

# Zscaler™ Cloud Protection en un coup d'œil

## Avantages de Zscaler Cloud Protection (ZCP) :

### ✓ Cloud sécurisé par une posture de sécurité

Inventaire permanent et correction de tous les services des plateformes cloud (Azure, AWS, GCP) et des applications SaaS

### ✓ Accès sécurisé des utilisateurs aux charges de travail dans le cloud

Zero trust offre un accès utilisateur sans surface d'attaque exposée et sans VPN

### ✓ Communication sécurisée d'application à application

Sécurise et simplifie les communications de charge de travail vers Internet, les data centers et les clouds

### ✓ Suppression du mouvement latéral de la menace

L'automatisation de l'identité des applications et du ML facilite la microsegmentation et empêche la propagation latérale des menaces

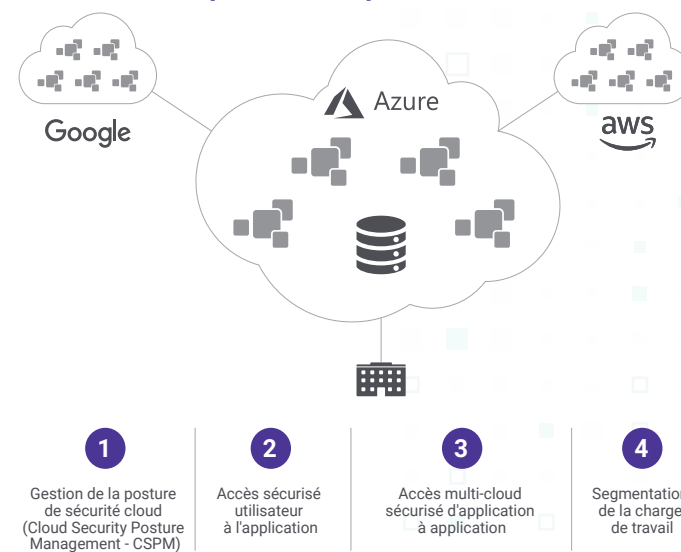
Le cloud ne cesse d'accélérer la transformation numérique de tout type d'industrie, ouvrant la voie à une nouvelle ère d'évolutivité, de performance et d'agilité pour les applications cloud d'entreprise. Malheureusement, ces mêmes atouts du cloud qui permettent aux entreprises d'évoluer rapidement et à grande échelle viennent avec des failles de sécurité.

L'approche « lift-and-shift » consistant à adapter la sécurité des data centers obsolètes aux environnements de cloud public est coûteuse, compliquée et statique. Raison pour laquelle les équipes InfoSec sont incapables de suivre le rythme du développement et du déploiement des DevOps.

Le ZCP s'appuie sur l'architecture Zscaler Zero Trust Exchange afin de réduire le risque de migrer vers le cloud ainsi que la complexité opérationnelle. Les quatre composantes du ZCP s'attaquent aux principaux défis à relever en matière de sécurité et d'opérations pour un déploiement sécurisé du cloud :

- Identifier les charges de travail dans le cloud et s'assurer qu'elles disposent d'une posture de sécurité renforcée
- Garantir un accès sécurisé aux applications et réservé aux utilisateurs autorisés
- Permettre aux charges de travail d'accéder en toute sécurité à d'autres clouds, à d'autres data centers et à Internet si nécessaire
- Minimiser les risques en restreignant le mouvement latéral d'un hacker

## Les quatre composantes du ZCP



# Capacités principales de Zscaler Cloud Protection



## Gestion de la posture de sécurité cloud (Cloud Security Posture Management - CSPM)

- Inventorier, surveiller en permanence et corriger automatiquement tous les services cloud, y compris le IaaS, le PaaS, les conteneurs, le serverless, etc.
- Une politique de couverture approfondie dans les domaines AWS, Azure, GCP et SaaS, avec plus de 3000 modèles de politiques préconfigurés et mis en correspondance avec 16 cadres réglementaires importants



## Accès sécurisé utilisateur à l'application

- Tirez parti du Zero trust pour fournir un accès non pas à votre réseau, mais aux applications, limitant ainsi de potentielles menaces extérieures sans les casse-tête de gestion. Réduisez aussi les mauvaises expériences utilisateur et les surfaces d'attaque exposées qui sont courantes avec les VPN traditionnels



## Communication d'application à application entre les clouds rendue sécurisée

- Déployez et configurez automatiquement la connectivité de cloud à cloud et de cloud au data center sans la complexité, les coûts et les frais que créent la gestion des passerelles de transit, les hubs de transit, les pare-feux virtuels, les VPN, les routeurs, les politiques de réseau et le peering
- Sécurisez et facilitez l'accès cloud à Internet grâce à l'évolutivité, aux performances et à la fiabilité avérées du Zero Trust Exchange, garantissant un accès sûr et contrôlé à partir de n'importe quel cloud sans aucune surface d'attaque exposée



## Microsegmentation basée sur l'identité

- Vérifier l'identité des charges de travail du cloud et du data center et micro-segmenter automatiquement tout cloud ou data center pour éliminer la surface d'attaque et empêcher le mouvement latéral et la propagation des programmes malveillants
- Réduire le nombre de politiques de 90 % ou plus

"Presque toutes les attaques réussies sur les services cloud sont le résultat d'une mauvaise configuration, d'une mauvaise gestion et d'erreurs".

– Gartner

Pour en savoir plus sur les avantages de Zscaler Cloud Protection, consultez [zscaler.com/ZCP](https://www.zscaler.com/ZCP) >

