UN APPRENTISSAGE FACILE

Une 2e édition spéciale de Palo Alto Networks®

Sécurité et conformité dans le cloud

pour les nuls®
A Wiley Brand

Adoptez les DevSecOps

Initiez-vous à la sécurité des applications « cloud native »

Utilisez une stratégie Zero Trust

Proposé par

PRISMA® CLOUD
BY PALO ALTO NETWORKS

Lawrence Miller, CISSP
Petros Koutoupis

À propos de Palo Alto Networks®

Palo Alto Networks est le leader mondial de la cybersécurité. Grâce à nos solutions de sécurité nouvelle génération, à nos services d'experts et à notre Threat Intelligence de pointe, les entreprises de tous les secteurs peuvent se transformer en toute confiance. Avec Prisma® Cloud, Palo Alto Networks propose la plateforme de protection des applications « cloud native » (CNAPP) la plus complète du marché, avec une couverture de sécurité et de conformité étendue pour les applications, les données et l'ensemble de la pile technologique « cloud native ». Cette solution couvre l'intégralité du cycle de développement, ainsi que les environnements hybrides et multicloud. Notre approche intégrée permet aux opérations de sécurité et aux équipes DevOps de rester agiles, de collaborer efficacement et d'accélérer le développement d'applications « cloud native » sécurisées.

Sécurité et conformité dans le cloud

Une 2e édition spéciale Palo Alto Networks

par Lawrence Miller, CISSP et Petros Koutoupis

pour les nuls®

Sécurité et conformité dans le cloud pour les Nuls®, 2e édition spéciale de Palo Alto Networks

Publié par
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-89825-2 (pbk) ; ISBN 978-1-119-89826-9 (ebk)

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un livre sur mesure *pour les Nuls* destiné à votre entreprise ou organisation, veuillez contacter notre service de développement commercial aux États-Unis, par téléphone au 877-409-4177, par e-mail à info@dummies.biz, ou consulter notre site www.wiley.com/go/custompub. Pour obtenir des informations sur la licence de la marque *pour les Nuls* pour des produits ou services, veuillez contacter BrandedRights&Licenses@Wiley.com.

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Rédacteur projet : Elizabeth Kuball

Rédacteur chargé des acquisitions : Ashley Coffey

Responsable éditorial : Rev Mengle

Responsable de compte client : Cynthia Tweed

Éditeur de production : Saikarthick Kumarasamy

Table des matières

Introduction

La technologie numérique est désormais au cœur des enjeux de compétitivité. Dans un effort constant d'amélioration de leurs services, les organisations multiplient les applications innovantes et plébiscitent les technologies cloud pour leur efficacité et leur évolutivité. En conséquence, le périmètre traditionnel de l'entreprise s'estompe et les travailleurs mobiles utilisent de plus en plus d'applications de type Software as a Service (logiciel en tant que service - SaaS). Les entreprises combinent désormais services de cloud privé et de cloud public, gage d'économies, d'agilité et de rapidité.

La transformation numérique place la gestion des risques et la protection des données en tête des préoccupations pour les organisations qui migrent vers le cloud. Les responsables informatiques s'inquiètent de la sécurité de l'entreprise. Qu'elle soit sur site, dans le cloud ou mobile, l'architecture informatique doit être sécurisée dans son ensemble pour préserver l'intégrité et la pérennité de l'entreprise.

Les outils, stratégies et processus de sécurité d'ancienne génération, conçus pour les data centers et les opérations informatiques classiques, ne sont pas adaptés aux applications SaaS ni au modèle de déploiement continu et à la cadence des changements dans le cloud. En dépit d'un large éventail de solutions de sécurité du cloud – dont les services de sécurité natifs des fournisseurs de cloud public –, les produits de sécurité cloisonnés, les opérations manuelles et les erreurs humaines continuent de ralentir l'activité et créent des risques.

La visibilité et le contrôle du cloud sont difficiles, et les environnements cloud sont complexes.

Pour tirer leur épingle du jeu, les entreprises doivent adopter une approche cohérente de la sécurité qui couvre tous leurs environnements d'exploitation, des data centers sur site aux multiples clouds publics et privés. Elles ont besoin d'outils et de processus qui simplifient les opérations grâce à l'automatisation pilotée par le Machine Learning et l'analyse, et de capacités multiplateformes qui empêchent les compromissions de données dans le cloud, le data center et les terminaux.

À propos de ce livre

L'ouvrage *Sécurité et conformité dans le cloud pour les Nuls®* comporte six chapitres qui explorent respectivement les points suivants :

- L'évolution du cloud et de l'informatique « cloud native » et la sécurité dans le cloud (chapitre 1)
- Comment sécuriser le cloud et les applications « cloud native » dans votre organisation (chapitre 2)
- Le paysage réglementaire dans le cloud (chapitre 3)
- Comment constituer une équipe efficace pour la cybersécurité et tirer parti de l'automatisation dans le cloud (chapitre 4)
- Tendances à venir en matière de sécurité dans le cloud (chapitre 5)
- Recommandations de bonnes pratiques pour sécuriser le cloud (chapitre 6)

Quelques suppositions

On dit que la plupart des hypothèses ont survécu à leur inutilité, mais nous en faisons tout de même quelques-unes !

- Vous êtes directeur des systèmes d'information (DSI), directeur de la technologie (CTO), responsable de la sécurité des systèmes d'information (RSSI), architecte cloud, gestionnaire de la conformité et des risques informatiques, ingénieur DevSecOps ou un professionnel de la sécurité ou des réseaux.
- Vous maîtrisez le cloud computing dans ses grandes lignes et son effet de levier sur l'agilité de votre entreprise.
- Vous souhaitez mieux comprendre la portée et la répartition des risques liés au cloud et comment déployer une sécurité sans faille pour prévenir les compromissions de données sans affecter négativement vos besoins métier et de développement, aujourd'hui et demain.

Si vous vous reconnaissez dans l'une de ces descriptions, ce livre est fait pour vous, sans hésitation ! Si aucune de ces catégories ne vous correspond, poursuivez quand même votre lecture : cet ouvrage très riche vous en apprendra certainement beaucoup sur la sécurité et la conformité dans le cloud.

Icônes utilisées dans ce livre

Ce livre est émaillé de différentes icônes destinées à attirer l'attention du lecteur sur des informations importantes :

RAPPEL

Cette icône signale des informations importantes à retenir – ou, si vous nous permettez l'analogie, à inscrire durablement dans votre mémoire non volatile, non loin des dates d'anniversaire, par exemple !

CONSEIL

Un petit conseil est toujours le bienvenu : nous espérons que vous apprécierez ces informations utiles.

ATTENTION

Ne négligez surtout pas ces alertes : elles vous feront gagner du temps et vous éviteront de la frustration inutile.

Ressources complémentaires

Ce sujet est tellement vaste qu'il est impossible de tout aborder dans cet ouvrage. Si à la fin du livre vous pensez : « Oh, ce livre était génial ! Où puis-je en savoir plus ? », il suffit de vous rendre sur le site `www.paloaltonetworks.com/prisma/cloud/cnapp-5-must-have`.

Par quoi commencer ?

Si vous ne savez pas où vous allez, n'importe quel chapitre vous y conduira, mais le chapitre 1 est un bon point de départ ! Toutefois, si un sujet particulier vous intéresse, n'hésitez pas à passer directement au chapitre concerné. Chaque chapitre est écrit pour être autonome, de sorte que vous pouvez commencer votre lecture n'importe où et passer au contenu qui vous intéresse ! Lisez cet ouvrage dans le sens qui vous convient, mais nous vous déconseillons de le lire à l'envers ou de droite à gauche.

DANS CE CHAPITRE

- **Comprendre l'évolution du cloud et des applications « cloud native »**
- **Déterminer le niveau de maturité cloud de votre organisation**
- **Évaluer les risques dans le cloud**
- **Définir les responsabilités des clients et des fournisseurs de services cloud**

Chapitre 1
L'évolution des applications « cloud native » et leur impact sur la sécurité

Les données sont le moteur du marché. Pour prospérer, une organisation doit donc rendre ses données constamment accessibles aux utilisateurs. Ce souci permanent d'accessibilité est l'une des principales raisons de la migration de plus en plus fréquente des infrastructures informatiques vers le cloud, où un accès instantané 24h/24 et 7j/7 est la norme. Cette évolution vers un réseau plus large et plus accessible a obligé les équipementiers et prestataires de services à repenser leurs stratégies et à s'adapter à de nouveaux modèles de stockage des informations et de fourniture de ressources applicatives.

De nos jours, le *cloud* est synonyme non seulement de stockage de données, mais également de services web qui accèdent régulièrement à ces données en arrière-plan. Le cloud computing simplifie l'accès aux ressources de serveurs, de systèmes de stockage, de bases de données et d'applications et permet aux utilisateurs de

provisionner et d'utiliser un minimum de ressources pour leurs besoins applicatifs spécifiques. La technologie cloud est conçue pour faire évoluer ses ressources à la hausse et à la baisse afin de s'adapter à l'évolution continue des demandes. Ce modèle a favorisé la migration de la majorité, voire de l'intégralité, des workloads des data centers locaux vers le cloud.

Dans ce chapitre, nous vous proposons une introduction aux principes du cloud, de l'informatique « cloud native » et de la transition vers ces technologies. Nous nous pencherons ensuite sur les méthodes permettant d'évaluer le niveau de maturité de votre organisation en matière de cloud computing. Enfin, nous ferons un point sur l'évolution du risque dans le cloud et sur les implications du modèle de partage des responsabilités pour votre organisation.

Parlez-vous cloud ?

Aujourd'hui, le cloud semble omniprésent. Mais pour nous assurer d'être sur la même longueur d'onde, commençons par définir un lexique commun avec l'aide du National Institute of Standards and Technology (NIST), organisme de normalisation des États-Unis.

Dans la *Publication spéciale 800-145*, le NIST définit les cinq caractéristiques essentielles suivantes du cloud computing :

- **Libre-service à la demande :** « Un utilisateur peut unilatéralement provisionner des capacités informatiques, telles que des ressources serveur et de stockage réseau, selon ses besoins, et de manière automatique, sans avoir à interagir avec chaque fournisseur de services. »
- **Accès large au réseau :** « Les capacités informatiques sont disponibles sur le réseau et accessibles via des mécanismes standard qui favorisent l'utilisation de plateformes clientes hétérogènes, légères ou lourdes (téléphones portables, tablettes, ordinateurs portables, postes de travail, etc.). »
- **Mutualisation des ressources :** « Stockage, traitement, mémoire, bande passante… les ressources informatiques du fournisseur sont regroupées pour servir plusieurs utilisateurs selon un modèle d'architecture mutualisée, avec des ressources physiques et virtuelles attribuées et réattribuées dynamiquement suivant la demande. »
- **Élasticité rapide :** « Les ressources peuvent être provisionnées et libérées de manière élastique et automatique pour augmenter ou

diminuer rapidement la charge en fonction de la demande. Pour l'utilisateur, les capacités disponibles pour le provisionnement apparaissent souvent comme illimitées et peuvent être utilisées en toute quantité et à tout moment. »

- **Service mesuré :** « Les systèmes cloud contrôlent et optimisent automatiquement l'utilisation des ressources par des moyens de mesure à certains niveaux d'abstraction appropriés au type de service (stockage, traitement, bande passante, comptes d'utilisateurs actifs, etc.). La surveillance, le contrôle et la génération de rapports sur l'utilisation des ressources garantissent la transparence pour les fournisseurs et les utilisateurs des services. »

Le NIST définit les quatre modèles de déploiement cloud suivants (même si les clouds communautaires ne sont pas si courants) :

- **Cloud privé :** « L'infrastructure cloud est fournie pour une utilisation exclusive par une seule organisation comprenant plusieurs utilisateurs (par exemple, des unités opérationnelles). Cette infrastructure peut se situer sur ou hors site, et être détenue, gérée et exploitée par l'organisation, un tiers ou les deux. »
- **Cloud communautaire :** « L'infrastructure cloud est provisionnée pour une utilisation exclusive par une communauté spécifique d'utilisateurs issus d'organisations ayant des préoccupations communes (par exemple, une mission, des exigences de sécurité, une politique, ou des considérations de conformité). Elle peut se situer sur ou hors site, et être détenue, gérée et exploitée par une ou plusieurs organisations de la communauté, par un tiers ou par une combinaison de ceux-ci. »
- **Cloud public :** « L'infrastructure cloud est provisionnée pour une utilisation ouverte par le grand public. Elle peut être détenue, gérée et exploitée par une entreprise, un établissement universitaire, une organisation gouvernementale, ou par une combinaison de ceux-ci. Elle est hébergée par un fournisseur de services cloud. »
- **Cloud hybride :** « L'infrastructure cloud comporte deux infrastructures cloud distinctes ou plus (privées, communautaires ou publiques) qui restent des entités uniques, mais qui sont liées entre elles par une technologie standardisée ou propriétaire permettant la portabilité des données et des applications (par exemple, le « cloud bursting » pour l'équilibrage de charge entre les clouds). »

Enfin, le NIST définit les trois modèles de services de cloud computing suivants :

- **Logiciel en tant que service (SaaS) :** « L'utilisateur exploite des applications provenant du fournisseur et fonctionnant sur une infrastructure cloud. Les applications sont facilement accessibles grâce à une interface client légère, comme un navigateur web (par exemple, une messagerie web), ou une interface de programme. L'utilisateur ne peut pas gérer ou contrôler l'infrastructure cloud sous-jacente (réseau, serveurs, systèmes d'exploitation, stockage) ni même les fonctions des applications à l'exception de certains paramètres de configuration utilisateur limités. »
- **Plateforme en tant que service (PaaS) :** « L'utilisateur peut déployer sur l'infrastructure cloud des applications qu'il a lui-même créées ou acquises, en utilisant les langages, bibliothèques, services et outils pris en charge par le fournisseur. Il ne peut pas gérer l'infrastructure cloud sous-jacente (réseau, serveurs, systèmes d'exploitation, stockage), mais il exerce un contrôle sur les applications déployées et potentiellement sur les paramètres de configuration de l'environnement hébergeant les applications. »
- **Infrastructure en tant que service (IaaS) :** « L'utilisateur peut provisionner des services de traitement, de stockage, de réseau et d'autres ressources informatiques fondamentales grâce auxquels il peut déployer et exécuter n'importe quel type de logiciel, pouvant inclure des systèmes d'exploitation et des applications. Il ne gère pas l'infrastructure cloud sous-jacente, mais contrôle les systèmes d'exploitation, le stockage, les applications déployées et, potentiellement et de façon limitée, certains composants réseau (par exemple, les pare-feu hôtes). »

Maintenant que nous avons établi un langage commun en ce qui concerne le cloud, examinons la prochaine ère du cloud computing.

Présentation de l'informatique « cloud native »

L'*informatique « cloud native »* est une nouvelle méthode de conception, de déploiement et d'hébergement des applications qui s'exécute entièrement sur un environnement cloud. Ce concept bouscule la norme établie et donne plus de pouvoir à l'application elle-même, en faisant abstraction de son architecture sous-jacente.

Chaque application ou processus est encapsulé dans un container individuel, qui est ensuite planifié et géré sur un cluster de nœuds de

serveurs. Cette approche permet aux applications de s'affranchir des dépendances du matériel et des systèmes d'exploitation, et de s'installer dans leur propre environnement autonome et de sandbox, qui peut s'exécuter de manière transparente dans l'ensemble du data center. L'approche « cloud native » consiste à séparer les différents composants de la livraison d'applications.

RAPPEL

Les containers permettent de séparer les applications logicielles du système d'exploitation, offrant aux utilisateurs un environnement informatique propre et minimal. Tout le reste est exécuté à l'intérieur d'un ou de plusieurs containers isolés. Il s'agit de la solution la plus proche de la technologie « bare metal » que l'on peut obtenir lorsqu'on exécute une instance virtuelle. Cette technologie offre des avantages considérables, car elle n'impose que peu voire pas de surcharge (overhead). L'objectif principal du container est de lancer un ensemble limité d'applications ou de services (souvent appelés microservices) et de les exécuter dans leur propre environnement de type « sandbox ».

Pourquoi adopter une stratégie de sécurité « code to cloud » ?

Les applications « cloud native » diffèrent de leurs homologues traditionnelles en ce sens qu'elles sont conçues dès le départ pour fonctionner dans le cloud. Par conséquent, toute stratégie de sécurité de nouvelle génération doit avoir une portée globale et se concentrer sur la fourniture d'applications *sécurisées* dans le cloud. Les équipes DevOps, d'infrastructure cloud et de sécurité doivent bénéficier d'une visibilité équivalente et disposer d'un ensemble intégré de fonctionnalités pour garantir la sécurité des applications « cloud native » tout au long du cycle de vie de codage, de compilation, de déploiement et d'exécution. Il s'agit notamment de créer un code sécurisé et une infrastructure sécurisée propice à son exécution, sur plusieurs clouds.

Les solutions capables de couvrir l'ensemble de ce spectre sont connues sous le nom de plateformes de protection des applications « cloud native » (CNAPP, Cloud-Native Application Protection Platforms). Elles redéfinissent entièrement la notion de sécurité du cloud. Comme défini par Gartner, les CNAPP représentent une toute nouvelle approche de la sécurité « cloud native » – une approche qui privilégie l'identification et la correction systématiques et en temps réel des risques, à toutes les étapes du cycle de vie des applications.

Les CNAPP se distinguent des outils classiques de sécurité dans le cloud sur les points suivants :

- **Automatisation :** les CNAPP utilisent l'automatisation pour réduire l'effort manuel nécessaire à la sécurisation des applications « cloud native », ce qui accélère le déploiement et la mise à l'échelle des applications.
- **Stratégies de sécurité :** les CNAPP utilisent des stratégies de sécurité pour définir la posture de sécurité des applications. Ces stratégies permettent de configurer automatiquement l'infrastructure sous-jacente (pare-feu, équilibreurs de charge, etc.) afin de protéger les applications.
- **Visibilité :** les CNAPP offrent une visibilité sur la politique de sécurité des applications « cloud native », ce qui permet aux organisations d'identifier les incidents de sécurité et d'y répondre rapidement.
- **Intégration :** les CNAPP s'intègrent à d'autres outils et technologies de sécurité, tels que les plateformes de Threat Intelligence, les analyseurs de vulnérabilités et les outils de réponse aux incidents, pour fournir une solution de sécurité complète.
- **Évolutivité :** les CNAPP sont conçues pour gérer l'échelle et la complexité des applications « cloud native » de nouvelle génération, pour assurer leur protection avec un minimum de surcharge.

Les CNAPP protègent les applications tout au long du cycle de vie du développement – de l'écriture et de la compilation du code jusqu'au déploiement dans l'environnement d'exécution. Elles peuvent identifier les problèmes de sécurité dans le code source, ainsi que dans les packages et les images de containers qui sont testés avant le déploiement des applications. Pendant l'exécution, les CNAPP surveillent également les risques et les vulnérabilités afin de détecter les problèmes qui ont échappé aux analyses précédentes.

Les problèmes de sécurité sont ainsi identifiés plus efficacement qu'avec les outils classiques de sécurité du cloud. Bien qu'il soit théoriquement possible de combiner des solutions de sécurité traditionnelles pour détecter différents types de risques et y répondre au cours des nombreuses étapes du cycle de livraison des applications cloud, seule une CNAPP permet d'identifier et de gérer ces risques de façon complète et centralisée, en tenant compte des exigences de sécurité uniques des workloads dans le cloud.

Sécuriser le cycle de vie des applications avec une CNAPP

Le développement d'applications « cloud native » innovantes suit un cycle de vie qui diffère des modèles traditionnels en cascade. Auparavant, les applications faisaient l'objet de mises à jour majeures une ou deux fois par an. Mais aujourd'hui, le développement d'applications utilise un pipeline d'intégration continue/de livraison continue (CI/CD) qui permet de développer, de corriger et d'améliorer rapidement les applications.

Les développeurs actuels sont agiles. Ils utilisent un modèle DevOps qui peut se résumer à trois étapes du cycle de vie des applications :

- **Codage/compilation (build) :** les applications sont codées et assemblées (le plus souvent à partir de composants tiers open source).
- **Déploiement :** le logiciel est inséré dans un package pour un référentiel de containers.
- **Exécution :** l'application est opérationnelle, souvent sur différents clouds publics et privés.

Considérons maintenant le cycle de vie des applications du point de vue de la *sécurité*. Des risques et des menaces spécifiques peuvent survenir à chacune de ces étapes :

- **Codage/compilation (build) :** une seule faille de sécurité dans le code peut conduire à des centaines de vulnérabilités dans l'environnement d'exécution.
- **Déploiement :** l'image d'un container peut être infectée par un code malveillant avant d'être exécutée.
- **Exécution :** les vulnérabilités compromettantes des applications web et des interfaces de programmation d'applications (API) sont des cibles courantes pour les attaquants.

Il est essentiel de sécuriser chaque étape, et ce, pour les raisons suivantes :

- **Codage/compilation (build) :** l'identification des infrastructures en tant que code (IaC) mal configurées et des mauvaises configurations avant de valider le code permet d'accroître la sécurité des services cloud.

- **Déploiement :** des stratégies doivent être appliquées pendant le déploiement pour s'assurer que seules les applications de confiance peuvent être lancées dans l'environnement d'exécution du cloud.
- **Exécution :** la capacité d'identifier rapidement les comportements attendus et de prévenir les comportements anormaux est essentielle pour sécuriser les applications dans les environnements d'exécution.

De nombreuses organisations pensent, à tort, que la sécurité dans le cloud relève de la responsabilité du fournisseur de services cloud. Or, bien que ces fournisseurs soient responsables de la sécurité du cloud, le client demeure responsable de la sécurité de ses workloads, services et données dans le cloud. C'est ce que l'on appelle le modèle de *partage des responsabilités*, que nous allons expliquer ci-après.

Comprendre le modèle de partage des responsabilités

Pour améliorer l'agilité organisationnelle et réduire les coûts, les applications basées sur le cloud et les données qui les accompagnent sont de plus en plus réparties entre différents environnements. Ces environnements comprennent des clouds privés, des clouds publics (hybrides ou dédiés) et des applications SaaS, chacun offrant des avantages uniques en termes d'agilité et soulevant un certain nombre de problématiques de sécurité.

Les inquiétudes concernant l'exposition des données ont fait de la sécurité dans le cloud une priorité. Le défi consiste à équilibrer le besoin d'agilité de l'organisation tout en améliorant la sécurité des applications et en sécurisant les données lorsqu'elles circulent entre les différents clouds. Il est indispensable d'accroître la visibilité et de prévenir les attaques qui cherchent à extraire des données, que ce soit à partir d'un emplacement externe ou par une attaque latérale, sur tous les sites où se trouvent les applications et les informations.

Dans une organisation, divers groupes – y compris les équipes chargées du réseau, de la sécurité, des applications, de la conformité et/ou de l'infrastructure – peuvent partager la responsabilité de la sécurité dans le cloud. Cependant, cette sécurité est également une responsabilité partagée entre le fournisseur de services cloud et l'organisation :

- **Cloud privé :** les entreprises sont responsables de tous les aspects de la sécurité dans le cloud, car celui-ci est hébergé dans leurs propres data centers. Leur responsabilité englobe le réseau physique, l'infrastructure, l'hyperviseur, le réseau virtuel, les systèmes d'exploitation, les pare-feu, la configuration des services, la gestion des identités et des accès, etc. L'entreprise est également propriétaire des données et de leur sécurité.
- **Cloud public :** dans les clouds publics, comme Amazon Web Services (AWS), Google Cloud ou Microsoft Azure, le fournisseur de services cloud possède l'infrastructure, le réseau physique et l'hyperviseur. L'entreprise est propriétaire du système d'exploitation des workloads, des applications, du réseau virtuel, de l'accès à son environnement/compte de locataire et des données.
- **SaaS :** les fournisseurs de SaaS sont les premiers responsables de la sécurité de leur plateforme, qui comprend la sécurité physique, l'infrastructure et la sécurité des applications. Cependant, ils ne sont pas propriétaires des données des clients et n'assument aucune responsabilité quant à l'utilisation que ceux-ci font des applications. En tant que telle, l'entreprise est responsable des systèmes de sécurité qui permettent de prévenir et de minimiser le risque d'exfiltration de données, d'exposition accidentelle ou d'insertion de logiciels dans un but malveillant.

Lorsque les entreprises passent du cloud privé au cloud public ou aux applications SaaS, la responsabilité de la sécurisation des données, des applications et de l'infrastructure incombe moins à l'entreprise qu'au fournisseur (voir Figure 1-1). Toutefois, quelle que soit la plateforme utilisée, l'entreprise demeure responsable de la sécurité et de la confidentialité de ses propres données.

Pour assurer la sécurité des applications et des données, les services informatiques doivent bien comprendre où se situent les responsabilités des fournisseurs de services cloud et celles qui leur incombent. Pour assumer leur part du contrat en matière de sécurité dans le cadre du modèle de partage des responsabilités, les organisations doivent disposer des bons outils. Ces outils doivent fournir une visibilité sur l'activité dans l'application cloud ; des analyses détaillées sur l'utilisation afin de prévenir les risques liés aux données et les violations de la conformité ; des contrôles de stratégie adaptés au contexte à appliquer afin d'empêcher les violations ou d'intervenir lorsqu'elles se produisent ; et des informations en temps réel sur les menaces connues et inconnues pour détecter et prévenir l'insertion de nouveaux malwares.

Comparaison des responsabilités – Qui fait quoi ?

Sur site	Infrastructure en tant que service (IaaS)	Plateforme en tant que service (PaaS)	Logiciel en tant que service (SaaS)
Applications	Applications	Applications	Applications
Données	Données	Données	Données
Middleware	Middleware	Middleware	Middleware
Système d'exploitation	Système d'exploitation	Système d'exploitation	Système d'exploitation
Virtualisation	Virtualisation	Virtualisation	Virtualisation
Serveurs	Serveurs	Serveurs	Serveurs
Stockage	Stockage	Stockage	Stockage
Réseau	Réseau	Réseau	Réseau

Votre responsabilité	Responsabilité du fournisseur

FIGURE 1-1 : La sécurité dans le cloud est une responsabilité partagée.

DANS CE CHAPITRE

- Intégrer la sécurité du cloud dans vos processus dès le début
- Établir des responsabilités clairement définies dans votre entreprise
- Connaître vos risques dans le cloud
- Reconnaître les limites des outils existants
- Créer une stratégie multicloud sécurisée
- Implémenter de bonnes pratiques de sécurité dans le cloud

Chapitre 2
Premiers pas dans la sécurité des applications cloud et « cloud native »

Ce chapitre examine les responsabilités individuelles en matière de sécurité dans le cloud et « cloud native » que vous devez définir dans votre entreprise. Vous découvrirez comment évaluer les risques dans le cloud et examinerez vos outils de sécurité existants dans ce domaine. Vous découvrirez également ce qu'il faut pour créer une stratégie cloud sécurisée pour les environnements tels que l'IaaS (infrastructure en tant que service), le PaaS (plateforme en tant que service), le SaaS (logiciel en tant que service), le multicloud et les containers, tout en explorant les bonnes pratiques de sécurité spécifiques au cloud.

Créer un environnement en pensant à la sécurité dans le cloud

Il est fréquent que la sécurité soit négligée tout au long du cycle de développement, de livraison et de déploiement des logiciels, pour être reléguée aux étapes finales de ce processus. Avant les DevOps, le processus de développement, de déploiement et de sécurisation des logiciels prenait des mois, voire des années.

Maintenant que de plus en plus d'entreprises ont adopté un modèle d'intégration continue/de livraison continue (CI/CD), les mises à jour ont tendance à être plus fréquentes. La pratique du CI/CD permet aux ingénieurs logiciels d'apporter des modifications incrémentielles au code de manière fréquente et fiable, tout en déployant rapidement et de manière transparente le code mis à jour en production. Il ne faut parfois que quelques semaines, voire quelques jours, pour qu'une nouvelle révision d'une application soit publiée.

Reporter la vérification de la sécurité de l'application (et de l'environnement dans lequel elle s'exécute) à la dernière minute risque de compromettre le processus et peut créer des dysfonctionnements ou des interruptions de service. C'est pourquoi vous devez vous assurer que votre écosystème est sécurisé au maximum, afin de pouvoir prévenir ou atténuer tout problème lorsqu'une application n'a pas fait l'objet de tests de sécurité complets avant d'être déployée.

Définir les responsabilités de l'organisation en matière de sécurité dans le cloud

RAPPEL

Au-delà du modèle de partage des responsabilités (voir chapitre 1), il est important de définir les responsabilités individuelles en matière de sécurité dans le cloud au sein de votre organisation et de veiller à ce que chacun sache ce qu'il doit faire. Il ne suffit pas – et c'est même un cliché – de dire : « La sécurité est l'affaire de tous. » Au lieu de traiter la sécurité dans le cloud comme une politique autonome, la stratégie de l'entreprise doit englober l'ensemble de l'environnement, y compris les data centers sur site et les clouds publics et privés. L'adoption d'une approche globale et cohérente, fondée sur une automatisation pilotée par l'analytique, permet de réduire la complexité de la tâche.

En commençant par le sommet de la hiérarchie, l'adhésion des dirigeants est essentielle. Heureusement, dans le paysage réglementaire actuel (voir chapitre 3), ce soutien est pratiquement obligatoire. L'impact financier potentiel de la non-conformité réglementaire sur une entreprise peut être aussi dévastateur (voire pire) qu'une compromission de données. Outre les sanctions financières, de nombreuses réglementations prévoient des sanctions pénales pour les dirigeants et autres administrateurs d'une entreprise.

Le soutien des dirigeants commence par l'exemplarité, en joignant l'acte à la parole. Si la politique de l'entreprise exige, par exemple, que les données des appareils mobiles soient chiffrées et que l'accès aux applications SaaS nécessite une authentification multifacteur, aucune exception « ponctuelle » ne doit être accordée aux dirigeants.

C'est également à ces derniers qu'échoit la responsabilité de s'assurer que les initiatives en matière de sécurité et de conformité bénéficient du soutien et des ressources nécessaires, et que l'impact des décisions stratégiques sur la position globale de l'organisation en matière de sécurité et de conformité est toujours pris en compte.

Les équipes chargées de la sécurité et de la conformité doivent définir et faire observer des stratégies appropriées qui permettent à l'entreprise de fonctionner en toute sécurité. Pour cela, elles doivent maîtriser et respecter les objectifs de l'entreprise. Elles doivent également travailler de manière fluide et ne pas être un frein à la productivité et à l'efficacité.

Il incombe aux responsables métier de veiller à ce que tous les membres de leur département comprennent et respectent les politiques de gouvernance de l'entreprise en matière de sécurité et de conformité dans le cloud. À mesure que les besoins de l'entreprise évoluent, ces managers doivent évaluer le risque lié à l'adoption de nouveaux outils, en collaboration avec les équipes de sécurité. La règle interdit de contourner une stratégie de sécurité (par exemple l'obligation d'utiliser uniquement des applications SaaS approuvées) pour atteindre un objectif commercial ou de productivité à court terme. Au contraire, les outils de sécurité doivent s'adapter aux besoins de l'entreprise et induire le comportement utilisateur souhaité.

CONSEIL

En matière de sécurité et de conformité, la collaboration permet également à l'ensemble des secteurs d'activité de bénéficier des relations entre l'organisation et ses fournisseurs et prestataires de services cloud pour acquérir des services de manière plus économique et bénéficier d'une assistance rapide en cas de besoin, plutôt que d'opérer en vase clos avec des solutions cloud segmentées.

Les équipes DevOps sont soumises à une pression constante pour livrer rapidement projets et mises à jour logicielles et pour réduire les délais de mise sur le marché. Pour répondre à ces exigences, elles doivent définir et maîtriser les exigences de sécurité dès le début d'un projet et, idéalement, les intégrer dans le workflow de livraison de l'application. Ainsi, les équipes de développement peuvent avancer sans s'interrompre constamment pour résoudre les failles de sécurité et les violations de conformité. C'est là un rôle essentiel des DevSecOps dans le processus de développement et de livraison.

Enfin, il incombe aux utilisateurs de respecter la gouvernance d'entreprise en matière de sécurité et de conformité dans le cloud. Ils doivent comprendre les risques inhérents au cloud et protéger les données qui leur ont été confiées comme s'il s'agissait des leurs.

Avancer avec les DevSecOps

Les DevSecOps intègrent la sécurité à l'application ou à la fonctionnalité dès le début du processus de développement. Une bonne stratégie consisterait à déterminer la tolérance aux risques et à effectuer une analyse des risques pour cette seule fonctionnalité. Voici les principales questions à vous poser lors de la définition de la portée d'un projet :

- Quel degré de sécurité êtes-vous prêt à accorder à la fonctionnalité ?
- Dans quelle mesure avez-vous respecté cette exigence tout au long du cycle de vie de la fonctionnalité ?
- Que se passe-t-il lorsque vous adaptez ce modèle à plusieurs fonctionnalités, parfois simultanément ?

L'automatisation est un élément clé pour garantir la conformité du développement et de l'intégration d'un produit avec les exigences de sécurité tout en minimisant, voire en éliminant, les perturbations.

Les principaux avantages de l'adoption d'un modèle DevSecOps sont les suivants :

- Vitesse et agilité accrues pour les équipes de sécurité
- Diminution du temps de réponse pour faire face au changement et aux besoins
- Augmentation ou amélioration de la collaboration et de la communication entre les équipes
- Possibilités accrues de builds automatisées et de tests d'assurance qualité
- Identification précoce des vulnérabilités dans le code de l'application

L'objectif ultime des DevSecOps est d'imprégner la cybersécurité dans la culture de votre organisation. Ce faisant, la sécurité est dissociée du workflow applicatif pour s'assurer qu'elle suit le rythme de l'innovation.

Les DevSecOps reposent sur six piliers :

- Capacité à fournir du code en petits morceaux pour identifier rapidement les vulnérabilités
- Vitesse et efficacité accrues pour la gestion du code source, et capacité à déterminer l'impact d'un changement récemment soumis

- Maintien d'un état de conformité constant (en d'autres termes, prêt pour l'audit)
- Capacité à identifier les menaces émergentes potentielles avec chaque mise à jour de code, ce qui donne à l'organisation la possibilité de réagir rapidement
- Capacité à identifier les nouvelles vulnérabilités avec l'analyse du code, ce qui donne à l'organisation la possibilité de corriger le code affecté
- Formation en continu des ingénieurs sur les consignes de sécurité pour les routines définies

Si la partie « sécurité » des DevSecOps semble tenir plus d'un état d'esprit ou d'une philosophie, une grande part du défi consiste toutefois à identifier les risques à un stade précoce et à utiliser les outils appropriés pour mener à bien l'ensemble du processus, de la conception au déploiement.

Évaluer les risques dans le cloud

Pour évaluer correctement les risques dans le cloud, les entreprises doivent appliquer des processus internes d'évaluation des risques à leurs déploiements dans le cloud. Elles doivent également envisager d'utiliser un cadre d'évaluation, tel que le CCM (Cloud Controls Matrix) de la Cloud Security Alliance (CSA). Le CCM se compose de 16 domaines qui décrivent les principes et les bonnes pratiques en matière de sécurité dans le cloud. Son objectif est d'aider les organisations à évaluer le risque global de sécurité d'un fournisseur de services cloud. Ces 16 domaines sont les suivants :

- Sécurité des applications et des interfaces
- Assurance de l'audit et conformité
- Gestion de la continuité d'activité et résilience opérationnelle
- Contrôle des modifications et gestion de la configuration
- Sécurité des data centers
- Sécurité des données et gestion du cycle de vie des informations
- Chiffrement et gestion des clés
- Gouvernance et gestion des risques
- Ressources humaines
- Gestion des accès et identités
- Sécurité de l'infrastructure et de la virtualisation
- Interopérabilité et portabilité

- Sécurité mobile
- Gestion des incidents de sécurité, découverte électronique et forensique du cloud
- Gestion, transparence et responsabilité de la chaîne d'approvisionnement
- Gestion des menaces et des vulnérabilités

Le CCM établit également une correspondance entre les contrôles individuels du cloud et les réglementations et normes pertinentes en matière de protection des données et de sécurité des informations, notamment : AICPA (American Institute of Certified Public Accountants), SOC 2 (System and Organization Controls), *loi* canadienne *sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), Organisation internationale de normalisation (ISO) 27001/27002/27017/27018, *loi américaine sur la portabilité et la responsabilité de l'assurance maladie* (HIPAA), norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), et bien d'autres encore.

CONSEIL

Pour vous aider à évaluer le risque de votre organisation et de vos fournisseurs de services cloud, le questionnaire CAIQ (Consensus Assessments Initiative Questionnaire) regroupe près de 300 questions couvrant les 16 domaines du CCM. Rendez-vous à l'adresse `https://cloudsecurityalliance.org` pour en télécharger un exemplaire gratuit.

Évaluer les outils de sécurité existants

La plupart des approches de sécurité cloud les plus courantes actuellement ne fournissent pas la vision d'ensemble nécessaire à la détection et à la prévention des menaces avancées et des compromissions de données. Voici un bref résumé des plus populaires d'entre elles et de leurs faiblesses.

Sécurité native du cloud public

La sécurité dans le cloud est une responsabilité partagée entre le fournisseur de services cloud et le client. Dans le cas de l'IaaS, les clients sont responsables de la protection de leurs applications et de leurs données exécutées dans le cloud public. Dans le cas du SaaS, en revanche, ils ne sont responsables que de la sécurité de leurs données.

Pour faciliter la protection, les fournisseurs de services cloud proposent des services de sécurité natifs de base, notamment des contrôles d'accès et des outils de protection des données. Cependant, le niveau de sécurité fourni par ces services natifs n'est

pas suffisant pour répondre aux exigences des entreprises, et il est limité au seul fournisseur de services cloud. Par exemple, ces services exploitent des outils axés sur le contrôle d'accès en fonction des informations de port (à l'aide de listes de contrôle d'accès [ACL] et de pare-feu basés sur les ports). Ils n'inspectent qu'un petit ensemble d'applications (à l'aide de pare-feu d'applications Web [WAF]). Il en résulte souvent une sécurité fragmentée et une surcharge de gestion complexe, car les entreprises ont tendance à utiliser les offres IaaS, PaaS et SaaS de plusieurs fournisseurs cloud. Par conséquent, les entreprises doivent compléter ces services natifs avec des outils et des services de sécurité internes.

Produits ponctuels

La multiplication des outils de sécurité et des fournisseurs pour résoudre des cas d'utilisation spécifiques fait émerger un environnement de sécurité fragmenté, dans lequel les équipes informatiques doivent corréler manuellement les données pour mettre en œuvre des protections de sécurité exploitables. Ce niveau d'intervention augmente le risque d'erreurs humaines, ce qui expose les organisations à des menaces et à des compromissions de données. Les CASB (Cloud Access Security Brokers), par exemple, sont utiles pour atténuer les risques au sein des environnements SaaS. Au lieu d'ajouter un outil de sécurité ponctuel qui augmente la complexité opérationnelle, les capacités des CASB devraient faire partie d'une plateforme de cybersécurité élargie.

Sécurité des réseaux et des contenus existants

Les fournisseurs de sécurité traditionnels prétendent offrir un niveau de protection adéquat pour vos environnements cloud. Cependant, leur offre se réfère le plus souvent à une instance virtualisée du matériel placé dans le cloud public. Cette approche ne permet pas une véritable intégration de la sécurité dans le cloud et elle finit par annuler les avantages de ces plateformes dématérialisées en termes de disponibilité à la demande et d'agilité. De plus, elle ne dispose pas de l'automatisation nécessaire pour assurer une sécurité cohérente et sans failles dans l'ensemble de votre environnement multicloud.

Établir une stratégie de sécurité

Dans l'idéal, la sécurité doit permettre d'accélérer le développement des applications et la croissance de l'entreprise tout en évitant les pertes de données et les interruptions d'activité. Votre fournisseur de services de sécurité doit utiliser les mêmes technologies que celles que vous utilisez pour fournir des services à vos clients :

- **La sécurité fournie en tant que service** pour assurer une protection cohérente sur tous les sites et dans tous les clouds, grâce à un écosystème agile et évolutif
- **Des analyses** pour automatiser en toute confiance la prévention et définir les priorités de votre activité
- **L'automatisation** pour combler le déficit de compétences en cybersécurité en transformant la détection des menaces en prévention, en s'adaptant aux environnements dynamiques grâce à des stratégies d'accès basées sur le contexte, et en accélérant la réponse grâce à l'analyse et au Machine Learning

ATTENTION

Les fournisseurs de services cloud avanceront que leur sécurité est meilleure que la vôtre (et c'est probablement le cas), mais les cybercriminels ne se soucient pas de l'endroit où se trouvent vos données. Ils n'ont qu'un objectif en tête : compromettre votre réseau, accéder à une cible (qu'il s'agisse de données, de propriété intellectuelle ou de ressources informatiques) et atteindre leur objectif final.

Pour minimiser les interruptions d'activité, les entreprises doivent protéger leurs actifs dans le cloud. Face aux attaques sophistiquées d'aujourd'hui, seule une sécurité d'entreprise avancée permet de prévenir les compromissions. Plus important encore, les capacités de sécurité doivent protéger l'ensemble de l'environnement informatique, dont les environnements multiclouds (clouds privés, IaaS, PaaS et SaaS), les data centers de l'organisation et les utilisateurs mobiles, à l'aide d'une approche cohérente et sans failles.

Exigences de sécurité IaaS et PaaS

De nombreuses entreprises passeront au cloud en suivant une méthodologie « lift and shift » qui déplace leurs applications d'entreprise directement vers l'IaaS en utilisant uniquement des composants fondamentaux – calcul, réseau et stockage. Au fil du temps, ces mêmes organisations ont commencé à créer des applications qui tirent parti de l'efficacité du cloud. Aujourd'hui, les applications consomment de multiples composants des services IaaS et PaaS (voir Figure 2-1). Les offres PaaS réduisent considérablement le temps de développement et permettent aux applications d'évoluer efficacement en fonction de la demande.

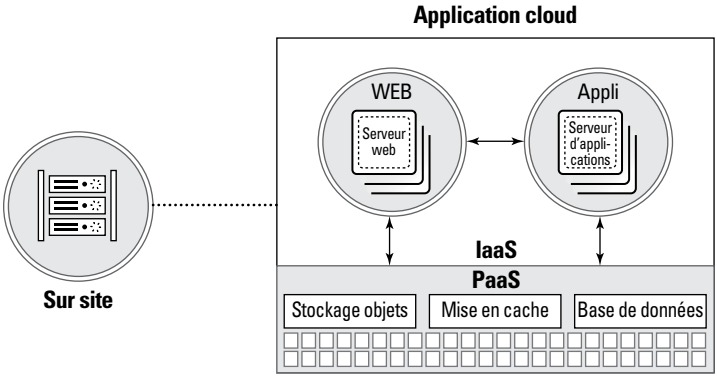

FIGURE 2-1 : Développement d'applications en IaaS et PaaS.

Pour assurer la sécurité à l'échelle de l'entreprise requise pour les applications dans les environnements IaaS et PaaS, une approche multidimensionnelle est nécessaire (voir Figure 2-2) :

- **En ligne :** protégez et segmentez les charges de travail cloud pour vous prémunir contre les menaces internes et externes. En étudiant les communications dans votre environnement cloud, vous bénéficiez d'une visibilité au niveau des applications sur le trafic nord-sud entrant et sortant de votre environnement cloud, ainsi que sur le trafic est-ouest entre les charges de travail. Les stratégies de segmentation garantissent des niveaux d'interaction appropriés entre les différentes charges de travail cloud, telles que les applications web et les charges de travail de base de données.
- **Utilisation d'une API (interface de programmation d'applications) :** assurez une découverte et une surveillance continues, des rapports de conformité et la sécurité des données. L'approche basée sur une API est transparente pour les développeurs et permet aux équipes de sécurité de découvrir et de surveiller les ressources et les actifs du cloud en cas d'activité suspecte, de sécuriser les services de stockage en empêchant les erreurs de configuration et de se conformer aux normes de l'industrie (telles que CSA CCM, ISO 27017/27018, PCI DSS et SOC 2), ainsi qu'aux réglementations (telles que le règlement général sur la protection des données [RGPD], l'HIPAA, la directive sur les réseaux et les systèmes d'information [NIS], la LPRPDE et la *loi Sarbanes–Oxley* [SOX]) avec des rapports et des contrôles personnalisables.
- **Utilisation d'un hôte :** sécurisez le système d'exploitation (OS) et les applications dans les charges de travail. Un agent hôte léger déployé dans l'instance cloud détecte les attaques zero-day et garantit

l'intégrité du système d'exploitation et des applications. Lorsque les cybercriminels découvrent des vulnérabilités, l'approche basée sur un agent permet de fournir une protection jusqu'à ce que les organisations soient en mesure de corriger les composants.

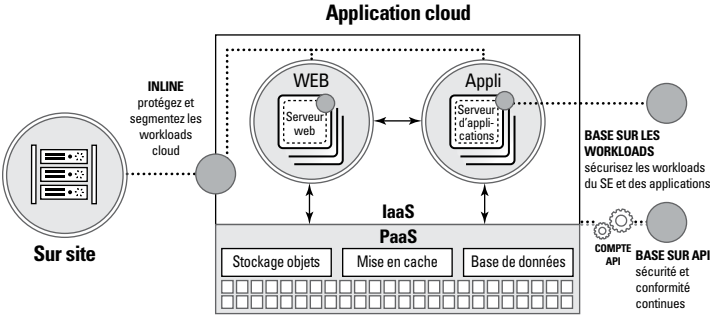

FIGURE 2-2 : Protections cloud essentielles pour les IaaS et PaaS.

Afin de garantir une approche de sécurité cohérente et infaillible dans l'ensemble de l'infrastructure multicloud, la sécurité doit intégrer l'automatisation dans le processus de développement. Les développeurs n'ont pas besoin d'être des experts en sécurité tant que des protections automatisées et cohérentes peuvent être ajoutées dans l'environnement. En outre, il est essentiel de comprendre que les exigences de sécurité pour l'IaaS et le PaaS doivent être satisfaites grâce à une approche de sécurité cohérente prenant en charge les applications et les données sur les trois principales plateformes de services cloud : Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Vous trouverez ci-dessous les modes de déploiement des fonctions CASB, ainsi que des recommandations supplémentaires pour garantir une sécurité complète de vos applications et données SaaS (voir Figure 2-3) :

- **Le déploiement en ligne** offre une visibilité sur l'utilisation des applications SaaS et une application granulaire et en temps réel des stratégies. En utilisant des services de sécurité basés sur le cloud ou des appareils matériels ou virtuels pour assurer une protection en ligne, vous pouvez comprendre comment vos utilisateurs se servent des services SaaS et élaborer des stratégies pour contrôler votre exposition aux risques en conséquence. Les stratégies peuvent également être appliquées lorsque des appareils non gérés accèdent à des applications SaaS autorisées. Cela permet d'éviter l'exfiltration de données sensibles dans toutes les applications cloud.

» **Le déploiement de l'API** fournit des protections plus approfondies pour les applications approuvées par l'entreprise et effectue plusieurs fonctions, y compris la prévention des fuites de données pour toutes les données au repos dans l'application ou le service cloud, ainsi que la surveillance continue de l'activité des utilisateurs et des configurations administratives.

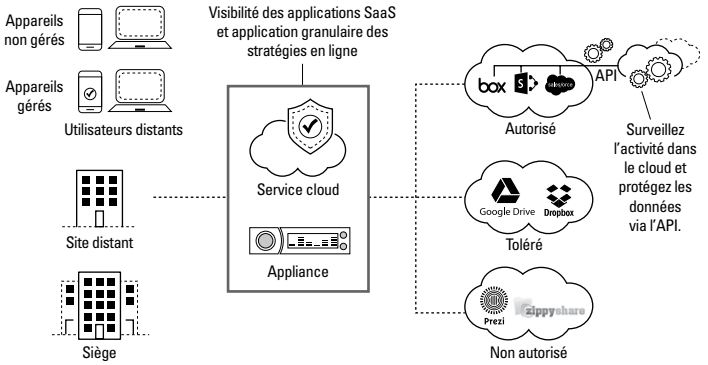

FIGURE 2-3 : Approches en matière de sécurité SaaS.

De la même manière que les composants IaaS et PaaS doivent être sécurisés, les applications SaaS (Box, Dropbox, GitHub, Google Drive, Office 365, Salesforce, etc.) doivent également être protégées par la mise en œuvre cohérente des stratégies, indépendamment de l'application et du fournisseur de services cloud.

Exigences en matière de sécurité multicloud

Les données et les applications d'entreprise sont désormais souvent réparties dans une multitude d'environnements cloud, privés et publics, couvrant l'IaaS, le PaaS et le SaaS.

Malgré cette tendance, plusieurs obstacles en ralentissent encore l'adoption, et la sécurité reste une préoccupation majeure. En outre, bien que les procédés de sécurité natifs du cloud public assurent un certain degré de contrôle d'accès et de gestion des identités, les compromissions sont souvent le résultat d'une utilisation inappropriée, de mauvaises configurations ou de menaces avancées. Pour accélérer en toute confiance le passage au cloud, il est nécessaire de mettre en place des protections cohérentes et automatisées dans le cadre de déploiements multiclouds, afin de prévenir les pertes de données et les interruptions d'activité.

Alors que les entreprises adoptent des architectures multiclouds, nombre d'entre elles continueront à prendre en charge des

applications sur site dans des data centers traditionnels ou des clouds privés. La protection de ces data centers, ainsi que des environnements multiclouds, nécessite une stratégie de sécurité globale et cohérente. Une sécurité cohérente est encore plus efficace lorsque les informations sur les menaces sont partagées au sein de l'infrastructure de sécurité.

ARCHITECTURES DE MICROSERVICES ET SÉCURITÉ DES CONTAINERS

Les architectures de microservices (abordées au chapitre 1) et les technologies de containers, comme Docker, Kubernetes et OpenShift, permettent, entre autres, de mettre en place de nouvelles architectures pour les applications héritées, les applications remaniées et les microservices. Les containers sont populaires parmi les équipes DevOps, car ils offrent une solution rapide et relativement simple pour déployer de nouvelles charges de travail d'application de manière autonome. En utilisant l'infrastructure en tant que code (IaC), les containers permettent la standardisation, la portabilité, l'efficacité et l'évolutivité des déploiements.

Cependant, ces nouvelles architectures d'application introduisent également de nouveaux vecteurs d'attaque, notamment des attaques du plan de contrôle contre l'orchestrateur, des attaques basées sur le réseau à travers l'infrastructure, des attaques du registre des containers et des attaques du système d'exploitation de l'hôte.

Les approches actuelles visant à sécuriser l'infrastructure des containers sont insuffisantes. Il s'agit notamment de la sécurité intégrée des containers qui est immature et inefficace, de produits ponctuels de sécurité des containers qui ont une portée limitée et ne répondent pas aux besoins de sécurité des applications hybrides utilisant des containers et des machines virtuelles, ainsi que des outils de sécurité réseau hérités qui annulent la valeur des containers.

Pour sécuriser correctement les environnements de containers, les entreprises doivent déployer des protections de réseau en ligne et une sécurité du système d'exploitation hôte, ainsi qu'une surveillance continue et des contrôles de conformité basés sur l'API. Ces outils de sécurité permettent de prévenir les compromissions, d'analyser les registres et d'orchestrer les protections pour l'assurance, l'évaluation et la surveillance des informations.

En plus de sécuriser vos environnements multiclouds, une plateforme de sécurité complète couvre également le réseau et les terminaux. Ces mécanismes de sécurité – qu'ils se trouvent dans les clouds, les

réseaux ou les terminaux – agissent comme des capteurs et des points d'application des règles. Ensemble, ils fournissent à votre entreprise l'intelligence collective nécessaire pour prévenir les cyberattaques.

Identifier les bonnes pratiques en matière de déploiement

Pour assurer une protection efficace aux entreprises qui utilisent le cloud et les applications « cloud native », il est primordial de comprendre les différentes couches qui composent leur pile cloud (voir Figure 2-4). Ces différentes couches (services, identité, périphérie des applications, équilibreur de charge, calcul et stockage) créent de multiples cibles potentielles. Pour les personnes compétentes, chacune d'entre elles représente un élément de l'environnement cloud qui peut être protégé contre les menaces.

En vous concentrant sur les différents éléments de la pile cloud et en vous attaquant aux menaces de sécurité qui leur sont propres, vous pouvez rendre votre environnement bien plus résistant face aux attaques de cybersécurité. Les bonnes pratiques suivantes vous aideront à sécuriser toutes les couches de votre pile.

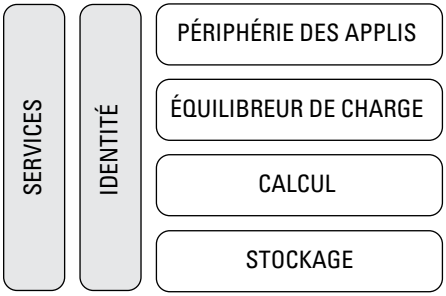

FIGURE 2-4 : Les couches de la pile cloud.

Verrouillez la gestion des identités

La gestion des identités et des accès détermine l'accès que vous avez aux différentes parties de la pile cloud ainsi que les actions que vous pouvez effectuer une fois que vous y êtes connecté. Si un acteur malveillant parvient à accéder à vos systèmes en utilisant vos informations d'identification, cela peut causer de graves problèmes de sécurité. Procédez donc ainsi :

- **Exigez des mots de passe sécurisés.** Utilisez un mot de passe ou une phrase secrète ayant une longueur maximale autorisée par le

système, ou un mot de passe complexe comprenant un mélange de lettres, de chiffres et de symboles.

- **Implémentez l'authentification multifacteur partout.** Aujourd'hui, il ne suffit plus d'avoir un mot de passe fort. Plusieurs couches de protection sont requises. L'utilisation d'une deuxième méthode de validation ou d'authentification fournit une couche de protection supplémentaire pour la connexion des utilisateurs.
- **Créez des rôles à moindre privilège.** Limitez l'accès des utilisateurs uniquement aux comptes et systèmes strictement nécessaires à leur productivité. Vous limiterez ainsi les dégâts en cas d'erreur ou d'accès au compte par un acteur mal intentionné. Ceci est particulièrement important pour les images de containers, car elles fournissent un chemin plus direct vers le noyau du système d'exploitation hôte. C'est pourquoi la procédure standard consiste à supprimer les privilèges le plus rapidement possible et à exécuter tous les microservices avec un utilisateur non root dans la mesure du possible. Lorsqu'un processus conteneurisé doit accéder au système de fichiers sous-jacent, il est alors conseillé de monter le système de fichiers en lecture seule.
- **Désactivez les comptes inactifs.** Lorsque des collaborateurs quittent votre organisation, désactivez immédiatement leur accès à tous les systèmes et leurs clés d'accès. Les comptes inactifs constituent une vulnérabilité supplémentaire pour les terminaux, et leur activité n'est généralement pas surveillée avec autant d'attention que celle des comptes actifs.
- **Surveillez les comportements suspects des utilisateurs ou les informations d'identification compromises.** Utilisez une surveillance en temps réel qui tire parti du Machine Learning et de l'analyse pour identifier les activités suspectes et les informations d'identification de compte éventuellement compromises.

Sécurisez la couche de calcul

Prenez des mesures pour sécuriser votre couche de calcul afin de garantir la disponibilité des systèmes et des données, et d'empêcher les acteurs malveillants d'utiliser votre puissance de calcul pour diffuser davantage de malwares dans votre entreprise et sur Internet. Procédez donc ainsi :

- **Renforcez la sécurité du système d'exploitation.** Supprimez les programmes inutiles qui ne font qu'élargir votre surface d'attaque. Restez à jour sur les packs de services et les correctifs autant que possible. Vous serez néanmoins toujours vulnérable à une attaque

zero-day, mais cela rend une telle attaque beaucoup moins probable.

- **Vérifiez en permanence les erreurs de configuration et les anomalies.** Utilisez des outils automatisés pour détecter les changements dans l'environnement, ainsi que les comportements anormaux.
- **Utilisez les connexions sécurisées.** Délivrez des clés SSH (Secure Shell) aux utilisateurs. Vos actifs seront ainsi protégés lorsqu'ils circuleront sur des réseaux non sécurisés.
- **Implémentez des règles de pare-feu pour le trafic entrant et sortant.** Établissez des règles précises relatives au contenu, au volume et aux personnes habilitées à envoyer et à recevoir des données entrantes et sortantes et à y accéder. De nombreuses organisations hésitent à établir des règles pour le trafic sortant. Cependant, étant donné que les cybercriminels tentent de voler (exfiltrer) vos données sensibles et votre propriété intellectuelle, il est crucial de définir explicitement de telles règles. Ces règles de pare-feu doivent être créées au niveau de l'application plutôt qu'au niveau du transport ou du réseau (informations sur l'adresse IP et le port) afin d'empêcher les attaquants de se servir des ports ouverts (notamment DNS sur le port 53).
- **N'utilisez que des images approuvées.** Créez vos propres images ou modèles ou obtenez-les auprès de sources fiables comme AWS ou Microsoft Azure. N'utilisez pas d'images provenant de Stack Overflow ou de forums de discussion et de communautés d'utilisateurs non fiables. Lorsque vous déployez une image inconnue ou non officielle, vous augmentez le risque d'exécuter un code vulnérable, compromis ou bogué dans votre environnement.

Sécurisez votre stockage

Si les données sont le nouvel or noir, il est impératif de garantir la protection de vos inestimables ressources. Si des attaquants accèdent à votre couche de stockage, ils peuvent potentiellement supprimer ou exposer des volumes entiers de données. Procédez donc ainsi :

- **Gérez l'accès aux données.** Les stratégies de gestion des accès et identités (IAM) et les listes de contrôle d'accès (ACL) vous permettent de centraliser le contrôle des autorisations d'accès à votre espace de stockage. Les stratégies de sécurité permettent d'accorder ou de refuser des autorisations selon le compte, l'utilisateur ou en fonction de critères spécifiques tels que la date, l'adresse IP, ou encore si la requête a été réalisée durant une session sécurisée grâce au protocole SSL (Secure Sockets Layer).

- **Classez les données.** Catégorisez automatiquement les données pour déterminer leur type ainsi que leur emplacement de stockage. Les stratégies de classification des données doivent être harmonisées avec les stratégies de sécurité, et toute infraction doit être signalée ou entraîner des actions correctives automatiques.
- **Chiffrez encore et toujours vos données.** Chiffrez vos données en transit et au repos. Notez que les métadonnées ne sont souvent pas chiffrées. Veillez donc à ne pas stocker d'informations sensibles dans les métadonnées de votre stockage cloud.
- **Activez le contrôle de version et la journalisation.** Le contrôle de version vous permet de conserver, de récupérer et de restaurer des données en cas de problème. Lorsque le contrôle de version est activé, vous pouvez toujours restaurer les données à partir d'une version plus ancienne si une menace ou une défaillance de l'application entraîne une perte de données. La maintenance des journaux d'accès fournit une piste d'audit au cas où quelqu'un ou quelque chose pénètre dans votre système.
- **N'autorisez pas les droits de suppression (ou exigez une authentification multifacteur pour la suppression).** Vous pouvez configurer des rôles dans votre infrastructure cloud qui ne permettent pas aux utilisateurs de supprimer des données. Dans de nombreuses solutions de stockage cloud, vous pouvez également activer une fonctionnalité qui exige une authentification multifacteur pour supprimer toute version des données stockées dans votre espace de stockage.
- **Vérifiez en permanence les erreurs de configuration et les anomalies.** Employez des outils automatisés afin d'identifier les configurations incorrectes des paramètres de stockage et d'autorisation, ainsi que les comportements inhabituels concernant l'accès aux fichiers.
- **Protégez vos services cloud.** Après avoir sécurisé le périmètre et appliqué des stratégies intelligentes, vous devez vous concentrer sur la sécurité spécifique de vos services dans le cloud. Utilisez le contrôle de code source pour sécuriser les versions, l'accès aux builds et les instances de déploiement. Vous réduirez ainsi la surface d'exposition de votre code et limiterez les possibilités d'attaques au sein de votre réseau.

DANS CE CHAPITRE

- **Explorer l'impact du cloud sur le RGPD, les NIS et d'autres réglementations**
- **Tirer parti de l'automatisation et de la surveillance continue pour contribuer à la conformité**
- **Comprendre comment les DevSecOps peuvent être utilisées pour implémenter ces stratégies au début du processus de développement**
- **Aller de l'avant avec une stratégie de conformité proactive**

Chapitre 3
La conformité réglementaire dans le cloud

Ce chapitre vous renseigne sur plusieurs lois relatives à la protection des données et à la cybersécurité applicables au cloud. Il explique la nécessité d'une surveillance automatisée et continue de la conformité et vous montre comment être proactif dans vos efforts de conformité.

S'orienter dans le paysage réglementaire

Le paysage réglementaire est en constante évolution, avec un nombre croissant de lois et de statuts juridiques à travers le monde imposant des exigences en matière de sécurité de l'information et de protection des données. Parallèlement aux réglementations et normes plus établies, telles que la *loi américaine sur la portabilité et la responsabilité en matière d'assurance maladie* (HIPAA), la *loi américaine sur la protection des données* (GLBA), les politiques de protection des données SWIFT, la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et la *loi canadienne sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), les lois et

réglementations récentes ont suscité beaucoup d'attention, notamment le règlement général sur la protection des données (RGPD) et la directive sur les systèmes d'information et de réseau (NIS) de l'Union européenne (UE 2016/1148) qui sont tous deux entrés en vigueur en 2018. Ces nouvelles lois, parmi d'autres, ont des implications importantes pour les organisations opérant dans le cloud.

RAPPEL

Les exigences de conformité sont généralement basées sur les bonnes pratiques en matière de sécurité de l'information, mais il importe de se souvenir que la sécurité et la conformité sont deux choses différentes. La sécurité consiste à protéger les actifs de l'entreprise contre les dommages ou l'exposition aux risques ; la conformité consiste à respecter les réglementations (et à éviter les amendes en cas de non-respect).

RGPD

Le RGPD s'applique aux entités qui contrôlent ou traitent les données personnelles des personnes situées dans l'Union européenne (UE). La loi définit les *données personnelles* de manière assez large comme toute information relative à une personne physique identifiée ou identifiable. En général, cela s'applique dans l'un des scénarios suivants :

- Les données identifient une personne ou peuvent être utilisées pour la contacter (par exemple, le nom, l'adresse électronique, la date de naissance, l'identifiant de l'utilisateur).
- Les données identifient un appareil unique (potentiellement) utilisé par une seule personne (par exemple, une adresse IP ou un identifiant d'appareil unique).
- Les données reflètent ou représentent le comportement ou l'activité d'une personne (par exemple, la localisation, les applications téléchargées, les sites web visités, etc.).

Le RGPD représente un changement fondamental pour la protection des données personnelles dans l'UE. Cette réglementation est nettement plus rigoureuse que les législations antérieures relatives à la protection des données, avec une portée élargie – y compris pour les entreprises basées hors de l'UE – ainsi que de nouvelles obligations en matière de signalement des compromissions de données et des amendes administratives conséquentes.

Le RGPD introduit également des obligations de notification pour les compromissions de données personnelles. Dans la majorité des cas, les autorités de contrôle doivent être informées si des données personnelles sont perdues, volées ou compromises d'une manière quelconque, sans retard excessif et, si possible, dans un délai

maximum de 72 heures après en avoir pris connaissance. Dans certains cas, les personnes concernées doivent également être informées. Les notifications doivent contenir un ensemble de détails concernant la compromission, tels que sa nature, les catégories et le nombre d'enregistrements de données personnelles concernés, les conséquences probables, ainsi que les mesures mises en œuvre pour y remédier et en atténuer les effets.

Le RGPD prévoit également des amendes administratives. Les conséquences de la non-conformité (qu'elle soit délibérée ou accidentelle) peuvent être lourdes : une amende maximale potentielle de 4 % du chiffre d'affaires annuel mondial (ou jusqu'à 20 000 000 d'euros, selon le montant le plus élevé) en cas de non-respect des obligations liées au traitement et à la gestion des données (telles que l'obtention du consentement ou diverses règles concernant les transferts de données vers des pays tiers) et de 2 % (ou jusqu'à 10 000 000 d'euros, selon le montant le plus élevé) pour les obligations relatives à la sécurité et à la notification des compromissions de données, entre autres.

Le risque pour la réputation en cas de compromission de données, ajouté à l'obligation de notification imposée par le RGPD, à la possibilité d'enquêtes menées par les régulateurs et aux importantes amendes administratives, a solidement élevé la protection des données personnelles au rang des préoccupations majeures des conseils d'administration.

ATTENTION

Afin de se conformer au RGPD, les entreprises devront vraisemblablement réaliser des investissements significatifs en termes de technologie et de personnel, ainsi que des ajustements de leurs processus métier. Le RGPD affectera divers groupes au sein d'une organisation, notamment le département juridique, le bureau de la protection de la vie privée, le responsable de la sécurité des systèmes d'information (RSSI), ainsi que les équipes commerciales et les ingénieurs produits, qui devront intégrer la protection de la vie privée dès la conception. La *protection de la vie privée* dès la conception implique que, dans l'architecture de l'application, du réseau ou du transport, l'organisation a mis en place des mesures pour assurer la confidentialité des données personnelles, quel que soit leur type.

À cette fin, l'organisation doit comprendre les risques liés à la collecte de ces informations et doter ses systèmes d'une sécurité appropriée. Cela représente un changement de mentalité pour de nombreuses organisations, car elles doivent désormais intégrer la sécurité dans leur processus de conception pour les architectures qui traitent tout type de comptes ou de données. La protection de la vie privée par défaut est un concept lié à la protection de la vie privée dès la

conception, dans la mesure où il prend en considération les informations collectées et la manière dont les organisations doivent s'efforcer de recueillir uniquement les données minimales requises et de limiter le plus possible le traitement de celles-ci.

La grande majorité des exigences du RGPD concernent la gestion des données, à savoir la collecte et le traitement des données. Des obligations de notification lors de la collecte de données personnelles, des interdictions de traitement non autorisé des données, des obligations de tenir des registres des activités de traitement des données, la nécessité de nommer un délégué à la protection des données (DPD) dans certaines situations, et des règles concernant le transfert de données personnelles à des tiers et à des pays tiers sont notamment en vigueur.

Mais cela ne doit pas faire oublier que la sécurité des données est également un pilier du RGPD. Le règlement contient des termes spécifiques à la sécurité, comme décrit dans le Tableau 3-1. De plus, un aspect essentiel de la protection des données personnelles réside dans leur sécurisation, tant contre l'exfiltration par des hackers que contre les fuites internes. Par conséquent, tandis que les organisations s'efforcent de se conformer au RGPD, il est crucial qu'elles associent les investissements dans les activités de conformité, les processus et les technologies de gestion de l'information à des investissements adéquats en matière de cybersécurité.

TABLEAU 3-1 **Résumé des dispositions pertinentes du RGPD**

Sujet	Résumé des dispositions
Sécurité du traitement des données	Les organisations doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque. Ces mesures doivent tenir compte de l'état des connaissances techniques. **[Article 32]** Les données à caractère personnel doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement. **[Considérant, paragraphe 39]** Lors de l'évaluation des risques liés à la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite. **[Considérant, paragraphe 83]**

Sujet	Résumé des dispositions
Notification de compromission de données	Les autorités de contrôle doivent être notifiées en cas de perte, de vol ou de compromission de données personnelles, à moins que la compromission en question ne soit pas susceptible d'engendrer un risque important pour la personne concernée. La notification de compromission doit être effectuée dans les meilleurs délais, et si possible 72 heures au plus tard après en avoir pris connaissance. Dans certains cas, les personnes concernées doivent être informées. Les notifications doivent inclure un certain nombre d'informations notamment la nature de la compromission, les catégories et le nombre d'enregistrements de données à caractère personnel concernés, les conséquences probables, les mesures prises pour y remédier et en atténuer les effets. **[Articles 33 et 34]**
Amendes administratives	Les autorités de contrôle peuvent imposer des amendes administratives pour les infractions au RGPD, au cas par cas. Lorsqu'elles décident d'imposer une amende et d'en fixer le montant, les autorités sont invitées à prendre en considération de nombreux facteurs, dont le degré de responsabilité dans la mise en œuvre des mesures techniques et organisationnelles, en tenant compte de l'état des connaissances techniques conformément à l'Article 32. **[Article 83]**

CONSEIL

Le RGPD exige des mesures de sécurité techniques et organisationnelles qui tiennent compte de l'état des connaissances techniques. Les systèmes de sécurité actuels, composés de solutions ponctuelles improvisées, se sont avérés insuffisants pour prévenir l'augmentation du volume, de l'automatisation et de la sophistication des cyberattaques. Les RSSI doivent examiner attentivement ces anciens produits pour déterminer s'ils répondent aux exigences du RGPD en matière d'état des connaissances techniques.

Directive NIS

La directive NIS est la première loi de l'UE spécifiquement axée sur la cybersécurité. Son objectif est d'améliorer les capacités de cybersécurité des infrastructures critiques de l'UE en établissant des obligations de sécurité et de notification des incidents pour diverses organisations qui offrent des services essentiels et numériques. La directive NIS exige également que les États membres adoptent des stratégies nationales de cybersécurité et s'engagent dans une coopération transfrontalière au sein de l'UE, entre autres mesures.

À ne pas confondre avec un règlement, la directive NIS fixe des objectifs et des politiques à atteindre par le biais d'une législation au niveau des États membres de l'UE dans un certain délai (un processus appelé *transposition*). Les États membres étaient tenus de transposer la directive NIS en droit national avant le 9 mai 2018.

La directive NIS exige que les opérateurs de services essentiels (OSE) et les fournisseurs de services numériques (FSN) utilisent des technologies de pointe pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information utilisés pour fournir les services couverts. Ces entités doivent également prendre les mesures appropriées pour prévenir et minimiser l'impact des incidents affectant la sécurité des réseaux et des systèmes d'information qui sont utilisés pour fournir des services essentiels ou numériques afin d'assurer la continuité de ces services. Les incidents de sécurité d'une certaine ampleur doivent également être signalés aux autorités nationales compétentes. Ces obligations s'appliquent que l'OSE ou le FSN gère son propre réseau et ses systèmes d'information ou qu'il les externalise vers le cloud public, par exemple.

Reconnaître l'importance d'une surveillance automatisée et continue

La sécurité et la conformité sont des responsabilités partagées dans le cloud public. De nombreuses organisations commettent l'erreur de croire que parce qu'un fournisseur de cloud public gère la sécurité et la conformité *du* cloud, il est également responsable de la sécurité et de la conformité *dans le* cloud. Ce n'est pas le cas. En fin de compte, il s'agit de vos données et, en cas de compromission ou de non-conformité, votre entreprise en portera la responsabilité. Le fournisseur de services cloud fournit un service ; la sécurité de vos workloads et de vos données relève de votre responsabilité en tant que consommateur du service. Ce sont vos revenus, votre réputation et vos relations avec vos clients qui sont en jeu.

Un modèle de sécurité cloud doit se concentrer sur la surveillance continue et la gestion des risques et des menaces liés à la sécurité dans le cloud. Dans le paysage moderne des menaces, il est absolument essentiel d'utiliser des outils modernes et des techniques d'automatisation pour s'assurer que l'organisation est consciente des vulnérabilités et qu'elle est prête à y remédier à tout moment. Les organisations doivent être capables de détecter et d'identifier rapidement les menaces en temps réel, d'évaluer leur gravité et de réagir immédiatement grâce à des stratégies, des processus et des contrôles automatisés. Les snapshots ponctuels de l'environnement ne suffisent plus à assurer la protection face à des menaces automatisées qui sont dynamiques et en constante évolution.

Les organisations doivent mesurer en permanence les résultats en matière de sécurité et de conformité et disposer de solides capacités de reporting. Pour atteindre cet état de conformité continue axée sur la

sécurité, il est nécessaire de disposer d'outils modernes et d'une plateforme de sécurité exploitant l'architecture centrée sur les API (interfaces de programmation d'applications) du cloud public.

En utilisant une plateforme qui permet une surveillance et une gestion continues de la sécurité dans le cloud, les équipes informatiques et de sécurité auront une plus grande confiance quant à la conformité de l'organisation à toutes les politiques et réglementations applicables dans les cadres requis.

Ce modèle permet aux organisations de :

- Compiler une vue complète et unifiée de tous les services cloud.
- Générer des rapports de conformité sans avoir besoin de connaissances spécialisées.
- Identifier les risques de conformité, les prioriser et y remédier dès qu'ils se présentent, grâce à l'automatisation pilotée par le machine learning et l'analytique – sans nécessiter d'interaction humaine.
- Contrôler la conformité tout au long du cycle de développement.
- Éviter les « grandes manœuvres de dernière minute » pour satisfaire aux exigences de conformité.
- Démontrer aux auditeurs que l'organisation gère la sécurité 24 heures sur 24, 7 jours sur 7 et 365 jours par an – et pas seulement dans les dernières semaines précédant un audit.

Les équipes chargées de la conformité et du développement des applications peuvent toutes deux bénéficier d'une surveillance continue et d'une automatisation de la conformité. La mise en conformité peut réduire considérablement le temps consacré aux audits de sécurité effectués par des tiers. Les équipes de développement d'applications ne seront pas entravées par des audits de conformité qui interrompent les projets de développement, ce qui permet à la vitesse d'innovation et de développement d'être un facteur de différenciation par rapport à la concurrence.

CONSEIL

Avec la bonne plateforme de sécurité dans le cloud, les entreprises peuvent tirer parti de l'automatisation pour réduire les risques et supprimer le facteur humain des processus vitaux. Cette automatisation leur permet d'obtenir une visibilité complète et continue sur tous les déploiements dans le cloud, avec à la clé des déploiements standardisés et cohérents entre les environnements d'utilisation tels que le développement, la préproduction et la production.

Éviter le piège du « rattrapage » en matière de conformité

Pour de nombreuses organisations, la conformité est un cycle sans fin d'audits, de mesures réactives pour corriger les écarts identifiés et d'une dégradation inévitable du niveau de conformité au fil du temps. Cette « voie sans issue » est source de frustration pour tous les membres de l'organisation et peut faire dérailler d'autres projets et initiatives en matière de sécurité. Les déploiements rapides et les changements fréquents dans le cloud rendent impossible et, pour être honnête, inutile, l'utilisation d'outils hérités et de processus manuels pour assurer la sécurité et la conformité des environnements cloud des organisations.

Heureusement, de nouveaux outils de sécurité dans le cloud sont désormais disponibles, avec une plateforme sans agent conçue spécifiquement pour les clouds publics et les environnements SaaS. Ces solutions s'appuient sur l'API du cloud pour bénéficier d'une grande souplesse dans l'évolution et la gestion de la sécurité et de la conformité dans le cloud.

Voici un bref résumé du fonctionnement d'une approche moderne et automatisée de la sécurité et de la conformité en continu dans le cloud :

1. **Surveillance.**

   L'environnement cloud évolue en permanence. Ces changements peuvent être des activités normales et routinières des équipes DevOps ou informatiques ; ils peuvent aussi être le fait de personnes souhaitant nuire à l'entreprise. Au fur et à mesure que des modifications sont apportées – dans l'ensemble des clouds, régions et services – la plateforme de sécurité dans le cloud surveille les configurations de l'infrastructure pour s'assurer qu'elle respecte les bonnes pratiques en matière de sécurité et de conformité.

2. **Évaluation.**

   La plateforme de sécurité collecte des données sur les services cloud de l'organisation de façon sécurisée et effectue des vérifications continues par rapport à une série de bonnes pratiques de sécurité et de directives de conformité prédéterminées. En outre, elle procède à des vérifications personnalisées basées sur des signatures prédéfinies. Ces contrôles

déterminent en permanence s'il existe des vulnérabilités potentiellement exploitables.

3. **Analyse approfondie.**

   La plateforme effectue une analyse pour déterminer si les erreurs de configuration et les expositions découvertes sont classées comme présentant un risque élevé, moyen ou faible.

4. **Résolution automatisée.**

   L'analyse qui en résulte est affichée sur un tableau de bord et des éléments prédéterminés peuvent être envoyés à des systèmes intégrés pour que des workflows d'autorésolution interviennent lorsque c'est possible et approprié.

5. **Rapports fiables.**

   Des rapports détaillés sont disponibles pour permettre aux équipes de consulter des informations sur les risques, y compris l'attribution des utilisateurs et l'affectation des ressources. Les rapports d'audit issus du reporting et du suivi sont également disponibles pour les efforts de mise en conformité.

Implémenter une approche proactive grâce aux DevSecOps

Le rôle des ingénieurs DevSecOps s'étend à l'ensemble de la pile informatique (soit la sécurité des réseaux, des serveurs, des hôtes, des containers, des clouds et des applications) et à l'ensemble du cycle de vie du développement de logiciels (développement et opérations). En matière de développement, l'accent est mis sur l'identification et la prévention des vulnérabilités. Dans les opérations, l'accent est mis sur la surveillance et la défense contre les attaques internes et externes, tout en maintenant la conformité. Afin de limiter le risque d'exposition dans ce dernier cas, il devient de plus en plus important d'intégrer des pratiques de sécurité dès le début du processus de développement.

Lorsqu'une organisation implémente un pipeline d'intégration continue/de livraison continue (CI/CD) dans son modèle de développement actuel pour la livraison d'applications, elle doit intégrer la sécurité et la conformité dans ce même pipeline. Chaque phase doit comprendre des tâches automatisées dédiées à la sécurité et à la conformité, ce qui oblige l'organisation à adopter des outils et des processus qui valident en permanence l'application au fur et à mesure que le code est écrit,

intégré, testé, déployé et, enfin, exploité. Ces outils de sécurité sont susceptibles de couvrir les éléments suivants :

- **Tests unitaires :** il s'agit de la première occasion de tester un morceau de code par rapport à ses fonctionnalités.
- **Analyse des dépendances :** chaque projet logiciel repose sur des bibliothèques, et celles-ci sont souvent externes au projet. L'analyse de ces dépendances pour détecter les vulnérabilités permet de s'assurer que les bibliothèques peuvent être utilisées en toute sécurité et de recommander de nouvelles versions de bibliothèques de logiciels sans vulnérabilités.
- **Tests dynamiques de sécurité des applications (DAST) :** dans cette phase, l'application est testée pour détecter les vulnérabilités sans analyser le code, technique également appelée *test de boîte noire*. Parmi les exemples, on peut citer les API, les injections SQL, les scripts intersites et d'autres méthodes externes qui envoient des paramètres d'entrée à l'application.
- **Tests statiques de sécurité des applications (SAST) :** les SAST se concentrent sur le code, ce qui permet de trouver des vulnérabilités plus tôt et au cours de la phase de développement, sans exécuter le code.
- **Scans de sécurité des containers :** même lorsque vous obtenez ou créez des images de containers à partir de sources fiables, il est essentiel de les analyser pour détecter les vulnérabilités, les malwares, ainsi que de procéder à d'autres mesures de sécurité, afin de s'assurer qu'aucune faille ne peut être exploitée en production.

Quatre façons d'améliorer la sécurité et la conformité dans le cloud

Le cloud nécessite une nouvelle approche en matière de sécurité. Les technologies et méthodologies traditionnelles de sécurité des data centers et des terminaux ne sont pas adaptées à la protection de l'architecture hautement connectée du cloud. Sans une approche moderne, axée sur le cloud, la sécurité sera compromise en raison d'une série de facteurs.

Les entreprises peuvent relever les défis liés aux risques inhérents en utilisant une plateforme de sécurité conçue pour le cloud qui tire parti de l'automatisation pour assurer la surveillance, l'analyse, la

prévention et la correction en continu de la sécurité dans le cloud et pour assurer la conformité.

Il s'agit d'un nouveau modèle qui offre une protection complète dans le cloud. Alors que les entreprises continuent de s'appuyer sur le cloud public pour mener leurs activités quotidiennes et innover, elles doivent réduire les risques de sécurité et simplifier les processus nécessaires pour assurer la protection et la conformité. La sécurité et la conformité continues offrent une nouvelle opportunité de maximiser la valeur du cloud public tout en minimisant les risques.

Les experts en sécurité recherchent des solutions innovantes et utilisables. Selon eux, il est important de se concentrer sur les quatre éléments clés suivants pour parvenir à une sécurité et à une conformité continues et automatisées dans le cloud :

- **Découverte rapide pour suivre la cadence des changements dans le cloud :** compte tenu de l'ampleur des déploiements dans le cloud, il n'est pas rare que les organisations disposent de millions de points de données (tels que le comportement des utilisateurs ou des applications et les paramètres de configuration des services cloud) à évaluer. Il s'agit donc de disposer d'une plateforme capable de traiter toutes les données en temps réel et d'isoler rapidement toute variation de sécurité ou tout écart par rapport aux états connus.
- **Un « écran unique » pour visualiser l'ensemble de votre environnement cloud :** lorsque les équipes sont très nombreuses, la communication peut en pâtir. Si chaque équipe utilise des outils différents pour visualiser l'environnement, les informations deviennent cloisonnées et difficiles à comprendre pour les autres équipes. Votre plateforme doit permettre aux équipes de s'approprier leur propre sécurité, tout en offrant une vue d'ensemble aux équipes chargées des opérations de sécurité et à la direction de l'entreprise. La plateforme doit être capable d'évaluer les données de sécurité de manière isolée, qu'il s'agisse d'une base de clients mondiale ou de l'évolution de la sécurité au fil du temps et de la géographie, pour signaler les problèmes potentiels avant qu'ils ne surviennent.
- **Réponse automatisée :** les organisations doivent automatiser non seulement la surveillance et l'analyse, mais aussi la correction des erreurs d'autorisation ou de configuration. Elles doivent disposer d'une certaine souplesse pour déterminer le déroulement de la réponse automatisée, avec la possibilité

d'informer les administrateurs humains si une autre action peut s'avérer nécessaire.

- **Rapports solides :** les équipes doivent être capables de mesurer et de démontrer les progrès réalisés en matière de sécurité et de conformité au quotidien, et pas seulement lors de l'audit annuel. Avec la bonne plateforme, vous pouvez montrer votre position en matière de sécurité et de conformité en appuyant sur un seul bouton.

DANS CE CHAPITRE

- Identifier les ressources et les compétences en matière de cybersécurité dont votre organisation a besoin
- Aligner les niveaux de maturité et d'automatisation du cloud
- Créer une culture de développement d'applications sécurisée

Chapitre 4
Bâtir une culture organisationnelle axée sur la sécurité

Ce chapitre examine les éléments clés de la création d'une équipe de cybersécurité efficace, la manière de tirer parti de l'automatisation pour renforcer cette équipe et la marche à suivre pour instaurer une culture de développement d'applications sécurisées au sein de votre organisation.

Gérer la cybersécurité à l'ère moderne

Protéger la sécurité des entreprises n'est pas une tâche facile, et la rapidité avec laquelle les entreprises évoluent pour innover et fournir des services numériques ne facilite pas la tâche. À cause des calendriers serrés et des délais de livraison, il est facile de négliger la discipline nécessaire pour assurer une sécurité efficace. Mais dans le monde hyperconnecté d'aujourd'hui et dans les environnements cloud qui évoluent rapidement, les entreprises ne peuvent tout simplement pas se permettre de laisser filer la sécurité, ne serait-ce qu'un instant. Pour réussir, elles doivent mettre en place les processus et la technologie – et surtout le personnel – nécessaires à la sécurisation adéquate des systèmes.

La cybersécurité ne se résume pas à la technologie nécessaire pour sécuriser l'environnement informatique d'une organisation. La culture de la cybersécurité dans une entreprise englobe l'attitude, les connaissances, les hypothèses, les normes et les valeurs de son personnel, et est influencée par les objectifs, la structure, les politiques, les processus et le leadership de l'organisation. Les personnes au sein de l'organisation sont l'outil le plus efficace pour répondre aux cyberattaques et aux menaces de sécurité. Il est donc essentiel de favoriser un environnement dans lequel les employés ont les connaissances et l'instinct nécessaires pour identifier les cybermenaces et y répondre immédiatement. Une culture axée sur la cybercompétence et la sécurité renforce la réputation d'une organisation auprès de ses clients tout en augmentant la fierté de ses employés.

Créer une équipe de cybersécurité efficace

La création d'une équipe de cybersécurité efficace commence par une évaluation des besoins de l'organisation. Cela implique notamment l'identification des équipes qu'il peut être nécessaire de créer (par exemple, des équipes de réponse aux incidents et d'audit de conformité), ainsi que des compétences requises pour chacune d'entre elles. Ensuite, identifiez les déficits de compétences au sein de votre équipe de cybersécurité actuelle et décidez si ces lacunes peuvent être comblées par des actions de formation. Si ce n'est pas le cas, vous devrez peut-être recruter.

CONSEIL

Lorsque vous évaluez les besoins de votre organisation en matière de cybersécurité, n'oubliez pas que l'automatisation aide à réagir plus rapidement aux incidents de sécurité en éliminant les tâches manuelles. L'automatisation permet aux membres de l'équipe en place de se consacrer à d'autres tâches à valeur ajoutée dans le domaine de la cybersécurité, tout en limitant la nécessité de recruter.

Planifier votre stratégie d'automatisation

L'automatisation peut contribuer à combler les lacunes en matière de cybertalents qualifiés sur le marché, afin de mettre en œuvre une cybersécurité efficace. Un récent projet de recherche mené conjointement par l'Enterprise Strategy Group (ESG) et l'Information Systems Security Association (ISSA) a révélé que 28 % des professionnels de la cybersécurité et des membres de l'ISSA estiment que leurs organisations dépendent d'un trop grand nombre de processus manuels pour leurs opérations de sécurité quotidiennes, comme la recherche et l'analyse des données, l'examen des alertes faussement positives ou la gestion des tâches de résolution. Cette situation est exacerbée par une pénurie imminente de professionnels qualifiés dans le domaine de la cybersécurité.

Il n'y a tout simplement pas assez d'heures dans la journée pour tout faire, quel que soit le niveau de compétence de votre équipe de cybersécurité. Grâce à l'automatisation, à l'analyse avancée et à l'intégration de la sécurité, vous pouvez commencer à combler ce fossé. Du point de vue du cyberdéfenseur, l'automatisation peut aider une organisation de trois manières :

- **Transformer la détection des menaces en prévention des menaces.** Les organisations ne doivent pas perdre de temps à prévenir manuellement les menaces connues, car la prévention devrait être automatique. Il en va de même pour les menaces inconnues : elles doivent être automatiquement analysées et bloquées si elles sont malveillantes.
- **S'adapter aux environnements dynamiques grâce à des stratégies d'accès basées sur le contexte.** Le paysage informatique est en constante évolution. Les équipes chargées de la sécurité doivent être en mesure de définir des stratégies en fonction de ce qui doit être protégé : utilisateurs, données et applications. Les politiques contextuelles résistent à l'épreuve du temps et s'adaptent aux changements de l'entreprise sans nécessiter de mises à jour constantes.
- **Automatiser les enquêtes à l'aide de l'analyse et du Machine Learning.** L'automatisation fournit un levier essentiel et donne aux organisations une longueur d'avance sur les attaquants grâce aux informations et au contexte des failles et des techniques. Avec des pare-feu de nouvelle génération capables d'ingérer des flux de données de tiers et de mettre à jour dynamiquement les stratégies, l'automatisation transforme l'information en prévention. Grâce à l'utilisation de données de sécurité enrichies, collectées sur l'ensemble des sites et des types de déploiement, l'analyse et le Machine Learning permettent de détecter les menaces cachées et de reconstituer les attaques. Ces deux possibilités d'automatisation permettent de gagner un temps précieux.

CONSEIL

Un fournisseur de solutions de sécurité qui propose l'automatisation vous redonne du temps pour effectuer des tâches plus utiles et plus stratégiques pour l'entreprise. Il permet à vos équipes chargées de la sécurité de se détacher des tâches opérationnelles de base et de se concentrer sur des efforts stratégiques qui profitent directement à, et améliorent la posture de sécurité et de conformité de votre organisation. Les équipes peuvent également se former aux concepts, outils et méthodes les plus récents en matière de sécurité et de déploiement d'applications.

Évaluer l'efficacité de la sécurité

Enfin, il est important de savoir à quoi ressemble le succès pour l'équipe. Des indicateurs clés de performance (KPI) doivent être définis pour l'aider à évaluer en permanence l'efficacité de la protection des actifs de l'entreprise dans le cloud. Voici quelques exemples de KPI :

- Nombre et types d'incidents de sécurité signalés
- Utilisation de logiciels en tant que service (SaaS), y compris les mauvaises configurations, le partage accidentel et le partage excessif
- Instances de clouds privés virtuels (VPC) mal sécurisés dans Amazon Web Services (AWS) et Google Cloud Platform (GCP), et de réseaux virtuels (VNets) dans Microsoft Azure
- Délai de détection des failles de sécurité
- Temps nécessaire pour remédier aux compromissions et aux incidents
- Vulnérabilités identifiées et corrigées
- Prévention des menaces

Comprendre comment la maturité du cloud affecte les niveaux d'automatisation

La maturité cloud de votre organisation (abordée au chapitre 1) est souvent liée au niveau d'automatisation mis en œuvre dans votre environnement. L'automatisation peut souvent être appliquée aux processus dans l'ensemble de l'organisation de la sécurité, et pas seulement dans le cloud. Les organisations qui utilisent largement l'automatisation dans leurs processus de cybersécurité comprennent à quel point elle est importante pour réduire les risques d'erreurs de configuration et permettre une réponse rapide en cas de détection de menaces.

Pour les entreprises intermédiaires et avancées qui adoptent le cloud, l'automatisation devient de plus en plus cruciale à mesure qu'elles intensifient leur utilisation du cloud, étendent leurs déploiements à plusieurs fournisseurs de cloud et optimisent leurs opérations dans le cloud. Grâce à l'automatisation, ces organisations peuvent faire évoluer leurs opérations de cybersécurité et réduire le risque d'erreur, et ainsi protéger l'ensemble de leur empreinte dans le cloud.

RAPPEL

L'automatisation contribue à sécuriser l'entreprise en :

- Créant des déploiements sans contact pour assurer la sécurité des équipes de développement d'applications.
- Protégeant l'environnement des menaces sans ralentir l'activité de l'entreprise.
- Signalant les services non conformes au fur et à mesure qu'ils sont créés.
- Mettant à jour dynamiquement des stratégies en fonction de l'évolution de l'environnement ou de la collecte de nouvelles informations sur les menaces.

Intégrer la sécurité dans le workflow des développeurs

Agir à la vitesse du cloud soulève l'inquiétude que des erreurs coûteuses puissent se produire. La crainte est qu'une organisation puisse compromettre sa sécurité lorsqu'elle automatise ses processus et prend des décisions rapides dans un environnement qui privilégie l'agilité. Différentes parties prenantes (telles que les équipes de développement d'applications et les différents groupes d'entreprises), qui ne sont pas forcément axées sur la sécurité au sens large, jouent désormais un rôle plus important dans le débat sur le cloud. Si la sécurité n'est pas correctement prise en compte, des conséquences inattendues peuvent s'ensuivre, telles que des failles de sécurité dues à une mauvaise configuration, le choix d'une sécurité « suffisante » ou l'abandon pur et simple des considérations de sécurité.

Pour aggraver les choses, les entreprises sont confrontées à une pénurie sans précédent de professionnels possédant des compétences en cybersécurité, en particulier des compétences qui sont essentielles lorsqu'il s'agit de sécuriser les organisations DevOps et les environnements cloud. Il suffit de voir à quel point cet écart s'est creusé ces dernières années : selon l'International Information System Security Certification Consortium ou ISC², le déficit de personnel dans le domaine de la cybersécurité a augmenté de 26,2 % en 2022 par rapport à l'année précédente, malgré l'arrivée de 464 000 professionnels dans le secteur.

Le cloud computing permet de simplifier certains domaines de la sécurité, mais il ne simplifie pas tout. Les entreprises restent responsables de la sécurité de leurs données, de leurs applications, de leurs systèmes d'exploitation, de leur réseau, de la configuration de

leurs pare-feu, etc. Et bien que les DevOps contribuent à accélérer le développement, il peut être difficile d'adapter les techniques de sécurité pour suivre le rythme des nouvelles capacités de développement et de déploiement d'applications.

Dans « 10 Things to Get Right for Successful DevSecOps » (10 choses à faire correctement pour une mise en œuvre réussie des DevSecOps), publié en octobre 2017, Gartner a écrit :

> Ne forcez pas les développeurs DevOps à adopter les anciens processus de la sécurité informatique. Prévoyez plutôt d'intégrer de manière transparente la garantie continue de sécurité dans la chaîne d'outils et les processus d'intégration et de développement continus (CI/CD) des développeurs.

Plus facile à dire qu'à faire, bien entendu. Cela nécessite certainement d'avoir la bonne technologie et les bons processus en place. À cette fin, vous devez à la fois constituer la bonne équipe et vous assurer que tous les membres de l'équipe jouent leur rôle. Les éléments stratégiques suivants permettront à une entreprise de former un cadre intelligent pour gérer une organisation DevSecOps (voir chapitre 2).

Formation continue et amélioration des compétences en matière de cybersécurité

Les équipes DevSecOps adhèrent aux bonnes pratiques de sécurité, mais la manière dont elles sont implémentées et la vitesse à laquelle elles sont utilisées doivent s'adapter à la vitesse et à l'agilité d'un environnement DevOps. Pour bien mettre en œuvre les éléments essentiels de la sécurité, l'ensemble de l'équipe DevOps doit en comprendre les principes fondamentaux, notamment les suivants :

- Gérer l'accès sécurisé aux environnements cloud
- Maintenir les configurations dans un état sécurisé
- Mettre en place des contrôles automatisés

Cet objectif est réalisable moyennant une formation polyvalente et un développement des compétences en matière de sécurité. Les organisations doivent former les équipes opérationnelles aux bonnes pratiques de sécurité, à l'utilisation des outils de sécurité appropriés et à la sécurisation des scripts. Il en va de même pour les développeurs, qui doivent être formés en permanence aux pratiques de codage sécurisé pour créer des champions de la sécurité au sein de l'équipe DevSecOps. Et surtout, les professionnels de la sécurité doivent être en contact et collaborer en permanence avec les autres équipes technologiques (par exemple, les équipes de développement et réseau).

RAPPEL

Pour former une équipe capable de sécuriser les systèmes au rythme rapide des DevOps, il est nécessaire de disposer d'un personnel collaboratif qui comprend les forces et les faiblesses de chacun, qui s'entraide pour compenser ces différences et qui suit une formation continue croisée.

La sécurité : de la conception à la production

Les efforts de sécurité doivent faire partie intégrante de l'ensemble du processus informatique, depuis la phase de conception d'un produit, d'une fonctionnalité ou d'une application jusqu'à sa mise en production, en passant par le développement et les tests d'application. Trop souvent, la sécurité est abordée pour la première fois au cours de la phase d'assurance qualité ou, pire, en production. Le maintien de la sécurité et de la conformité exige une surveillance continue et automatisée de la sécurité de tous les systèmes fonctionnant en production.

CONSEIL

L'intégration de processus de sécurité et de contrôles de sécurité intégrés dans les DevOps permet aux équipes de développement d'applications de disposer d'un modèle DevSecOps qui garantit que la sécurité est correctement prise en compte tout au long du cycle de développement de l'application.

Direction générale

Demandez à n'importe quel directeur des systèmes d'information (DSI) ou responsable de la sécurité des systèmes d'information (RSSI) ce qu'il faut faire pour constituer une équipe DevOps sensibilisée à la sécurité, et la réponse la plus fréquente – presque unanime – sera que le soutien de la direction est le facteur déterminant. Pour réussir à établir une organisation DevOps sécurisée, il est indispensable d'avoir un leadership capable de guider et d'inculquer une culture et des processus de sécurité.

Automatisation

Lorsqu'un processus peut être automatisé, il doit l'être. Grâce à l'automatisation, il est possible d'accomplir deux tâches essentielles axées sur la prévention :

- Intégrer la sécurité dans le processus de développement de votre application, en veillant à ce que la sécurité suive le rythme du développement.

- Ingérer des informations externes qui peuvent être utilisées pour piloter ou créer des stratégies qui sont mises à jour dynamiquement lorsque des workloads sont ajoutés ou supprimés de votre environnement cloud ou lorsque de nouvelles menaces potentiellement malveillantes sont découvertes.

Cultiver l'esprit de collaboration

L'esprit des DevOps consiste à briser les silos dans les départements informatiques en intégrant les développeurs, les équipes d'exploitation, la direction informatique, l'assurance qualité et la sécurité, et à faire de la sécurité une priorité dans tous les aspects du développement et de la gestion. Cependant, pour la plupart des entreprises, la sécurité a été plus perçue comme un obstacle que comme un outil.

La communication entre les responsables de la sécurité et toutes les autres équipes est essentielle pour que chaque collaborateur comprenne les rôles et les défis de chacun, et soit capable d'identifier les opportunités d'amélioration. La relation entre la sécurité et les autres équipes informatiques et de développement a toujours été la même, mais c'est particulièrement vrai pour les DevOps. La communication et l'empathie à l'égard des besoins des autres sont des facteurs de réussite essentiels.

Enfin, pour favoriser la collaboration en matière de sécurité, il convient de mettre en place les bonnes mesures d'incitation, par exemple en établissant des indicateurs de performance liés à la sécurité qui couvrent plusieurs équipes. Créez un environnement dans lequel les équipes de sécurité collaborent avec d'autres groupes et mettez en place des mesures incitatives pour maintenir cette collaboration.

Responsabilité en matière de sécurité

Il est crucial d'avoir un responsable qui dirige les efforts de sécurité afin que l'équipe DevOps et l'ensemble de l'organisation aient les mêmes objectifs lorsqu'il s'agit d'atténuer les risques métier. Les dirigeants doivent montrer activement qu'ils se soucient de la sécurité, et des conversations régulières, continues et complètes doivent avoir lieu à tous les niveaux de l'entreprise sur les programmes de sécurité qui doivent être mis en place. La meilleure façon d'y parvenir est de créer un poste de RSSI (Responsable de la sécurité des systèmes d'information), avec le soutien du conseil d'administration. L'engagement permet de créer un leadership compétent en matière de sécurité qui s'aligne sur les DevOps et assure la synchronisation des efforts de sécurité avec les besoins de l'entreprise.

DANS CE CHAPITRE

- L'évolution des menaces liées au cloud
- Analyser la tendance vers la consolidation des outils
- Regard sur l'avenir de la sécurité dans le cloud
- L'intelligence artificielle et le Machine Learning au service de l'automatisation
- Préparer l'avenir avec un plan de gestion des risques

Chapitre 5
Prévoir l'évolution de la sécurité dans le cloud et de la sécurité « cloud native »

Ce chapitre examine le paysage actuel des menaces dans le cloud et offre un aperçu de l'avenir du cloud computing et de la sécurité.

L'évolution des menaces liées au cloud

Bien que l'utilisation d'applications SaaS prolifère et que les workloads migrent de plus en plus vers l'IaaS, de nombreuses entreprises continuent d'avoir des applications, des systèmes de stockage et des clouds sur site. Cet environnement informatique hybride ne cesse de remettre en question les modèles de sécurité existants tout en créant une complexité supplémentaire, exposant les organisations à plusieurs risques :

- **Cloud jacking :** il s'agit généralement d'attaques par injection de code, effectuées via des bibliothèques tierces, par injection de code SQL ou par écriture de code intersite (XSS).

- **Phishing :** attaques visant à voler les informations d'identification de l'utilisateur pour les services cloud. Elles peuvent également conduire à des attaques locales. Les tentatives de phishing les plus innovantes sont lancées via des applications cloud, et non par e-mail comme cela se fait traditionnellement.
- **Vulnérabilités ou compromissions de l'API (interface de programmation d'applications) :** les attaques exploitant les API sont en train de devenir les menaces les plus courantes en matière de sécurité dans le cloud, mettant en danger la vie privée et les données des utilisateurs.
- **Exploitation des outils d'administration du système pour pénétrer dans les réseaux d'entreprise :** les cybercriminels continueront à utiliser ces outils pour exécuter des logiciels nuisibles sur les systèmes auxquels ils ont un accès direct ou qui sont accessibles dans le réseau désormais compromis.

Consolider les outils et l'importance de la CNAPP

L'approche des outils dispersés prend du temps à gérer, crée une surcharge inutile et des frictions entre la sécurité et le développement. Les équipes informatiques sont obligées de travailler en silos, ce qui peut entraîner des erreurs de configuration entre les outils, créant des vulnérabilités et ouvrant la voie à des attaques. Dans cet environnement, les entreprises ne sont pas en mesure de mettre en œuvre la sécurité dans le cloud et la sécurité « cloud native ». Conscients de cette lacune, les fournisseurs proposent désormais des outils convergents uniques dotés de multiples fonctions de sécurité adaptées aux applications et aux services. Ces outils réduisent les risques de sécurité, la surcharge et les coûts opérationnels.

La Cloud-Native Application Protection Platform (CNAPP) est une plateforme de sécurité dans le cloud qui réunit plusieurs fonctionnalités de sécurité et de conformité existantes. Initialement inventé par Gartner, le terme CNAPP fait référence à un nouveau type de plateforme de sécurité cloud axée sur la sécurisation des applications « cloud native », du développement à la production, tout en réduisant les frictions et en atténuant les risques qui résultent généralement du cloisonnement des outils.

De façon générale, la CNAPP incorpore trois éléments clés :

- **Gestion de la posture de sécurité dans le cloud (Cloud security posture management, CSPM) :** automatiser la détection et la correction des risques de sécurité par le biais d'évaluations de la sécurité et d'un contrôle de la conformité, et détecter les configurations erronées qui entraînent des compromissions de données.
- **Gestion des droits de l'infrastructure cloud (Cloud infrastructure entitlement management, CIEM) :** gérer l'accès et appliquer à le principe du moindre privilège dans le cloud en surveillant les identités cloud et en recommandant des stratégies.
- **Plateforme de protection des workloads cloud (Cloud workload protection platform, CWPP) :** protéger les workloads déployés dans les clouds publics, privés et hybrides. Intégrer des solutions de sécurité dès le début et de manière continue tout au long du cycle de développement de l'application.

Cependant, la CNAPP est bien plus que la combinaison de ces éléments. Elle est destinée à garantir :

- La visibilité claire des workloads et de l'infrastructure pour identifier et hiérarchiser les risques.
- L'amélioration de l'identification et de la correction des risques grâce à une approche cohérente du cycle de vie.
- Moins d'erreurs de configuration et la rationalisation de la gestion de tous les composants de votre environnement.
- Une surcharge et une complexité minimales dans la gestion des outils et des fournisseurs de logiciels et de matériel.
- L'intégration transparente des scans de sécurité dans le cycle de développement des logiciels et les outils de développement.
- L'adoption d'une approche « shift-left » (pour garantir la sécurité de l'application dès les premières étapes du cycle de développement).
- L'analyse des vecteurs d'attaque, telles que les autorisations et les configurations, et la gouvernance de cette analyse.
- Une sécurité « cloud native », et non une sécurité sur site adaptée pour le cloud.
- La sécurité des infrastructures et des applications.

CONSEIL

La CNAPP est une catégorie émergente, davantage considérée comme théorique que comme un outil doté de toutes les fonctionnalités convergées et déjà disponible sur le marché. Il n'empêche que les risques liés à la sécurité dans le cloud sont bien réels et tant que les fournisseurs ne proposeront pas ces fonctionnalités, il vous appartiendra de mettre en place la structure et les outils nécessaires pour lancer votre programme CNAPP en procédant comme suit :

- Créez un plan de sécurité dans le cloud.
- Recherchez des fournisseurs capables d'offrir une base solide pour le programme CNAPP et évaluez leurs offres.
- Analysez en permanence les artefacts, les containers, etc. pour identifier les vulnérabilités et les malwares.

Regard sur l'avenir de la sécurité dans le cloud

Selon le rapport sur l'état des lieux de la sécurité « cloud native » *(State of Cloud Native Security Report)* de Prisma Cloud, les workloads d'entreprise hébergés sur le cloud ont bondi en 2022 pour atteindre une moyenne de 59 % (contre 46 % en 2020). Ce document indique également que 69 % des 3 000 organisations interrogées hébergent désormais plus de la moitié de leurs workloads dans le cloud. Ce chiffre représente plus du double des 31 % interrogés en 2020.

Alors que les entreprises du monde entier continuent de migrer leurs applications stratégiques, leurs workloads et leurs données vers le cloud, les fournisseurs de services cloud (CSP) vont continuer à étendre rapidement l'empreinte de leurs data centers dans le monde entier. Les données, la propriété intellectuelle et les ressources informatiques – quel que soit leur emplacement – sont autant de cibles pour les cybercriminels.

L'objectif des hackers est d'accéder au réseau, d'atteindre leur cible, puis d'exécuter leurs objectifs d'attaque. Le cloud public, par la nature même de sa croissance et de sa visibilité, leur fournira un environnement riche en cibles dans un avenir proche. Les cybercriminels comprennent le modèle de partage des responsabilités (voir chapitre 1) aussi bien, voire mieux, que la plupart des clients du cloud. Ils continueront donc, pour la plupart, à suivre la voie de la moindre résistance. Ils chercheront à exploiter le maillon le plus faible de la chaîne de cybersécurité d'une organisation pour accéder à ses ressources cloud,

au lieu de tenter un assaut direct sur les principaux fournisseurs de cloud publics tels qu'Amazon, Google et Microsoft, qui investissent eux-mêmes massivement dans des ressources de sécurité dans le cloud.

L'automatisation est une tendance de la cybersécurité qui se poursuivra clairement à l'avenir pour la sécurité dans le cloud. La rapidité et l'ampleur des changements font qu'il est impossible pour les organisations de gérer efficacement leur cybersécurité dans le cloud avec des outils et des processus manuels. Les acteurs malveillants se servent de l'automatisation pour propager leurs malwares, s'emparer d'identifiants de comptes par force brute et utiliser d'autres techniques d'attaque. Les équipes de cybersécurité doivent réagir en utilisant leurs propres outils et techniques d'automatisation.

Les architectures des applications cloud continueront également d'évoluer avec des ressources de calcul pratiquement infinies, une adoption accrue des containers et des innovations en matière d'informatique sans serveur. Des lacs de données extrêmement vastes seront également nécessaires pour gérer le flot de données généré par l'Internet des objets (IoT), l'analyse de données à grande et petite échelle, le Machine Learning, et autres.

Ces tendances auront elles-mêmes des répercussions sur la sécurité, mais elles auront également un impact sur les technologies utilisées pour sécuriser les environnements multiclouds et sur site des entreprises. Par exemple, les capteurs de collecte de données déployés dans les clouds, chez les utilisateurs, sur les sites, dans les régions et sur les appareils permettront une visibilité toujours plus grande et une surveillance continue dans des environnements hétérogènes. Les données générées par ces capteurs pourront être hébergées dans un lac de données rassemblant les événements de sécurité et les menaces. Les fournisseurs de services de sécurité pourront alors s'en servir pour créer des applications ou des services visant à améliorer la posture de sécurité et de conformité de leurs clients.

Avec la maturation et l'avancée des technologies d'intelligence artificielle et de Machine Learning, l'automatisation deviendra de plus en plus stratégique dans des domaines tels que la détection des menaces et l'analyse de la sécurité, en particulier en raison du volume important de données provenant des capteurs et des informations sur les menaces. Les anomalies seront de plus en plus souvent détectées et stoppées en temps réel, ce qui réduira la marge de manœuvre des cybercriminels.

Élaborer un plan de gestion des risques

Lorsque votre organisation migre vers le cloud, non seulement votre risque de compromission change, mais votre risque de panne accidentelle augmente. Rien qu'en cliquant sur un bouton ou en utilisant une ligne de code erronée lors du déploiement d'une application, les développeurs peuvent mettre un système hors service. Pour lutter contre ce problème, vous devez mettre en place des protections qui réduiront les risques de sécurité et garantiront également la disponibilité des systèmes et des données stratégiques. Lorsque vous réorganisez vos systèmes et commencez à utiliser de nouvelles technologies et architectures telles que les containers et les microservices (ou tout ce qui suivra), réfléchissez à la manière dont vous testerez les systèmes pour vous assurer qu'ils fonctionnent comme prévu et produisent les résultats escomptés.

Vous devez adapter les frameworks existants de gestion des risques et de cybersécurité pour prendre en compte le cloud, ainsi que les nouvelles technologies en constante évolution. Le framework de cybersécurité du National Institute of Standards and Technology (NIST) est un outil idéal pour vous aider à démarrer. Les sections suivantes traitent des fonctions essentielles d'un tel framework et de la manière dont elles sont affectées par votre migration vers le cloud.

Identification

RAPPEL

Si les données sont le nouvel or noir, le Machine Learning est la nouvelle raffinerie qui les rend utilisables par vos équipes et vos systèmes. L'utilisation d'algorithmes pour découvrir et classer de grandes quantités de données est indispensable dans le cloud.

Alors que vous vous préparez pour l'avenir, passez en revue vos outils et compétences actuels pour vous assurer que votre équipe est en mesure de tirer parti des nouvelles avancées en matière de surveillance automatisée, de détection, de reporting et de Machine Learning. Les solutions traditionnelles de data center sont souvent incapables de faire face au volume élevé de données et à la rapidité des changements. Intégrez les scans de sécurité automatisés dans vos workflows DevSecOps, afin que l'analyse et les tests fassent partie intégrante de votre cycle de développement. Pour accélérer l'adoption, n'obligez pas les développeurs à apprendre de nouveaux outils. Au lieu de cela, recherchez des outils qui fonctionnent avec des API et fournissent un contexte enrichi.

Protection

Auparavant, une organisation ne devait protéger et défendre que ce qui se trouvait à l'intérieur du périmètre de son data center et de son réseau. Cependant, à mesure que les entreprises transfèrent de plus en plus de workloads vers des systèmes SaaS et le cloud, les périmètres réseau s'étendent de manière exponentielle et leurs limites s'estompent. Vous devez désormais assurer la protection à l'intérieur de votre réseau, dans plusieurs clouds et jusqu'à l'endroit où vos utilisateurs mobiles se connectent au réseau. Maintenant votre périmètre s'étend à l'échelle planétaire, vous avez besoin de moyens et d'outils différents pour le protéger. L'implémentation d'un modèle de sécurité Zero Trust (voir chapitre 6) donnera à votre organisation toutes les chances de réussir sa migration vers le cloud.

Détection

La pénurie de talents en cybersécurité n'épargne personne. Il devient donc impératif que les organisations de toutes tailles commencent à utiliser l'automatisation pour surveiller et analyser en permanence les événements et l'efficacité des contrôles et des protections déployés. N'oubliez pas que les services, les machines virtuelles et les configurations peuvent changer rapidement dans le cloud. En effet, il est possible que certains microservices n'existent dans votre environnement cloud que pendant quelques minutes. Vous devez vous assurer que les outils que vous utilisez pour détecter et enregistrer les changements peuvent suivre le rythme de ces fluctuations rapides.

CONSEIL

Les technologies cloud peuvent rendre la détection plus difficile sous certains aspects, mais elles peuvent également être utilisées à votre avantage. Envisagez d'utiliser des technologies et des services de sécurité dotés de techniques avancées pour détecter les problèmes, qu'il s'agisse de vulnérabilités ou d'attaques, dans vos réseaux et systèmes. Les technologies et les outils qui utilisent le Machine Learning pour résoudre des problèmes de sécurité bien définis (classification des données à des fins de conformité, analyse et corrélation des événements dans les fichiers journaux pour détecter les menaces internes, identification des malwares et des menaces avancées sur tous vos terminaux, etc.) n'en sont que quelques exemples.

Réponse

Lorsque les choses tournent mal, vous ne devez pas vous contenter d'arrêter l'attaque. Vous devez aussi savoir ce qui a été touché, comprendre quelles données ont été consultées, déterminer s'il y a infraction à vos obligations de conformité et connaître vos responsabilités en matière de signalement de l'incident.

Aujourd'hui, cette fonction est autant une réponse commerciale qu'une réponse technique. Les dirigeants d'entreprise doivent travailler en étroite collaboration avec les équipes IT et sécurité pour s'assurer que les projets sont exécutés avec un niveau de risque acceptable. Les plans de réponse doivent être portés à la connaissance du conseil d'administration et du Comex afin qu'ils soient prêts à faire face à un incident majeur qui affecterait l'entreprise. Les leçons tirées de la compromission des données d'Equifax ou de l'impact des compromissions de Yahoo! sur son rachat par Verizon rappellent clairement l'importance de la sécurité et des relations publiques dans l'évaluation et la viabilité à long terme d'une entreprise.

Dans le cadre de votre plan de réponse, vous pouvez utiliser des technologies avancées, telles que des outils de sécurité qui rationalisent l'orchestration de la Cyber Threat Intelligence (CTI) et l'application de contrôles préventifs. De nouveaux outils peuvent supprimer le travail manuel de collecte de CTI en vous donnant accès à des sources publiques, privées et commerciales mises à disposition par des acteurs publics et privés. Ils vous permettent également de partager vos indicateurs de menace avec des pairs de confiance afin de contribuer aux efforts de cyberdéfense au niveau mondial. Ces technologies unifient vos équipes opérationnelles, de sécurité et de gestion des risques par le biais d'un référentiel unique et centralisé (Single Source of Truth), réunissant les mêmes données de sécurité contextuelles provenant de vos systèmes.

Récupération

Pour vos efforts de récupération, il est important de disposer de suffisamment d'informations pour savoir comment l'attaque a pu se produire, puis prendre des mesures pour y remédier. Mais dans les environnements cloud, ce volume de données est énorme. Recherchez des outils qui vous fourniront une vue d'ensemble de tous vos journaux d'événements et de sécurité et qui normaliseront des types de données disparates. Vos équipes opérationnelles pourront ainsi établir un nouveau cadre de référence pour votre sécurité qui vous aidera à réévaluer vos risques existants et suggérer des améliorations possibles.

DANS CE CHAPITRE

- Envisager l'avenir des DevSecOps
- Adopter une approche centrée sur le cloud et connaître ses responsabilités
- Appliquer au cloud le principe de « ne jamais faire confiance, toujours vérifier »
- Impliquer les parties prenantes à un stade précoce
- Comprendre votre exposition potentielle et vos adversaires
- Évaluer vos options et reconnaître que savoir, c'est pouvoir
- Prévenir les menaces connues et inconnues dans les environnements IaaS et PaaS
- Tirer parti de l'automatisation

Chapitre 6
Dix recommandations (ou presque) en matière de sécurité dans le cloud

Ce chapitre souligne le rôle important que jouent les DevSecOps dans le data center du futur et présente quelques recommandations clés pour protéger les données et les applications dans le cloud.

Adoptez les DevSecOps

Aujourd'hui, les DevSecOps se concentrent sur l'implémentation de protocoles de gestion de la sécurité et des risques dans les workflows de développement, garantissant un code sécurisé et conforme dès le début du processus de développement. Dans les cinq prochaines années, il s'agira probablement de la façon standard dont les

organisations utiliseront les DevOps. Et grâce à l'automatisation, la sécurité continuera à intervenir plus en amont dans le cadre d'une approche « shift-left », avec un nombre croissant de contrôles de sécurité et de conformité intégrés dans le cycle de vie DevOps. Les DevOps et DevSecOps vont fusionner, partageant les mêmes philosophies.

La croissance se poursuivra dans l'espace du cloud public, laissant davantage d'organisations et leurs utilisateurs exposés à des risques. Les DevSecOps seront une condition essentielle pour opérer dans le monde numérique. Elles serviront de moteur à l'ensemble des organisations pour adopter leurs approches et leurs principes dans un cycle de développement plus sûr.

Plus nous intégrons précocement la sécurité dans le cycle de développement logiciel, plus il y a de chances que le terme *DevSecOps* disparaisse. L'aspect sécurité des DevOps ne disparaîtra pas, mais il sera normalisé dans le processus d'intégration continue/de livraison continue (CI/CD). Il ne sera plus nécessaire d'avoir un terme distinct mettant l'accent sur la « sécurité » dans les DevOps.

Adoptez une approche centrée sur le cloud

Le cloud permet à votre organisation de relever ses défis métiers avec une approche plus souple et plus évolutive. Pour en tirer pleinement parti, appliquez les concepts du data center moderne à votre architecture de déploiement cloud, tout en laissant de côté les structures traditionnelles. Votre organisation pourra ainsi bénéficier d'une haute disponibilité et d'une grande évolutivité de façon intrinsèque.

Comprenez le modèle de sécurité partagée

Les fournisseurs de clouds publics tels qu'Amazon Web Services (AWS), Google Cloud Platform (GCP) et Microsoft Azure indiquent clairement que la sécurité est une responsabilité partagée. Dans ce modèle, le fournisseur est chargé de veiller à ce que la plateforme soit toujours en service, disponible et à jour. En réalité, l'infrastructure du data center mondial des fournisseurs de services cloud (CSP) est souvent plus sécurisée que les datacenters de la plupart des organisations. Toutefois, c'est à vous, le client, qu'il incombe de protéger vos propres applications et données exécutées dans le cloud public.

La Figure 6-1 présente la répartition des responsabilités. Vous êtes totalement maître de la sécurité à mettre en œuvre et vous devez prendre des mesures pour protéger votre contenu, qu'il s'agisse de données clients ou de propriété intellectuelle. L'avantage du modèle de sécurité partagée est que votre équipe peut se concentrer sur la protection de vos applications et de vos données, à savoir le capital n°1 de nombreuses entreprises.

Responsabilité de la sécurité dans le cloud public

La sécurité dont vous êtes responsable	Les applications (système d'exploitation compris) et les données associées déployées
	Le contrôle des comptes (contrôle d'accès, services activés, etc.)
	Architecture de déploiement, gestion de la configuration, et ainsi de suite.
La sécurité relevant de la responsabilité du fournisseur	Infrastructure mondiale (présence régionale, etc.)
	Ressources physiques (bâtiments, matériel serveur, résilience, etc.)
	Infrastructure informatique (réseau, base de données, stockage, etc.)

FIGURE 6-1 : Modèle de partage des responsabilités pour les clouds publics.

Utilisez une stratégie Zero Trust

Lorsque vous signez un contrat avec un CSP ou un prestataire de services web, ce dernier accepte de vous fournir une gamme de services, mais il n'assume pas la responsabilité de la gestion de vos cyber-risques. À la place, le fournisseur vous propose un certain nombre d'options pour l'implémentation et la configuration de ses outils de sécurité.

Les stratégies de sécurité traditionnelles, centrées sur le périmètre, ne permettent pas d'offrir une visibilité, un contrôle et une protection adéquats du trafic des utilisateurs et des applications. Les architectures Zero Trust appliquent un principe qui consiste à « ne jamais faire confiance, toujours vérifier » à toutes les entités (utilisateurs, appareils, applications et paquets), indépendamment de leur nature *ou* de leur emplacement par rapport aux limites du réseau d'entreprise (voir Figure 6-2).

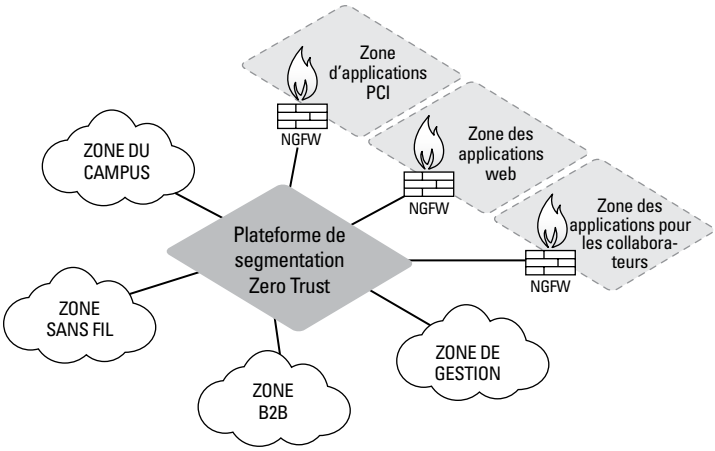

FIGURE 6-2 : Une plateforme de segmentation Zero Trust.

Lorsque les dirigeants étudient la possibilité de souscrire un contrat avec un CSP, ils doivent commencer à élaborer un modèle de sécurité pour protéger l'activité numérique. De plus, comme la plupart des entreprises utilisent plusieurs environnements cloud, elles doivent être en mesure de mettre en place et de superviser une stratégie qui englobe plusieurs plateformes dans plusieurs endroits, où les réglementations peuvent varier considérablement.

En établissant des zones Zero Trust – tout comme elles le feraient pour compartimenter les différents segments de leurs propres réseaux – les entreprises peuvent mieux protéger les données stratégiques hébergées dans le cloud contre les applications ou les utilisateurs non autorisés, réduire l'exposition des systèmes vulnérables et empêcher la propagation de malwares dans leur réseau.

Communiquez le plus tôt possible avec les fonctions métiers, la gouvernance et les DevOps

La plupart des projets cloud sont pilotés par des fonctions métiers et gérés par des équipes DevOps. La création rapide de produits ou de prototypes fonctionnels est monnaie courante et peut se faire en quelques heures seulement.

Dans de trop nombreux scénarios, l'équipe de sécurité est amenée à revoir l'architecture *après coup*, une fois que le workload est déjà en cours d'exécution dans le cloud. En intégrant la sécurité et la gouvernance plus tôt dans le processus, les décisions métiers et architecturales peuvent être prises dans le cadre d'une approche « security-first ». Cela permet de réduire considérablement la charge liée au maintien d'un environnement sécurisé et à la mise en conformité lorsqu'elle est nécessaire.

Déterminez votre exposition potentielle

L'utilisation des clouds publics est répandue en raison de la facilité avec laquelle il est possible d'obtenir des ressources de calcul et de stockage. Les employés qui font ce qui est « bon pour l'entreprise maintenant » plutôt que ce qui est « bon pour l'entreprise tout court » peuvent créer des failles de sécurité si l'environnement n'est pas configuré correctement. Il est impératif de savoir qui, au sein de votre organisation, utilise le cloud et de s'assurer que l'environnement est correctement configuré.

Pour réduire les risques liés au cloud, procédez comme suit :

- **Contrôlez l'utilisation du cloud.** Le moyen le plus rapide de déterminer l'utilisation est sans doute de regarder combien votre organisation dépense sur AWS, GCP et/ou Microsoft Azure.
- **Appliquez les bonnes pratiques de configuration.** Configurez l'environnement en tenant compte des bonnes pratiques de sécurité. Établissez des paramètres sécurisés par défaut pour l'accès aux identités et aux ressources, activez toutes les fonctionnalités d'audit et de journalisation de sécurité, et segmentez correctement les workloads dans des environnements dédiés. Vous disposerez ainsi d'une base de référence sécurisée pour mettre en œuvre des configurations spécifiques aux workloads en question.
- **Exigez une authentification multifacteur.** Afin de minimiser le risque d'accès malveillant au moyen d'identifiants volées, l'authentification multifacteur devrait être obligatoire. L'utilisation de mécanismes intelligents de réponse à des défis peut également protéger les applications dans le cloud contre tout accès non autorisé.
- **Verrouillez les interfaces administratives.** Par exemple, Secure Shell (SSH) sur le port 22 est une méthode privilégiée pour gérer les serveurs cloud. Or, ce port est souvent laissé

exposé dans les environnements AWS, GCP et Microsoft Azure pour des raisons de commodité, ce qui peut entraîner des vulnérabilités de sécurité. Les autres ports administratifs – y compris ceux des systèmes de gestion des containers, des consoles d'administration des applications et d'autres interfaces similaires – doivent être strictement contrôlés et protégés.

Mettez-vous dans la peau des cybercriminels

Les attaquants s'appuient sur l'automatisation pour trouver des cibles potentielles en quelques minutes. Après avoir identifié ces cibles, ils recherchent des faiblesses, en vérifiant les mots de passe par défaut, ou encore en sondant les mauvaises configurations SSH, etc. Afin de montrer les effets dévastateurs de l'automatisation des attaques, Palo Alto Networks a créé un environnement de test dans le cloud public, comprenant une base de données et un serveur web. L'environnement a été sondé dans plus de 35 pays avec plus de 25 applications malveillantes différentes. Lors de ses recherches, Palo Alto Networks a mené une analyse globale exhaustive des serveurs AWS, GCP et Azure qui a duré 23 minutes et a permis de détecter des dizaines de milliers de systèmes exposés. Contrairement à un data center privé, où l'on se préoccupe moins de l'exposition publique, les ressources du cloud public sont largement exposées et doivent être manipulées avec précaution.

Évaluez vos options en matière de sécurité et de conformité

Plusieurs options de sécurité peuvent être choisies lors du passage au cloud, dont la plupart sont proches de celles des réseaux physiques, notamment les suivantes :

- **Services de sécurité natifs :** les fournisseurs de services cloud (CSP) offrent des services de sécurité natifs, notamment des groupes de sécurité, des pare-feu d'applications web (WAF), le suivi des configurations… Ces outils constituent un bon point de départ pour ceux qui ne disposent pas de technologies de sécurité supplémentaires, mais ils doivent être complétés par des offres de sécurité professionnelles. Les deux exemples suivants illustrent la nécessité de disposer d'outils de sécurité tiers.

- Les groupes de sécurité et les pare-feu basés sur les ports sont essentiellement des listes de contrôle d'accès basées sur les ports, offrant des capacités de filtrage. Ils ne peuvent pas identifier les applications en fonction de leur contenu, et vous ne serez pas en mesure de prévenir les menaces ni, plus important encore, d'empêcher l'exfiltration de données, comme le fait un pare-feu nouvelle génération (NGFW).
- Les pare-feu d'applications web sont limités, car ils ne peuvent protéger que les applications HTTP (Hypertext Transfer Protocol) et HTTPS (Hypertext Transfer Protocol Secure). Cela signifie qu'ils ne peuvent pas protéger les applications qui utilisent un large éventail de ports pour fonctionner correctement. En outre, ils ne constituent pas un moyen efficace d'identifier et de contrôler les outils de gestion ou d'accès à distance, tels que SSH ou Microsoft Remote Desktop Protocol (RDP).

» **Produits spécialisés :** les organisations qui utilisent des produits spécialisés, conçus pour résoudre un cas d'usage particulier, finissent par déployer de nombreux produits provenant de différents fournisseurs. Ainsi, l'utilisation d'un ensemble fragmenté d'outils de sécurité qui ne s'intègrent pas et ne communiquent pas entre eux crée une complexité supplémentaire. De plus, leur fonctionnement et leur gestion requièrent des compétences spécialisées. L'automatisation devient difficile, voire impossible, à réaliser.

» **Sécurité « maison » :** certaines entreprises choisissent une approche « maison » pour sécuriser les workload cloud, en utilisant des scripts personnalisés et des projets open-source pour protéger les déploiements. Les inconvénients de cette stratégie sont notamment la charge que représentent l'amélioration et le déploiement d'outils personnalisés, le manque d'expertise pour gérer l'implémentation et les opérations de sécurité, et l'absence de soutien en cas de compromission de la sécurité.

ATTENTION

Les organisations qui comptent sur leurs équipes internes pour gérer les déploiements cloud et la sécurité doivent être prêtes à faire face à un surmenage et un turnover élevés. En général, seuls quelques ingénieurs ont une connaissance approfondie de l'environnement, mais ils ne disposent pas forcément du temps nécessaire pour maintenir une documentation adéquate ni pour gérer les exigences de partage des connaissances.

» Plateformes de sécurité : l'objectif de nombreuses organisations est de se débarrasser de leur approche fragmentée dans

laquelle les outils de sécurité ne communiquent pas entre eux pour prévenir les attaques. Pour relever ce défi, elles se tournent généralement vers une approche par plateforme. Cette approche garantit la sécurité grâce à des technologies de protection inline, basées sur une API et sur un hôte, qui collaborent entre elles pour minimiser les possibilités d'attaque :

- Sécurisez le trafic inline pour implémenter des protections entrantes et sortantes, une segmentation des workload et des capacités de prévention des menaces.
- Surveillez et protégez les ressources des clouds publics via les API des fournisseurs de services cloud. Ces ressources doivent faire l'objet d'un suivi continu plutôt que de contrôles ponctuels.

Protégez l'intégrité du système d'exploitation et des applications sur les workloads virtuels en bloquant les exploits, les ransomwares, les malwares et les attaques sans fichier.

Utilisez les connaissances à votre disposition

John Antonios, consultant en marque personnelle, a dit un jour : « Le savoir plus l'action, c'est le pouvoir. » Dans le domaine de la sécurité du cloud, les connaissances commencent par l'ingestion de grands ensembles de données produites par le cloud, le réseau et les terminaux. L'action consiste à analyser les données et à identifier les menaces qui doivent être prises en compte pour protéger votre cloud.

Les outils de sécurité doivent pouvoir partager ces informations sur les menaces avec d'autres parties du cloud, des points de contrôle, ainsi qu'avec l'écosystème IT de l'entreprise au sens large. Ensuite, pour contribuer à la lutte contre les attaques de grande envergure et assurer la détection future d'attaques similaires, l'organisation doit partager ces informations avec l'ensemble de la communauté et du secteur de la sécurité. Les hackers devront alors développer de nouveaux outils, acquérir de nouvelles infrastructures ou mettre au point des techniques d'attaque différentes de celles déjà exposées. Ces changements nécessitent du temps, de l'argent et d'autres ressources, ce qui augmente le coût de l'attaque. Lorsque vous élaborez votre stratégie de sécurité dans le cloud pour votre environnement, assurez-vous que vos outils de sécurité sont capables de partager des données de Cyber Threat Intelligence (CTI) dans l'ensemble de votre entreprise et de recevoir des données CTI de sources externes.

Pour accélérer l'adoption du cloud sécurisé, consultez des experts en sécurité cloud via des communautés ou des fournisseurs. En suivant ces conseils, vous serez en mesure d'établir des bases solides en matière de sécurité pour votre entreprise, ce qui vous permettra de travailler efficacement dans le cloud.

Croyez en la prévention

Certains pensent que les hackers ont déjà « gagné » et choisissent donc de se concentrer principalement sur une approche de détection et de remédiation. Or, si vous vous contentez de seulement réagir, vous aurez toujours un temps de retard. L'adoption de principes de prévention est essentielle pour faire face aux menaces de manière proactive. Une prévention efficace, c'est une réduction du nombre de réponse aux incidents grâce à une neutralisation précoce des attaques sophistiquées, avant que les cybercriminels ne puissent accéder à des données confidentielles. La prévention des cyberattaques dans le cloud nécessite quatre fonctionnalités essentielles :

- **Fournir une visibilité complète.** La combinaison du savoir et de l'action est un outil de sécurité puissant. Il est essentiel d'identifier toutes vos ressources cloud, vos activités cloud en cours, le risque relatif lié aux mesures de sécurité actuelles et tout changement apporté à votre environnement. Grâce à ces connaissances, vous pouvez déployer une stratégie de sécurité plus cohérente à l'échelle mondiale afin de protéger votre cloud contre les attaques connues ou non.

CONSEIL

- Les outils et techniques de sécurité conçus pour les data centers traditionnels doivent évoluer pour s'adapter aux spécificités du cloud. Pour avoir une vision complète, assurez-vous que vos outils de sécurité vous donnent une visibilité totale sur les ressources IaaS, PaaS et SaaS.
- **Réduire les possibilités d'attaque.** L'utilisation d'une approche de sécurité Zero Trust (ne jamais faire confiance, toujours vérifier) et de l'identité des applications comme moyen d'appliquer un modèle de sécurité positif réduit les possibilités d'attaque en n'autorisant que les applications approuvées et en refusant toutes les autres. Vous pouvez aligner l'utilisation des applications sur les besoins de l'entreprise, contrôler les fonctions des applications et empêcher les menaces d'accéder à votre infrastructure cloud et réseau et de s'y déplacer latéralement.

- **Prévenir les menaces connues.** L'exploitation d'une Threat Intelligence partagée à l'échelle mondiale pour appliquer des stratégies de prévention est une étape clé dans l'adhésion aux principes de prévention. Ces stratégies de prévention peuvent bloquer les menaces connues, y compris les exploits de vulnérabilités, les malwares et le trafic de commande et de contrôle (CnC) généré par ces derniers.
- **Prévenir les menaces inconnues.** Les fichiers inconnus et potentiellement malveillants doivent être analysés en fonction de centaines de comportements. Si un système détermine qu'un fichier est malveillant, il déploie rapidement et automatiquement un mécanisme de prévention. L'organisation peut ensuite utiliser les informations obtenues grâce à l'analyse des fichiers pour améliorer continuellement toutes les autres capacités de prévention.

Sécurisez les IaaS et PaaS

Les équipes de développement et les administrateurs cloud sont chargés de veiller à la sécurité de leurs données et de leurs applications, comme le prévoit le modèle de partage des responsabilités. Voici quelques mesures spécifiques à prendre pour remplir votre part du contrat :

- **Désactivez les clés d'accès à l'API du compte root.** L'*utilisateur root* est l'identifiant de connexion que vous avez utilisé pour créer votre compte cloud. Les bonnes pratiques recommandent de n'utiliser l'utilisateur root que pour créer vos comptes administratifs initiaux. Vous devez ensuite effectuer toutes les opérations d'administration par l'intermédiaire de comptes de gestion des accès et identités (IAM) nouvellement créés.
- **Activez les jetons d'authentification multifacteur partout.** L'authentification multifacteur doit être exigée de tous les utilisateurs, tant à l'intérieur qu'à l'extérieur de votre organisation.
- **Suivez le principe du moindre privilège.** C'est l'informaticien Jerry Saltzer qui l'a le mieux décrit : « Chaque programme et chaque utilisateur du système doit fonctionner avec le minimum de privilèges nécessaires pour effectuer ses tâches. »
- **Réduisez le nombre d'utilisateurs disposant de droits d'administration.** Plus l'accès à vos comptes cloud est granulaire, plus vous protégez votre entreprise en cas de compromission.

- **Modifiez régulièrement toutes les clés.** Les informations d'identification, les mots de passe et les clés d'accès à l'API doivent tous faire l'objet d'une rotation régulière. Si des informations d'identification sont compromises, cela limite la durée de validité de la clé.
- **N'activez aucune autorisation 0.0.0.0/0 à moins que vous ne le vouliez vraiment.** Autoriser le trafic à partir d'une adresse 0.0.0.0/0 signifie que chaque machine, où qu'elle soit, peut établir une connexion avec vos ressources cloud – et cela signifie également que vos systèmes peuvent établir des connexions sortantes avec tous les systèmes, où qu'ils soient. Utilisez plutôt des groupes de sécurité et des listes de contrôle d'accès au réseau pour limiter le trafic entrant et sortant.
- **Activez la journalisation partout.** Trop souvent, l'enregistrement des activités dans les environnements cloud est désactivé ou n'est jamais activé. Sans journaux, comment savoir si votre environnement a été infiltré ?

CONSEIL

- Du point de vue du développeur de logiciels, en rédigeant le code d'une application, veillez à ce qu'il y ait suffisamment de routines de journalisation pertinentes et claires pour isoler davantage les erreurs d'application, exposant potentiellement les risques de sécurité, lorsqu'elles sont exécutées en production.
- **Activez le chiffrement.** Assurez-vous que vos données sont chiffrées dès le départ. Il est beaucoup plus difficile de revenir en arrière et de trier les données pour essayer de les rechiffrer après coup. Tout comme l'activation du service lui-même, le chiffrement permet de sécuriser vos données.

Utilisez l'automatisation pour éliminer les goulets d'étranglement

L'automatisation est un principe central du cloud public, où les changements rapides sont constants. Lorsqu'une organisation suit de bonnes pratiques de sécurité en matière de contrôle des changements, les retards dans le processus peuvent engendrer des frictions, ralentir les déploiements et, pire encore, affaiblir la sécurité si le déploiement est effectué avant la mise en place du contrôle des modifications.

Voici deux ensembles d'outils d'automatisation qui peuvent aider les entreprises à éliminer les frictions liées à la sécurité et à bénéficier de la flexibilité et de l'agilité offertes par le cloud public :

- Des systèmes de déploiement automatisés et des frameworks d'orchestration qui permettent de déployer l'infrastructure de sécurité « en tant que code » (IaC) de manière transparente et zero-touch
- Des outils d'automatisation qui utilisent la surveillance continue, l'analyse des données et l'application des politiques de sécurité pour répondre plus rapidement à l'évolution constante du paysage des menaces

Élaborez une stratégie de sécurité « code to cloud »

Les entreprises migrent rapidement leurs applications et données stratégiques vers le cloud, tout en adoptant de plus en plus une stratégie multicloud. L'un des avantages de la migration des applications vers le cloud est la rapidité de livraison et d'innovation. Cependant, les outils, stratégies et processus de sécurité d'ancienne génération, conçus pour les data centers et les opérations informatiques traditionnels, ne peuvent pas s'adapter aux applications SaaS ni au modèle de déploiement continu et au rythme du changement dans le cloud. Dans cet ouvrage, vous apprendrez à bien gérer les risques inhérents au cloud, sans ralentir le déploiement grâce à une approche cohérente de la sécurité et de la conformité qui couvre toutes les étapes du cycle de vie des applications cloud (code, build, déploiement et exécution).

À l'intérieur…

- Consolider les outils avec une CNAPP
- Intégrer la sécurité dans le workflow des développeurs
- Comprendre le modèle de partage des responsabilités
- Trouver les conditions nécessaires à l'élaboration d'une stratégie de sécurité multicloud
- Élaborer un plan de gestion des risques

PRISMA® CLOUD
BY PALO ALTO NETWORKS

Lawrence Miller travaille depuis plus de 25 ans dans le domaine des technologies de l'information dans différentes industries. **Petros Koutoupis** est développeur de logiciels et travaille dans le secteur du stockage de données depuis près de 20 ans.

Allez sur Dummies.com®
pour voir des vidéos, des tutoriels visuels, des articles pratiques ou pour faire des achats !

ISBN: 978-1-119-89825-2

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.