IBM **Security**

Create secure digital experiences across hybrid environments

Silos across on-premises environments create security gaps

With continued hybrid cloud adoption, security teams are finding difficulties **scaling their security solutions across multiple environments**

As these environments grow, so do their **threat landscapes**, putting a strain on resources needed to keep up and maintain security.

Additionally, **new and evolving data privacy and compliance regulations,** paired with consumer demand for better security are pushing organizations to prioritize and embed data security within their greater business strategy.

The IBM Security Guardium Data Protection Solution

Discover and respond to threats in near real-time

Product Overview

IBM Security Guardium Data Protection is a data security platform delivering visibility into your data across on-premises and cloud environments.

By complementing and extending native security controls on Azure, Guardium discovers and classifies sensitive data, monitors and secures your entire data landscape, and leverages analytics to identify and understand how to respond to threats and vulnerabilities.

Guardium enables organizations to quickly identify and resolve security vulnerabilities across on-premises and cloud environments

Product Benefits

- Scalable architecture. Meet the everchanging data security needs of expanding data and threat landscapes to protect data across both on-premises and cloud environments.
- Pre-build security template. Leverage pre-built templates that streamline compliance and audit workflows, freeing up resources to focus on preventing data threats.
- Analytics-backed security. Identify and prioritize threats to enable security teams to understand and resolve potentially malicious activity, such as an insider threat.
- Simplified tool integration. Seamlessly integrate Guardium with existing security tools to create a broader security strategy that breaks down data silos

IBM

Why Guardium Data Protection?

Data monitoring flexibility

Guardium delivers both active and passive monitoring, ingesting audit log data from Amazon Kinesis to monitor across multiple AWS data sources.

Identify vulnerabilities and threats

Proactively scan for vulnerabilities with more than 3000 assessment tests and identify user risks with advanced analytics.

Integrate to remediate

Orchestrate threat remediation and response by integrating with common security tools.

Discover sensitive data wherever it resides

Identify regulated data in your environment and automatically define and map apps to their sources.

Visibility across hybrid environments

Guardium provides cloud-native and containerized agents to monitor and enforce policies at the data source

Protect & Comply

Guardium enables administrators to define policy and track progress against compliance regulations

IBM Security Guardium Data Protection on Azure

Guardium takes a continuous approach to help organizations achieve data security and compliance across on-premises and Azure.

Guardium operates through a single console, enabling security teams to set and monitor policies across all their environments from one place. With pre-built regulatory templates, Guardium makes it easier for organizations to meet regulatory and privacy requirements.

Additionally, IBM Security Services offers resources to enhance Guardium deployments on Azure by guiding organizations through comprehensive, tailored security strategies.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM **Security**