IBM Guardium Data Security Center

Protect your data from current and emerging risks through a unified experience

Highlights

Protect your structured and unstructured data on-premise and in the cloud

Manage the full data security lifecycle from discovery to remediation

Empower security teams to collaborate through integrated workflows and an open ecosystem

Hybrid cloud and artificial intelligence (AI) are cornerstones of an organization's digital transformation strategy as they can help to enhance operations and boost innovation. Yet, as data expands into hybrid cloud and generative AI deployments, there is an expanded threat surface. Rapid advancement of quantum computing technology and "harvest now, decrypt later" attacks by bad actors, pose additional threats to the security of our digital landscape. Business and technology innovation can leave critical data unprotected.

There can be a loss of visibility of where data is stored, who has access to it, and how it is protected. Growing usage of generative AI deployments - with training and fine-tuning data, models and applications - can lack a security and governance lifecycle to protect against risks. Organizations are struggling with how to prioritize risks and address security gaps across a spectrum of use cases — from shadow data, shadow AI to cryptographic posture. In addition, data protection is becoming increasingly complex and difficult when using separate tools to address component parts of the data security lifecycle.

Traditional methods of data protection must evolve to protect data in the cloud, in AI and in the quantum era. To simplify data protection in the future, a shift from point products to a data security platform is occurring. Organizations need a modern solution to help protect sensitive data across these emerging risk sources in addition to their traditional data security missions. They also need a unified solution to bring siloed teams and tools together to protect their critical assets – organization data.

IBM® Guardium® Data Security Center protects your data from current and emerging risks, including AI threats and cryptographic attacks, through unified security controls. Manage the full data security lifecycle, from discovery to remediation, across all your data environments. It allows you to break down organizational silos and empowers security teams to collaborate across the organization through integrated workflows, a common view of data assets, centralized compliance policies and an open ecosystem.

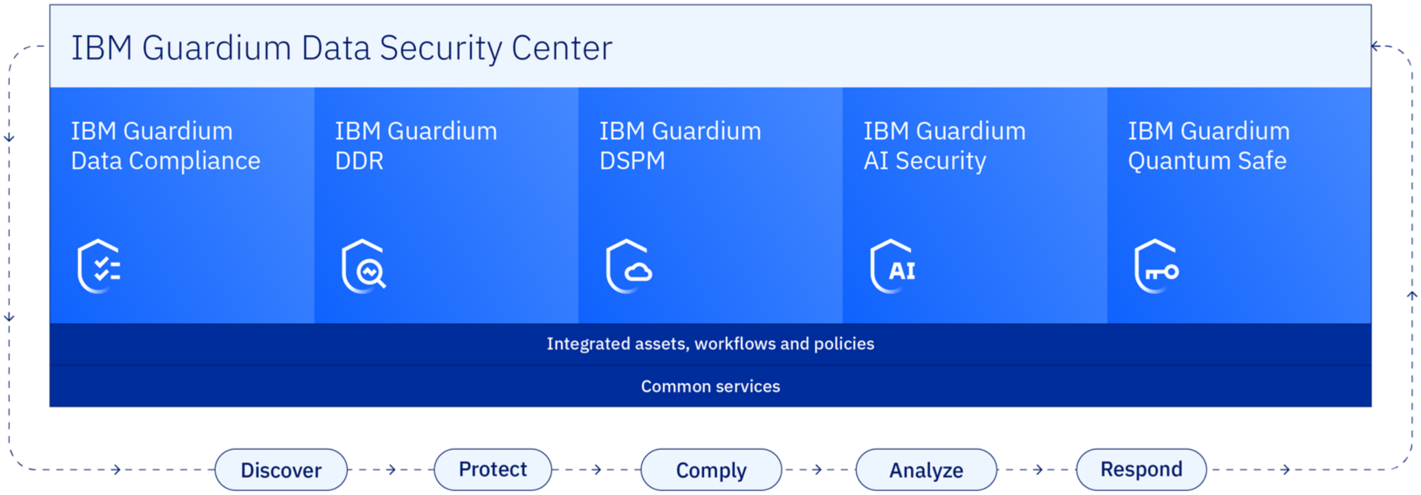
IBM Guardium Data Security Center
IBM Guardium Data Compliance
IBM Guardium DDR
IBM Guardium DSPM
IBM Guardium AI Security
AI
IBM Guardium Quantum Safe
Integrated assets, workflows and policies
Common services
Discover
Protect
Comply
Analyze
Respond

Figure 1 IBM Guardium Data Security Center

80%
of data breaches involved data stored in cloud environments.[1]

76%
of current Generative AI projects are not secured.[2]

Unified data security solution

IBM Guardium Data Security Center is designed to share data, events and insights between modules. Each module contributes to and consumes information from the platform. It offers users a powerful combination of common services, such as identity and access, risk and policy engines, data ingestion and warehouse, and an integration gateway. Additionally, shared experiences bring intelligence and workflows together across modules. At the heart of the solution are common standards, accessibility and common design for optimal user interface and user experience.

The modules of IBM Guardium Data Security Center (Figure 1) include :

IBM® Guardium® Data Compliance: Programmatically simplify data regulation needs, enhance visibility, and streamline monitoring.

IBM® Guardium® DDR: Safeguard your data with ready-to-use integrations that enable your SOC to locate signals in the noise.

IBM® Guardium® DSPM: Automatically discover, classify and secure your data across multiple cloud environments and SaaS applications.

IBM® Guardium® AI Security: Manage the security risk of sensitive data being used in AI models. Discover AI deployments, mitigate vulnerabilities in AI models and protect sensitive data, while meeting regulatory requirements.

IBM® Guardium® Quantum Safe: Monitor your enterprise's cryptography use, uncover cryptographic vulnerabilities, and prioritize remediation to secure your data from both conventional and quantum-enabled risks.

.

Guardium Data Security Center empowers you to continually assess risks and vulnerabilities in your environment with near real-time automated notifications. As a robust data security platform, this single solution will help organizations to efficiently protect their data, manage the full data security lifecycle, and empower security teams to collaborate – especially with the rapid business and technology innovation with hybrid cloud and AI, and in the quantum era. As your organization's data security requirements change and scale, Guardium Data Security Center's simplified pricing and packaging make it easy to adjust and expand its usage.

For more information

To learn more about IBM Guardium Data Security Center, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/guardium-data-security-center.

1. Cost of a Data Breach Report 2024, July 2024
2. Securing Generative AI, May 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
October 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.