Cloud Security Protection

Les charges de travail cloud renferment souvent des données sensibles telles que les informations sur les clients, la propriété intellectuelle et les données financières. Les entreprises doivent garantir qu'elles bénéficient d'une protection adéquate.

Cloud Security Protection protège les hôtes, les conteneurs, les systèmes Kubernetes et les fonctions sans serveur dans les environnements multi-cloud pendant tout le cycle de vie des applications (build, deploy and run).
Cloud Security Protection est une solution CWP (Cloud Workload Protection) qui offre une protection complète pour les charges de travail cloud par une analyse des vulnérabilités, un monitoring continu, une détection proactive des menaces et des mesures de sécurité automatisées. Il est possible d'étendre le service pour y inclure des fonctions modulaires en fonction des besoins du client et de le relier à un Security Operations Center (SOC).

Vos avantages avec Cloud Security Protection

Monitoring continu

Permet un monitoring sans faille de vos charges de travail cloud en temps réel pour détecter suffisamment tôt des risques potentiels en matière de sécurité. ✓

Détection proactive des menaces

Identifie et réagit automatiquement aux menaces avant qu'elles ne puissent causer des dégâts. ✓

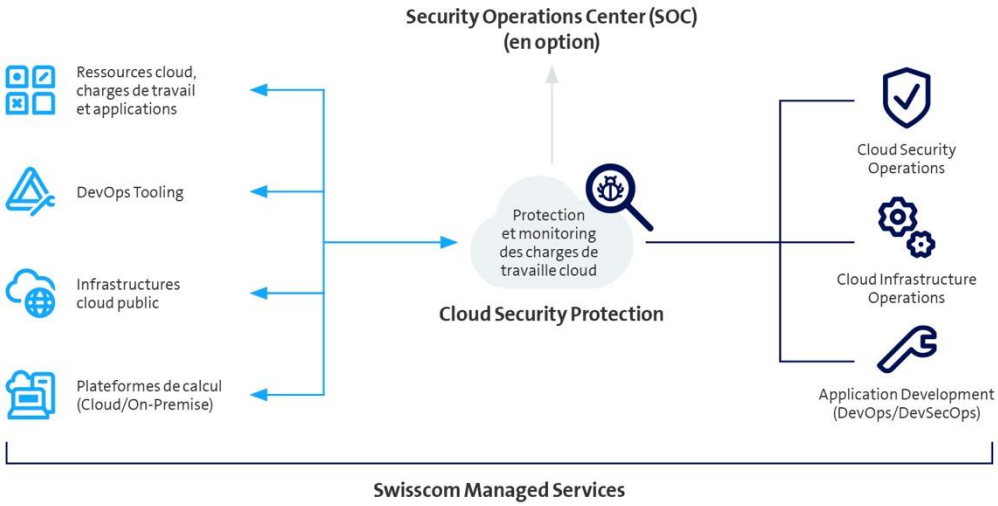
Gestion des vulnérabilités

Identifie et évalue les vulnérabilités dans les charges de travail cloud pour permettre des mesures de sécurité ciblées visant à atténuer les risques. ✓

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 installées sur les différentes infrastructures cloud public. Les implémentations de sécurité établies restent inchangées en cas de changement de fournisseur cloud. ✓

Voici comment fonctionne Cloud Security Protection



swisscom

Faits & chiffres

Services de base

Cloud Workload Protection (CWP) / Vulnerability Management (VM)
Ce module de service comprend une solution CWP et VM qui offre une protection flexible pour les MV dans le cloud, les conteneurs et les applications Kubernetes, les fonctions sans serveur et les tâches conteneurisées. Les équipes DevOps et les équipes chargées de l'infrastructure cloud peuvent reprendre l'architecture qui répond à leurs exigences.

- Soutien pour les clouds publics et privés
- Protection flexible basée sur agent et balayage sans agent
- Sécurité intégrée pendant toute le cycle de vie de l'application
- Accès au tableau de bord
- Livrables du projet pour l'introduction de la solution et de son cycle de vie
- Exploitation du service, gestion des alertes et des incidents
- Le décompte mensuel dépend du nombre de charges de travail cloud surveillées

Services en option

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 référentiels 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.

Web Application and API Security (WAAS)
Le module WAAS offre une approche intégrée pour la sécurité des applications web et des API. Il soutient l'OWASP Top 10 et la protection des API, avec des fonctions comme la gestion des vulnérabilités, la conformité et la protection au niveau de l'exécution. Le module identifie et protège automatiquement les applications web basées sur des microservices et les API dans les environnements cloud et sur site.

Software Composition Analysis (SCA)
Correction proactive des vulnérabilités des sources ouvertes, gestion des licences et priorisation contextuelle.

Secrets Security
Découverte et sécurisation des secrets exposés et vulnérables dans tous les fichiers des référentiels et des pipelines CI/CD.

Data Security
Classification des données et balayages antimaliciels dans les stockages public cloud.

Threat Detection and Response – SOCaaS
Intégration et fourniture des données du Cloud Security Protection Service avec le Swisscom Threat Detection and Response – SOCaaS ou un autre Security Operations Center spécifique au client.

Autres services
- 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