IBM Security

Modernized Data Security

How IBM Security Guardium compares to the competition

IBM

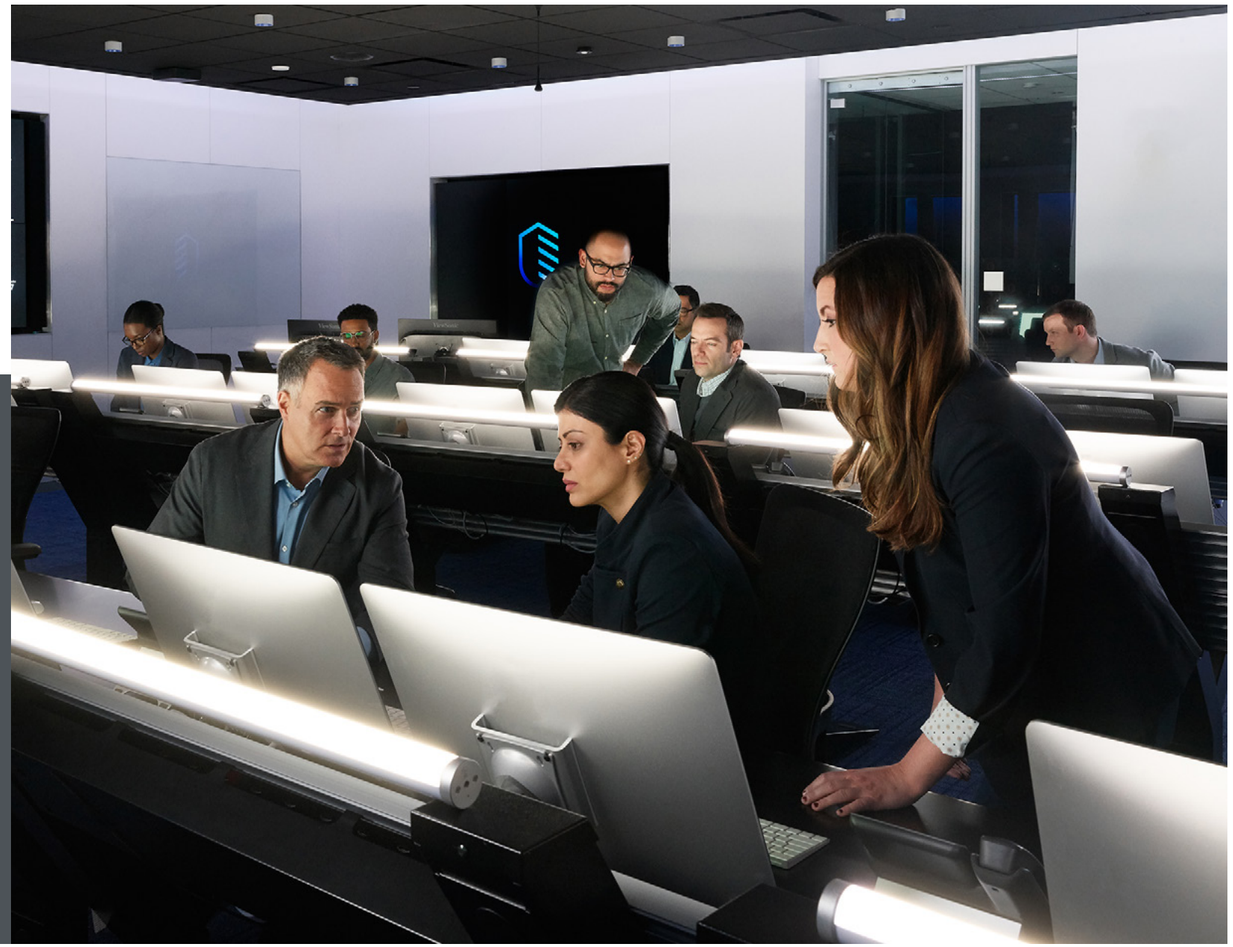
Begin your tour →

Overview

As the cost of a data breach continues to grow — with recent estimates at $3.86 million on average per breach[1] — the demand for modern, forward-looking data security solutions follows in kind. However, the data security market is consolidating. Dominant players have emerged, and established organizations that suddenly find themselves falling behind may merge – or acquire niche providers in an effort to achieve the kind of modernization needed. Organizations looking to select a data security provider are surely curious to understand how IBM Security Guardium stacks up against other solutions in the market. The purpose of this brief is to demystify the data security vendor landscape—a landscape where, according to The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019,[2] IBM Security Guardium is a Leader.

According to The Forrester Total Economic Impact of IBM Security Guardium, conducted by Forrester Research, sponsored by IBM Security, one large organization that was interviewed and deployed Guardium Data Protection had achieved a risk-adjusted return on investment (ROI) of 401%—or $4.0m.[3]

The Ponemon Institute reports, in a study sponsored by IBM Security, that 65% of surveyed customers deploying Guardium Data Protection realized value within 1 month of deployment.[4]



All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Contact IBM to see what we can do for you.

Modernization and Vision

Business pressures and client needs have changed, and organizations are pressing IT teams to start moving infrastructure to the cloud while supporting hybrid environments.

Guardium

A platform for the hybrid cloud

Guardium provides clients with a suite of modernized, containerized solutions on a hybrid multi-cloud architecture. What does this mean? It means that in order to suit clients' changing needs, the Guardium portfolio can be deployed flexibly – on-premises or in public or private clouds.

Unified data security to combat tool sprawl

This architecture provides the benefits of autoscaling, native disaster recovery, low latency with high ingestion performance, and in-place upgrades and multi-tenancy. The goal is a unified suite of data security capabilities that can be deployed flexibly, maintained easily, designed with the user experience in mind, and provides a connected and automated approach to data security.

Adjusted for risk, Guardium's modernized approach to data security—specifically Guardium Data Protection's ability to automate database analysis processes—saved one studied organization 1,000 hours per year and $822k over three years, according to The Forrester Total Economic Impact of IBM Security Guardium study sponsored by IBM Security.

Other solutions

A platform for the hybrid cloud

Many solutions in the market today employ one of two distinct and drastically different architectures. The first is a traditional hardware approach, limited in its scalability. The other, while traditional in its on-premises deployment, touts custom report and workflow creation but requires clients to familiarize themselves with specific backend databases and scripting languages—which can often present an expensive, specialized, and time-consuming learning curve.

Alignment with Gartner's Data Security Governance Framework

Considered a data security gold standard, Gartner's Data Security Governance Framework recommends that data governance, compliance, and security be effectively unified. Further, this framework outlines best practices and steps to achieve this comprehensive approach.

Guardium

Answering the call of the analysts

IBM can bring a breadth of capabilities to support Gartner's Framework through Guardium's broad suite of data security capabilities, which can discover and classify data across on-premises and cloud environments; monitor user activity in near real-time; analyze and assess risk via contextual advanced analytics; protect through encryption and data access policies; respond to threats in near real-time and send actionable alerts; and simplify overall data security policy and compliance.

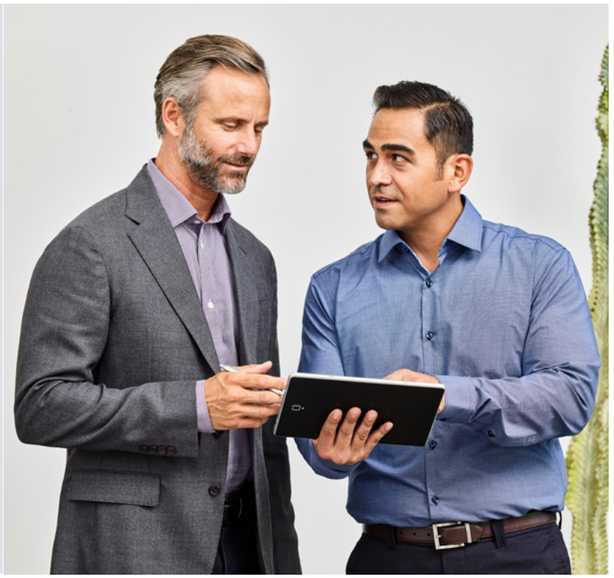
Coordination across the SOC

Beyond data security, Guardium's integration with IBM Cloud Pak for Security, IBM Cloud Pak for Data, the IBM Security portfolio, and 3rd party SIEM, ticketing, log, and native API sources can expand the aperture of this unified strategy, sharing data security and compliance data across IT operations and security teams.

According to The Forrester Total Economic Impact of IBM Security Guardium study sponsored by IBM Security, Guardium Data Protection's ability to help clients address compliance regulations—such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA)—yielded a risk-adjusted savings of $1.1m for one customer by reducing likelihood of a regulatory fine by 2%.[3]

Other solutions

As Gartner outlines in their Use the Data Security Governance Framework to Balance Business Needs and Risks report, "increasing numbers of data security, privacy and identity access management products are in use, but they do not integrate, do not share common policies, and have siloed coverage of data stores and security functionality." This illustrates the importance of a unified approach. Many customers without a unified solution will struggle to meet data management, governance, and threat response requirements—falling short of Gartner's guidance.



Support for Major Data Collection and Monitoring Types

When it comes to data collection and monitoring, there is no one-size-fits all approach. For comprehensive data security, flexibility, and variety in data collection methods are necessary for organizations striving to meet a wide variety of use cases.

Guardium

A broad spectrum of data collection selections with Guardium

Guardium supports a broad spectrum of collection methods, from agent- (Guardium S-TAP) and proxy- (Guardium E-TAP) based —meeting a range of real-time monitoring, compliance, and protection needs—to agentless (native or API audit log streaming, or via the Universal Connector) deployment. Through these approaches, Guardium can support near real-time and passive monitoring use cases to support modern, Cloud-based data sources and traditional data sources.

An expanded universe of data source connectivity

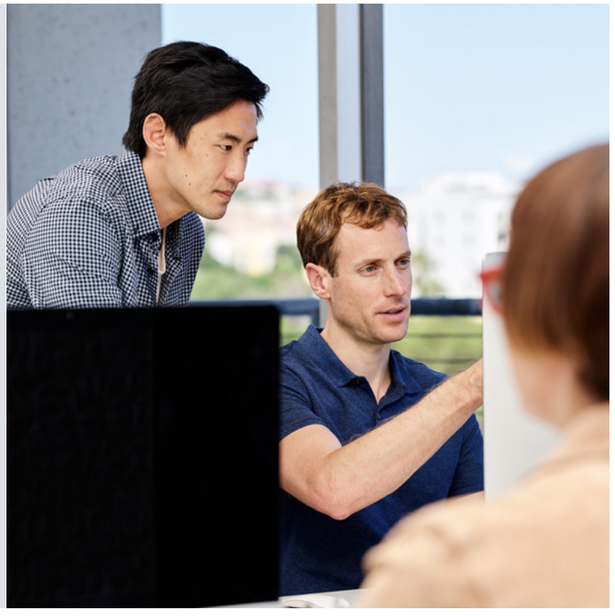
Through the Guardium Universal Connector, organizations can also receive support for additional data sources they need connected. This open-source approach helps clients collect the data they need without being hindered by incompatibility.

The ability to centralize data collection by supporting multiple sources within Guardium Data Protection, can streamline the collection and analysis of data for audit. According to The Forrester Total Economic Impact of IBM Security Guardium study sponsored by IBM Security, this streamlining reduced overall effort needed by one studied customer to conduct an audit by 75% after adjusting for risk—equivalent to a savings of $2.1m.3

Other solutions

Collection confusion can make it difficult to get a clear picture

Some solutions in the data security sphere might gravitate either towards the agent-based methods or the agentless approach. Even as we see market consolidation amongst industry leaders, it raises the question of how these methods can be quickly cobbled together when diametrically opposed platforms are suddenly combined. This could force unexpected client migrations, upsetting established deployments and illustrate the potential pitfalls of what may seem to be an opportunistic strategy.



Ease of Use and Integration

Beyond the collection of data security and audit data, data security specialists should able to quickly understand, investigate, and respond to anomalies, risks, and imminent threats. Cross-team collaboration through the sharing of data security events and integration with the SOC and other parts of the security stack can be a necessity—especially with if the IT and security organization struggles with tool sprawl.

Guardium

Data security should be everyone's business

With the Guardium dashboard, outside data sources, security tools, or ticketing systems can be connected. Customers can run out-of-the-box and custom reports. Security specialists can discover how to quickly integrate REST APIs. This connects data security with IBM or 3rd party data and security tools within the organization—from SIEM and case management to ticketing and logs.

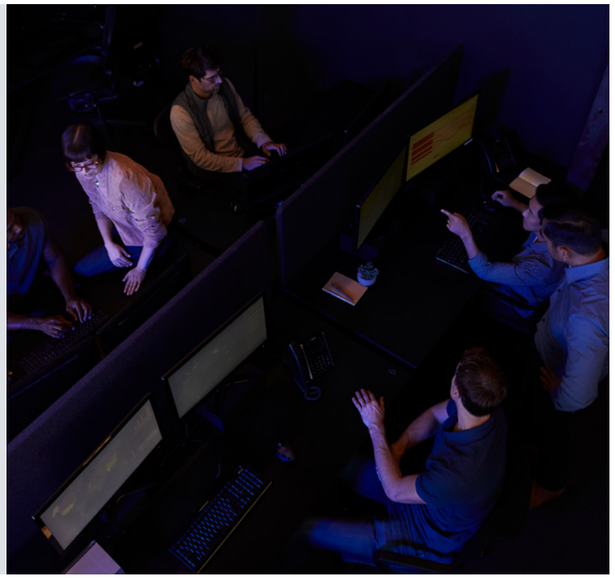
Remediation made easy through collaboration

Data security teams can orchestrate remediation actions within Guardium, such as opening a case while investigating an incident or sending an alert to the SIEM. All told, these simple workflows can deliver value by not requiring security teams to learn new skills just to integrate platforms. Once integrated, the focus on orchestration and collaboration effectively promotes Zero Trust principles—with Guardium being a central piece of IBM Security's Zero Trust framework.

Other solutions

A lasting legacy of difficulty

Some legacy technology solutions might require security teams to build knowledge on new languages and processes simply to deploy and use a data security platform. Something as integral and time sensitive as opening a ticket could take multiple steps. Custom integration points may have to be built to connect across tools and platforms. The costs of such additional effort can outweigh the benefits for many organizations, lending to the perpetuation of siloed security teams.



Encryption and Key Lifecycle Management

Proactive data protection measures can help protect against unauthorized users accessing sensitive data and reduce the scope of data required to meet industry and regulatory compliance. This protection can come in the form of encrypting, tokenizing, and masking sensitive data; managing the full lifecycle of the cryptographic keys; and enforcing access policies to help keep unauthorized users from decrypting data—all of which should be provided through a single solution to avoid the pitfalls of a piecemeal approach.

Guardium

Protect data wherever it resides

It should not matter if data is on-premises or in the cloud. Whether the goal is tokenization of data-at-rest, masking specific data fields, or full encryption at the file, database, or application level, Guardium can deliver through IBM Security Guardium Data Encryption.

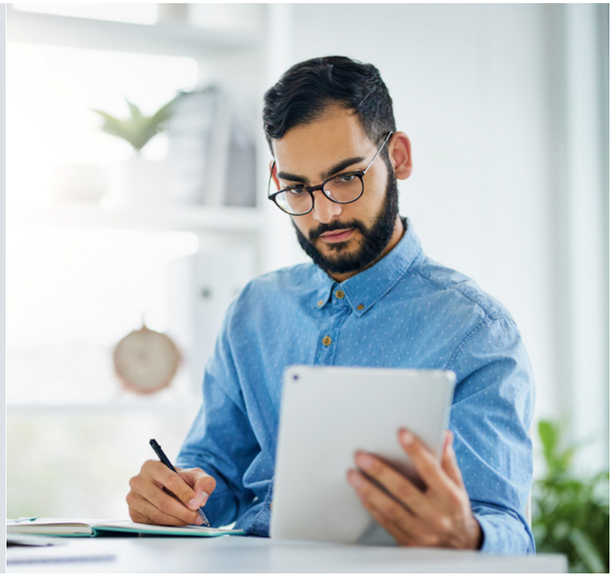
Guardium key management

Centralized, simplified, automated key management is provided through IBM Security Guardium Key Lifecyle Manager. Supporting major key exchange standards, Guardium Key Lifecycle Manager can deliver robust key storage and lifecycle management for self-encrypting solutions—whether those solutions are IBM or not. This expansive coverage can help avoid the headaches that come with point solutions.

Other solutions

Unmasking a piecemeal protection plan

Some solutions prioritize pieces of a data protection strategy. In most cases this means data masking without encryption or vice versa. This approach typically provides full coverage through the deployment of several point solutions, which does little to simplify a customer's IT and security environment.



Vulnerability Assessment

Guardium

Identify and defend against vulnerability

IBM's solution within the IBM Security portfolio finds strength in assessing vulnerabilities and responding to security events. Guardium, through IBM Security Guardium Vulnerability Assessment, identifies behavioral and technical vulnerabilities by employing static, pre-configured, and dynamic tests—as well as recommending detailed remediation steps to harden data and helping administrators orchestrate a response via IT ticketing integration.

According to The Forrester Total Economic Impact of IBM Security Guardium study sponsored by IBM Security, vulnerability management capabilities from Guardium Data Protection reduced the likelihood of a breach for one studied organization by 40% after adjusting for risk—equivalent to a $990k cost savings over 3 years.3

Other solutions

Identify vulnerabilities with DIY defense

Some solutions can deliver vulnerability assessment, but they can stop short at the recommendation stage. Beyond highlighting steps administrators can take to better protect their databases, there can be little in the way of orchestration or direct incident response.

Advanced Analytics and Incident Response

Guardium

Advanced analytics to assess anomalies

Derived from the combined knowledge of IBM Watson and IBM Research, Guardium's analytics recognize normal logical operations and can quickly identify suspicious activities and changes. Additionally, Guardium's analytics can spot suspicious user behaviors, threats, and anomalous activity.

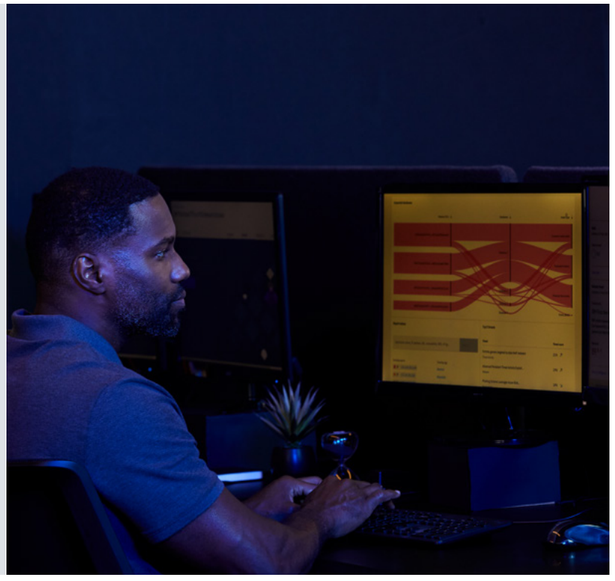
A united front to remediate threats

Respond to data security threats quickly through integrations with IBM Cloud Pak for Security, IBM Security Resilient, IBM Security QRadar, and 3rd party SIEM and incident response platforms. By facilitating cross-communication between data security and the greater security team, these integrations boost threat visibility and can help reduce the time it takes to respond.

Other solutions

Some assembly required for incident response

Data security vendors that do champion incident response may also require security teams to take on the time-consuming task of building out their own integrations between data security and threat management tools. This does little to reduce tool sprawl, support cross-team cooperation, or bolster digitally transformative agility.



IBM Security

Sources

1. “Cost of a Data Breach report 2020.” IBM Security. 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report
2. “The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019.” Forrester. 2019. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39199
3. “The Total Economic Impact of IBM Security Guardium.” Study conducted by Forrester Research, sponsored by IBM Security. 2020. https://www.ibm.com/account/reg/us-en/signup?formid=mrs-form-2454
4. “Ponemon Report: Client Insights on Data Protection with IBM Security Guardium.” Study conducted by Ponemon Institute, sponsored by IBM Security. 2019. https://www.ibm.com/downloads/cas/YMOWGORK

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2021

00000000USEN

IBM