Securing your AWS Cloud with native services and IBM Security Guardium

Executive Summary

Your data is valuable. Yet, threat actors are targeting your data like never before, with more frequent and more sophisticated attacks. Meanwhile, you have to contend with a variety of factors – the increased use of remote access, data located in a hybrid environment, growing regulatory compliance demands, and siloed IT teams – that introduce complexities in managing and securing your data.

You need a way to simplify your data management in a hybrid environment and make your data accessible to all who need it.

The global average cost of a data breach (up 13% in 2 years) is $4.35M. The highest country average is the United States, at $9.44M.

(IBM Security / United States Cost of a Data Breach Report 2022)

The State of Data Security: **Data Under Threat**

Your data is becoming increasingly vulnerable, while your security teams are facing mounting pressure.

Your users, once safely ensconced in company-owned offices using only company-supplied devices with controlled access to your internal network, may now be accessing your data using a variety of uncontrolled third-party devices over the unsecured public internet.

Having a remote workforce increases the average cost of a data breach by $338,477.
(IBM Security / Cost of a Data Breach Report 2022: United States)

The data that those workers are accessing, arguably one of the most valuable assets of your company, resides in both your on premise environment in data centers as well as in geographically dispersed cloud environments, each requiring you to fulfill differing levels or types of security responsibilities.

Misunderstanding cloud security requirements and the resultant data breaches increased the average total cost of a data breach by $495,566.
(IBM Security / Cost of a Data Breach Report 2022: United States)

Just as your data has become dispersed, so have your IT teams, with staff separated not just geographically, but by verticals aligned with function and technology. This separation often leads to isolated silos, with each team using different toolsets, procedures, and policies.

"89% of IT leaders report data silos are creating business challenges for their organizations' digital transformation initiatives."
(MuleSoft / Top 8 Trends Shaping Digital Transformation In 2021)[1]

Meanwhile, governments are applying stringent data privacy and compliance regulations while consumers are demanding better security and greater transparency. The United States alone has hundreds of data privacy and security laws among its states, governing the collection, storage, disposal, and use of personal data, as well as requirements regarding data breach notifications. If your organization operates internationally, you further have to abide by additional regulations in the countries where you're active, or where your customers are active.

"The current patchwork of different state privacy laws will likely prove to be a compliance headache for businesses. In 2021 alone, 27 comprehensive data privacy bills were introduced in 21 different states."

(JD Supra, LLC / U.S. Privacy Law: Past, Present and Future)[2]

All of this is occurring while increasingly sophisticated and aggressive threat actors are trying to target your data with phishing attacks, ransomware, SQL injections, cross-site scripting, and more.

On average, it takes 207 days to identify a data breach, and an additional 77 days to contain it.

(IBM Security / Cost of a Data Breach Report 2022: United States)

You can't afford to ignore these challenges. The damage done to your organization's reputation alone could be devastating, not to mention direct costs in lost business. You need a way of unifying your security solutions across both on-premise and cloud data stores.

For companies whose zero-trust security deployment has reached a mature stage, the cost of a data breach is, on average, $2.51 million less than that of organizations who have not yet started such a deployment.

(IBM Security / Cost of a Data Breach Report 2022: United States)

Combining leading cloud infrastructure with world class security

Cloud computing allows organizations to reduce infrastructure and administration costs, while increasing efficiency by scaling their resources up or down on demand.

Working together, AWS and IBM Security form a comprehensive solution delivering full data, zero-trust protection your AWS Cloud, or hybrid-cloud environment.

IBM Security solutions integrate with AWS native controls such as:

- Amazon CloudWatch
- AWS RDS Data Sources
- AWS CloudTrail

Consider two industry-leading solutions to these challenges.

Amazon Web Services: The Preeminent Cloud Solution

While there's a profusion of cloud providers, Amazon Web Services (AWS) consistently leads the pack with more than a third of the cloud infrastructure services market, providing compute, containers, databases, and machine learning services.

> **"AWS had 34% market share in Q2, more than the combined market share of its two largest competitors."**
> *(Electronics Weekly / AWS Still Rules The Roost, 2022)*[3]

AWS has comprehensive security tools built-in:
Amazon Macie identifies sensitive data contained in Amazon S3 buckets, and Amazon CloudWatch monitors the health of your AWS environment. Further, AWS has been designed to integrate it's native controls with advanced security technology like IBM Security Guardium.

IBM Security Guardium: Secure Your AWS or Hybrid Cloud

IBM Security Guardium is a suite of products providing end-to-end data security by addressing discovery, classification, monitoring, and encryption of your organization's sensitive data across hybrid environments, both on-premises and in the cloud.

When used to monitor AWS environments and in conjunction with native AWS security controls, IBM Security Guardium provides a holistic risk-based approach to cloud security.

Consider just some of the advantages provided by IBM Security Guardium.

- Gain visibility, compliance, and protection for data in motion and at rest with a zero-trust approach to data security.
- Simplify regulatory compliance and streamline the reporting process, freeing up IT resources to focus on preventing data threats.
- Clearly define and enforce policies that discover and block internal and external threats, and identify regulated data.
- Eliminate data silos and create comprehensive solutions using simple point-and-click connections to integrate security tools and unify security policies from across your organization.
- Enable comprehensive data protection across your hybrid environment by monitoring activity wherever it occurs and implementing consistent threat response actions.

These two components of the IBM Security Guardium suite are currently available on the AWS Marketplace for procurement or deployment on AWS Cloud:

IBM Security Guardium Data Protection is built on a scalable architecture to extend your data security policies across your on-premises and cloud environments. It delivers visibility into your structured, semi-structured, and unstructured data wherever it resides, while identifying potential vulnerabilities in that data.

IBM Security Guardium Insights secures your data while preserving compliance throughout the data security life cycle. Integrating easily with other IT and security tools, it allows you to identify data risks, threat patterns, and suspicious user behavior across on-premises and cloud data sources.

Westfield Insurance: Protecting Business Data with IBM Security Guardium

Challenge:
Westfield Insurance Group, a property and casualty insurer, needed to modernize their business with cloud-driven initiatives. At the same time, as Westfield's data security staff saw the increase in cyberattacks against financial services companies, they realized they needed to more quickly uncover and respond to both external and internal risks to their customer data.

Solution:
By deploying IBM Security Guardium, Westfield has been able to automate data discovery and classification, continuously monitor data access, and proactively uncover vulnerabilities and risks. They are able to protect their growing volumes of customer data, while sharing security intelligence with agents and customers.

Results:
Westfield Insurance data security staff now take a more proactive approach to security across their organization. They now quickly identify where customer data is stored, who's accessing it, and why they're accessing it to more rapidly respond to potential security threats.

*To learn more about the role IBM Security Guardium played in modernizing and securing Westfield's data environment, visit **here**.*

IBM Security Guardium and AWS: **Your Data Security Partners**

Imagine having a team of security guards protecting your facilities. They know who should have access, to which areas each visitor should have access, and what those visitors should be allowed to do while they're there. They provide in-depth reports on activity at all locations, alert you whenever a visitor attempts to access sensitive areas, and block all unauthorized activity.

You can have such a team protecting your AWS and hybrid environment data by deploying IBM Security Guardium in conjunction with native AWS controls.

Learn more about how IBM Security Guardium can simplify your data security landscape across your hybrid cloud environment.

Ready to move ahead with IBM Security Guardium in your AWS environment? Purchase and deploy IBM Security Guardium Insights and IBM Security Guardium Data Protection from the AWS Marketplace.

[1] https://www.mulesoft.com/ty/report/top-digital-transformation-trends-2021
[2] https://www.jdsupra.com/legalnews/u-s-privacy-law-past-present-and-future-4213418/
[3] https://www.electronicsweekly.com/blogs/mannerisms/markets/aws-rules-the-roost-2022-08/