Audit Guard

Increasing digitisation is leading to a growth in the risk of deliberate data theft. Data protection laws and industry-specific regulations require companies to be able to document the traceability of user activities in the event of an incident.

Audit Guard makes it possible to deal transparently with sensitive data in companies and flags up any breaches of industry-specific standards.

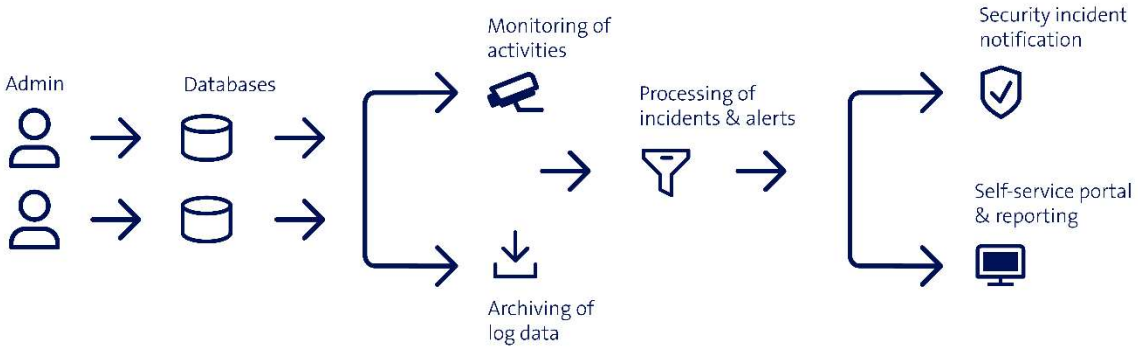
What is Audit Guard?

The *Audit Guard* service logs user and system activities on predefined objects to be protected, such as applications, servers and databases. All activities are monitored, classified, and analysed based on standardised security rules. If there is a breach of the applicable security regulations, you are notified promptly so that you can respond quickly to suspicious activity. Evidence is generated periodically to ensure compliance with the various regulations or traceability in the event of an incident.

Your benefits with Audit Guard

- Identification and monitoring of your vulnerable buildings
- Transparency and documentation of all user and system activities on sensitive data
- Tried and tested policy for meeting your industry-specific compliance requirements.
- Immediate notification in the event of breaches of applicable security rules
- Activity logs archived for at least 18 months
- Evidence of your compliance requirements
- Managed Service – benefit from our many years of expertise

The solution at a glance



swisscom

Facts & figures

Basic services	Monitoring of user and system activities
	Log data archived for 18 months
	Standardised rule set for security incidents (policies)
	Systematic analysis of activities
	Detection and validation of incidents
	Processing and reporting of security incidents
	Provision of a self-service portal
	Monthly security standard report
Optional services	Customised rule set for security incidents (policies)
	Daily event summary report
Supplementary services	**Data Loss Prevention (DLP)** lets you monitor channels such as e-mail, web traffic, devices and SharePoint, thereby preventing the unauthorised leakage of sensitive information. This means that you can also supply the evidence required for compliance purposes.
	Sensitive Data Service (SDS) gives you an accurate overview of where your sensitive data are stored (e.g. personal and customer data, patient information, contracts and patents).
	Compliance consulting: With "Data Protection Check", we define together the type of data that is particularly sensitive for your company in the context of GDPR.

Find out more about Audit Guard at www.swisscom.ch/auditguard

Swisscom (Switzerland) Ltd Enterprise Customers, P.O. Box, CH-3050 Bern, Telephone 0800 800 900, www.swisscom.ch/enterprise

swisscom