



Companies are storing more and more of their data, applications and IT resources in the public cloud.

This not only increases flexibility, but also the complexity and security requirements.

Cloud Security Governance offers a simple and scalable security solution for multi-cloud, giving you full transparency over the security situation of your cloud resources at all times.

Cloud Security Governance is a CSPM (cloud security posture management) solution that monitors your cloud resources, provides transparency and checks

cloud resources for misconfigurations and vulnerabilities. It detects changes to policies and ensures compliance is maintained at all times. A regular report helps businesses and enables complete visibility and transparency for IT operations in public or multi-cloud environments.

Your benefits with Cloud Security Governance

Visibility and transparency

This service provides insight into your cloud infrastructure and its security requirements. The results are documented in a regular report.



Fulfilment of policies and compliance requirements

Breaches of policies and compliance are automatically detected and presented with automated discovery scans.



Detection of misconfigurations and vulnerabilities

The solution continuously checks the vulnerability rating of your cloud infrastructure, including potential misconfigurations and security settings.

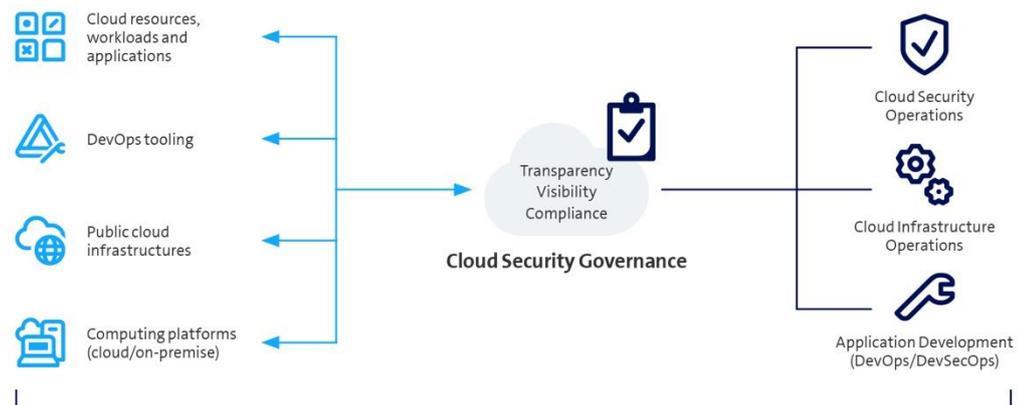


Independent of public cloud providers

The solution is independent of public cloud providers (Azure, AWS, GCP) and can be used in a multi-cloud environment. It also offers the same protection for solutions installed on different public cloud infrastructures. When switching cloud providers, the established security implementations remain unchanged.



How Cloud Security Governance works





Facts & Figures

The information in this document does not constitute a binding offer. Subject to changes at any time.

Swisscom (Schweiz) AG Enterprise Customers, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise

Cloud security posture management (CSPM)

This service module ensures comprehensive transparency, compliance and governance for cloud resources. This is achieved with the continuous monitoring and checking of all cloud resources for misconfigurations, vulnerabilities as well as anomalous and malicious behaviour.

Basic services

- Full transparency and visibility over misconfigurations, breaches of policies and compliance, as well as (agent-less) detection of vulnerabilities in a multi-cloud environment (Azure, AWS, GCP).
 - Operation of a CSPM solution.
 - Regular provision of reports.
 - Project services for the introduction of the solution and its lifecycle.
 - Monthly billing is determined by the number of monitored cloud resources.
-

Cloud infrastructure and entitlement management (CIEM)

CIEM enables the evaluation of effective entitlements assigned to users, workloads and data (also known as permissions) within the monitored cloud instance. As a result, identity and access management (IAM) policies can be correctly managed and access enforced according to the principle of minimising entitlements.

Optional services

- Visibility of permissions that affect the network
- Predefined policies and assignment of rights
- Checking of IAM permissions and privileges
- Integration of ID providers
- User and entity behaviour analytics (UEBA)

Infrastructure as Code (IaC)

The IaC module scans templates for misconfigurations and disclosed secrets throughout the entire development cycle. The security policies are embedded in the development environments, tools for continuous integration, repositories and run-time environments. IaC uses automation to implement policies in code at an early stage, preventing security issues and offering automatic corrections.

- Continuous governance to implement policies in code
- Embedded in DevOps workflows and tools
- Automated corrections of misconfigurations via pull requests

Further services

- Access to the dashboard
 - Consulting services for introducing and continuously improving cloud security
 - Advice, customer-specific adjustments and changes (time and material) during live operations
-