IBM Security Guardium on AWS: Data Compliance in a Hybrid Multicloud World

As organizations accelerate IT modernization and cloud migration, complexity associated with maintaining data compliance across a disparate landscape is increasing. This complexity threatens to stall transformation efforts and expose businesses to ongoing risk.

Data compliance in a multicloud world is layered and complicated. Customers migrating data and workloads to Amazon Web Services (AWS) need to understand the nuances between security responsibilities in an on-premises data center and in the cloud. As part of this new landscape, organizations face a variety of security challenges: protecting and ensuring visibility across data silos, accommodating the surge in remote work, and enforcing data compliance standards throughout the greater enterprise.

aws | IBM

Companies in intensely regulated industries face an even higher bar, as they are subject to an increasing number of regulations governing the collection, storage, usage and disposal of data. In those heightened regulatory climates, there are also strict rules governing data breach notifications. Some are specific to certain industries and others pertinent to geographic location. In the United States alone, there is a patchwork of different state privacy laws — in 2021, there were 27 data privacy bills introduced in 21 states — and regulations are mounting on a global scale. PCI DSS, SOX, HIPAA, GDPR, and CPRA are among the more prominent regulations enterprises must handle.

The shift to hybrid and remote work has also complicated the security equation. With users no longer working on company-supplied devices with controlled access to internal networks, traditional safeguards no longer suffice, exposing companies to greater risk. In fact, having a remote workforce increases the average cost of a data breach by $388,477, according to IBM Security's "Cost of a Data Breach 2022" report.[1] At the same time, geographically and functionally dispersed IT teams tend to gravitate to different tool sets, procedures, and policies, creating silos that add to the data security challenge.

Although there are established standards and practices for data security and compliance for on-premises systems, they don't always translate directly to cloud. Organizations that practice proper governance for data compliance in their own data centers need to ensure that they carry over and enforce those practices in their cloud environment, especially given the pace of migration to cloud.

The public cloud's shared-responsibility model requires a different approach from how security has been orchestrated in the past. Organizations must be fully aware of how safeguards are delineated under the new paradigm. For instance, providers such as AWS are responsible for the security "of" the cloud whereas customers are expected to take ownership of all security practices related to anything "in" the cloud, such as data, applications, and workflows.

"Everyone is racing to the cloud without necessarily understanding that the requirements and regulations are still there," says Matt Simons, senior product manager, Data Security, for IBM Security. "Moving to the cloud does not absolve you of responsibility for compliance. Even in the shared-responsibility model, you are still responsible for the data and regulations that pertain to that data."

The stakes for getting security right couldn't be higher: IBM Security confirmed that the global average cost of a data breach is $4.35 million, up 13% over the last two years.[2] Companies that don't fully understand their role in the shared-responsibility model are also up against additional risk factors. The IBM Security report calculated that customer misinterpretation of cloud security requirements and the resultant data breaches amplified the average total cost of a data breach by $495,566.

IBM Security and AWS Take On the Compliance Challenge

IBM Security and AWS' long-standing partnership tackles the complex compliance challenges of a hybrid, multicloud world.

IBM Security Guardium Data Protection and Guardium Insights on AWS centralize visibility and compliance insights in a flexible and scalable data security platform. In keeping with the shared-responsibility model, AWS native security controls, in concert with IBM Security Guardium Data Protection and Guardium Insights, help customers fulfill their part of the cybersecurity contract while adequately protecting data and applications running in the cloud.

"AWS Cloud protects access controls, security groups, and firewalls, whereas Guardium Insights is purpose-built for monitoring, reporting, and auditing activity against the data," Simons explains.

"Guardium also applies a risk scoring engine to activities to tell you when something looks out of place." he adds.

A new cloud-native software-as-a-service (SaaS) version of Guardium Insights is now available on AWS, expanding capabilities beyond the existing self-deployed version currently offered in the AWS Marketplace. This next-generation SaaS offering is easier to deploy and scale at the speed of cloud and is available at a lower price point, making it a more favorable option for small and midsize organizations.

Guardium Insights SaaS is available through a subscription-based pricing model. This is the preferred approach for some firms partial to a more modern OpEx spending model, compared to traditional IT capital expenditures.

Simplified SaaS deployment on the AWS Cloud also means that customers don't need to staff a robust talent bench of security and cloud experts. With this SaaS offering, IBM and AWS handle all the maintenance upgrades and patching of hardware and software. In addition, Guardium Insights SaaS shortcuts manual compliance processes through automated and schedulable reporting while delivering prebuilt templates and workflows to meet internal and regulatory requirements. The modernized platform can also monitor activity related to data in both on-premise and cloud-based data stores.

To further streamline compliance activities, Guardium Insights enables customization of predefined security and compliance policy templates, based on audit and regulatory requirements. Policies can be customized to detect any threat scenario against data, using the most common audit constructs and other contextual information. Compliance tasks are further automated by production of data

[1]IBM Security, "Cost of a Data Breach 2022" https://www.ibm.com/reports/data-breach
[2]IBM Security, "Cost of a Data Breach 2022" https://www.ibm.com/reports/data-breach

and compliance content in seconds with out-of-the-box and customizable reports, dashboards, and integrations.

Retention and maintenance of data security and audit data over long periods of time have been ongoing compliance challenges for organizations. With Guardium Insights on AWS, policies and rules can be updated and tagged for specific data security and privacy regulations to help avoid duplicative administrative work. In addition, data is retained over long periods of time to support compliance efforts.

The combination of Guardium Data Protection and Guardium Insights delivers big results. Research shows that audit prep time can be reduced by 75% through automated compliance auditing and reporting. Centralized visibility and advanced analytics can cut the risk of data breaches by up to 40%. Automated processes also cut as many as 1,000 hours of DBA time, a Forrester report found.[3]

Moving toward a SaaS model eliminates much of the complexity and cost associated with a traditional software implementation. “Things like maintenance, updates, and patching will no longer be something customers have to worry about,” says Senthil Nagaraj, solutions architect, Amazon Web Services. "When customers opt for a SaaS version, that’s all handled by IBM Security and AWS.”

Breaking Down Guardium Insights SaaS

Guardium Insights SaaS is available in three editions on AWS:

- **Premium.** This version is comparable to the existing Guardium Insights software. Among the highlights are integration with the broad Guardium Data Protection portfolio, risk-based analytics with machine learning, and automated threat detection. Guardium Insights SaaS supports an accelerated deployment model, simplified pricing, and an OpEX spending model.

- **Standard.** This edition is designed for organizations that are just beginning their data security and compliance journey. The offering boasts a simplified UX, includes guided compliance journey maps, and introduces data security. This option is ideal for small-to-medium-size enterprises that need to conform to the ever-changing regulatory landscape but also want the flexibility to create their own reports and dashboards to satisfy growing data security concerns.

- **Essentials.** This version, focused on smaller enterprises that are concerned solely with regulatory compliance, delivers a guided compliance journey, automated prebuilt reports, and easy-to-produce audit trails to satisfy auditors, all at a low entry price point.

[3]Forrester Research, “The Total Economic Impact of IBM Security Guardium” https://www.ibm.com/account/reg/us-en/signup?fmid=mrs-form-2454

All Guardium Insights SaaS versions offer the advantages of procurement through AWS Marketplace, including one-stop shopping, consolidated billing, improved vendor onboarding, and increased licensing flexibility. They also offer the ability to take advantage of the AWS Enterprise Discount Program (EDP).

The impact is significant. One Forrester study found that AWS Marketplace listings resulted in a 10% reduction in licensing costs; streamlined procurement practices, including a 66% reduction in time spent searching for and selecting vendors; and a 50% time reduction in invoicing tasks. IBM Security has a variety of software listings on the AWS Marketplace and maintains three official security competencies with AWS for security software, security services, and managed services.

"AWS has always been at the forefront of cloud solutions that support elasticity and scalability, which comes with the normal way of doing business," Simons says.

"Those abilities channeled to our Guardium Insights software are really where the magic is, from a partnership perspective."

IBM Security's deep roots in the security space are another major asset. IBM Security has more than 5,500 security experts in 130 countries, and the company's nine global security centers monitor more than 70 billion events every day. IBM Security is also certified for three security competencies with AWS, including security software, security services, and MSSP.

The Bottom Line

Securing a multicloud, hybrid world is challenging but essential. IBM Security and AWS continue to expand their partnership with services and tools that help organizations advance business transformation without being mired in security mitigation.

www.ibm.com/security/partners/aws