Cloud Security Governance

Les entreprises migrent de plus en plus leurs données, applications et ressources informatiques vers le cloud public, ce qui accroît non seulement la flexibilité mais aussi la complexité et les exigences en matière de sécurité.

**Cloud Security Governance propose une solution de sécurité simple et évolutive pour le multi-cloud qui vous permet d'avoir à tout moment une totale transparence sur la sécurité de vos ressources cloud.**
Cloud Security Governance est une solution CSPM (Cloud Security Posture Management) qui surveille vos ressources cloud, crée de la transparence et vérifie que la configuration des ressources cloud ne renferme pas d'erreurs ni de vulnérabilités. Elle reconnaît les changements apportés aux directives (policies) et s'assure que la conformité est respectée à tout moment. Un rapport régulier soutient les entreprises et leur donne une visibilité et une transparence totales pour leurs opérations informatiques si elles utilisent un cloud public ou un multi-cloud.

## Vos avantages avec Cloud Security Governance

**Visibilité et transparence**

Ce service donne un aperçu de votre infrastructure cloud et des configurations de sécurité de cette dernière. Les résultats sont documentés dans un rapport régulier.

**Respect des directives (policies) et des exigences de conformité**

Les infractions aux directives et à la conformité sont automatiquement détectées et affichées par des scans de découverte automatisés.

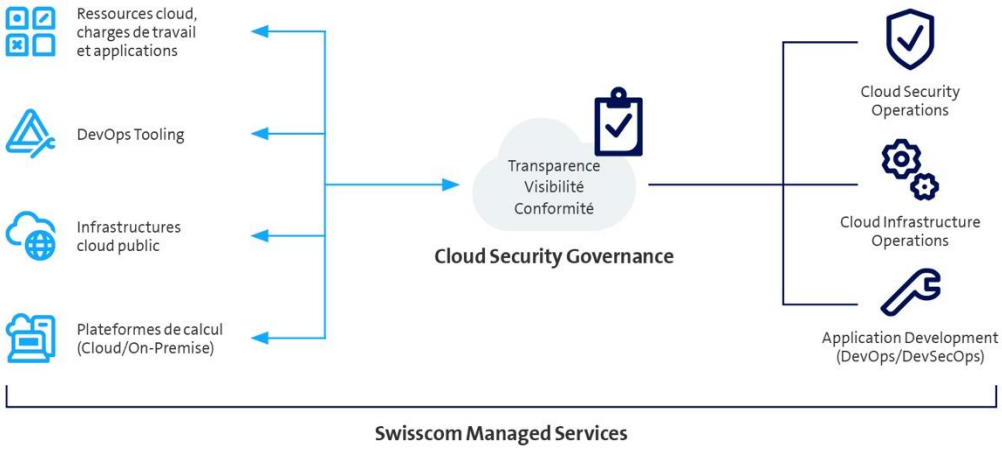
**Identification des erreurs de configuration et des vulnérabilités**

La solution vérifie en permanence l'évaluation des vulnérabilités de votre infrastructure cloud, y compris d'éventuels paramètres de sécurité et erreurs de configuration.

**Indépendante du fournisseur de cloud public**

La solution est indépendante du fournisseur de cloud public (Azure, AWS, GCP) et peut être utilisée dans un environnement multi-cloud. Elle offre en outre la même protection pour des solutions qui sont installées sur différentes infrastructures de cloud public. Les implémentations de sécurité établies restent inchangées en cas de changement de fournisseur de cloud.

## Voici comment fonctionne Cloud Security Governance




swisscom

# Faits & chiffres

## Services de base

### Cloud Security Posture Management (CSPM)

Ce module de service garantit une transparence, une conformité et une gouvernance complètes pour les ressources cloud. Cela est possible grâce à une surveillance et à un contrôle continus de toutes les ressources cloud pour identifier les erreurs de configuration, les vulnérabilités, ainsi que tout comportement anormal et malveillant.

- Transparence et visibilité totales pour repérer les erreurs de configuration, infractions aux directives (policies) et à la conformité, ainsi que détection des vulnérabilités (sans agent) dans un environnement multi-cloud (Azure, AWS, GCP).
- Exploitation d'une solution CSPM
- Fourniture régulière de rapports
- Livrables du projet pour l'introduction de la solution et de son cycle de vie
- Le décompte mensuel dépend du nombre de ressources cloud surveillées.

## Services en option

### Cloud Infrastructure and Entitlement Management (CIEM)

CIEM permet d'évaluer les autorisations effectives qui sont affectées aux utilisateurs, charges de travail et données (également appelées privilèges) à l'intérieur de l'instance cloud surveillée. Il est ainsi possible de gérer correctement les directives de gestion des identités et des accès (IAM) et de faire respecter l'accès selon le principe du moindre privilège.

- Visibilité des autorisations sur le réseau
- Directives prédéfinies et affectation des droits
- Contrôle des autorisations et privilèges IAM
- Intégration de fournisseurs d'identité
- User and Entity Behavior Analytics (UEBA)

### Infrastructure as Code (IaC)

Le module IaC scanne des modèles pendant tout le cycle de développement pour détecter les erreurs de configuration et les secrets divulgués. Les politiques en matière de sécurité sont intégrées dans les environnements de développement, les outils d'intégration continue, les répertoires et les environnements d'exécution. IaC fait respecter suffisamment tôt les directives dans le code grâce à l'automatisation, empêche les problèmes de sécurité de se propager et propose des corrections automatiques.

- Gouvernance continue en faisant respecter les directives dans le code
- Intégrée dans les workflows et outils DevOps
- Corrections automatisées des erreurs de configuration par le biais de pull requests

### Autres services

- Accès au tableau de bord
- Service de consultation pour introduire et améliorer en permanence la sécurité sur le cloud
- Conseils, adaptations et modifications spécifiques au client (temps et matériel) en cours d'exploitation



**Swisscom (Suisse) SA** Enterprise Customers, Case postale, CH-3050 Berne, tél. 0800 800 900, www.swisscom.ch/enterprise