloud - un impératif gravé dans le marbre par des cadres juridiques tels que le California Consumer Protection Act (CCPA) aux États-Unis et le Règlement Général sur la Protection des Données (RGPD) de l’UE.

Une bonne gouvernance des données permet d’instaurer la confiance - un facteur tout aussi essentiel : les équipes, les clients internes et externes comptent sur les entreprises pour fournir un environnement qui facilite l’engagement sans compromettre la sécurité. Cela oblige les entreprises de toutes tailles à réfléchir à la manière dont leurs systèmes peuvent être améliorés pour atténuer le risque de violation des données et répondre efficacement aux cybermenaces en constante évolution.

Pour commencer, les dirigeants doivent reconnaître que la protection des données et la cybersécurité sont les principaux moteurs de la réussite des entreprises à l’ère des données.

Au sein d’une culture qui défend l’intégrité de l’information, les outils et les technologies peuvent permettre un traitement intelligent des données à un niveau granulaire. Ce n’est qu’à partir de là que les entreprises peuvent construire une infrastructure informatique durable qui fonctionne dans un environnement numérique de plus en plus complexe - en restant compétitives, conformes à la législation, cyber-sécurisées et respectueuses des propriétaires des données dont ces organisations sont les gardiennes.

“Si vous réorientez votre organisation en plaçant les données comme l’actif le plus sensible, vous prendrez des décisions différentes quant à la mise en œuvre de votre programme de cybersécurité”, explique Rob McDonald, vice-président exécutif de la plateforme chez Virtru, leader mondial de la confidentialité et de la protection des données.

Que signifie d’être centré sur les données ?

Traditionnellement, la sécurité des entreprises passe par une stratégie de défense périmétrique, comprenant une série d’entités allant de la protection de base via un pare-feu à la sécurité réseau de bout en bout qui englobe le réseau de l’entreprise.

Cette structure en “boîte à biscuits” était conçue pour empêcher les attaques malveillantes ou les données potentiellement infectées de pénétrer dans l’infrastructure informatique. Cependant, la couche de défense unique signifiait que, si le périmètre était violé, tout ce qui se trouvait à l’intérieur était potentiellement compromis.

Ce choix, populaire au cours des dernières décennies, n’est tout simplement pas adapté à l’ère numérique caractérisée par les environnements multi-cloud et distribués qui ont accéléré la complexité de la cybersécurité. Cependant, si les entreprises protègent les données au niveau de l’objet - en sécurisant chaque fichier, courriel ou autre actif de données avec sa propre couche de chiffrement - le périmètre n’est pas une vulnérabilité aussi critique. Chaque objet d’information reste protégé, où qu’il voyage - et si le périmètre est violé, chaque objet à l’intérieur reste protégé par sa propre couche de sécurité.

À mesure que les entreprises se familiarisent avec les enjeux, nous assistons à une évolution indéniable vers un état d’esprit plus sûr, plus tourné vers l’avenir, capable de faire face à des cyberattaques de plus en plus sophistiquées.

“Les cybercriminels et systèmes impliqués sont si sophistiqués qu’il est impossible de rester protégé avec une approche périmétrique. Au cours des deux dernières années, nous avons constaté une augmentation significative du passage à une stratégie centrée sur les données”, explique Rob.

L’approche centrée sur les données

Au lieu de donner la priorité aux contrôles de sécurité pour le matériel et l’infrastructure informatique, une approche centrée sur les données se concentre sur la protection des données là où elles sont stockées et traitées.

À partir de là, l’entreprise est en mesure d’exploiter ces données, de prendre des décisions plus intelligentes et de générer une plus grande valeur dans tous les domaines de l’entreprise. Le résultat final est un environnement de données sain et durable qui permet d’économiser de l’argent et de stimuler la productivité.

Appliqué à la stratégie de protection des données, le fait d’être centré sur les données implique de prendre des décisions concernant votre attitude globale en matière de sécurité et de gestion de l’information en utilisant la donnée elle-même comme élément essentiel pour guider votre approche. Ainsi, le degré d’importance que vous accordez à vos données influencera le développement de vos programmes de sécurité et de formation

D’un point de vue technique, le fait d’être centré sur les données donne l’occasion de réexaminer les fournisseurs de technologies sous un nouvel angle :

Quels fournisseurs vous accompagneront pour faire progresser votre entreprise dans ce schéma ? Apporteront-ils à vos employés la combinaison de flexibilité et de sécurité nécessaire pour favoriser l’innovation ? À quels fournisseurs ferez-vous confiance pour protéger les données les plus vitales de votre entreprise et garantir leur intégrité ? En fin de compte, c’est à vous de déterminer les capacités réellement importantes pour soutenir l’avenir de votre organisation.

En définitive, une entreprise doit s’assurer que, chaque fois que des données sont utilisées, des contrôles techniques sont en place pour superviser les requêtes, régir l’accès et contrôler les niveaux de protection à tout moment.

> ***“L’adoption d’une approche centrée sur les données comporte à la fois un aspect stratégique et un aspect technique. Certaines organisations réussissent mieux que d’autres, mais les deux aspects sont interdépendants et essentiels dans le cadre d’une approche globale centrée sur les données”, explique Rob.***

Stratégie Zero Trust dans un environnement centré sur les données

En pratique, l’approche Zero Trust signifie que lorsqu’un échange d’informations a lieu, la confiance ne joue aucun rôle dans le mouvement des données d’un point à l’autre. Elle est remplacée par la garantie que l’intégrité et la sécurité des données seront maintenues à tout moment, car tout le trafic est validé.

Une approche Zero Trust de la sécurité part donc du principe qu’une violation des données se produira. Les niveaux de sécurité dépendent alors du contexte des données à protéger, de leur valeur et des contrôles de conformité entourant ces données, ce qui permet de mettre en œuvre une protection locale et technique appropriée.

Cette confiance zéro est particulièrement décisive en tant que culture de protection en raison du nombre impressionnant de facettes au sein d’une entreprise moderne, chacune d’entre elles jouant un rôle dans la confidentialité des données - des personnes aux documents et aux commutateurs de réseau, en passant par les pare-feu et les ordinateurs. Si une personne effectue un échange de données, celles-ci peuvent transiter par cinq ou six entités différentes : par exemple, à partir d’un équipement, via un réseau vers un autre réseau, via un fournisseur de cloud computing, et au-delà.

Grâce à l’autorisation et à l’authentification rendues possibles par une approche centrée sur les données, les entreprises peuvent développer la cybersécurité de manière à garantir le Zero Trust à chaque étape de la vie des données.

Comme le détaille la National Security Agency, les principes clés du Zero Trust sont les suivants :

- “Ne jamais faire confiance, toujours vérifier : Considérer chaque utilisateur, équipement, application/processus et flux de données comme non fiable. Authentifier et autoriser explicitement chacun d’eux au plus bas niveau de privilège requis en utilisant des politiques de sécurité dynamiques.”
- “Présupposer la faille : Opérer et protéger délibérément les ressources en supposant qu’un adversaire est déjà présent dans l’environnement. Refuser par défaut et examiner minutieusement tous les utilisateurs, dispositifs, flux de données et demandes d’accès. Enregistrer, inspecter et surveiller en permanence tous les changements de configuration, les accès aux ressources et le trafic réseau pour détecter toute activité suspecte.”
- “Vérifier explicitement : L’accès à toutes les ressources doit être effectué de manière cohérente et sécurisée en utilisant de multiples attributs (dynamiques et statiques) pour dériver les niveaux de confiance pour les décisions d’accès contextuel aux ressources.”

Pourquoi poursuivre une stratégie centrée sur les données ?

Une approche centrée sur les données est plus pertinente que jamais.

L'augmentation marquée des cyberattaques provoquée par la pandémie n'est qu'une des nombreuses raisons à l'origine du besoin de renforcer la cybersécurité aujourd'hui.

La conformité à une législation sur les données en constante évolution, l'obligation d'optimiser la gouvernance des données et la nécessité d'exploiter le big data et les tendances technologiques telles que l'IA, contribuent également à expliquer pourquoi le marché de la sécurité centrée sur les données devrait atteindre 7,3 milliards de dollars d'ici 2025.

Une approche centrée sur les données permet aux entreprises de réduire les cybermenaces et de surmonter les obstacles à la croissance créés par des approches plus traditionnelles de la sécurité, suggère une étude de Capgemini et Forrester intitulée Making Your Business Cyber-Resilient In 2021.

Nous examinons ci-dessous quelques-uns des principaux avantages commerciaux qu'une entreprise peut espérer tirer d'une stratégie centrée sur les données.

Responsabiliser les employés, libérer la productivité et la collaboration

Grâce au centrage sur les données, celles-ci sont protégées, ce qui élimine les préoccupations inhérentes au travail à domicile et à d'autres tendances croissantes en matière de travail. L'amélioration de la cyber-résilience signifie que les employés peuvent partager des données en toute confiance, ce qui augmente la productivité et encourage des comportements de travail plus rapides et plus cohérents au sein des équipes et avec les partenaires.

"En renforçant la collaboration et l'innovation, l'approche centrée sur les données devient décisive dans la capacité d'une entreprise à attirer et à retenir les talents", explique Rob. "Lorsque les employés sont habilités à collaborer plus librement, ils peuvent innover beaucoup plus efficacement, ainsi que mettre de nouveaux produits sur le marché plus rapidement, créant ainsi un environnement de travail plus positif et, au final, plus fructueux."

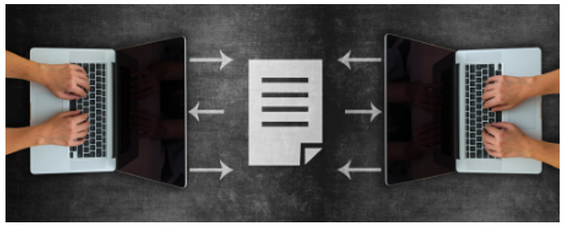
Réduction des coûts

La donnée elle-même est l'élément le plus sensible que les solutions basées sur le périmètre sont conçues pour protéger. Cependant, une approche centrée sur les données supprime les intermédiaires pour mettre en œuvre une approche plus pragmatique et robuste de la cybersécurité, capable de s'adapter à un paysage de menaces en constante évolution.

L'adoption de modèles centrés sur les données apporte également de la valeur car ils améliorent la visibilité des applications, des outils et des équipements dans toute l'entreprise.

La sécurité centrée sur les données s'adapte au contexte, avec une allocation plus intelligente des ressources, gage d'économies financières à long terme. A Contrario, si vous ne parvenez pas à réorganiser votre environnement de cybersécurité informatique en adoptant une approche centrée sur les données, la charge financière s'alourdit à mesure que les besoins de protection évoluent et se complexifient.

"En investissant dans le centrage sur les données, vous créez une stratégie plus durable en matière de protection de vos données. Vous faites quelque chose qui transcendera les changements technologiques à venir, car le dénominateur commun sera toujours les données elles-mêmes."



Protéger les données tout au long de la chaîne d'approvisionnement

Les données organisationnelles ont généralement été protégées de manière très segmentée, avec le chiffrement des applications, le chiffrement des bases de données et d'autres technologies contribuant à une approche pour laquelle un certain nombre de groupes différents au sein d'une organisation sont responsables.

L'approche centrée sur les données assure une protection appropriée et de haut niveau des données, qu'elles soient stockées, traitées ou en transit. Cela garantit la meilleure protection pour votre entreprise et ses partenaires. Pour une protection plus importante, les entreprises peuvent étiqueter leurs données de manière à prendre en charge la gouvernance de l'accès en fonction des rôles et des informations d'identification des utilisateurs, ce que l'on appelle le contrôle d'accès basé sur les attributs (ABAC). La gestion des données de cette manière garantit que l'accès aux données se fait sur la base du "besoin de savoir".

Préparez votre pile technologique pour l'avenir

"En investissant dans le centrage sur les données, vous créez une stratégie plus durable en matière de protection de vos données. Vous faites quelque chose qui transcendera les changements technologiques à venir, car le dénominateur commun sera toujours les données elles-mêmes", explique Rob.

De même, une entreprise qui adopte le centrage sur les données peut s'attendre à être plus forte face aux cybermenaces à mesure qu'elles évoluent. Cette posture dynamique et robuste offre un bien meilleur retour sur investissement à mesure que votre entreprise se développe. Au fil du temps, au fur et à mesure de l'adoption d'investissements centrés sur les données, la mise à l'épreuve de la pile technique entraînera une réduction mesurable du coût total de possession.

"De nombreux CSO repensent leurs dépenses techniques car ils se rendent compte que leur pile technologique n'est pas aussi efficace qu'ils l'espéraient", explique Rob.

La culture centrée sur les données et les gains d'efficacité associés deviendront également un facteur de différenciation positif. Les entreprises avant-gardistes ont la possibilité de démontrer leur compétence en matière de gouvernance des données, de renforcer la confiance et d'accroître leur notoriété.

"L'adaptation au centrage sur les données devient elle-même un avantage concurrentiel", ajoute Rob.

Comment s’y prendre

“Adopter une toute nouvelle approche de la protection des données peut sembler intimidant et le danger est que les gens se rabattent simplement sur ce qu’ils connaissent bien, à savoir les solutions existantes”, explique Rob.

Le voyage commence par la connaissance des données dont vous disposez, de leur emplacement et de la manière d’y accéder.

> Check liste pour un audit de données

Votre entreprise peut avoir des données résidant dans plusieurs endroits, à travers différents logiciels, applications, serveurs et programmes. Dressez une liste des données dont vous disposez et des personnes qui y ont accès au sein de votre entreprise, y compris les tiers.

Si vous n’êtes pas en mesure de parler individuellement aux employés, discutez avec les chefs d’équipe ou les chefs de service des données que les individus utilisent et auxquelles ils ont accès.

Demandez où se trouvent ces données, de quelle quantité de données les collaborateurs ont réellement besoin pour faire leur travail et quels problèmes ils peuvent rencontrer avec ces données.

> Prioriser les besoins de protection des données tout au long de leur cycle de vie

Déterminez le rôle que joue chaque type de données dans votre organisation. Demandez à quoi servent les données, puis décidez si elles doivent être conservées ailleurs pour améliorer l’alignement organisationnel.

“Il est tellement important de prendre du recul et d’examiner simplement ce qui fonctionne ou ne fonctionne pas. Une fois que vous avez ce raisonnement, vous pouvez commencer à convaincre les autres de l’importance de ce que vous essayez d’accomplir”, souligne Rob.

La hiérarchisation des données est essentielle. Par exemple, un magasin de vente en ligne attachera de l’importance aux adresses électroniques et aux adresses postales, tandis qu’une société de marketing direct pourra ne donner la priorité qu’aux adresses postales. En outre, les différents départements d’une organisation peuvent avoir des interprétations différentes des mêmes données : ce que le département marketing considère comme sensible peut différer de ce que les finances ou les ventes considèrent comme tel. La participation de tous les services à ce processus garantit que les données sont traitées avec le soin nécessaire et qu’elles sont utiles à tous les secteurs de l’entreprise. Une fois les données cartographiées, réfléchissez à la valeur qu’elles apportent aux acteurs clés et à la manière dont elles génèrent des bénéfices. Vous pouvez constater que votre entreprise stocke les dates de naissance de ses clients depuis dix ans, alors que ce n’est pas nécessaire. Un tel stockage ne fait qu’augmenter les coûts, absorber les ressources et accroître les risques.

Dans la mesure du possible, supprimez les données anciennes, inutilisées ou non conformes, puis déterminez si des mesures de protection plus ou moins importantes sont nécessaires en fonction de la mission de votre entreprise. Cela vous permettra d’élaborer une stratégie de stockage, de découverte et de cybersécurité plus efficace.

> Sélectionnez des partenaires qui peuvent vous aider à mettre en œuvre et à développer votre stratégie au fil du temps.

L’étape suivante consiste à mettre en œuvre les politiques dans l’ensemble de l’entreprise, par le biais des systèmes, des réseaux, des applications et des produits.

“La priorité ici est de donner les bons outils à votre personnel et à vos écosystèmes de partenaires pour qu’ils puissent faire leur travail. Un inventaire des outils et des environnements sera nécessaire pour atteindre la valeur promise aux clients, partenaires et autres utilisateurs”, explique Rob.

Lorsque les bonnes politiques sont en place, une entreprise peut aller sur le marché pour essayer de trouver les meilleures solutions de sécurité en fonction des besoins, en s’intéressant aux fournisseurs qui adoptent une approche Zero Trust.

Le chiffrement ou la tokenisation doit être utilisé pour protéger les données, mais une solution doit également permettre l’accès aux données déprotégées sur la base de droits d’utilisateur préétablis qui permettent d’accéder à des informations sensibles en cas de nécessité.

Enfin, réfléchissez à l’environnement réglementaire sur lequel vous vous alignerez - qu’il s’agisse du NIST ou d’un organisme similaire qui contribuera en permanence au cadre Zero Trust et aux modèles de sécurité auxquels vous souscrirez.

“Nous constatons que les fournisseurs sont plus nombreux que jamais à adopter des normes et des protocoles Zero Trust. Il n’accélère plus vite du point de vue des applications historiques, car une voie d’adoption est en train d’être créée. Les responsables de la sécurité informatique constatent qu’ils peuvent réellement le faire”, explique Rob.

Conclusion

“Les concepts et les normes axés sur les données n’ont jamais été aussi importants”, rappelle Rob.

Lorsqu’une entreprise comprend que la protection des données est une priorité en matière de cybersécurité, elle peut commencer à s’éloigner des cultures et des mécanismes désuets qui ne font qu’accroître les risques pour l’entreprise à l’ère numérique.

En adoptant une stratégie centrée sur les données, celles-ci sont gérées de manière précise et granulaire, ce qui facilite grandement la lutte contre les cybermenaces omniprésentes.

Dans un environnement informatique plus intelligent et durable, qui s’amortit au fil du temps, la stratégie de cybersécurité favorise l’innovation et la croissance saine de l’entreprise.

À propos de Virtru : Votre partenaire pour la mise en œuvre d’une stratégie centrée sur les données.

Virtru est un leader mondial de la protection des données et de la confidentialité, offrant aux entreprises des solutions de chiffrement de données flexibles et de bout en bout qui protègent les e-mails, fichiers, bases de données, vidéos, et bien plus encore.

Les outils de Virtru sont faciles à utiliser et s’intègrent parfaitement à Gmail, Outlook, Google Workspace, ainsi qu’à d’autres applications d’entreprise telles que Salesforce, SAP et Zendesk. De plus, grâce à des fonctionnalités telles que les contrôles d’accès, la gestion des clés, les règles DLP et l’audit persistant, les entreprises sont en mesure de répondre aux exigences de confidentialité et de conformité telles que GDPR, HIPAA, ITAR et CJIS.

Pour découvrir comment prendre le contrôle total des données de votre organisation, partout où elles sont partagées, contactez Virtru pour entamer la conversation dès aujourd’hui.

Contact Virtru