Zscaler™ CSPM

zscaler™

Table des matières

Introduction

Nous vivons dans un monde qui évolue rapidement. Chaque industrie est en pleine transformation numérique, faisant du logiciel une partie intégrante de toute entreprise. Afin de rester compétitives, les nouvelles applications doivent être développées rapidement et le cloud public est le seul environnement qui supporte le rythme nécessaire au changement.

Pourtant, la sécurité, le risque et les leaders d'entreprise continuent de se battre contre les problèmes suivants:

1. Les violations de données résultant d'une mauvaise configuration de l'infrastructure cloud continuent d'exposer d'énormes quantités de données confidentielles des clients, ce qui entraîne une responsabilité juridique et des pertes financières.
2. Il est impossible d'assurer une conformité continue pour les charges de travail basées sur le cloud en utilisant les outils et processus traditionnels sur site.
3. Les défis liés à la mise en œuvre de la gouvernance du cloud (visibilité, application des politiques dans les différentes unités opérationnelles, manque de connaissances sur les contrôles de sécurité du cloud) continuent de s'accroître à mesure que l'adoption du cloud prend de l'ampleur au sein de l'entreprise.

Ce document examine le fossé croissant entre la vitesse du développement d'applications cloud et le retard dans l'application des règles de sécurité, notamment les solutions natives d'assurance de sécurité proposées par les fournisseurs de cloud, lesquels n'offrent que des fonctionnalités élémentaires. Nous y abordons la nécessité d'une visibilité accrue et dynamique de la posture de sécurité et d'une collaboration fluide entre les équipes de sécurité et de développement pour faire respecter les normes de sécurité.

> Il ne s'agit pas tant de savoir si le cloud est sécurisé... Il s'agit surtout de savoir dans quelle mesure vous l'utilisez en toute sécurité.
>
> **- Gartner**

Le cloud exige une approche différente en matière de sécurité

Les violations de données ont un impact important sur l'entreprise

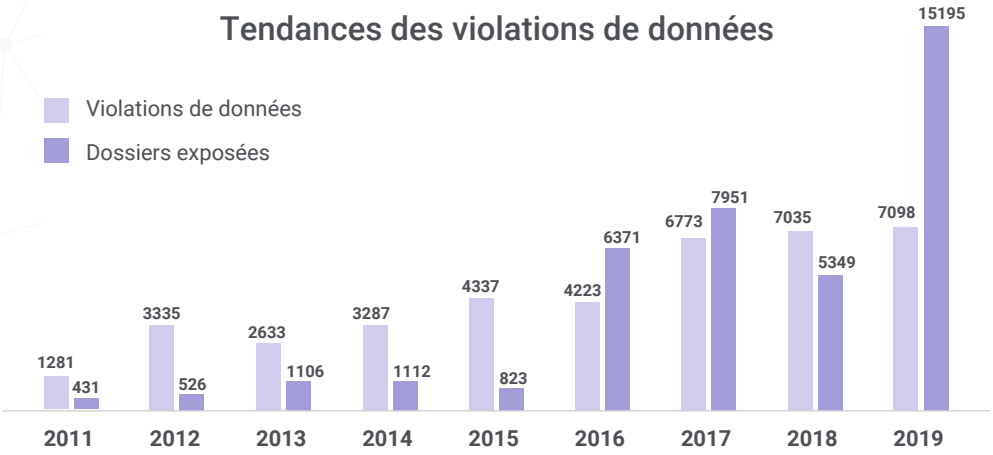
Le rapport IBM Cost of a Data Breach de 2019[1] estimait à 3,9 millions de dollars le coût moyen d'une violation de données à l'échelle mondiale, et à 8,2 millions de dollars le coût à l'échelle nationale. La perte de confiance des clients et la perte d'activité qui en découle sont les principaux éléments de ce calcul de coût moyen.

Coût moyen d'une violation de données

À l'échelle mondiale	Etats-Unis
3.9 $ millions	8.2 $ millions

[1] Cost of a Data Breach Report, IBM, 2019

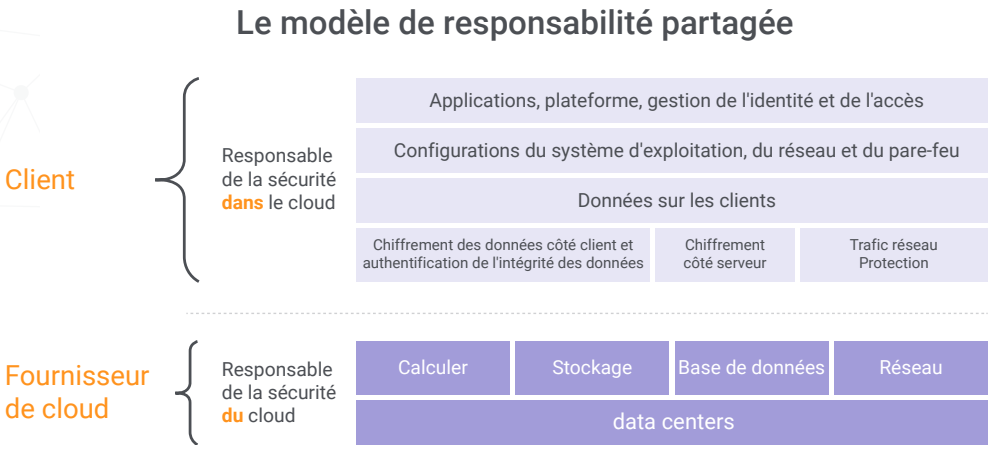
Un récent rapport de Risk Based Security sur les violations de données[2] révèle que 15 milliards de dossiers ont été exposés en 2019, soit un bond important par rapport aux dernières années. Quatre violations causées par des bases de données mal configurées ont exposé 6,7 milliards de dossiers au quatrième trimestre de 2019.



Le rapport 2020 de l'IBM X-Force Threat Intelligence Index[3] a montré une augmentation de près de dix fois d'une année sur l'autre du nombre de dossiers exposés en raison de mauvaises configurations, représentant 86% du total des dossiers compromis en 2019.

Responsabilité de sécurité partagée dans le cloud

Les fournisseurs de services cloud (CSP) ont bâti leur infrastructure à l'aide de divers composants matériels et logiciels (calcul, stockage, base de données, mise en réseau). Les CSP sont responsables de la sécurité "du" cloud. Ils ont fait d'importants investissements dans la sécurité des infrastructures cloud et offrent de multiples certifications de conformité.

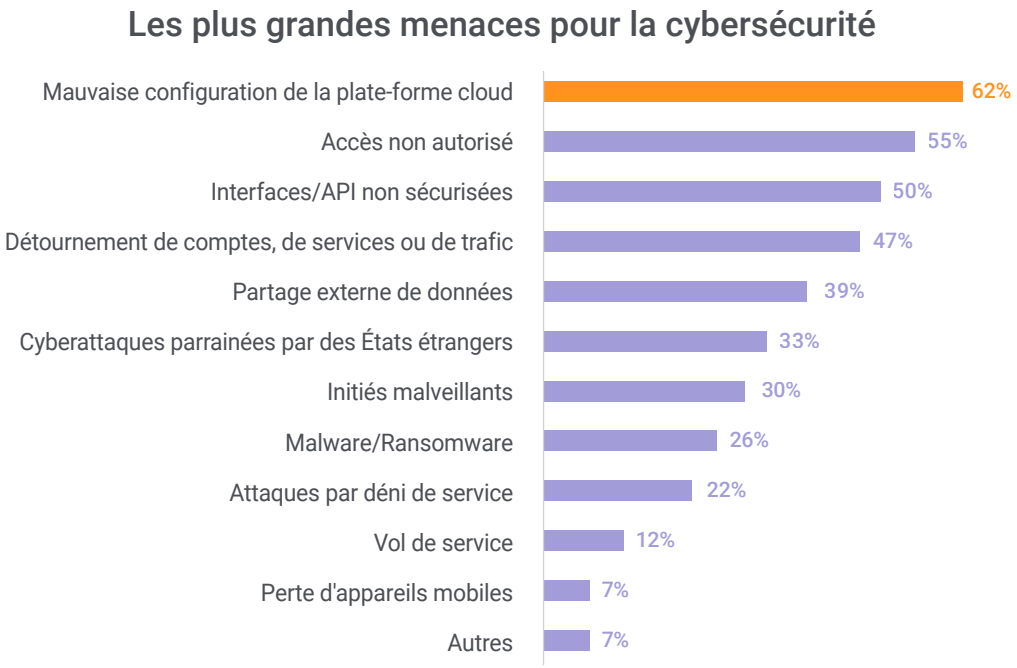


Si les CSP veillent à ce que l'infrastructure sous-jacente soit sécurisée, il incombe au client de s'assurer que les applications sont correctement ficelées, que les données ne sont pas exposées et que les configurations sont définies en toute sécurité. Ceci est vrai pour tous les services cloud consommés par le client, tels que les clusters hôtes et conteneurs, les IaaS, PaaS, SaaS et les services de sécurité.

[2] 2019 Year End Data Breach QuickView Report, Risk Based Security, 2020
[3] IBM X-Force Threat Intelligence Index, 2020

La mauvaise configuration est la plus grande menace pour la sécurité

Les professionnels de la sécurité ont identifié la mauvaise configuration comme la plus grande menace de sécurité du cloud.[4] Mais si l'on considère les autres facteurs de menaces possibles (telles que les accès non autorisés, les interfaces non sécurisées, le détournement de comptes), les causes probables de leur apparition sont principalement des erreurs de configuration.



Les analystes de la recherche ont également reconnu la menace consécutive à une mauvaise configuration. "Presque toutes les attaques réussies sur les services cloud sont le résultat d'une mauvaise configuration, d'une mauvaise gestion et d'erreurs de la part des clients. Les leaders de la sécurité et de la gestion des risques devraient investir dans des processus et outils de gestion de la posture de sécurité du cloud afin d'identifier et de corriger ces risques de manière proactive et réactive", indique le rapport Gartner Innovation Insight for Cloud Security Posture Management.[5]

Les approches traditionnelles de sécurité ne sont plus à la hauteur

Il fut un temps où les entreprises utilisaient le réseau comme périmètre de sécurité pour protéger leurs précieuses informations stockées dans des bases de données et des partages de fichiers. Dans le cloud, une base de données peut être exposée individuellement à Internet avec quelques simples changements de configuration. Un stockage de données verrouillé agit comme un inhibiteur pour les développeurs pendant les phases de développement et ils peuvent le garder ouvert. Ces configurations peuvent se glisser involontairement dans les environnements de production.

Les évaluations de sécurité traditionnelles sont trop lentes

Les audits traditionnels de sécurité et de conformité sont des processus manuels fastidieux et lents. Les évaluateurs interrogent les équipes informatiques et prennent des captures d'écran des configurations de produits comme preuve de conformité. Dans le cloud, la vitesse de changement de l'infrastructure cloud est tellement élevée qu'à la fin d'un audit, l'infrastructure aurait pu être reconstruite à maintes reprises. L'automatisation de la sécurité et de l'assurance de la conformité est le seul moyen pour la sécurité de suivre le rythme de développement et la fréquence des diffusions dans le cloud.

[4] Cloud Security Report, Cybersecurity Insiders, 2018
[5] Innovation Insight for Cloud Security Posture Management, 2019

Les défis à relever pour prouver la conformité

Les industries réglementées doivent se conformer à des repères sectoriels spécifiques tels que PCI DSS pour la distribution de détail, HIPAA pour les soins de santé, FFIEC pour les services financiers, NIST, et bien d'autres. Les entreprises procèdent encore à des évaluations de la conformité sur la base d'entrevues. Rassembler des preuves et les faire correspondre aux cadres de contrôle est une entreprise de grande envergure. Ces cadres de conformité fournissent des contrôles de haut niveau qui doivent être respectés en permanence. De nombreux cadres de conformité (tels que PCI DSS) intègrent le concept de conformité continue comme une exigence. Tous ces problèmes sont aggravés par la charge de travail du cloud qui évolue rapidement.

Les fournisseurs de services cloud offrent des fonctionnalités de base

Les CSP offrent des outils permettant aux clients d'avoir de la visibilité sur la sécurité et la posture de conformité. Ces produits offrent une couverture de base de la politique de sécurité et soutiennent un ensemble limité de cadres de conformité. Pour permettre une sécurité et une assurance de conformité à l'échelle de l'organisation, une importante intégration et un développement personnalisé sont nécessaires. Par conséquent, les entreprises qui déploient des applications dans le cloud public sont obligées d'accepter des compromis entre la vitesse de développement et les risques de sécurité. Les grandes entreprises, qui comptent des centaines de développeurs et qui mettent continuellement de nouveaux codes en production, devront mettre en place une solution de sécurité cloud et d'assurance de conformité entièrement automatisée.

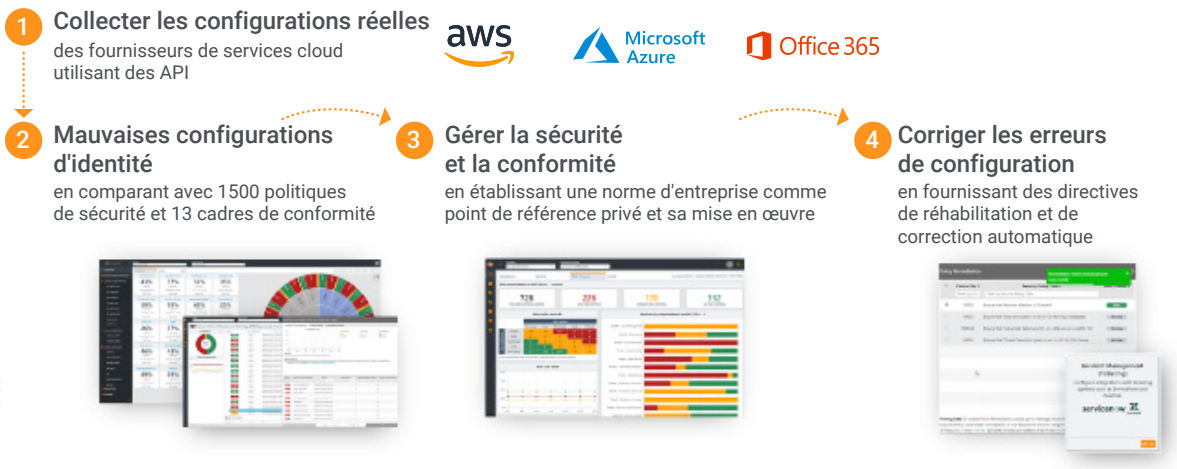
Intégrez la CSPM (Cloud Security Posture Management)

Gartner a défini une nouvelle catégorie de produits qui résolvent plusieurs problèmes de conformité avec la sécurité traditionnelle en automatisant l'assurance de la sécurité et de la conformité et en répondant au besoin d'un contrôle adéquat sur les configurations d'infrastructure cloud, appelant cette catégorie CSPM (Cloud Security Posture Management). En 2020, l'adoption des solutions CSPM est forte et croissante, et devrait atteindre 25 % dans les toutes prochaines années. Les entreprises se rendent compte qu'il s'agit d'un "incontournable" outil de sécurité cloud.

L'Approche de Zscaler en matière de CSPM

Le défi avec la plupart des solutions CSPM est que, en tant que produits ponctuels, ils ne peuvent pas s'intégrer dans les outils de sécurité et de protection des données de plus grandes entreprises, de sorte qu'ils fournissent une visibilité cloisonnée et compliquent l'insertion de la CSPM dans les processus existants d'une entreprise.

Zscaler CSPM résout de manière unique le problème d'intégration en identifiant et en corrigeant automatiquement les mauvaises configurations d'applications, dans le cadre des capacités de protection des données complètes et à 100 % fournies dans le cloud de la plateforme de sécurité cloud de Zscaler.



Zscaler CSPM offre un large éventail d'innovations et de capacités de produits qui automatisent la sécurité et la conformité dans le cloud, offrant une visibilité continue et faisant respecter les politiques de sécurité et les cadres de conformité.

Collecter les configurations réelles

L'application Zscaler CSPM est autorisée à accéder aux environnements cloud des clients (AWS, Azure, Office 365, Google Cloud ou tout autre fournisseur de services cloud). Il collecte ensuite les configurations réelles de l'infrastructure cloud à travers les API. Un petit sous-ensemble de politiques peut nécessiter l'installation d'un agent.

Mauvaises configurations d'identité

Zscaler CSPM compare les configurations découvertes aux politiques de sécurité intégrées et identifie les erreurs de configuration au niveau de la politique de sécurité et des ressources. Il fournit également une cartographie complète des politiques de sécurité dans divers cadres de conformité. Des tableaux de bord et des rapports intuitifs permettent d'examiner ces informations.

Gérer la sécurité et la conformité

Zscaler CSPM permet de mettre en place diverses fonctionnalités de gouvernance du cloud, notamment la hiérarchisation de la posture de sécurité en fonction des risques, la gestion des politiques (par exemple, les dérogations, les exceptions, les compensations par des tiers), et la configuration de points de références privés pour les entreprises qui ont plusieurs normes de conformité ou les équipes de sécurité des informations qui doivent personnaliser l'ensemble des politiques pour une architecture spécifique.

Corriger les erreurs de configuration

Des étapes de correction peuvent être appliquées pour chaque politique de sécurité et une auto-réparation pour un sous-ensemble des politiques de sécurité les plus critiques.

Collecter les configurations réelles

Intégration

Fournir l'accès aux environnements cloud des clients (intégration) est un processus rapide et facile. L'intégration des comptes cloud implique la création d'un rôle d'enregistrement d'application dans Azure et Office 365 et d'un rôle de SecurityAudit dans AWS, puis l'octroi d'autorisations d'accès adéquates (principalement en lecture seule).

Pour certaines politiques, les CSP ne fournissant pas les API nécessaires, Zscaler CSPM a développé des agents pour automatiser la collecte de métadonnées et obtenir la couverture de politiques de sécurité la plus exhaustive.

Multicloud

De nombreuses entreprises mettent en place des initiatives multicloud afin de tirer parti, pour leurs applications professionnelles, des meilleurs services cloud en termes de coûts, de capacités, de sécurité et d'évolutivité. De même, Zscaler CSPM prend en charge de multiples environnements cloud et prévoit de poursuivre son expansion en accord avec la feuille de route du produit.

Multicloud

CSP	2018	2019	2020
Microsoft Azure	■	■	■
Office 365	■	■	■
aws		■	■
Google Cloud Platform			■

Multi-géo

Zscaler CSPM prend en charge plusieurs options de déploiement, y compris le SaaS public (par défaut) et le SaaS privé pour les entreprises qui ont besoin de plus de contrôle sur leurs données. Ces déploiements sont hébergés dans plusieurs régions (géographies) souveraines en matière de données, conformément aux exigences de souveraineté des données du client.

Évolutivité

Les entreprises dont l'environnement est plus vaste et qui disposent de plus de 10.000 ressources cloud ont besoin:

- d'une grande évolutivité dans la collecte des métadonnées de configuration à travers un large éventail de ressources cloud;
- de la possibilité de stocker de grandes quantités de métadonnées collectées dans la base de données;
- de réduire au maximum la durée de la numérisation par balayage; et
- d'afficher rapidement les données relatives à la posture de sécurité sur des tableaux de bord et des rapports intuitifs.

Zscaler CSPM utilise les dernières avancées en matière de cloud computing, telles que la fonctionnalité sans serveur pour la collecte de métadonnées et les bases de données NoSQL (Cosmos DB) pour le stockage des informations. Pour chaque analyse de l'infrastructure cloud, des milliers de fonctions parallèles sans serveur sont créées pour la collecte et le stockage parallèles de métadonnées dans la base de données. La base de données NoSQL est le moyen le plus évolutif et le plus rapide pour stocker et récupérer des données dans le cloud. Zscaler CSPM ne nécessite que quelques minutes pour effectuer une numérisation par balayage et générer des rapports pour une analyse plus approfondie.

Sécurité des données

Les informations stockées dans le cadre du processus de collecte des métadonnées concernent les configurations réelles de l'infrastructure cloud. Si une telle information devient accessible, elle peut conduire à une exposition accrue aux acteurs malveillants. En conséquence, les produits CSPM exigent un chiffrement complet des données en transit et au repos, conformément aux contrôles d'accès basés sur des règles (RBAC) les plus stricts et aux politiques de conservation des données clairement définies.

Les entreprises offrant CSPM en tant qu'offre SaaS vont après la certification SOC 2 pour prouver l'adhésion aux meilleures pratiques de sécurité et la maturité organisationnelle afin de suivre des processus définis.

Mauvaises configurations d'identité

Couverture de la politique de sécurité

L'étendue de la couverture de la politique de sécurité en ce qui concerne la variété des services cloud pris en charge détermine si les solutions CSPM peuvent évaluer correctement tous les services cloud utilisés par le client et l'exhaustivité de la couverture pour chaque service cloud.

Zscaler CSPM propose un ensemble complet de plus de 1500 politiques de sécurité (meilleures pratiques de sécurité dans le cloud) et augmentera même davantage la couverture des politiques à court terme.

Couverture des politiques de sécurité

Infrastructure cloud

IaaS Compute AWS EC2, Azure VMs, VM scale sets, Azure Service Fabric Cluster

PaaS et Serverless fonctions, Lambdas, Applications Web, Applications API, applications mobiles

Mise en réseau Azure Vnet AWS VPC, Cloud Firewall, NSG, groupes de sécurité, DDoS, WAF, ports, protocoles

Data Analytics HDInsight, data lake

Stockage Azure Storage, AWS S3

PaaS Databases Azure SQL DB, SQL serveurs, SQL DW, NoSQL DBs, AWS RDS, AWS RedShift, AWS Aurora DB, AWS Dynamo DB, Postgres SQL, MySQL

Sauvegardes Coffres de sauvegarde, rétention, chiffrement, accès

Journalisation, Audit et Suivi Azure Monitor, Application Insights, CloudWatch, CloudTrail

Cloud Account Security paramètres compte root, paramètres compte IAM, profils de surveillance, configuration des centres de sécurité/hub

Contrôles des accès IAM MFA, usage de rôles intégrés, utilisateur invité

Ligne de base du système d'exploitation de machine virtuelle Windows 2012 R2, Windows 2016

Kubernetes Control Planes Correctif AKS, Integrations ASC, Integrations AD

Key Management Azure Key Vault, AWS KMS

Données en transit TLS/SSL, authentication de certificat, application passerelle, OWASP WAF configurations

SaaS

Identité & Authentification Authentification de base et moderne, self-service Réinitialisation du mot de passe, administrateurs globaux

Permissions d'applications SafeLinks, utilisateurs externes, ATP

Utilisation des applications applications risquées, menaces d'initiés, compte compromis se connecte

Vérification journalisation, rapports d'activité

Données et gestion des données

Gestion de l'appareil gestion d'appareil mobile, Configurations Intune, politiques relatives au mot de passe de l'appareil

Email Sécurité/Échange

Partage de document liste blanche de domaine externe

L'objectif est de couvrir l'ensemble des services cloud les plus fréquemment utilisés et de répondre aux besoins spécifiques supplémentaires des clients. Chaque CSP a son propre ensemble de politiques requises. Zscaler CSPM a toujours été le leader en matière de couverture de politique pour Microsoft Azure et Office 365; et grâce à de récents ajouts, la politique de couverture AWS est parmi les meilleures du secteur de l'industrie.

Cadres de conformité

Zscaler CSPM offre 13 cadres de conformité, y compris la cybersécurité et les points de références du secteur, les lois et les réglementations. Cet ensemble est en cours d'expansion pour inclure des cadres de conformité régionaux pour l'Europe, ainsi que pour l'Australie et d'autres pays.

Cadre de conformité

Points de référence de la cybersécurité

NIST CSF | NIST 800-53r4 — CIS — CSA cloud security alliance®

Lois et règlements

HIPAA COMPLIANCE — General Data Protection Regulation

Points de référence de l'industrie

NIST CSF | NIST 800-53r4 — ISO 27001 — PCI Data Security Standard V 3.2 — AICPA SOC — SOC 2

FFIEC — GxP

Gérer la sécurité et la conformité

Zscaler CSPM permet de mettre en place diverses fonctionnalités de gouvernance du cloud, notamment la priorisation de la posture de sécurité en fonction des risques, la gestion des politiques et la configuration de points de références privés.

Gestion des politiques

Zscaler CSPM offre diverses fonctionnalités pour gérer l'application des politiques de sécurité aux actifs découverts.

- Les exclusions de politiques permettent aux clients de définir une exclusion temporaire (limitée dans le temps) ou permanente d'une politique aux comptes cloud.
- Les dérogations aux politiques permettent aux clients de marquer certaines politiques comme "approuvé" (indiquant la conformité) dans les cas où les clients ont des contrôles compensatoires de tiers qui ne peuvent pas être déterminés par le produit du CSPM
- Les politiques manuelles permettent aux clients de suivre les meilleures pratiques lorsque l'automatisation ne serait pas disponible (par exemple, les CSP ne fournissent pas d'API, ou le client n'aurait pas accordé à Zscaler CSPM l'accès pour scanner ses données sensibles).

Points de référence privés

Les exigences de sécurité varient considérablement d'une entreprise à l'autre en fonction de facteurs tels que l'industrie et la taille. Les clients pourraient décider de regrouper tous leurs contrôles (sur l'ensemble de la conformité et des meilleures pratiques) dans un référentiel privé. Plusieurs personnes au sein de l'entreprise peuvent collaborer à la création du référentiel et à son application à des comptes cloud spécifiques.

Zscaler CSPM offre une interface de configuration facile à utiliser pour créer des points de références privés à partir d'une norme existante ou à partir de rien, en fonction des besoins de chaque entreprise. Puisque ces points de références privés sont contrôlés par version, les clients l'utilisent également pour appliquer continuellement des normes plus élevées sur une certaine période. Un point de référence privé v1 sera appliqué au départ, un autre v2 sera appliqué pour améliorer la posture de sécurité dans les versions ultérieures, et ainsi de suite.

Matrice de risque

La matrice Zscaler CSPM de priorisation basée sur le risque respecte la norme ISO 27005. La matrice de risque catégorise automatiquement chaque politique de sécurité en fonction de l'impact sur les risques et de la probabilité. L'*impact* sur les risques va de "Pas probable", "Faible", "Modéré" et "Élevé" à "Certain". La *probabilité* de risques va de "Très faible", "Faible", "Modéré" et "Élevé" à "Critique". L'impact sur les risques est prédéfini pour chaque politique de sécurité. La probabilité de risque est calculée dynamiquement en fonction de plusieurs paramètres et d'un algorithme d'apprentissage automatique.

Matrice des risques (basée sur ISO 27005)

Niveau de risque

Elevé 109

Modéré 150

Bas 201

Probabilité du risque	Impact des risques: Très faible	Faible	Modéré	Élevé	Critique
Certain	10	50	61	27	15
Élevé	0	0	0	1	0
Modéré	0	0	0	2	5
Faible	0	0	0	0	0
Peu probable	0	75	126	72	16

Les couleurs indiquent le niveau de risque et les chiffres indiquent le nombre de politiques de sécurité.

La matrice des risques comporte un axe X et un axe Y indiquant le nombre de politiques de sécurité dans chaque segment X / Y. En conséquence, les politiques de sécurité ayant un impact et une probabilité de risque élevés sont classées comme étant à risque "élevé".

Corriger les erreurs de configuration

Directives pour la remise en état

Lorsque les entreprises déploient manuellement une infrastructure cloud, elles doivent mettre à jour leurs guides de configuration et assainir les ressources pour les conformer à toutes les politiques de sécurité de leur référentiel privé. Zscaler CSPM offre des directives de correction de la politique de sécurité sous la forme d'étapes faciles à comprendre en utilisant la console CSP et des lignes de commande ou des scripts, lorsque cela est possible.

Résolution automatique

Lorsque certains types d'erreurs de configuration surviennent en production, l'on peut ne pas avoir le temps d'attendre qu'un ticket soit attribué à la bonne personne ou que la bonne personne soit disponible à cette période de travail pour les corriger. Des questions de sécurité critiques de ce genre doivent être résolues sans délai.

Zscaler CSPM offre des politiques de correction automatique qui sont déclenchées quelques instants après qu'un changement de déploiement a été initié par un client (par exemple, un nouveau déploiement ou la modification manuelle de configurations à l'aide de consoles de fournisseurs cloud). Zscaler CSPM fournit un plan de gouvernance pour que les clients puissent, parmi des centaines disponibles, sélectionner des politiques de correction automatique et décider de les piloter pour les environnements de pré-production. Après avoir été testées en pré-production, ces politiques peuvent être appliquées dans les environnements de production.

Automatisation du déploiement

S'il est important d'avoir une bonne visibilité sur les mauvaises configurations, il est également important d'empêcher que celles-ci ne soient mises en production. Les entreprises qui déploient manuellement une infrastructure cloud devraient automatiser le déploiement pour toutes les ressources essentielles.

Zscaler CSPM fournit des scripts d'automatisation Quick Win ainsi que des recommandations. L'on conseille aux entreprises d'établir un dépôt central de données pour l'automatisation du déploiement. Lorsque le déploiement des ressources essentielles est automatisé, l'entreprise peut commencer à se diriger vers une automatisation complète des DevSecOps.

Intégration de la billetterie

Zscaler CSPM s'intègre aux systèmes de billetterie des clients pour automatiquement générer et affecter des tickets au membre de l'équipe Cloud Operations (CloudOps) approprié. Ces tickets contiennent des informations vitales sur les ressources non conformes et les directives de remédiation. Zscaler CSPM attribue automatiquement la priorité aux tickets afin de faciliter la gestion de leur capacité par l'équipe CloudOps. Un administrateur de Zscaler CSPM peut configurer et limiter la fréquence des tickets créés (par exemple, ne pas exécuter, quotidien, hebdomadaire, mensuel, etc.).

Intégration du DevOps

Les entreprises qui mettent en œuvre des processus de sécurité et d'assurance de la conformité dans le Cloud se rendent compte que le déploiement manuel ou semi-automatisé d'une infrastructure Cloud est toujours sujet à l'erreur humaine.

La plupart des entreprises mettent en œuvre l'automatisation pour augmenter leur vitesse de diffusion des logiciels. Les changements de déploiement fréquents ont un énorme potentiel pour modifier la posture de sécurité dans une direction inattendue. Afin de garantir une amélioration continue de la posture de sécurité, ces validations de sécurité sont intégrées dans des filières de conformité continue/développement continu (CI/CD).

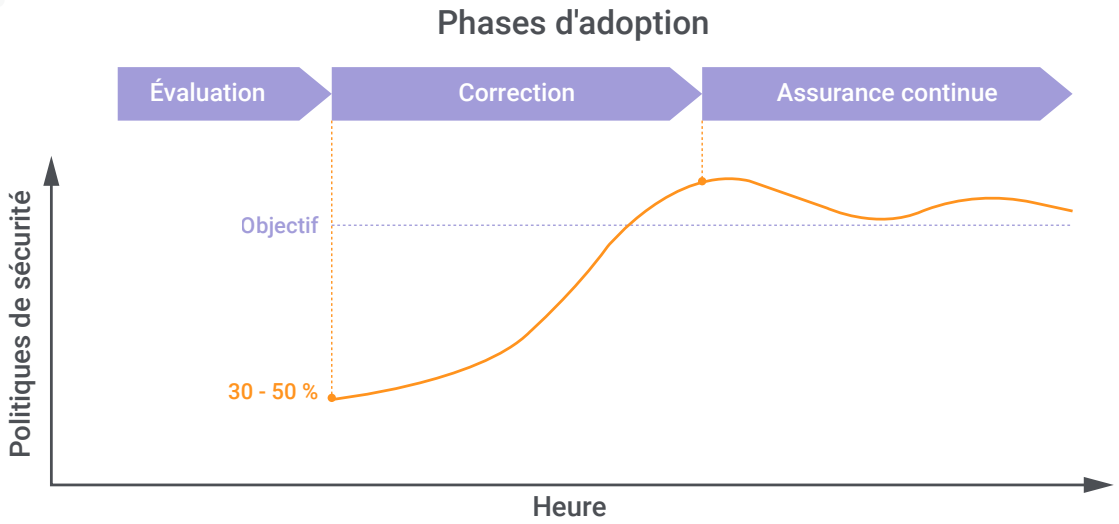
Zscaler CSPM prend en charge toutes les intégrations CI/CD requises. Un compte cloud nouvellement créé peut être automatiquement intégré à Zscaler CSPM. Une demande peut être envoyée pour lancer une analyse de la sécurité de l'infrastructure et une autre pour récupérer la posture de sécurité et la conformité. Une analyse automatique peut être effectuée pour déterminer s'il faut maintenir un déploiement en production ou le réduire. Ces fonctionnalités DevSecOps sont conformes au changement de sécurité prévu.

CSPM est une collaboration entre plusieurs équipes

Les étapes de l'adoption

Évaluez votre posture de sécurité

Les entreprises utilisent les solutions de CSPM pour fournir des preuves de conformité basées sur des cadres de cybersécurité communs tels que CIS ou NIST; dans les secteurs réglementés, elles soutiennent des cadres de conformité spécifiques à l'industrie tels que HIPAA pour les soins de santé, SOC 2 pour les éditeurs de logiciels indépendants, PCI DSS pour le commerce électronique, ISO 27001 pour les entreprises ayant des activités internationales et FFIEC pour les services financiers.



Les solutions CSPM peuvent être utilisées pour effectuer une évaluation de l'infrastructure cloud existante afin de déterminer la posture actuelle de sécurité. Généralement, un projet est ensuite initié pour identifier les politiques de sécurité "indispensables", en collaboration avec l'équipe de sécurité de l'information (InfoSec), et lancer les activités de remédiation.

Réhabiliter pour atteindre l'objectif

La réhabilitation nécessite une formation spécialisée de l'équipe CloudOps sur les meilleures pratiques en matière de sécurité du cloud ainsi que des nouvelles exigences de configuration. Les réhabilitations sont d'abord validées dans les environnements de pré-production pour s'assurer que les nouvelles configurations d'infrastructure cloud n'influenceront pas les applications ni n'affecteront les performances. Les environnements de développement, de test et de pré-production sont reconstruits selon de nouvelles configurations en adéquation avec la posture de sécurité souhaitée. Par conséquent, la posture de sécurité s'améliore pour atteindre et/ou dépasser les objectifs.

Assurance continue

Une fois la réhabilitation effectuée, les équipes CloudOps se chargent de la sécurité et de l'assurance de la conformité. Elles surveillent quotidiennement la posture de sécurité dans l'environnement de production pour s'assurer que les corrections ou mises à jour de dernière minute ne génèrent pas de mauvaises configurations.

Des outils d'assurance sécurité sont également utilisés en permanence dans les environnements de développement, de test et de pré-production pour valider l'exactitude des configurations avant de déployer de nouvelles versions d'applications dans les environnements de production.

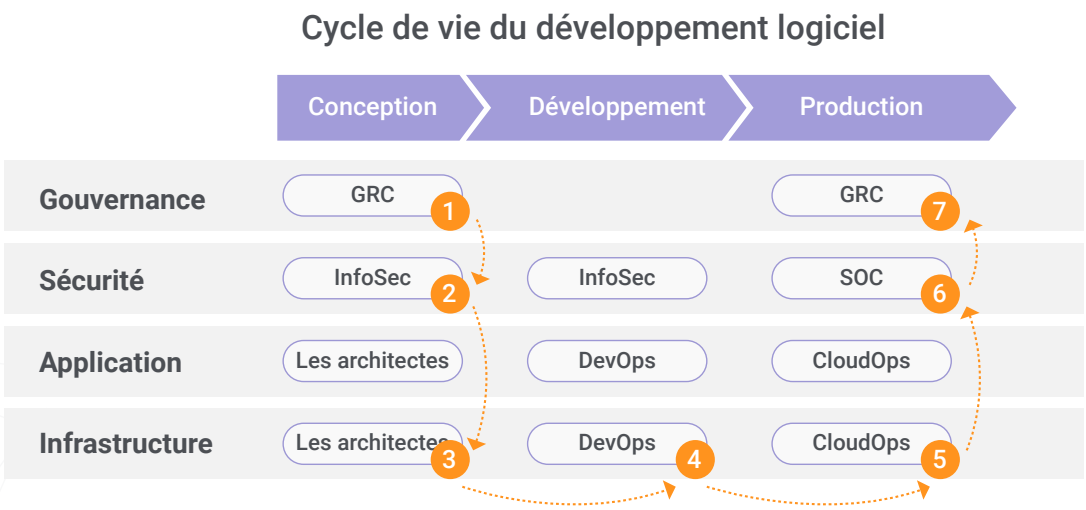
Les équipes d'opérations de sécurité (SOC) devraient ajouter à leurs tableaux de bord le contrôle de la posture de sécurité et faire remonter rapidement toute erreur de configuration critique détectée dans l'environnement de production.

Collaboration interministérielle

Le déploiement de CSPM améliore la collaboration entre les équipes InfoSec, SOC et de développement d'applications (AppDev). Bien que l'équipe InfoSec soit responsable de la définition de la norme d'entreprise (objectif), les équipes de développement d'applications et de gestion d'infrastructure doivent en fin de compte assumer la responsabilité de la mise en œuvre des normes de sécurité et de conformité.

Le processus CSPM comprend les étapes suivantes:

1. La GRC précise les cadres de conformité requis
2. InfoSec définit les normes de sécurité des informations de l'entreprise
3. Les architectes du cloud créent des configurations sécurisées d'architecture d'applications
4. DevOps déploie une infrastructure cloud
5. CloudOps corrige les erreurs de configuration découvertes
6. SOC surveille la posture de sécurité
7. GRC fournit des preuves de conformité continue



GRC: Cadres de conformité

Les équipes GRC spécifient les cadres de conformité requis du secteur (points de référence, lois et règlements définis par l'industrie). Zscaler CSPM prend en charge divers cadres de conformité et en ajoute continuellement de nouveaux en fonction des besoins des clients.

InfoSec: Norme d'entreprise

L'équipe InfoSec a la responsabilité de définir un ensemble de politiques de sécurité "incontournables" pour son entreprise, y compris des points de référence de la cybersécurité et des politiques supplémentaires propres à l'entreprise. En outre, Zscaler CSPM offre la possibilité d'ajouter des points de référence privés que les clients peuvent suivre et appliquer.

Architectes cloud: Guides de configuration

Les architectes conçoivent l'infrastructure cloud, en tenant compte des meilleures pratiques en matière d'architecture cloud, et créent des guides de configuration sécurisée pour les équipes CloudOps. Zscaler CSPM fournit des définitions détaillées pour toutes les politiques de sécurité ainsi que des conseils de configuration sous forme d'étapes de remédiation.

DevOps: Déployer les infrastructures

Dans de nombreuses entreprises, l'infrastructure cloud est déployée manuellement par l'équipe de gestion de l'infrastructure, tandis que d'autres entreprises ont un déploiement automatisé de l'infrastructure cloud par l'équipe DevOps. L'équipe de gestion de l'infrastructure ou l'équipe DevOps scanne l'infrastructure cloud à l'aide de Zscaler CSPM dans l'environnement de pré-production. Toute mauvaise configuration découverte doit être corrigée avant de passer au déploiement de la production. Nous décrivons le scénario entièrement automatisé plus loin dans la section DevSecOps de ce document.

CloudOps: Corriger les erreurs de configuration

L'équipe CloudOps entreprend une analyse immédiatement après le déploiement dans l'environnement de production. Si l'infrastructure cloud déployée répond aux normes requises, elle peut rester en production. CloudOps programme également des scans quotidiens de l'infrastructure cloud. Toute erreur de configuration découverte doit être corrigée rapidement en fonction de la priorité et de leur niveau de risque.

SOC: Surveillance continue

Les environnements de production devraient être analysés quotidiennement pour valider toute modification manuelle de dernière minute de la configuration. Les équipes SOC surveillent les écarts et font remonter les erreurs de configuration critiques qui nécessitent des corrections immédiates.

GRC: Preuves de conformité

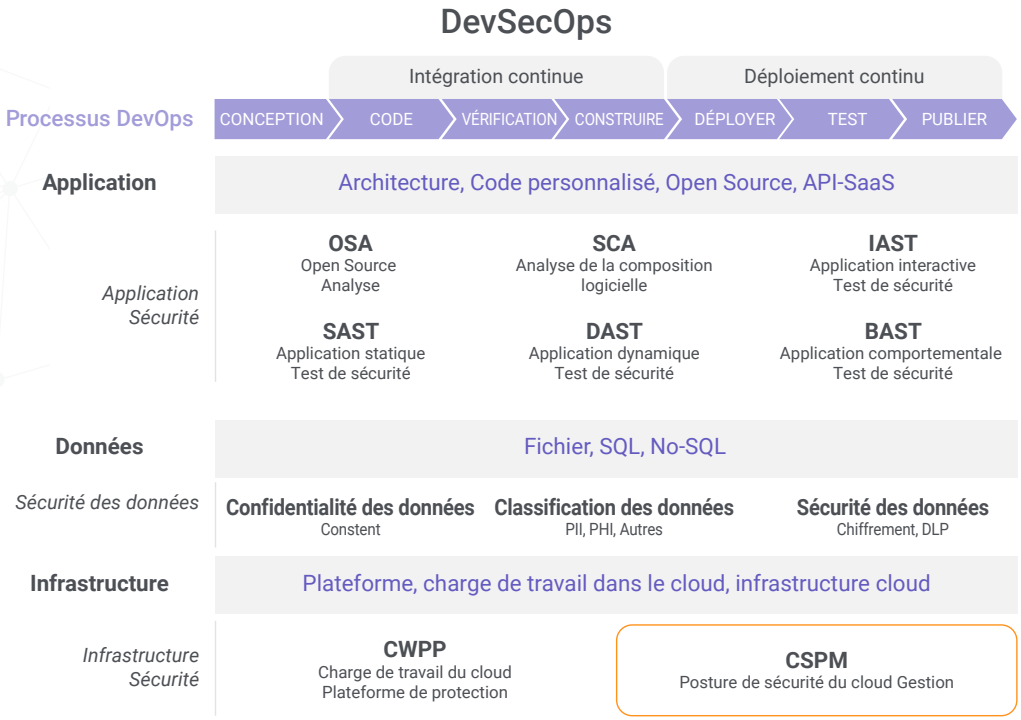
Les équipes de conformité ont accès à des résultats de contrôle quotidiens et peuvent fournir ces rapports comme preuve de conformité continue aux régulateurs et aux auditeurs.

Réaliser les DevSecOps

Pratiques du DevSecOps

Sécurité des applications: Le terme DevSecOps est normalement utilisé pour décrire l'intégration des pratiques de sécurité des applications dans le cycle de développement des applications. Les tests de sécurité des applications statiques (SAST), les tests de sécurité d'applications dynamiques (DAST) et d'autres outils sont utilisés pour comparer les meilleures pratiques de codage, découvrir les problèmes de sécurité et consigner les défauts. Les tests de pénétration sont utilisés pour valider la robustesse du code de l'application avant sa mise en production. L'autoprotection des applications d'exécution peut être mise en œuvre.

Sécurité des données: La sécurité des données a pris une importance significative avec l'introduction du règlement RGPD. La confidentialité des données, la classification des données et les pratiques de sécurité des données doivent être validées dans l'environnement de pré-production dans le cadre de DevSecOps.



Infrastructure cloud: Consommée à partir du CSP, l'infrastructure cloud peut être déployée et configurée en utilisant Infrastructure as Code (IoC). Ce qui n'est pas communément compris, c'est que la configuration de l'infrastructure cloud fait également partie intégrante du modèle d'exploitation global de DevSecOps.

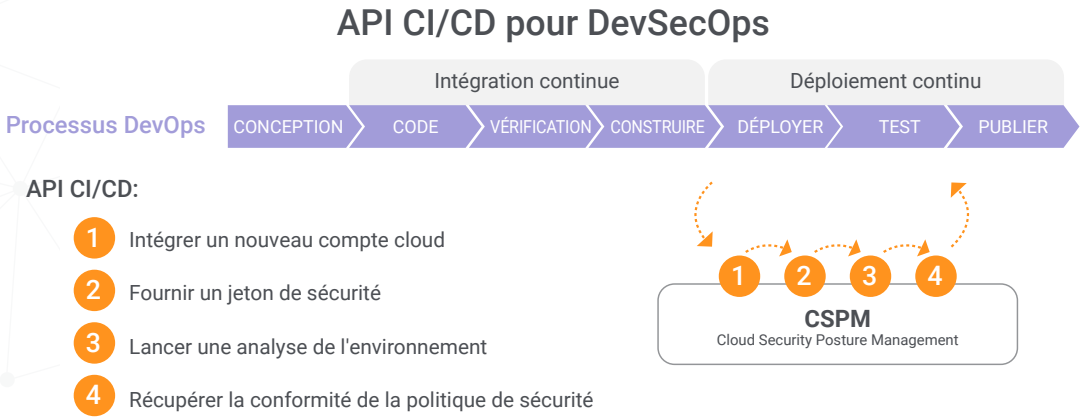
En fin de compte, les entreprises doivent s'orienter vers un processus DevSecOps intégré couvrant les meilleures pratiques de sécurité pour les applications, les données et l'infrastructure. Un changement de sécurité doit intervenir pour identifier les mauvaises configurations dans les environnements de pré-production et les empêcher d'entrer dans les environnements de production.

Alors que l'automatisation du déploiement devient partie intégrante de la filière CI/CD, il est essentiel que les configurations des infrastructures cloud soient également validées par rapport aux meilleures pratiques de sécurité du cloud. Les produits du CSPM doivent fournir des API pertinents qui peuvent être appelés par les pipelines CI/CD.

API CI/CD requises

Les produits CSPM doivent soutenir des processus de bout en bout, notamment:

1. Intégration d'un nouveau compte cloud
2. Fourniture de jeton de sécurité
3. Lancement d'une analyse de l'environnement (dev, test, autre)
4. Obtention automatique d'informations sur la politique de sécurité "approuvée" ou "rejetée" pour les comparer aux normes des entreprises



Les équipes DevOps peuvent utiliser les API CI/CD de Zscaler CSPM pour lancer automatiquement une nouvelle analyse après la construction de l'environnement et recevoir le statut de conformité pour toutes les politiques de sécurité. Les équipes peuvent analyser les résultats d'un scanner et mettre à jour leur dépôt d'automatisation des IoC conformément aux normes de configuration. Des conseils de Zscaler CSPM sur les mesures correctives sont également disponibles pour soutenir ces efforts.

Zscaler CSPM

Zscaler CSPM automatise la sécurité et la conformité dans le cloud, en offrant une visibilité continue et en imposant l'adhésion à l'ensemble le plus complet de politiques de sécurité et de cadres de conformité. Offert en tant que SaaS multi-entité, le produit permet une intégration transparente à l'infrastructure cloud du client, une collecte rapide des données, des tableaux de bord complets et des rapports. Zscaler CSPM supporte les intégrations avec les pipelines CI/CD et les systèmes de billetterie, permet l'auto-réparation et supporte les points de référence privés. Les clients peuvent facilement appliquer leurs normes de sécurité des informations d'entreprise dans les environnements AWS, Azure et Office 365 afin d'éviter les violations de données liées à une mauvaise configuration.

Leader du marché

Zscaler CSPM automatise la visibilité du statut de plus de 1500 politiques de sécurité et de 13 cadres de conformité sur AWS, Azure et Office 365. Le produit permet également aux entreprises de créer leurs propres points de référence privés, prend en charge des environnements d'application à grande échelle et permet l'adoption rapide de DevSecOps.

Empêcher les erreurs de configuration

La mauvaise configuration de l'infrastructure cloud est le plus grand risque pour la sécurité du cloud. En automatisant la sécurité du cloud et l'assurance de la conformité, les organisations peuvent considérablement réduire leurs risques en matière de cybersécurité et démontrer une conformité continue à leurs organismes de réglementation.

Mettre en œuvre les DevSecOps

Les processus manuels de sécurité et de conformité ne sont d'aucune utilité étant donné la nature dynamique des environnements cloud. Zscaler CSPM offre une couverture des politiques de sécurité à la pointe et propose une intégration rapide et facile basée sur une API avec les outils DevSecOps.

Accélérez l'adoption du cloud

Lorsque la sécurité et la conformité sont sous contrôle, les dirigeants peuvent donner leur feu vert à une adoption plus rapide du cloud. Les initiatives de transformation numérique peuvent s'accélérer, donnant aux clients de Zscaler CSPM un avantage concurrentiel.

Adoptez la gouvernance numérique

CSPM est une première étape importante dans la transformation des fonctions de sécurité, de conformité, de gestion des risques et de confidentialité des données pour s'adapter à la vitesse du cloud. Les entreprises numériques bénéficient de processus de gouvernance automatisés.

Pour plus d'informations, consulter zscaler.com/CSPM

A propos de Zscaler

Zscaler permet aux plus grandes organisations internationales d'adapter en toute sécurité leurs réseaux et leurs applications à un monde résolument tourné vers le mobile et le cloud. Ses services phares que sont Zscaler Internet Access™ et Zscaler Private Access™, créent des connexions rapides et sécurisées entre les utilisateurs et les applications, et ce quels que soient l'appareil, l'emplacement ou le réseau. Les services Zscaler sont à 100% fournis dans le cloud et offrent la simplicité, une sécurité renforcée ainsi qu'une amélioration de l'expérience utilisateur inégalables par les appliances traditionnelles ou les solutions hybrides. Adopté dans plus de 185 pays, Zscaler gère une plate-forme multi-entité de sécurité cloud distribuée qui protège des milliers de clients contre les cyberattaques et les pertes de données. Pour en savoir plus, accédez à zscaler.com ou suivez nous sur Twitter @zscaler.

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com