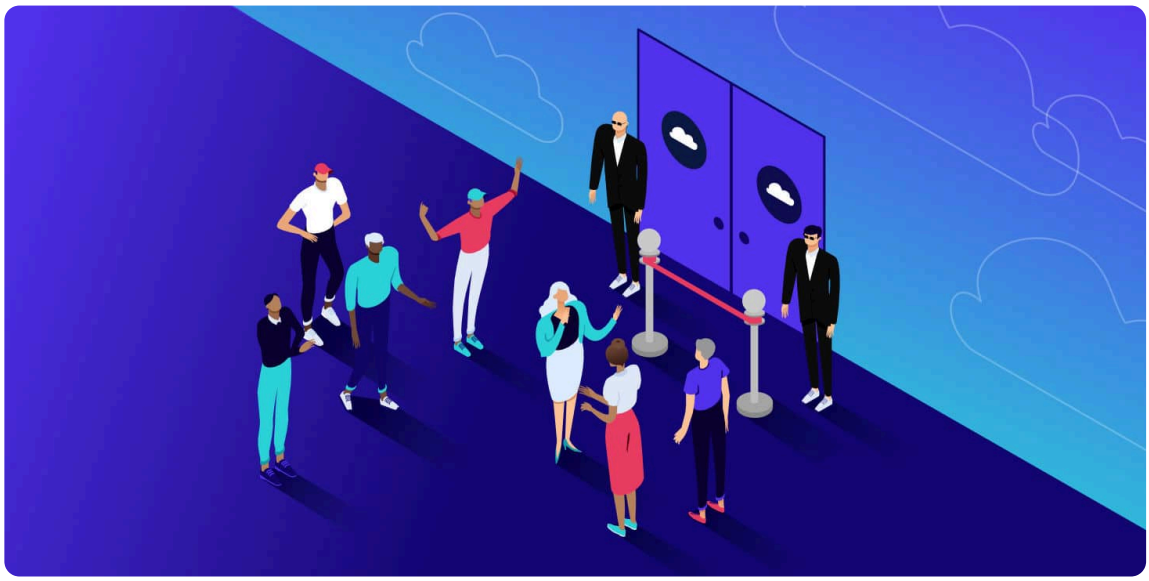
Blog

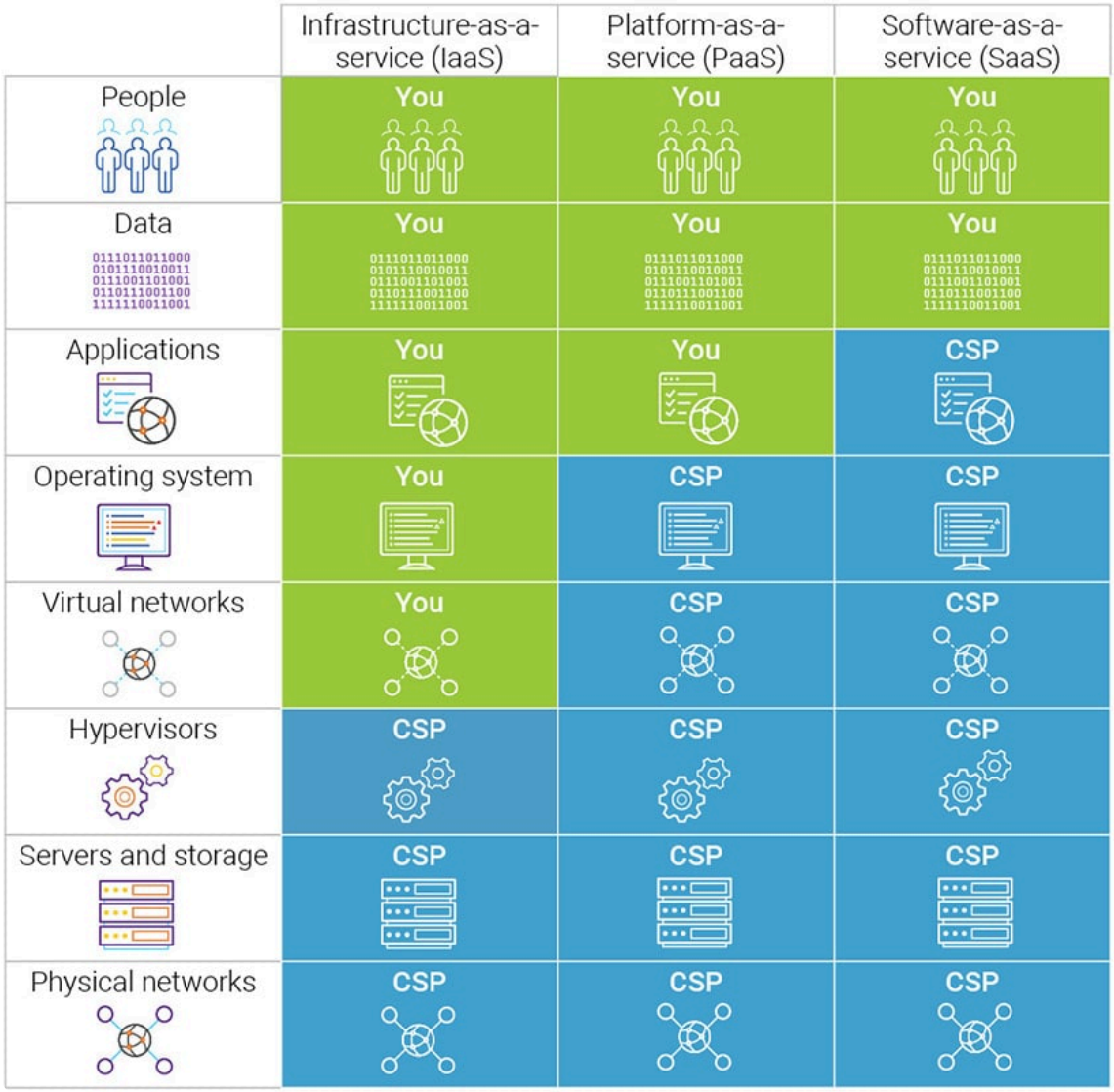
Un guide complet sur la sécurité du Cloud en 2024 (risques, meilleures pratiques, certifications)

Edward Jones | Publié: 10 mars 2020 | Mis à jour: 7 novembre 2022



La sécurité du Cloud englobe les technologies, les contrôles, les processus et les politiques qui se combinent pour protéger vos systèmes, données et infrastructures basés sur le Cloud. Il s'agit d'un sous-domaine de la sécurité informatique et, plus largement, de la sécurité de l'information.

Il s'agit d'une responsabilité partagée entre vous et votre fournisseur de services de Cloud. Vous mettez en œuvre une stratégie de sécurité dans le Cloud pour protéger vos données, respecter la conformité réglementaire et protéger la vie privée de vos clients. Celle-ci vous protège à son tour contre les conséquences financières, juridiques et sur la réputation des violations et des pertes de données.



– Modèle de responsabilité partagée pour la sécurité du Cloud (Source de l'image : Synopsys)

La sécurité dans le Cloud est une exigence essentielle pour toutes les organisations. Surtout avec les dernières études de l'ISC2 indiquant que 93 % des organisations sont modérément ou extrêmement préoccupées par la sécurité dans le Cloud, et qu'une organisation sur quatre a confirmé un incident de sécurité dans le Cloud au cours des 12 derniers mois.

Dans cet article, nous allons créer un guide complet sur la sécurité dans le Cloud. Vous explorerez les risques de sécurité liés au passage au Cloud, comprendrez pourquoi la sécurité du Cloud est nécessaire et découvrirez les meilleures pratiques en matière de sécurité du Cloud. Nous aborderons également des sujets tels que la manière d'évaluer la sécurité d'un fournisseur de services dans le Cloud et d'identifier les certifications et la formation nécessaires pour améliorer votre sécurité dans le Cloud.

Commençons.

Table des matières

- Comment fonctionne la sécurité dans le Cloud ?
- 7 Risques de sécurité du cloud computing
- Pourquoi la sécurité du Cloud est nécessaire
- Meilleures pratiques pour la sécurité du Cloud
- Les dix principales recommandations de la liste de contrôle de sécurité pour les clients du Cloud
- Qu'est-ce que la Cloud Security Alliance ?
- Qu'est-ce que le Kaspersky Security Cloud ?
- Qu'est-ce qu'un courtier en sécurité pour l'accès au Cloud (CASB) ?
- Un aperçu des 10 meilleures certifications de sécurité dans le Cloud en 2024

Comment fonctionne la sécurité dans le Cloud ?

La sécurité dans le Cloud est une interaction complexe de technologies, de contrôles, de processus et de politiques. Une pratique qui est hautement personnalisée en fonction des exigences uniques de votre organisation.

Il n'existe donc pas d'explication unique qui englobe le « fonctionnement » de la sécurité dans le Cloud.

– A Model for Securing Cloud Workloads (Image source: HyTrust)

Heureusement, il existe un ensemble de stratégies et d'outils largement établis que vous pouvez utiliser pour mettre en place une solide sécurité dans le Cloud, notamment

Gestion des identités et des accès

Toutes les entreprises doivent disposer d'un système de gestion des identités et des accès (IAM) pour contrôler l'accès aux informations. Votre fournisseur de cloud computing s'intégrera directement à votre IAM ou proposera son propre système intégré. Un IAM combine des politiques d'authentification et d'accès des utilisateurs à plusieurs facteurs, vous aidant à contrôler qui a accès à vos applications et à vos données, ce à quoi ils peuvent accéder et ce qu'ils peuvent faire à vos données.

Sécurité physique

La sécurité physique est un autre pilier de la sécurité dans le Cloud. Il s'agit d'une combinaison de mesures visant à empêcher l'accès direct et la perturbation du matériel hébergé dans le centre de données de votre fournisseur de cloud computing. La sécurité physique comprend le contrôle de l'accès direct par des portes de sécurité, une alimentation électrique ininterrompue, la vidéo en circuit fermé, des alarmes, le filtrage de l'air et des particules, la protection contre les incendies, etc.

Renseignement, surveillance et prévention des menaces

Le renseignement sur les menaces, les systèmes de détection d'intrusion (IDS), et les systèmes de prévention des intrusions (IPS) constituent l'épine dorsale de la sécurité dans le Cloud. Les outils de renseignement sur les menaces et les IDS offrent des fonctionnalités pour identifier les attaquants qui ciblent actuellement vos systèmes ou qui constitueront une menace future. Les outils IPS mettent en œuvre des fonctionnalités permettant d'atténuer une attaque et de vous avertir de sa survenance afin que vous puissiez également y répondre.

Cryptage

En utilisant la technologie du Cloud, vous envoyez des données vers et depuis la plateforme du fournisseur de Cloud, souvent en les stockant dans leur infrastructure. Le cryptage est une autre couche de la sécurité dans le Cloud pour protéger vos données, en les encodant lorsqu'elles sont au repos et en transit. Cela garantit que les données sont quasiment impossibles à déchiffrer sans une clé de décryptage à laquelle vous seul avez accès.

Test de vulnérabilité et de pénétration du Cloud

Une autre pratique pour maintenir et améliorer la sécurité dans le Cloud est des tests de vulnérabilité et de pénétration. Ces pratiques impliquent que vous - ou votre fournisseur - attaquiez votre propre infrastructure de Cloud afin d'identifier toute faiblesse ou exploitation potentielle. Vous pouvez ensuite mettre en œuvre des solutions pour corriger ces vulnérabilités et améliorer votre position en matière de sécurité.

Micro-Segmentation

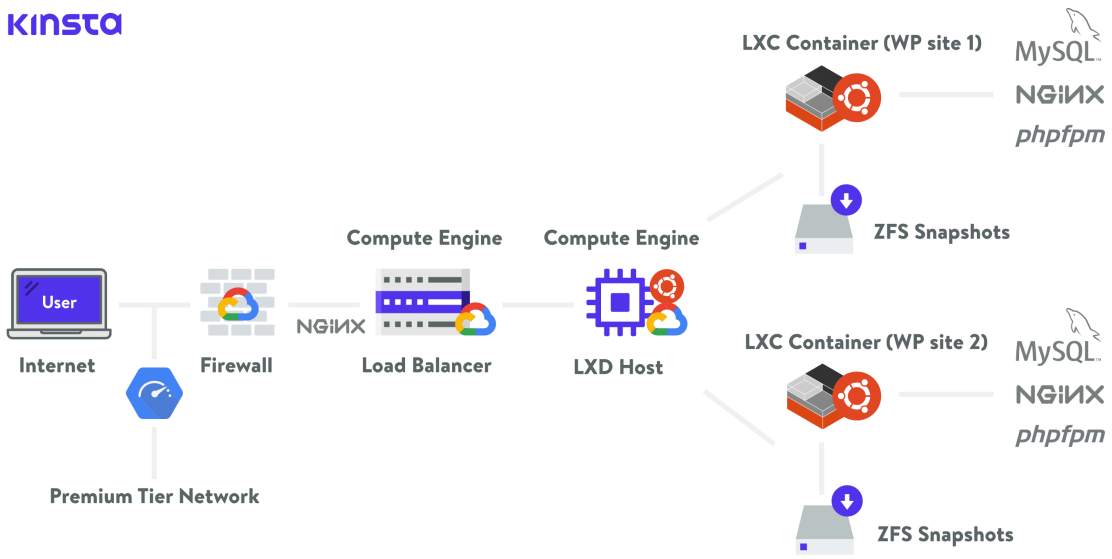
La micro-segmentation est de plus en plus courante dans la mise en œuvre de la sécurité dans le Cloud. Il s'agit de la pratique consistant à diviser votre déploiement dans le Cloud en segments de sécurité distincts, jusqu'au niveau de la charge de travail individuelle.

En isolant les charges de travail individuelles, vous pouvez appliquer des politiques de sécurité flexibles pour minimiser les dommages qu'un attaquant pourrait causer, s'il y avait accès.

Pare-feu de nouvelle génération

Les pare-feu de nouvelle génération sont une autre pièce du puzzle de la sécurité dans le Cloud. Ils protègent vos charges de travail en utilisant les fonctionnalités traditionnelles des pare-feux et des fonctionnalités avancées plus récentes. La protection traditionnelle du pare-feu comprend le filtrage de paquets, l'inspection d'état, le proxy, le blocage d'IP, le blocage de noms de domaine et le blocage de ports.

Les pare-feu de nouvelle génération ajoutent un système de prévention des intrusions, une inspection approfondie des paquets, un contrôle des applications et une analyse du trafic crypté pour assurer une détection et une prévention complètes des menaces.



– Architecture d'hébergement de Kinsta

Ici, chez Kinsta, nous sécurisons tous les sites derrière le pare-feu de la plateforme Google Cloud (GCP). Offrant une protection de pointe et la possibilité de s'intégrer plus étroitement aux autres solutions de sécurité GCP.

7 Risques de sécurité du cloud computing

Que vous opériez ou non dans le Cloud, la sécurité est une préoccupation pour toutes les entreprises. Vous serez confronté à des risques tels que le déni de service, les logiciels malveillants, L'injection SQL, les violations de données et les pertes de données. Tous ces éléments peuvent avoir un impact significatif sur la réputation et les résultats de votre entreprise.

Lorsque vous passez au Cloud, vous introduisez un nouvel ensemble de risques et changez la nature des autres. **Cela ne signifie pas que le cloud computing n'est pas sécurisée**. En fait, de nombreux fournisseurs de cloud computing offrent un accès à des outils et des ressources de sécurité très sophistiqués auxquels vous ne pourriez pas accéder autrement.

Cela signifie simplement que vous devez être conscient de l'évolution des risques afin de les atténuer. Examinons donc les risques de sécurité propres au cloud computing.

- Perte de visibilité
- Violations de conformité
- Absence de stratégie et d'architecture de sécurité du Cloud
- Menaces d'initiés
- Violations contractuelles
- Interface utilisateur d'application non sécurisée (API)
- Mauvaise configuration des services de Cloud

1. Perte de visibilité

La plupart des entreprises accèdent à une gamme de services de Cloud par l'intermédiaire de plusieurs appareils, services et géographies. Ce type de complexité dans une installation de cloud computing - sans les outils

appropriés en place - peut vous faire perdre la visibilité de l'accès à votre infrastructure.

Sans les processus appropriés en place, vous pouvez perdre de vue qui utilise vos services en ligne. Y compris les données auxquelles ils accèdent, qu'ils téléversent et téléchargent.

Si vous ne pouvez pas le voir, vous ne pouvez pas le protéger. Ce qui augmente le risque de violation et de perte de données.

2. Violations de conformité

Avec l'augmentation du contrôle réglementaire, vous devrez probablement respecter une série d'exigences de conformité strictes. En passant au Cloud, vous introduisez le risque des violations de conformité si vous ne faites pas attention.

Nombre de ces réglementations exigent que votre entreprise sache où se trouvent vos données, qui y a accès, comment elles sont traitées et comment elles sont protégées. D'autres réglementations exigent que votre fournisseur de services de Cloud détienne certaines références de conformité.

Un transfert négligent de données vers le cloud, ou un transfert vers le mauvais fournisseur, peut mettre votre organisation dans un état de non-conformité. Cela peut avoir de graves répercussions juridiques et financières.

3. Absence de stratégie et d'architecture de sécurité du Cloud

Il s'agit d'un risque de sécurité dans le Cloud que vous pouvez facilement éviter, mais que beaucoup n'ont pas. Dans leur hâte de migrer les systèmes et les données vers le cloud, de nombreuses organisations deviennent opérationnelles bien avant que les systèmes et les stratégies de sécurité ne soient en place pour protéger leur infrastructure.

Ici, chez Kinsta, nous comprenons l'importance d'un état d'esprit axé sur la sécurité lors du passage au cloud. C'est pourquoi Kinsta fournit des migrations WordPress gratuites pour assurer que votre transition vers le cloud est à la fois sécurisée et évite les temps d'arrêt prolongés.

Veillez à mettre en place une stratégie et une infrastructure de sécurité conçues pour que le cloud soit aligné avec vos systèmes et vos données.

4. Menaces d'initiés

Vos employés, entrepreneurs et partenaires commerciaux de confiance peuvent constituer certains de vos plus grands risques en matière de sécurité. Ces menaces internes ne doivent pas nécessairement avoir une intention malveillante pour causer des dommages à votre entreprise. En fait, la majorité des incidents d'initiés sont dus à un manque de formation ou à une négligence.

Bien que vous soyez actuellement confronté à ce problème, le passage au cloud change le risque. Vous contrôlez vos données à votre fournisseur de services de Cloud et introduisez une nouvelle couche de menace interne de la part des employés du fournisseur.

5. Violations contractuelles

Tout partenariat contractuel que vous aurez établi comportera des restrictions sur l'utilisation des données partagées, leur stockage et les personnes autorisées à y accéder. Vos employés qui déplacent involontairement des données restreintes dans un service de Cloud sans autorisation pourraient créer une rupture de contrat qui pourrait entraîner des poursuites judiciaires.

Assurez-vous de lire les conditions générales de vos fournisseurs de services de Cloud. Même si vous avez l'autorisation de transférer des données vers le cloud, certains fournisseurs de services incluent le droit de partager toute donnée téléversée dans leur infrastructure. Par ignorance, vous pourriez involontairement violer un accord de non-divulgation.

6. Interface utilisateur d'application non sécurisée (API)

Lorsque vous utilisez des systèmes d'exploitation dans une infrastructure de Cloud, vous pouvez utiliser une API pour mettre en œuvre le contrôle. Toute API intégrée dans vos applications web ou mobiles peut offrir un accès en interne au personnel ou en externe aux consommateurs.

Ce sont les API orientées vers l'extérieur qui peuvent introduire un risque de sécurité dans le Cloud. Toute API externe non sécurisée est une passerelle offrant un accès non autorisé aux cybercriminels qui cherchent à voler des données et à manipuler des services.

L'exemple le plus marquant d'une API externe non sécurisée est le Scandale de Cambridge Analytica de Facebook. L'API externe non sécurisée de Facebook a permis à Cambridge Analytica d'accéder aux données des utilisateurs de Facebook.

7. Mauvaise configuration des services de Cloud

La mauvaise configuration des services de Cloud est un autre risque potentiel pour la sécurité du Cloud. Avec la gamme et la complexité croissantes des services, ce problème prend de l'ampleur. Une mauvaise configuration des services de Cloud peut entraîner l'exposition publique, la manipulation ou même la suppression de données.

Parmi les causes communes, citons la conservation des réglages de sécurité et de gestion de l'accès par défaut pour les données hautement sensibles. D'autres incluent une gestion d'accès mal adaptée donnant accès à des personnes non autorisées, et un accès aux données mutilées où les données confidentielles sont laissées ouvertes sans autorisation.

Pourquoi la sécurité du Cloud est nécessaire

L'adoption massive de la technologie de Cloud, combinée à un volume et à une sophistication toujours plus grands des cyber-menaces, est à l'origine du besoin de sécurité dans le Cloud. Si l'on réfléchit aux risques de sécurité liés à l'adoption de la technologie dans le Cloud - décrits ci-dessus - l'incapacité à les atténuer peut avoir des conséquences importantes.

Mais tout n'est pas négatif, la sécurité dans le Cloud peut aussi offrir des avantages importants. Examinons pourquoi la sécurité dans le Cloud est une exigence essentielle.

- Les menaces pour la cybersécurité continuent de s'accroître

- Prévention des violations et des pertes de données
- Éviter les violations de conformité
- Maintenir la continuité des activités
- Avantages de la sécurité dans le Cloud
- Choisir un fournisseur de confiance

Les menaces pour la cybersécurité continuent de s'accroître

L'une des forces motrices des pratiques sécurisées dans le Cloud est la menace toujours croissante des cybercriminels, tant en volume qu'en sophistication. Pour quantifier cette menace, un rapport sur la sécurité du cloud de l'ISC2 a révélé que 28 % des entreprises ont connu un incident de sécurité du cloud en 2019. Avec le gouvernement britannique signalant également que 32 % des entreprises britanniques ont subi une attaque sur les systèmes au cours des 12 derniers mois.

Prévention des violations et des pertes de données

Une conséquence de ces cyber-menaces accrues est l'accélération de la fréquence et du volume des violations et des pertes de données. Rien qu'au cours des six premiers mois de 2019, le rapport sur les menaces émergentes de Norton a souligné que plus de 4 milliards d'enregistrements ont été violés.

Une perte ou une violation de données peut avoir des implications juridiques, financières et de réputation importantes. IBM estime maintenant le coût moyen d'une violation de données à 3,92 millions de dollars US dans son dernier rapport.

Éviter les violations de conformité

Nous avons déjà mentionné comment la sécurité dans le Cloud comporte le risque de violations de la conformité. Pour démontrer les implications de la non-conformité, il suffit d'observer l'organisme fédéral allemand de surveillance de la vie privée qui a récemment infligé à 1&1 Telecommunications une amende de 9,55 millions d'euros pour violation du règlement général de l'UE sur la protection des données (RGPD).

Maintenir la continuité des activités

Une bonne sécurité dans le Cloud contribue à maintenir la continuité de vos activités. La protection contre les menaces telles que les attaques par déni de service (DDoS). Les interruptions de service imprévues et les temps d'arrêt du système interrompent la continuité de vos activités et ont une incidence sur vos résultats. Une étude de Gartner estime ce temps d'arrêt à une moyenne de 5 600 $ américains par minute.

Avantages de la sécurité dans le Cloud

Au-delà de la protection contre les menaces et de l'évitement des conséquences de mauvaises pratiques, la sécurité dans le Cloud offre des avantages qui en font une **exigence pour les entreprises**. Parmi ces avantages, on peut citer :

1. Sécurité centralisée

De la même manière que l'informatique dématérialisée (cloud computing) centralise les applications et les données, la **sécurité dématérialisée centralise la protection**. Elle vous aide à améliorer votre visibilité, à mettre en place des contrôles et à mieux vous protéger contre les attaques. Elle améliore également la continuité de vos activités et la reprise après sinistre en ayant tout en un seul endroit.

> Info
>
> Kinsta offre un garantie de sécurité avec chaque plan et, en cas de problème, des spécialistes de la sécurité répareront votre site.

2. Réduction des coûts

Un fournisseur de services de Cloud réputé vous proposera du matériel et des logiciels intégrés destinés à sécuriser vos applications et vos données 24/24. Vous n'aurez donc pas besoin d'investir des sommes importantes dans votre propre installation.

3. Administration réduite

Le passage au Cloud introduit un modèle de responsabilité partagée en matière de sécurité. Cela peut permettre de réduire considérablement le temps et les ressources investis dans l'administration de la sécurité. Le fournisseur de services dans le Cloud assumera la responsabilité de la sécurité de son infrastructure – et de la vôtre – au niveau du stockage, de l'informatique, de la mise en réseau et de l'infrastructure physique

4. Fiabilité accrue

Un fournisseur de services de Cloud de premier plan offrira du matériel et des logiciels de sécurité dématérialisée de pointe sur lesquels vous pourrez compter. Vous aurez accès à un service continu où vos utilisateurs pourront accéder en toute sécurité aux données et aux applications depuis n'importe où, sur n'importe quel appareil.

Meilleures pratiques pour la sécurité du Cloud

Lorsque vous transférez vos systèmes vers le Cloud, de nombreuses mesures de sécurité et les meilleures pratiques restent les mêmes. Toutefois, vous serez confrontés à une nouvelle série de défis que vous devrez surmonter afin de maintenir la sécurité de vos systèmes et données dans le Cloud.

Pour vous aider à relever ce défi, nous avons compilé une série de **meilleures pratiques de sécurité pour les déploiements dans le Cloud**.

Choisir un fournisseur de confiance

Les meilleures pratiques en matière de sécurité dans le Cloud reposent sur la sélection d'un fournisseur de services de confiance. Vous souhaitez vous associer à un fournisseur de services dans le Cloud qui offre les meilleurs protocoles de sécurité intégrés et qui se conforme aux plus hauts niveaux des meilleures pratiques du secteur.

Un fournisseur de services qui vous propose une place de marché de partenaires et de solutions afin d'améliorer encore la sécurité de votre déploiement.

La marque d'un fournisseur de confiance se reflète dans l'éventail des certifications et de la conformité en matière de sécurité qu'il détient. Tout bon fournisseur met ces informations à la disposition du public. Par exemple, tous les grands fournisseurs comme Amazon Web Services, Alibaba Cloud, Google Cloud (qui alimente Kinsta), et Azure offrent un accès transparent où vous pouvez confirmer leur conformité et leurs certifications en matière de sécurité.

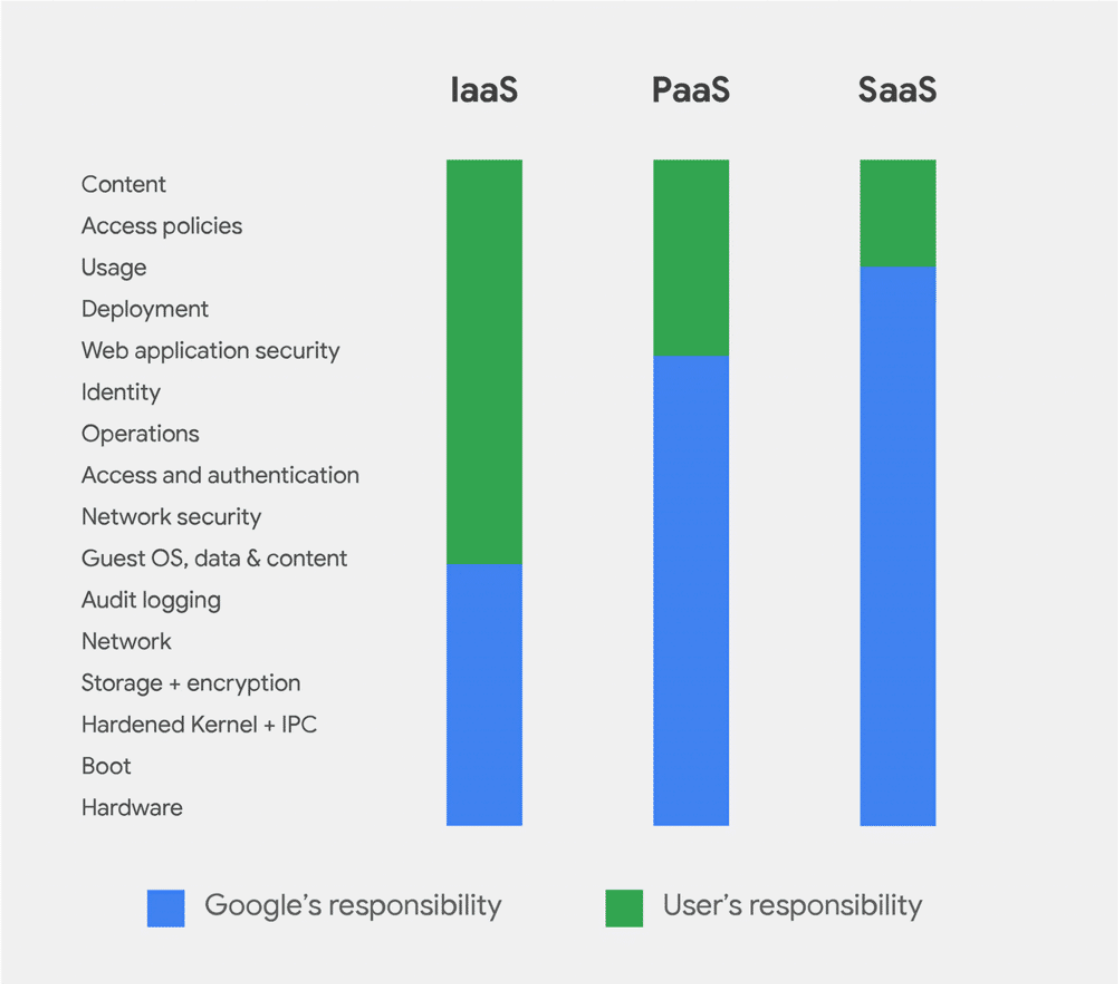
Au-delà de cela, de nombreux facteurs entrent en jeu dans le choix d'un fournisseur de confiance. Nous abordons ce sujet plus loin dans l'article, avec une liste de contrôle des dix principaux facteurs permettant d'évaluer la sécurité de tout fournisseur de services en ligne.

Comprendre votre modèle de responsabilité partagée

Quand vous vous associez à un fournisseur de services de Cloud et que vous transférez vos systèmes et vos données vers le Cloud, vous concluez un partenariat de responsabilité partagée pour la mise en œuvre de la sécurité.

Une partie essentielle des meilleures pratiques consiste à examiner et à comprendre votre responsabilité partagée. Découvrir quelles tâches de sécurité vous incombent et quelles tâches seront désormais prises en charge par le fournisseur.

Il s'agit d'une échelle mobile selon que vous optez pour le Software as a Service (SaaS), le Platform as a Service (PaaS), l'Infrastructure as a Service (IaaS) ou pour un centre de données sur site.



– Modèle de responsabilité partagée de la plateforme Google Cloud

Les principaux fournisseurs de services en nuage comme AWS, Azure, Google Cloud Platform, et Alibaba Cloud publient ce qui est connu comme un modèle de responsabilité partagée en matière de sécurité. Garantir la transparence et la clarté. Veillez à revoir votre modèle de responsabilité partagée des fournisseurs de services de Cloud.

Examinez vos contrats et accords de niveau de service (SLA) avec les fournisseurs de services en ligne

Vous ne devriez peut-être pas envisager de revoir vos contrats et accords de niveau de service dans le cadre des meilleures pratiques de sécurité. Les contrats SLA et les contrats de services de Cloud ne sont qu'une garantie de service et de recours en cas d'incident.

Les conditions générales, les annexes et les appendices qui peuvent avoir une incidence sur votre sécurité sont beaucoup plus nombreux. Un contrat

peut faire la différence entre le fait que votre fournisseur de services de Cloud soit responsable de vos données et qu'il en soit le propriétaire.

Selon le McAfee 2019 Cloud Adoption and Risk Report, 62,7 % des fournisseurs de Cloud ne précisent pas que les données des clients sont la propriété de ces derniers. Cela crée une zone d'ombre juridique où un fournisseur pourrait revendiquer la propriété de toutes vos données téléversées.

Vérifiez à qui appartiennent les données et ce qu'il advient de celles-ci si vous mettez fin à vos services. Cherchez également à savoir si le fournisseur est tenu d'offrir une visibilité sur les événements et les réponses en matière de sécurité.

Si vous n'êtes pas satisfait de certains éléments du contrat, essayez de négocier. Si certains ne sont pas négociables, vous devez déterminer si le fait d'accepter est un risque acceptable pour l'entreprise. Si ce n'est pas le cas, vous devrez rechercher d'autres options pour atténuer le risque par le biais du cryptage, de la surveillance ou même d'un autre fournisseur.

Formez vos utilisateurs

Vos utilisateurs constituent la première ligne de défense dans le domaine de l'informatique dématérialisée sécurisée. Leur connaissance et leur application des pratiques de sécurité peuvent faire la différence entre protéger votre système ou ouvrir une porte aux cyberattaques.

Comme meilleure pratique, assurez-vous de former tous vos utilisateurs - personnel et parties prenantes - qui accèdent à vos systèmes aux pratiques sécurisées de l'informatique dématérialiée. Sensibilisez-les à la manière de repérer les logiciels malveillants, d'identifier les e-mails de phishing et les risques de pratiques non sécurisées.

Pour les utilisateurs plus avancés - tels que les administrateurs - directement impliqués dans la mise en œuvre de la sécurité dans le Cloud, envisagez une formation et une certification spécifiques au secteur. Vous trouverez plus loin dans le guide une série de certifications et de formations recommandées en matière de sécurité dans le Cloud.

Contrôle de l'accès des utilisateurs

Mettre en œuvre un contrôle étroit des accès des utilisateurs par le biais de politiques est une autre bonne pratique de sécurité dans le Cloud. Elle vous aide à gérer les utilisateurs qui tentent d'accéder à vos services de Cloud.

Vous devez partir d'un lieu de confiance zéro, en ne donnant aux utilisateurs que l'accès aux systèmes et aux données dont ils ont besoin, rien de plus. Pour éviter la complexité lors de la mise en œuvre des politiques, créez des groupes bien définis avec des rôles attribués pour n'accorder l'accès qu'aux ressources choisies. Vous pourrez ainsi ajouter des utilisateurs directement à des groupes, plutôt que de personnaliser l'accès pour chaque utilisateur individuel.

Sécurisez vos points de terminaison (Endpoints) d'utilisateur

Un autre élément de la meilleure pratique en matière de sécurité dans les nuages est la sécurisation des points de terminaison de vos utilisateurs. La majorité des utilisateurs accèdent à vos services de Cloud par le biais de navigateurs web. Il est donc essentiel que vous introduisiez une sécurité avancée côté client pour que les navigateurs de vos utilisateurs restent à jour et protégés contre les exploitations.

Vous devriez également envisager de mettre en œuvre une solution de sécurité des points d'accès pour protéger les appareils de vos utilisateurs finaux. Vital avec l'explosion des appareils mobiles et le télétravail, où les utilisateurs accèdent de plus en plus à des services de Cloud par le biais d'appareils n'appartenant pas à l'entreprise.

Recherchez une solution qui comprend des pare-feu, des antivirus et des outils de sécurité Internet, de sécurité des appareils mobiles et de détection des intrusions.

Maintenir la visibilité de vos services en ligne

L'utilisation des services de Cloud peut être diverse et éphémère. De nombreuses organisations utilisent de multiples services de Cloud à travers un éventail de fournisseurs et de zones géographiques. Des recherches suggèrent que les ressources du Cloud ont une durée de vie moyenne de 2 heures.

Ce genre de comportement crée des angles morts dans votre environnement de Cloud. Si vous ne pouvez pas le voir, vous ne pouvez pas le sécuriser.

Veillez à mettre en place une solution de sécurité dans le Cloud qui offre une visibilité de l'ensemble de votre écosystème. Vous pourrez alors surveiller et protéger l'utilisation du Cloud dans l'ensemble de vos ressources, projets et régions disparates par le biais d'un seul portail. Cette visibilité vous aidera à mettre en œuvre des politiques de sécurité granulaires et à atténuer un large éventail de risques.

Mettre en œuvre le cryptage

Le cryptage de vos données est une bonne pratique de sécurité, quel que soir l'endroit où vous vous trouvez. En utilisant les services de Cloud, vous exposez vos données à un risque accru en les stockant sur une plateforme tierce et en les envoyant dans les deux sens entre votre réseau et le service de Cloud.

Veillez à mettre en œuvre les niveaux de cryptage les plus élevés pour les données en transit et au repos. Vous devriez également envisager d'utiliser vos propres solutions de cryptage avant de téléverser des données sur le Cloud, en utilisant vos propres clés de cryptage pour garder un contrôle total.

Un fournisseur de cloud computing peut offrir des services de cryptage intégrés pour protéger vos données contre les tiers, mais cela leur permet d'accéder à vos clés de cryptage.

Kinsta exploite une approche entièrement cryptée pour mieux protéger ses solutions d'hébergement sécurisé. Cela signifie que nous ne prenons pas en charge les connexions FTP, mais seulement les connexions cryptées SFTP et les connexions SSH (voici la différence entre FTP et SFTP).

Mettre en œuvre une politique de sécurité de mots de passe forts

Une solide politique de sécurité des mots de passe est la meilleure pratique, quel que soit le service auquel vous accédez. La mise en œuvre de la politique la plus stricte possible est un élément important pour empêcher les accès non autorisés.

Au minimum, tous les mots de passe doivent comporter une lettre majuscule, une lettre minuscule, un chiffre, un symbole et un minimum de 14 caractères. Obliger les utilisateurs à mettre à jour leur mot de passe tous les 90 jours et à le paramétrer de manière à ce que le système se souvienne des 24 derniers mots de passe.

Une telle politique de mots de passe empêchera les utilisateurs de créer des mots de passe simples, sur de multiples dispositifs, et permettra de se défendre contre la plupart des attaques par force brute.

Comme niveau supplémentaire de protection et de bonnes pratiques en matière de sécurité, vous devez également mettre en œuvre l'authentification multifactorielle. Obligation pour l'utilisateur d'ajouter deux - ou plus - éléments de preuve pour authentifier son identité.

Utiliser un courtier en sécurité pour l'accès au Cloud (CASB)

L'utilisation d'un CASB devient rapidement un outil central pour mettre en œuvre les meilleures pratiques de sécurité dans le Cloud. Il s'agit d'un logiciel qui se situe entre vous et votre ou vos fournisseurs de services de Cloud pour étendre vos contrôles de sécurité dans le Cloud.

Un CASB vous offre un ensemble d'outils sophistiqués de sécurité dans le Cloud pour vous permettre de visualiser votre écosystème dans le Cloud, d'appliquer les politiques de sécurité des données, de mettre en œuvre l'identification et la protection des menaces et de maintenir la conformité.

Vous en saurez plus sur le fonctionnement d'un CASB plus loin dans le guide, y compris une liste des 5 principaux fournisseurs de CASB.

Les dix principales recommandations de la liste de contrôle de sécurité pour les clients du Cloud

Lors de la migration vers le Cloud et du choix d'un fournisseur de services, l'un des facteurs les plus importants à prendre en compte est la sécurité.

Vous partagerez et / ou stockerez les données de votre entreprise avec le fournisseur de services que vous aurez choisi.

Vous devez avoir la certitude que vos données sont sécurisées. Il existe d'innombrables facteurs de sécurité à prendre en compte, depuis le partage des responsabilités jusqu'à la question de savoir si les normes de sécurité du fournisseur sont à la hauteur. Ce processus peut être décourageant, surtout si vous n'êtes pas un expert en sécurité.

Pour vous aider, nous avons établi une liste des 10 principaux contrôles de sécurité à effectuer lors de l'évaluation d'un fournisseur de services de Cloud.

- Protection des données en transit et des données au repos
- Protection des actifs
- Visibilité et contrôle
- Marché de la sécurité et réseau de partenaires de confiance
- Gestion sécurisée des utilisateurs
- Intégration de la conformité et de la sécurité
- Identité et authentification
- Sécurité opérationnelle
- Sécurité du personnel
- Utilisation sécurisée du service

1. Protection des données en transit et des données au repos

Lors du passage à un service en Cloud, un élément clé de la sécurité est la protection des données en transit entre vous (l'utilisateur final) et le fournisseur. Il s'agit d'une double responsabilité pour vous et le fournisseur. Vous aurez besoin d'une protection du réseau pour empêcher l'interception des données et d'un cryptage pour empêcher un attaquant de lire les données si elles sont interceptées.

Recherchez un fournisseur de services qui vous offre un ensemble d'outils pour vous aider à crypter facilement vos données en transit et au repos. Cela garantira le même niveau de protection pour tout transit de données interne au sein du fournisseur de services de Cloud, ou pour le transit entre le fournisseur de services de Cloud et d'autres services où les API peuvent être exposées.

2. Protection des actifs

Lorsque vous choisissez un fournisseur de services de Cloud, vous devez comprendre l'emplacement physique où vos données sont stockées, traitées et gérées. Ceci est particulièrement important suite à la mise en œuvre de la politique d'accès aux données des gouvernements et de l'industrie des réglementations comme le RGPD.

Pour garantir la protection de vos actifs, un bon fournisseur disposera d'une protection physique avancée dans son centre de données pour défendre vos données contre tout accès non autorisé. Il veillera également à ce que vos données soient effacées avant que des ressources ne soient réapprovisionnées ou éliminées pour éviter qu'elles ne tombent entre de mauvaises mains.

3. Visibilité et contrôle

Un facteur clé de la sécurité est la possibilité de voir et de contrôler ses propres données. Un bon prestataire de services vous proposera une solution qui vous offrira une visibilité totale de vos données et des personnes qui y accèdent, quels que soient l'endroit où elles se trouvent et le lieu où vous vous trouvez.

Votre fournisseur doit offrir la surveillance des activités afin que vous puissiez découvrir les changements de configuration et de sécurité dans votre écosystème. En plus de prendre en charge la conformité avec l'intégration de solutions nouvelles et existantes.

4. Marché de la sécurité et réseau de partenaires de confiance

Pour sécuriser le déploiement de votre Cloud, il vous faudra plus d'une solution ou d'un partenaire. Un bon fournisseur de services de Cloud vous permettra de trouver et de vous connecter facilement à différents partenaires et solutions par le biais d'une place de marché.

Cherchez un fournisseur dont la place de marché offre un réseau de partenaires de confiance ayant fait leurs preuves en matière de sécurité. La place de marché devrait également proposer des solutions de sécurité qui permettent un déploiement en un seul clic et qui sont complémentaires

pour sécuriser vos données, qu'elles soient exploitées dans le cadre d'un déploiement en Cloud public, privé ou hybride.

5. Gestion sécurisée des utilisateurs

Un bon fournisseur de services de Cloud offrira des outils qui permettent une gestion sécurisée des utilisateurs. Cela permettra d'empêcher l'accès non autorisé aux interfaces et aux procédures de gestion afin de garantir que les applications, les données et les ressources ne sont pas compromises.

Le fournisseur de services de Cloud devrait également offrir des fonctionnalités permettant de mettre en œuvre des protocoles de sécurité qui séparent les utilisateurs et empêchent tout utilisateur malveillant (ou compromis) d'affecter les services et les données d'un autre.

6. Intégration de la conformité et de la sécurité

Lorsqu'on envisage un fournisseur de services de Cloud, la sécurité et la conformité vont de pair. Ils doivent répondre à des exigences de conformité globales qui sont validées par un organisme tiers. Vous voulez un fournisseur de services dans le Cloud qui suit les meilleures pratiques du secteur en matière de sécurité de Cloud et qui, idéalement, détient une certification reconnue.

Le programme STAR (Security, Trust, and Assurance Registry) de la Cloud Security Alliance est un bon indicateur. De plus, si vous travaillez dans un secteur hautement réglementé – où les normes HIPPA, PCI-DSS et le RGPD peuvent s'appliquer – vous devrez également identifier un fournisseur ayant une certification spécifique à l'industrie.

Pour que vos efforts de mise en conformité soient à la fois rentables et efficaces, le fournisseur de services de Cloud doit vous offrir la possibilité d'hériter de ses contrôles de sécurité dans vos propres programmes de conformité et de certification.

7. Identité et authentification

Votre fournisseur de services de Cloud doit s'assurer que l'accès à toute interface de service est limité aux seules personnes autorisées et authentifiées.

Lorsque vous examinez les fournisseurs, vous souhaitez un service offrant des fonctionnalités d'identité et d'authentification, notamment un identifiant et un mot de passe, une authentification à deux facteurs, des certificats clients TLS et une fédération d'identité avec votre fournisseur d'identité existant.

Vous souhaitez également pouvoir restreindre l'accès à une ligne dédiée, à une entreprise ou à un réseau communautaire. Un bon fournisseur ne fournit une authentification que par des canaux sécurisés - comme le HTTPS - pour éviter l'interception.

Veillez à éviter les services dont les pratiques d'authentification sont faibles. Cela exposera vos systèmes à un accès non autorisé entraînant le vol de données, la modification de votre service ou un déni de service. Évitez également l'authentification par courrier électronique, HTTP ou téléphone.

Ces derniers sont extrêmement vulnérables à l'ingénierie sociale et à l'interception d'identité et des justificatifs d'authentification.

8. Sécurité opérationnelle

Lorsque vous choisissez un service de cloud computing, recherchez un fournisseur qui met en œuvre une sécurité opérationnelle solide pour détecter et prévenir les attaques. Cette sécurité doit couvrir quatre éléments essentiels :

Configuration et gestion des changements

Vous voulez un prestataire qui offre une transparence sur les actifs qui composent le service, y compris les configurations ou les dépendances éventuelles. Il doit vous informer de toute modification du service susceptible d'affecter la sécurité afin de garantir l'absence de vulnérabilités.

Gestion des vulnérabilités

Votre fournisseur doit disposer d'un processus de gestion des vulnérabilités pour détecter et atténuer toute nouvelle menace pesant sur son service.

Vous devez être tenu informé de ces menaces, de leur gravité et du calendrier prévu pour leur atténuation, y compris leur résolution.

Surveillance de la protection

Tout prestataire digne de ce nom disposera d'outils de surveillance avancés pour identifier toute attaque, abus ou dysfonctionnement du service. Ils prendront des mesures rapides et décisives pour faire face à tout incident, et vous tiendront informés des résultats.

Chez Kinsta, nous sommes fiers de fournir les normes de sécurité opérationnelle les plus élevées pour les solutions d'hébergement. Cela comprend la mise en œuvre des dernières mises à jour de sécurité, la surveillance continue du temps de fonctionnement, des sauvegardes automatiques, et des mesures actives et passives pour stopper toute attaque sur sa lancée.

Résultat : votre site est surveillé et sécurisé 24/7.

Gestion des incidents

Votre fournisseur idéal aura une gestion d'incidents pré-planifiée en place pour les types d'attaques les plus courants. Ils seront prêts à déployer ce processus en réponse à toute attaque.

Un itinéraire de contact clair vous sera indiqué pour signaler tout incident, avec un calendrier et un format acceptables.

9. Sécurité du personnel

Vous avez besoin d'un fournisseur de services de Cloud dont le personnel est digne de confiance, car il aura accès à vos systèmes et à vos données. Le fournisseur de services de Cloud que vous aurez choisi fera l'objet d'une procédure de contrôle de sécurité rigoureuse et transparente.

Ils doivent pouvoir vérifier l'identité de leur personnel, le droit au travail et vérifier les éventuelles condamnations pénales. Idéalement, vous voulez qu'ils se conforment aux normes de contrôle établies localement dans votre pays, telles que BS 7858:2019 pour le Royaume-Uni ou le formulaire I-9 aux États-Unis.

En plus du contrôle, vous voulez un prestataire de services qui s'assure que son personnel comprend ses responsabilités inhérentes en matière de sécurité et suit régulièrement des formations. Il doit également avoir une politique visant à réduire au minimum le nombre de personnes qui ont accès à vos services et qui peuvent les affecter.

10. Utilisation sécurisée du service

Vous pouvez choisir un fournisseur de services de Cloud doté d'une sécurité de pointe tout en subissant une brèche due à une mauvaise utilisation du service. Il est important de comprendre où se situent les responsabilités en matière de sécurité lorsque vous utilisez le service.

Votre niveau de responsabilité sera influencé par votre modèle de déploiement du Cloud, la façon dont vous utilisez les services et les caractéristiques intégrées de chaque service.

Par exemple, vous avez d'importantes responsabilités en matière de sécurité au sein de l'IaaS. En déployant une instance de calcul, il vous incomberait d'installer un système d'exploitation moderne, de configurer la sécurité et d'assurer les correctifs et la maintenance en continu. Il en va de même pour toute application que vous déployez sur cette instance.

Assurez-vous donc de bien comprendre les exigences de sécurité du service que vous avez choisi et toutes les options de configuration de sécurité qui s'offrent à vous. Veillez également à former votre personnel à l'utilisation sécurisée des services que vous avez choisis.

Qu'est-ce que la Cloud Security Alliance ?

Le secteur de l'informatique dématérialisée est un marché disparate, sans organe de direction central auquel les entreprises peuvent s'adresser pour obtenir des conseils. Cela peut être frustrant, surtout lorsqu'il s'agit de relever des défis tels que la sécurité du cloud computing.

Heureusement, à la place des organes directeurs, il existe un certain nombre d'organisations qui se consacrent au soutien de l'industrie. La Cloud Security Alliance est l'une de ces organisations.

– Logo de la Cloud Security Alliance

La Cloud Security Alliance (CSA) est une organisation à but non lucratif qui se consacre au développement et à la sensibilisation aux meilleures pratiques pour maintenir un environnement informatique sécurisé dans le Cloud.

Il s'agit d'une organisation de membres qui offre à l'industrie des conseils de sécurité spécifiques au Cloud sous forme d'éducation, de recherche, d'événements et de produits. Ces conseils sont directement issus de l'expertise combinée des praticiens de l'industrie, les associations, les gouvernements et les membres individuels et corporatifs de la CSA.

Pour vous permettre de mieux comprendre la Cloud Security Alliance, examinons de plus près la manière dont elle soutient l'industrie.

Adhésion

La CSA est construite sur la base de ses membres. En devenant membre du CSA, vous bénéficiez de différents avantages selon que vous êtes un particulier, une entreprise ou un fournisseur de solutions.

Ils entrent principalement dans des catégories similaires, notamment l'accès à leur réseau d'experts composé d'autres membres, un siège au conseil international de normalisation, des réductions sur les formations et l'accès à des événements et des webinaires exclusifs

Assurance

La CSA a développé l'un des programmes de certification de sécurité dans le Cloud les plus réputés : le Security, Trust &é Assurance Registry (STAR).

STAR est un programme d'assurance des fournisseurs qui assure la transparence par l'auto-évaluation, l'audit par des tiers et le contrôle continu par rapport aux normes. Le programme comprend trois niveaux, démontrant que le détenteur adhère aux meilleures pratiques tout en validant la sécurité de ses offres dans le Cloud.

Éducation

Pour soutenir l'amélioration continue de la sécurité dans le Cloud dans l'industrie, la CSA offre une gamme de services éducatifs. Vous pouvez obtenir une série de certifications en matière de sécurité dans le Cloud développées par la CSA, accéder à son centre de connaissances et participer à ses webinaires et événements éducatifs régulièrement programmés.

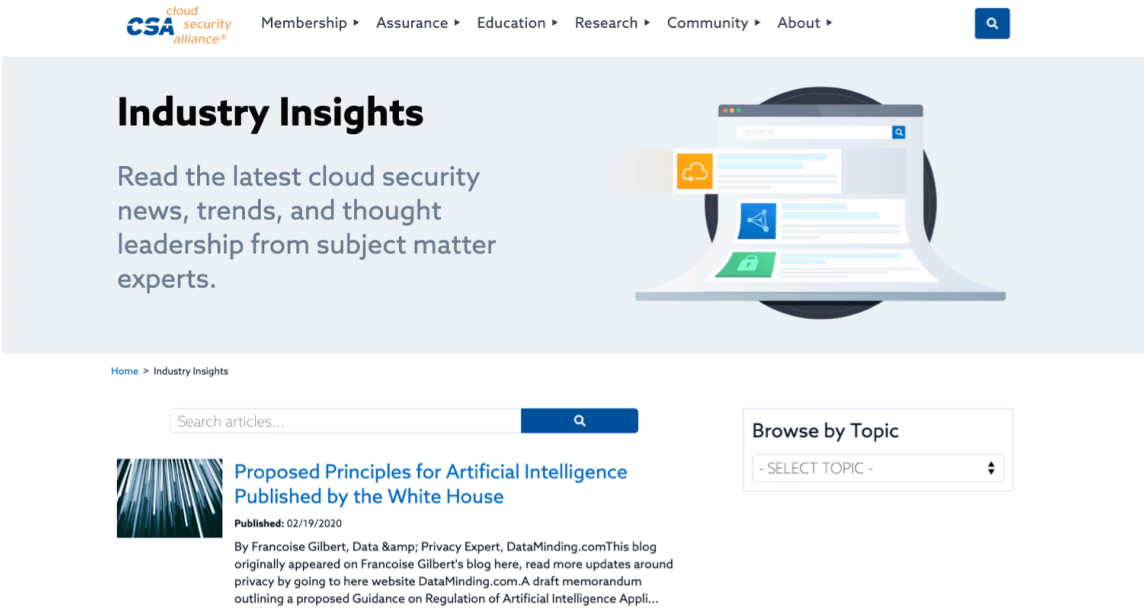
Recherche

La CSA continue de soutenir l'industrie en développant et en innovant les meilleures pratiques de sécurité dans le Cloud grâce à ses recherches permanentes. Ces recherches sont menées par ses groupes de travail qui couvrent désormais 30 domaines de la sécurité dans les nuages.

Parmi les plus récents et les plus avant-gardistes, on peut citer l'émergence de groupes de travail pour DevSecOps, l'Internet des objets, l'intelligence artificielle et Blockchain. La CSA publie continuellement ses recherches - gratuitement - afin que le secteur puisse se tenir au courant de l'évolution constante de la sécurité dans le Cloud.

Communauté

La CSA soutient également l'industrie en continuant à maintenir et à développer la communauté de la sécurité dans le Cloud. Elle a créé et maintient un large éventail de communautés qui permettent aux esprits de l'ensemble du secteur de la sécurité dans le Cloud de se connecter, de partager des connaissances et d'innover.



– Le blog de la CSA

Ces communautés en pleine croissance se présentent sous de nombreuses formes. Vous pouvez y rejoindre des chapitres de la CSA pour vous connecter aux professionnels locaux et aux sommets de la CSA où les meilleurs esprits partagent leur expertise avec les masses. Il y a même le blog de la CSA qui héberge une communauté d'abonnés désireux de suivre les pratiques de la CSA.

Qu'est-ce que le Kaspersky Security Cloud ?

Lorsqu'on parle de sécurité dans le Cloud, il est facile de se concentrer sur les entreprises et d'oublier les besoins des consommateurs individuels.

Si vous accédez à des services de Cloud pour votre usage personnel – des photos, fichiers – vous devez penser à la sécurité de vos données : Kaspersky Security Cloud, la nouvelle solution de sécurité adaptative basée sur le Cloud de Kaspersky.

– Kaspersky Security Cloud

Combinant les meilleures fonctionnalités et applications du logiciel antivirus de Kaspersky Lab, il crée une protection réactive des appareils des utilisateurs contre les menaces numériques.

La plateforme a été conçue pour les utilisateurs individuels, et non pour les entreprises.

Kaspersky Security Cloud protège vos appareils contre les logiciels malveillants et les virus, en ajoutant des fonctionnalités permettant d'adapter la façon dont vous utilisez chaque appareil pour assurer une protection maximale à tout moment. Il offre des fonctionnalités telles que l'antivirus, l'anti-ransomware, la sécurité mobile, la gestion des mots de passe, le VPN, le contrôle parental et une série d'outils de protection de la vie privée.

La plateforme est disponible sur Windows, macOS, Android et iOS. L'offre Kaspersky Security Cloud Family offre une protection pour un maximum de 20 appareils.

Fonctionnalité de base dans le Kaspersky Security Cloud

Pour vous aider à mieux comprendre l'offre de Kaspersky Security Cloud, nous avons examiné de plus près les fonctionnalités de base de la plateforme, qui est divisée en quatre sections :

Scanner

La fonctionnalité essentielle que vous attendez de toute solution de sécurité, Kaspersky Security Cloud peut scanner vos appareils et supprimer tout logiciel malveillant ou virus trouvé. Vous pouvez choisir parmi un certain nombre d'options d'analyse, y compris les fichiers individuels, l'analyse rapide, l'ensemble du système et la programmation.

Vie privée

Vous pouvez protéger votre vie privée en utilisant la fonctionnalité intégrée qui vous permet de vérifier vos comptes en ligne pour vous assurer qu'ils ne sont pas compromis, de bloquer l'accès à votre webcam et de bloquer le trafic sur le site web pour empêcher que vos activités de navigation soient surveillées.

Vous pouvez étendre votre confidentialité grâce à des téléchargements supplémentaires de Kaspersky Secure Connection et de Kaspersky Password Manager. La connexion sécurisée crypte toutes les données que vous envoyez et recevez tout en cachant votre emplacement, tandis que le gestionnaire de mots de passe stocke et sécurise vos mots de passe.

Réseau domestique

Home Network vous donne la visibilité de tous les appareils qui sont connectés à votre réseau domestique. Identifier ceux qui sont protégés par Kaspersky Security Cloud. Cette fonctionnalité vous permet d'être averti lorsqu'un nouvel appareil se connecte et de bloquer également tout appareil inconnu.

HD Health

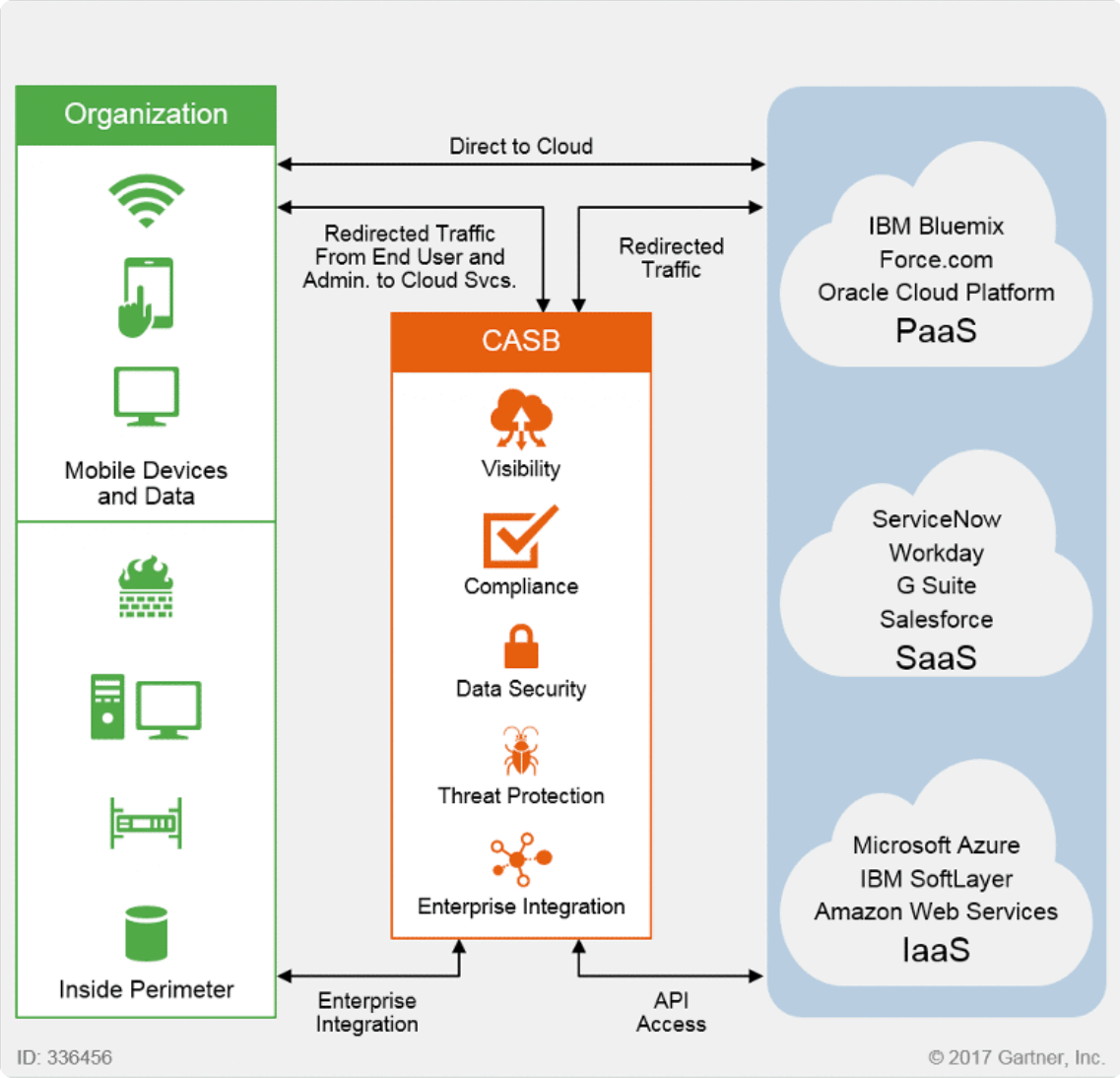
Utile, mais simple, la fonctionnalité HD Health vous donne une évaluation de l'état et de la température de vos disques durs. Elle donne des informations sur les taux d'erreur, les cycles de mise sous tension, les heures de mise sous tension, le nombre total de données lues et le nombre total de données écrites.

Kaspersky Security Cloud est un excellent exemple de la façon dont l'adoption des services de Cloud a créé le besoin de nouvelles solutions de sécurité.

Dans la section suivante, nous examinons un exemple similaire dans le monde de l'entreprise avec l'arrivée des courtiers en sécurité pour l'accès au Cloud.

Qu'est-ce qu'un courtier en sécurité pour l'accès au Cloud (CASB) ?

Un **courtier en sécurité d'accès au Cloud** (CASB) est un logiciel qui se situe entre vous, le consommateur de services de Cloud, et votre ou vos fournisseurs de services de Cloud. Un CASB étend vos contrôles de sécurité de votre infrastructure sur site vers le Cloud. Il vous aide à appliquer les politiques de sécurité, de conformité et de gouvernance pour vos applications dans le Cloud. Il est généralement installé sur place ou hébergé dans le Cloud.



– Modèle de courtier en sécurité pour l'accès au Cloud (Source de l'image : Gartner)

Un CASB vous aidera à vous défendre contre les risques de sécurité dans le Cloud de haut niveau et à soutenir la surveillance continue et l'atténuation des événements à haut risque. Pour ce faire, il sécurise les données circulant entre votre environnement sur site et votre environnement dans le Cloud en utilisant les politiques de sécurité de votre organisation.

Un CASB vous protégera des cyberattaques grâce à la prévention des logiciels malveillants et sécurisera vos données grâce à un cryptage de bout en bout empêchant les utilisateurs extérieurs de déchiffrer le contenu.

Comment fonctionne un CASB ?

Un CASB peut être déployé de trois manières différentes : en tant que proxy inverse, proxy direct, ou en « mode API ». Chacun a ses propres avantages et inconvénients, et de nombreux experts de l'industrie recommandent un déploiement multimode.

Examinons de plus près les différents modes de déploiement d'un CASB :

Proxy inverse

Un proxy inverse se trouve devant le service de cloud computing, offrant des capacités de sécurité en ligne en se plaçant dans le chemin du trafic réseau. La connexion du reverse proxy broker va de l'internet à votre serveur d'application, cachant derrière elle des informations provenant de la source originale.

Proxy direct

Un proxy direct (ou forward proxy) se trouve en face de l'utilisateur, le CASB envoyant le trafic par proxy vers plusieurs plateformes de Cloud. La connexion du proxy avancé part de vous, assis derrière votre pare-feu, et se dirige vers l'internet. Comme le proxy inverse, il offre également des fonctions de sécurité en ligne.

Mode API

Contrairement aux déploiements de proxy, l'utilisation de l'interface de programme d'application (API) permet l'intégration directe du CASB et d'un service de Cloud. Cela vous permet de sécuriser le trafic géré et non géré.

En fonction de la fonctionnalité API des fournisseurs de services de Cloud, vous pouvez visualiser l'activité, le contenu et prendre des mesures d'exécution.

Les piliers de la fonctionnalité dans les CASB

Un CASB fournit des fonctionnalités qui s'inscrivent dans quatre « piliers », à savoir :

1. Visibilité

Lorsqu'une application de Cloud se trouve hors de la vue de votre service informatique, vous créez des informations qui ne sont pas contrôlées par les processus de gouvernance, de risque et de conformité de votre entreprise.

Un CASB vous donne une visibilité de toutes les applications de Cloud et de leur utilisation. Il comprend des informations essentielles sur les utilisateurs de la plateforme, leur service, leur emplacement et les appareils utilisés.

2. Sécurité des données

L'utilisation d'une plateforme dans le Cloud augmente le risque de partager par inadvertance des données avec les mauvaises personnes. Si vous utilisez un stockage dans le Cloud, un outil de prévention des pertes de données (DLP) typique ne sera pas en mesure de suivre ou de contrôler qui accède à vos données.

Un CASB vous aide à appliquer une sécurité centrée sur les données au sein d'une plateforme en Cloud combinant cryptage, tokenisation, contrôle d'accès et gestion des droits d'information.

3. Protection contre les menaces

L'une des menaces les plus difficiles à protéger est votre propre personnel. Même les anciens employés qui ont été mis hors service des systèmes centraux de votre organisation peuvent encore avoir accès à des applications de Cloud contenant des informations critiques pour l'entreprise.

Les CASB vous permettent de détecter et de répondre aux menaces d'initiés malveillants ou négligents, aux utilisateurs privilégiés et aux comptes compromis au sein de votre infrastructure en nuage.

4. Conformité

Lorsque vos données sont transférées vers le Cloud, vous devez vous assurer que la sécurité et la confidentialité des données sont maintenues afin de respecter les réglementations industrielles et gouvernementales. Un CASB s'en chargera pour vous, en identifiant et en appliquant les politiques DLP sur les données sensibles dans votre déploiement sur le Cloud. Il vous aidera à respecter les réglementations, notamment la loi SOX et la loi HIPAA.

Un CASB vous aidera également à évaluer votre configuration de sécurité dans le Cloud par rapport aux principales exigences réglementaires telles que PCI DSS, NIST, CJIS, MAS et ISO 27001.

Le top 5 des courtiers en sécurité pour l'accès au Cloud en 2024

La migration massive des services vers le Cloud, associée à la nécessité de mettre en place une sécurité dans le Cloud en raison des risques importants de violation et de perte de données, a créé une explosion sur le marché des CASB.

En tant que technologie de nouvelle génération, les CASB sont devenus un élément essentiel de la stratégie de sécurité dans le Cloud. Une grande entreprise sur cinq utilise un CASB pour sécuriser ou gérer ses services de Cloud, selon un rapport du Gartner sur le « Magic Quadrant for Cloud Access Brokers » :

– Carré magique Gartner 2019 des courtiers en sécurité pour l'accès au cloud (CASB)

Gartner a identifié cinq leaders sur le marché des CASB à l'aide de son « Carré magique », parmi lesquels

McAfee

McAfee est entré sur le marché du CASB en janvier 2018, avec son acquisition très médiatisée de Skyhigh Networks. Désormais connue sous le nom de MVISION Cloud, la plateforme fournit une couverture sur les quatre piliers du CASB pour une large gamme de services de Cloud.

La plateforme fournit un moteur DLP complet et offre des contrôles avancés, notamment le cryptage et la symbolisation des données structurées et non structurées. Le CASB peut être déployé pour l'inspection de l'API avec des capacités de mode de proxy inverse et de proxy direct.

McAfee a également mis à disposition une application virtuelle sur site pour ceux qui en ont besoin.

Microsoft

L'offre CASB de Microsoft est appelée Microsoft Cloud Application Security. La plateforme prend en charge plusieurs modes de déploiement, y compris le proxy inverse et les connecteurs API. Microsoft continue à développer la solution CASB avec une visibilité accrue, des analyses, un contrôle des données et des fonctionnalités d'automatisation innovantes.

Microsoft Cloud Application Security s'intègre également en natif avec le portefeuille croissant de solutions de sécurité et d'identité de Microsoft, notamment Azure Active Directory et Microsoft Defender Advanced Threat Protection.

Cela permet à Microsoft d'offrir à ses clients une solution totalement intégrée sur l'ensemble de leurs plateformes Microsoft, avec des déploiements en un seul clic.

Netskope

Contrairement à de nombreux acteurs qui se contentent d'acquérir des fournisseurs de solutions CASB, Netskope reste une société indépendante. Le fournisseur est réputé pour son excellence dans la découverte d'applications et les évaluations de sécurité SaaS.

Netskope prend en charge des milliers de services de Cloud grâce à des API publiées et au décodage en ligne d'API non publiées. Le CASB propose le DLP et identifie les menaces en temps réel en combinant l'intelligence des menaces, l'analyse statique et dynamique et la détection d'anomalies basée sur l'apprentissage machine.

Symantec

L'offre CASB de Symantec s'appelle CloudSOC et a été améliorée en 2016 avec l'acquisition et l'intégration des produits Perspecsys et Elastica de Blue Coat Systems.

CloudSOC offre un DLP utilisant une classification automatisée des données et une supervision multimode à l'aide d'API natives pour le Cloud, un traitement du trafic en temps réel et la saisie de données provenant de

multiples sources. Vous pouvez identifier et éliminer automatiquement les menaces internes et externes à votre organisation grâce à l'analyse avancée du comportement des utilisateurs (UBA).

Bitglass

Bitglass Cloud Security est un CASB de nouvelle génération, conçu pour s'intégrer à n'importe quelle application, appareil ou réseau.

La plateforme fonctionne nativement à partir du Cloud et est réputée comme étant le seul fournisseur à sécuriser les données d'entreprise sur les appareils mobiles sans utiliser d'agents ou de profils. Bitglass a pris de l'importance en introduisant une approche « zero-day » axée sur les cotes de confiance, les niveaux de confiance et le cryptage au repos.

Un aperçu des 10 meilleures certifications de sécurité dans le Cloud en 2024

Pour protéger avec succès votre plateforme de Cloud, vous allez avoir besoin de compétences et de connaissances avancées en matière de sécurité dématérialisée. Vous devrez également acquérir des compétences spécifiques à la plateforme afin de pouvoir configurer l'accès, la sécurité du réseau et assurer la protection des données au sein du fournisseur de Cloud computing que vous aurez choisi.

Heureusement, le marché de la formation et de la certification dans le Cloud continue d'évoluer et offre un certain nombre de solutions. Vous pouvez désormais choisir parmi un large éventail de **certifications spécifiques à une plateforme et indépendantes des fournisseurs** pour vous aider à développer et à prouver les compétences dont vous avez besoin. Que vous souhaitiez acquérir des connaissances de base ou adapter vos compétences à un poste spécifique, il existe une certification pour vous.

Pour vous aider dans votre recherche, nous avons dressé une liste des **10 meilleures certifications de sécurité dans le Cloud** à obtenir en 2024.

L'obtention d'une seule de ces certifications vous aidera non seulement à mieux sécuriser votre déploiement dans le Cloud, mais vous rendra également plus employable et vous permettra d'augmenter votre salaire.

(ISC)2 - Professionnel certifié de la sécurité du Cloud (CCSP)

Le CCSP est une certification de sécurité du Cloud reconnue mondialement et destinée aux leaders de la sécurité informatique et de la sécurité de l'information.

Le fait de gagner le CCSP démontre que vous avez les compétences et les connaissances techniques avancées pour concevoir, gérer et sécuriser des données, des applications et des infrastructures dans le Cloud. Pour ce faire, vous utiliserez les meilleures pratiques, procédures et politiques élaborées par les experts en cybersécurité de l'(ISC)2. Le CCSP est idéal si vous êtes architecte d'entreprise, ingénieur système, administrateur de sécurité, architecte, ingénieur ou gestionnaire.

Avant de vous former et de vous présenter à l'examen du CCSP, vous devrez satisfaire à certaines exigences des exigences strictes en matière d'expérience. Vous devrez avoir cinq ans d'expérience à plein temps dans le domaine des technologies de l'information, dont trois ans dans la cybersécurité et un an dans un ou plusieurs des six domaines du CCSP CBK. Vous pouvez remplacer les exigences en matière d'expérience que vous possédez par celles, tout aussi élevées, de (ISC)² accréditation CISSP - intitulée « The World's Premier Cyber Security Certification ».

Cloud Security Alliance - Certificat de connaissances sur la sécurité du Cloud (CCSK)

Le certificat CCSK est une certification d'entrée de gamme largement reconnue dans le domaine de la sécurité du Cloud. Il a été développé par la Cloud Security Alliance, une organisation membre qui contribue à garantir la sécurité des environnements d'informatique dématérailisée en définissant et en sensibilisant les entreprises aux meilleures pratiques du secteur.

L'obtention de la certification CCSK prouvera que vous possédez les compétences et les connaissances de base nécessaires pour sécuriser les données dans le Cloud. Vous apprendrez comment établir une base de référence des meilleures pratiques de sécurité, en fonction d'un éventail de responsabilités allant de la configuration des contrôles de sécurité techniques à la gouvernance du Cloud.

En obtenant la certification CCSK, vous répondrez également à certaines conditions préalables requises si vous avez l'intention de poursuivre la certification plus avancée de la CCSP de (ISC)².

Sécurité certifiée AWS - Spécialité

AWS Certified Security - Spécialité est idéal si vous cherchez à développer votre carrière en travaillant avec la plate-forme AWS de Cloud.

En obtenant la certification de sécurité AWS, vous validerez vos compétences en matière de classification des données, de méthodes de cryptage, de protocoles Internet sécurisés et de mécanismes AWS nécessaires à leur mise en œuvre.

En vue de la certification, vous pouvez choisir entre un parcours d'apprentissage diversifié pour façonner vos connaissances et vos compétences dans les domaines des fondamentaux de la sécurité, de l'architecture et de l'ingénierie de la sécurité sur AWS. À la fin de ce parcours, vous aurez acquis le contrôle et la confiance nécessaires pour exécuter en toute sécurité des applications dans le Cloud AWS.

Pour commencer à travailler en vue de l'obtention de ce titre, vous devez occuper un poste de sécurité et avoir au moins deux ans d'expérience pratique dans la sécurisation des charges de travail des AWS.

Certification Microsoft : Azure Security Engineer Associate

Récemment, Microsoft a transformé ses processus de certification pour qu'ils soient basés sur les rôles. En obtenant l'une de leurs certifications, vous prouvez désormais que vous possédez les compétences et les connaissances requises pour exercer un rôle professionnel spécifique.

Ainsi, le fait de gagner la certification Azure Security Engineer Associate montre que vous avez les compétences nécessaires pour être ingénieur en sécurité sur la plateforme Azure Cloud. Cela inclut la capacité à protéger les données, les applications et les réseaux dans un environnement de Cloud. Mettre en place des contrôles de sécurité et une protection contre les menaces, ainsi que gérer les identités et les accès.

Il n'y a pas d'exigences de compétences préalables avant d'essayer l'AZ-500 : Examen sur les technologies de sécurité Microsoft Azure.

Google Cloud - Ingénieur professionnel en sécurité de Cloud

Gagner le titre d'ingénieur professionnel en sécurité dans le Cloud de Google prouve que vous pouvez concevoir, développer, mettre en œuvre et gérer une infrastructure sécurisée sur la plateforme Google dans le Cloud. Pour ce faire, vous utiliserez les technologies de sécurité de Google, conformes aux meilleures pratiques de sécurité et aux exigences du secteur.

En suivant la certification Professional Cloud Security Engineer, vous devrez apprendre à configurer l'accès, la sécurité du réseau et à assurer la protection des données au sein de la plate-forme Google Cloud. Vous devrez également acquérir les connaissances nécessaires pour assurer la conformité et la gestion des opérations.

Comme les certifications Azure et AWS, ce titre est idéal si vous cherchez à développer des compétences en matière de sécurité dans le Cloud spécifiques à la plateforme Google Cloud. Faites progresser votre carrière chez ce fournisseur de premier plan de services dans le Cloud.

Certification de sécurité du Cloud Alibaba ACA

Cette certification ACA Cloud Security est la première d'un parcours de certification à partir d'Alibaba. L'obtention de cette certification prouvera que vous avez les connaissances de base pour appliquer les principes de sécurité dans le Cloud dans un déploiement de Cloud d'Alibaba.

Vous développerez des compétences fondamentales avec Linux et les opérations de réseau. Vous apprendrez également à connaître les solutions d'hébergement, d'application, de réseau et de sécurité des données, le tout dans le cadre de la plateforme Alibaba Cloud. Vous découvrirez plusieurs produits de sécurité clés d'Alibaba, notamment Server Guard, WAF, Anit-DDoS basic et Pro.

Après avoir obtenu la certification de niveau associé, vous pouvez ensuite poursuivre la certification Alibaba ACP Cloud Security.

Alibaba ACP Cloud Security Certification

La certification ACP Cloud Security est la deuxième certification du parcours de sécurité du Cloud d'Alibaba. Il s'agit d'une certification plus avancée destinée aux architectes, aux développeurs et aux professionnels de l'exploitation et de la maintenance qui travaillent avec les produits de sécurité du Cloud Alibaba.

En vous appuyant sur les compétences et les connaissances de base acquises lors de la certification ACA Cloud Security, vous découvrirez les principaux produits d'Alibaba Cloud en matière de sécurité, de surveillance et de gestion.

Une fois que vous avez obtenu la certification de niveau professionnel, vous pouvez ensuite poursuivre la certification Alibaba ACE Cloud Security. Bien que la certification de niveau expert soit encore en cours de développement et devrait être lancée prochainement.

Cloud Credential Council - Certification professionnelle de gestionnaire de la sécurité de Cloud (PCS)

Le certificat CCC Professional Cloud Security Manager est une certification avancée du Cloud Credential Council. Elle est idéale si vous êtes un professionnel de la gouvernance et des risques, un spécialiste de la conformité des audits ou un spécialiste de l'informatique dématérialisée.

En travaillant à la certification, vous acquerrez les compétences et les connaissances nécessaires pour appliquer les meilleures pratiques dans un environnement de Cloud pour la sécurité et la gouvernance. Vous aborderez des sujets clés comme la gestion des services de Cloud, la gouvernance et la stratégie. Vous apprendrez également comment concevoir, déployer et faire migrer un service de Cloud dans un environnement sécurisé.

En raison du caractère avancé de la certification, il est recommandé d'être déjà titulaire de la CCC Cloud Technology Associate et de la CCC Cloud Virtualization Essentials, fournies par EXIN.

Associé certifié Oracle Cloud Platform Identity and Security Management 2019

Le titre de la certification de sécurité du Cloud d'Oracle est évidente, vous apprendrez la gestion des identités et de la sécurité sur la plateforme Oracle Cloud. Idéal si vous êtes un professionnel de la sécurité cherchant à démontrer son expertise dans la mise en œuvre de solutions de cloud computing.

En vous préparant à la certification, vous couvrirez les fonctionnalités de sécurité essentielles de la plateforme Oracle Cloud. Acquisition de connaissances et de compétences pour mettre en œuvre Oracle Identity Cloud Service, Oracle CASB Cloud Service, les services Architecture et Déploiement, et le cadre du centre d'opérations de sécurité de l'identité

La réussite de l'examen 1Z0-1070 vous certifiera en tant qu'Oracle Certified Associate (OCA), un titre reconnu dans le monde entier. Vous validerez vos capacités avec le portfolio Oracle Cloud Security, y compris la configuration des services. Avant de commencer, vous devrez avoir une expérience pratique et actualisée des mises en œuvre de la sécurité de Cloud dans un rôle d'administrateur.

SANS SEC524 : Fondamentaux de la sécurité et des risques liés au Cloud

Le SEC524 : « Cloud Security and Risk Fundamentals » est un cours, pas une certification. Je l'ai inclus malgré tout car il enseigne des compétences et des connaissances vitales non couvertes par les autres certifications énumérées.

Plus important encore, vous apprendrez à évaluer la sécurité des différents fournisseurs de cloud computing. Les modèles de fourniture de cloud computing - SaaS, PaaS et IaaS - et leurs exigences particulières en matière de sécurité. Ainsi que des considérations de sécurité supplémentaires dans le cadre d'un scénario d'informatique en Cloud public, privé ou hybride.

À la fin du cours, vous en sortirez avec une série de compétences clés. Comment évaluer les contrats de Cloud, adapter l'architecture, les outils et les processus de sécurité pour les utiliser dans des environnements de Cloud et effectuer des évaluations de vulnérabilité de votre installation de Cloud.

Résumé

Pour passer au Cloud, vous devez être prêt à mettre en œuvre une stratégie globale de sécurité du Cloud dès le premier jour. Cela commence par identifier les bons fournisseurs de services de Cloud, puis mettre en œuvre une stratégie combinant les bons outils, processus, politiques et meilleures pratiques.

Il est fondamental que vous compreniez votre responsabilité partagée et que vous vous concentriez sur le respect des règles.

En matière de sécurité dans le Cloud, votre personnel – ou celui de votre fournisseur de services dans le Cloud – est l'un des aspects les plus critiques et souvent négligés de la défense contre les cybercriminels.

Il est important de se rappeler que l'informatique dématérialisée n'est pas moins sûre que le déploiement de vos services sur place. En fait, de nombreux fournisseurs de cloud computing proposent du matériel et des logiciels de sécurité avancés auxquels vous n'auriez pas accès autrement.

Choisir le bon fournisseur améliorera votre position en matière de sécurité et réduira vos risques, indépendamment de ceux introduits par l'informatique dématérialisée.

Edward Jones

Edward Jones is a technology writer with 8 years of industry experience. He has published over 300 articles with major publications that include Microsoft, IBM, and Entrepreneur.

Articles similaires et sujets

Hébergement WordPress infogéré puissant

Débloquez un hébergement WordPress infogéré de qualité supérieure avec Kinsta. Des fonctionnalités de premier plan pour des performances de site in...

12 min de lecture · 5 juin 2024 · Page · Vidéo

En savoir plus

Google Cloud vs AWS en 2024 (Comparaison des géants)

Comparaison approfondie et riche en données de deux géants du cloud computing, Google Cloud vs AWS. Nous analyserons les produits et les avantages...

60 min de lecture · 31 août 2023 · Blog

SEO | Développement d'application | Base de données

Commentaires

Laissez un commentaire

Laisser un commentaire

Politique des commentaires : nous aimons les commentaires et apprécions le temps que les lecteurs passent pour partager des idées et donner des commentaires. Cependant, tous les commentaires sont modérés manuellement et ceux réputés pour être du spam ou uniquement promotionnels seront effacés.

Commentaire

Nom

E-mail

En envoyant ce formulaire : Vous acceptez le traitement des données personnelles soumises conformément à la Politique de Confidentialité de Kinsta, y compris le transfert de données vers les États-Unis.

Vous acceptez également de recevoir des informations de Kinsta relatives à nos services, événements et promotions. Vous pouvez vous désabonner à tout moment en suivant les instructions figurant dans les communications reçues.

Laisser un commentaire

Produits

Hébergement WordPress infogéré

Hébergement d'application web

Hébergement de base de données infogéré

Hébergement de site statique

Tarifs

Faits marquants

Intégration Cloudflare

API Kinsta

Support expert

Migrations gratuites

Outil APM

DevKinsta

Cache Edge

Plans de modules

Cas d'utilisation

Entreprises

Agences

Boutiques WooCommerce

Petites entreprises

Organisations caritatives

Sites uniques critiques

Études de cas

Ressources

Documentation

Journal des changements

Blog

Newsletter

Base de connaissances

Outils de développement

Kinsta et la concurrence

Annuaire d'agences

État du système

Toutes les ressources

Entreprise

À propos de nous

Pourquoi choisir Kinsta

Carrières

Partenaires

Programme d'affiliation

Presse

Sécurité et confiance

Nous contacter

Nous prenons la sécurité et la protection de la vie privée au sérieux

En savoir plus sur la sécurité et la conformité chez Kinsta

SOC 2 Type II GDPR CCPA

Français