Overcoming data security challenges in a hybrid multicloud world

Protect your data wherever it resides with the IBM Security Guardium platform

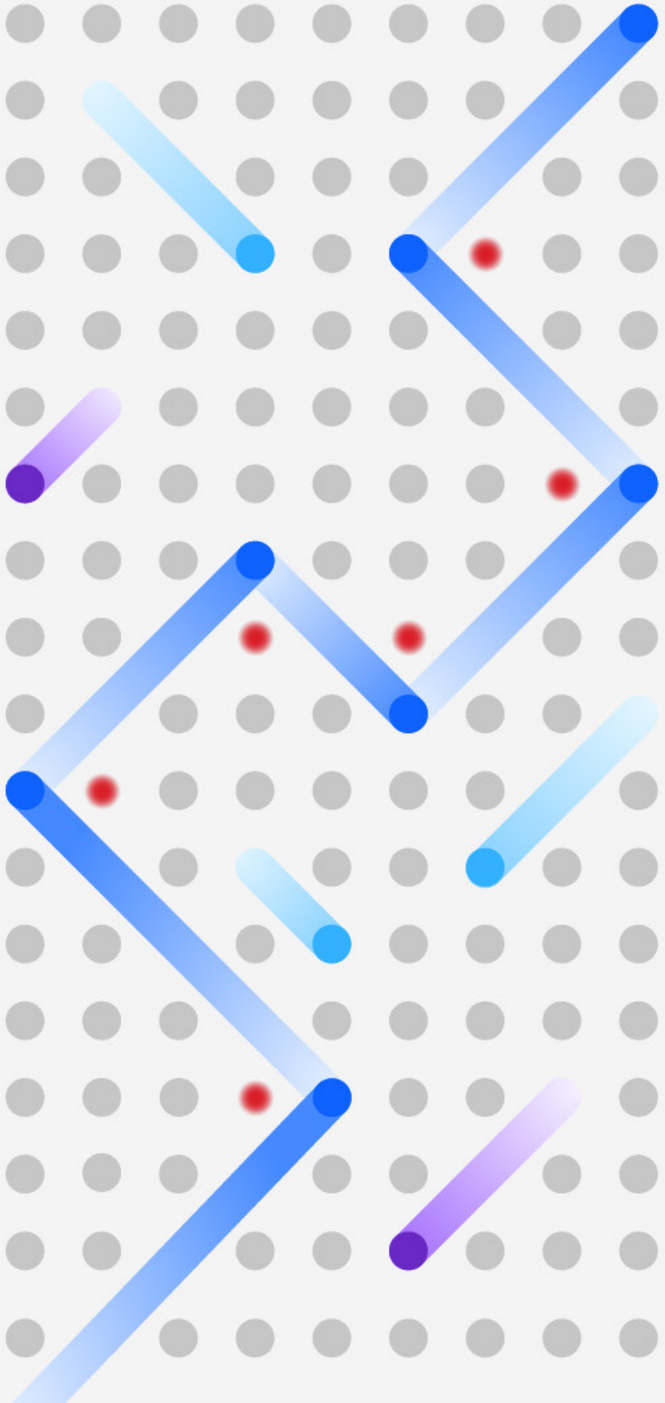
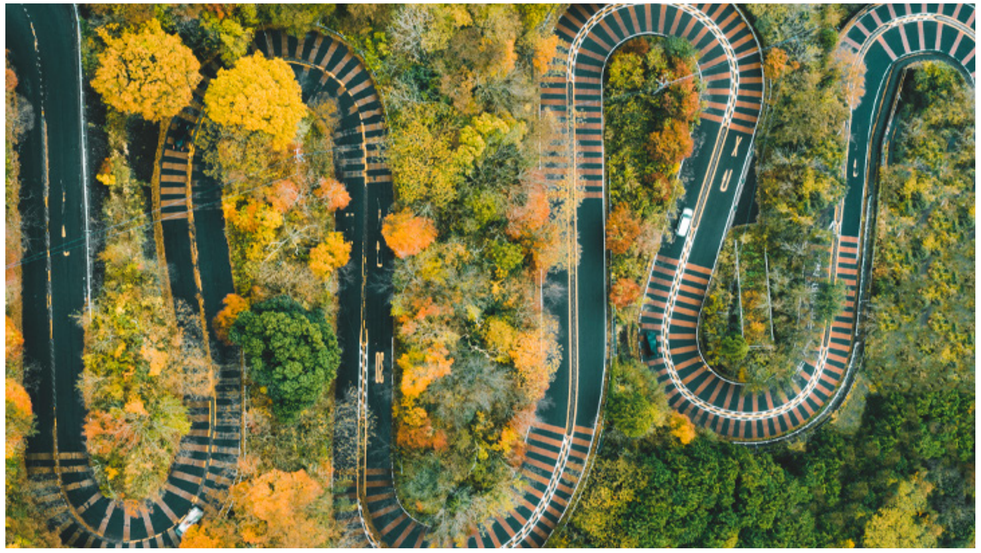


Table of contents

01

Data security challenges to your cloud environment



If your organization is like the vast number of businesses, your sensitive data resides in locations you can’t control and is managed by third parties that may have unfettered access.

Determining how best to store data is one of the most important decisions an organization can make. The cloud is well suited for long-term, enterprise-level data storage that allows organizations to benefit from massive economies of scale, which translates into lower expenses. And this feature often makes cloud-based data centers a smarter place to store business-critical information than a stack of servers down the hall.

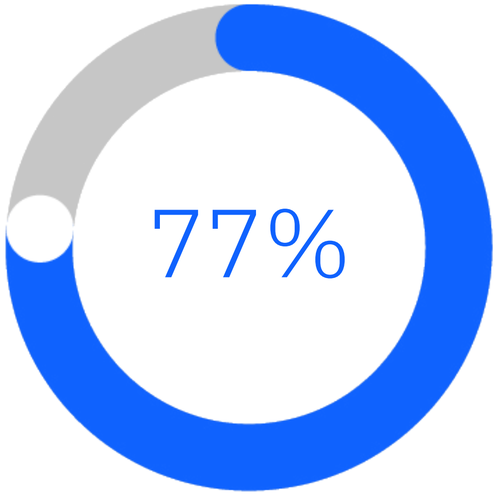
Even as the expense of acquiring storage drops, it can be expensive in the long term due to increased business use and the number of personnel managing the storage systems. However, although putting data storage in the hands of third-party service providers can help save money and time, it can also pose serious cybersecurity challenges and create new levels of risk.

Cloud deployments work on a shared responsibility model between the cloud service providers (CSPs) and the consumer. In the case of an infrastructure as a service (IaaS) model, cloud consumers have room to implement data security measures much like what they would normally deploy on premises, and exercise tighter controls.

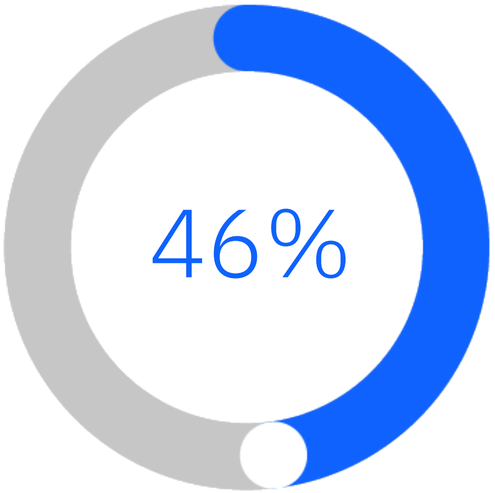
Data security challenges to your cloud environment

On the other hand, for a software as a service (SaaS) model, cloud consumers for the most part have to rely on the visibility provided by the CSP, which in essence limits their ability to exercise more granular controls.

It’s important to understand that whatever your deployment model or cloud service type is, data security must be a priority. What’s of great concern is that your sensitive data now sits in many places, both within your company’s walls and outside of them. And your cybersecurity controls must follow wherever your data goes.



77% of organizations reported that they are in the process of digitally transforming their business.[1]



46% of organizations have adopted a cloud-first policy for new applications.[1]

A smarter data security approach

As the cloud matures and scales rapidly, we must realize that effective data security isn’t a sprint but a marathon—an ongoing process that continues throughout the data lifecycle.

Though there’s no one-size-fits-all approach to data security, it’s crucial that organizations look to centralize data security and compliance tools that work well together. This approach can help security teams improve visibility and control over data across the enterprise and cloud.

What constitutes an effective data security strategy?

Discover your structured and unstructured sensitive data, online and offline, regardless of whether it resides in the cloud or SaaS applications.

Classify sensitive data that's subject to regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), European Union (EU) General Data Protection Regulation (GDPR), and California Privacy Rights Act (CPRA), formerly known as the California Consumer Privacy Act (CCPA).

Assess risk with contextual insights and analytics. How is your critical data being protected? Are access entitlements in accordance with industry and regulatory requirements? Is the data vulnerable to unauthorized access and cybersecurity risks based on a lack of protection controls?

Monitor data access and usage patterns to quickly uncover suspicious activity. Once the appropriate controls are in place, you need to be quickly alerted to anomalous activities and deviations from data access and usage policies. You must also be able to centrally visualize your data security and compliance posture across multiple data environments without relying on several disjointed consoles.

Protect sensitive data sources based on a deep understanding of what data you have and who has and should have access to it. Protection controls must accommodate the different data types and user profiles within your environment. Flexible access policies, data encryption and encryption key management can help keep your sensitive data protected.

Simplify compliance and its reporting. You need to be able to demonstrate data security and compliance to both internal and external parties and make appropriate modifications based on results. Demonstrating compliance with regulatory mandates often requires storing and reporting on years' worth of security and audit data. Data security and compliance reporting must be comprehensive, accounting for your entire data environment.

Respond to threats in real time. Once alerted to potential vulnerabilities and risk, you need the ability to respond quickly. Actions can include blocking and quarantining suspicious activity, suspending or shutting down user sessions or data access, and sending actionable alerts to IT security and operations systems.

02

Six data security strategies

With data growing at an exponential rate, organizations are facing a growing list of data compliance laws and regulations. What is at risk? Customers' personal information, such as payment card information, addresses, phone numbers and Social Security numbers, to name a few. To have an effective data security solution, organizations should adopt a risk-based approach to protecting customer data across environments.

Here are six strategies that could improve your organization's data security posture:

- Assure privacy.
- Address vulnerabilities.
- Monitor access controls.
- Encrypt sensitive data.
- Manage compliance.
- Improve productivity.

The IBM Security® Guardium® data security and compliance platform is designed to help your organization meet those challenges with smarter data protection capabilities across environments.

Learn more →

Assure privacy

With the proliferation of smartphones, tablets, smartwatches and laptops, managing access controls and privacy can become a daunting task. One of the challenges for security administrators is ensuring that only individuals with a valid business reason have access to personal information. For example, physicians should have access to sensitive information, such as a patient's symptoms and prognosis data, whereas a billing clerk only needs the patient's insurance number and billing address.

Your customers expect you to make their privacy a priority. Start with developing a privacy policy describing the information you collect about your customers and what you intend to do with it.

IBM Security Guardium Insights provides security teams with risk-based views and alerts along with the ability to reduce noise and exclude noncritical assets from your reports. Advanced analytics help you understand the broader story, identify data risks and threat patterns, enable immediate action and keep all stakeholders informed.

Learn more →

Address vulnerabilities

When it comes to defending against attackers, what worked in the past may not work today. Many organizations rely on diverse cybersecurity technologies that could be operating in silos.

The number of data repository vulnerabilities is vast, and criminals can exploit even the smallest window of opportunity. Some of these vulnerabilities include missing patches, misconfigurations and default system settings that can leave gaps that cybercriminals are hoping for. This complexity is increasingly difficult to keep track of and manage as data repositories become virtualized.

Furthermore, companies that move to the cloud often struggle to evolve their data security practices in a way that enables them to protect sensitive data while enjoying the benefits of the cloud. The more CSPs your organization uses, the more control you may need to manage the different environments.

Think about the use of homegrown tools that are in place today for data security. Will the homegrown tools you're using today work tomorrow? For example, with data-masking routines or database activity monitoring scripts, will coding changes be required to make them work on a virtual database? Chances are that a significant investment will be required to update these homegrown solutions. In short, organizations need a data-centric approach to security in which data security strategies are built into the fabric of their hybrid multicloud environments.

IBM Security Guardium Vulnerability Assessment helps teams identify security gaps in their data stores, such as missing patches, weak passwords, unauthorized changes, misconfigured privileges, excessive administrative login, anomalous activity and other behavioral vulnerabilities.

Learn more →

Monitor access controls

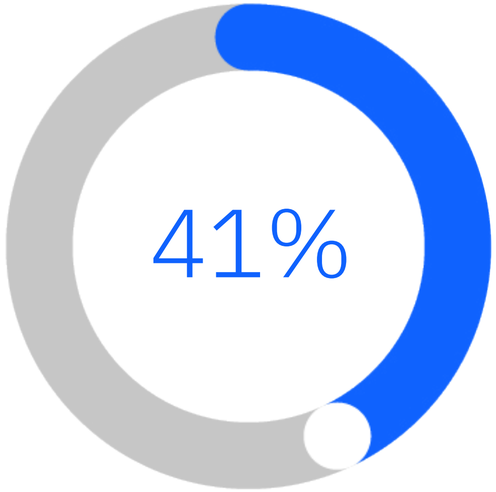
Cybercriminals can range from individuals to state-sponsored hackers with disruptive intentions. They can be rogue computer scientists trying to show off or make a political statement, or they may be tough, organized intruders. They can be disgruntled employees or even foreign state-sponsored hackers who want to collect intelligence from government organizations.

Breaches can also be accidental, such as stolen credentials, human error or misconfigurations, for example, when permissions are set incorrectly on a database table, or when an employee's credentials are compromised.

One way to avoid this issue is by authorizing both privileged and ordinary users with “least possible privilege” to minimize abuse of privileges and errors. Organizations should protect data from both internal and external attacks in physical, virtual and private cloud environments.

Perimeter defenses are important, but what’s more important is protecting the sensitive data wherever it resides. This way, if the perimeter is breached, sensitive data will remain secure and unusable to a thief. Declining perimeters is crucial to protecting data at its source.

A layered data security solution can help administrators examine data access patterns and privileged user behaviors to understand what’s happening inside their cloud environment. The challenge is to implement cybersecurity solutions without hampering the business’s ability to grow and adapt, therefore providing appropriate access and data protections to ensure data is managed on a need-to-know basis, wherever it resides.



For the second year in a row, phishing was the leading infection vector, identified in 41% of incidents.[2]

Encrypt sensitive data

Because we can no longer rely on the perimeter to secure an organization's sensitive data, it's crucial for today's business leaders to wrap the data itself in protection.

IBM Security Guardium Data Encryption is a suite of modular, integrated and highly scalable encryption, tokenization, access management and encryption key management solutions that can be deployed across all environments. These solutions encode your sensitive information and provide granular control over who has the ability to decode it.

Learn more →

Strong encryption is a common answer to the challenge of securing sensitive data wherever it resides. However, encryption raises complicated issues of portability and access assurance. Data is only as good as the security and reliability of the keys that protect it. How are keys backed up? Can data be transparently moved among cloud providers or shared between cloud-based and local storage?

IBM Security Guardium Key Lifecycle Manager can help enterprises that require more stringent data protection. The solution offers security-rich, robust key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP). With centralized management of encryption keys, organizations can meet regulations such as PCI DSS, SOX and HIPAA.

Learn more →

Manage compliance

The realities of cloud-based storage and computing mean that your sensitive data across hybrid multicloud systems could be subject to industry and government regulations.

If your data is in a public cloud, you must be aware of how the CSP plans to protect your sensitive data. For example, according to the GDPR, personal data that reveals a racial or ethnic origin, political affiliation, or religious or philosophical belief is deemed sensitive and therefore subject to protection under the mandate. These requirements apply even to companies located in other regions of the world that hold and access the personal data of EU residents.

Understanding where an organization's data resides, what types of information it consists of and how these relate across the enterprise can help business leaders define the right policies for securing and encrypting their data. Additionally, it could help with demonstrating compliance with regulations, such as:

- PCI DSS
- SOX
- CPRA
- HIPAA
- Security Content Automation Protocol (SCAP)
- Health Information Technology for Economic and Clinical Health (HITECH) Act

Guardium is designed to support ever-changing compliance regulations by monitoring and auditing data activity across databases, files, cloud deployments, mainframe environments, big data repositories, containers and SaaS applications. The process is streamlined with automated workflows and continuous monitoring, thus reducing costs and time for compliance requirements.

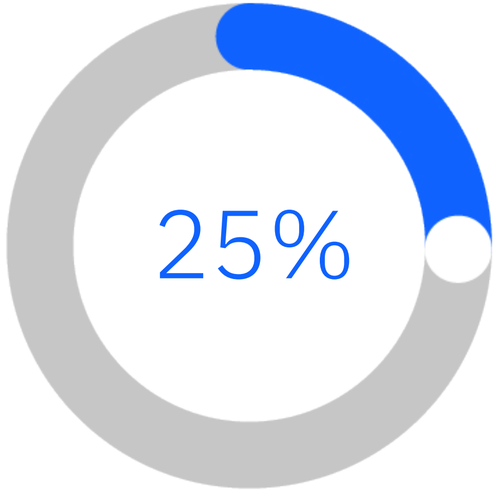
> We are going with 0% gap for SOX compliance. We can produce what they ask. That's the best measurement for us.
>
> A database security and compliance supervisor at an automotive organization in a Forrester Total Economic Impact (TEI) study

Read the Guardium TEI study →

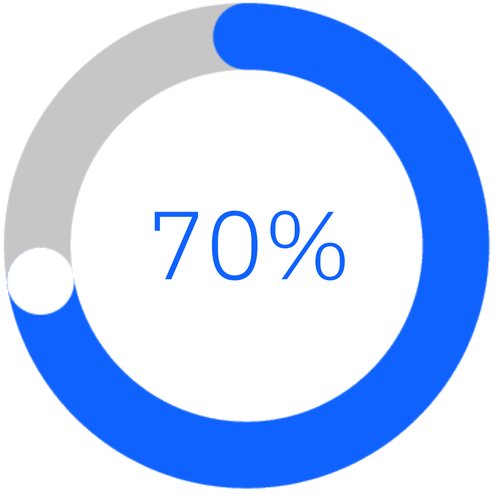
Improve productivity

Data security and privacy policies should enable and enhance, not interfere with business operations. Policies should be built into everyday operations and work seamlessly within and across all environments—in private, public, on-premises and hybrid environments—without impacting your productivity. For example, when private clouds are deployed to facilitate application testing, consider using encryption or tokenization to mitigate the risk of exposing that sensitive data.

Guardium solutions can help your cybersecurity teams monitor user activity and respond to threats in near real-time. This process is streamlined with automated and centralized controls, thus reducing the time spent on investigations and empowering database administrators and data security analysts to make more informed decisions.



25% of data security analysts' time saved[3]



70% reduction in time spent on auditing[3]

03

Conclusion

Given the evolving threat landscape, organizations must adopt a consistent and unified approach to hybrid multicloud data security. Consider the following questions:

- Am I aware of where all of my data resides?
- What data is staying on premises?
- What data is moving to the cloud?
- How can data access be monitored?
- What types of vulnerabilities should be considered?
- How can we demonstrate compliance with data security and regulatory requirements?

When choosing data security and compliance solutions, select solutions that are scalable across varying IT infrastructures—protecting physical, virtual and cloud environments from malicious external attacks, fraud, unauthorized access and insider breaches. These solutions must work in a cloud environment without complex and costly configurations. Such an approach provides an efficient platform for data security and compliance, helping you manage costs by reducing resources and providing greater agility and flexibility.

The Guardium platform provides a comprehensive solution for physical, virtual and cloud infrastructures through centralized, automated data security controls across heterogeneous environments. The solution helps streamline compliance, reduces risk and supports major cloud platforms, including IBM Cloud®, Microsoft Azure and Amazon Web Services, and operates across Microsoft Windows, UNIX and Linux® environments.

Guardium key features

- Automatically discover and classify sensitive data.
- Encrypt data across environments.
- Identify data at risk and get remediation recommendations.
- Use contextual insights and analytics.
- Simplify security and compliance reporting.
- Get a business perspective on data risk.
- Monitor access and protect data.

The Forrester Consulting TEI study, commissioned by IBM, shows these key business benefits enabled by Guardium.

406%

return on investment

USD 5.68M

benefits present value (PV)

Less than 6 months

for payback[3]

Why IBM Security?

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services infused with dynamic security AI and automation capabilities. The portfolio, supported by world-renowned IBM® X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement and manage security transformations.

IBM operates one of the world's broadest security research, development and delivery organizations; monitors more than 150 billion security events each day in more than 130 countries; and has been granted more than 10,000 security patents worldwide.

What's next?

Discover how IBM Security Guardium solutions can help you take a smarter, integrated approach to safeguarding critical data across your hybrid multicloud environments.

Contact us →

Book a live demo →

1. The Need for Data Compliance in Today's Cloud Era, Enterprise Strategy Group by TechTarget, April 2023.

2. IBM Security X-Force Threat Intelligence Index 2023, IBM Security, February 2023.

3. The Total Economic Impact™ (TEI) of IBM Security Guardium Data Protection, a Forrester Consulting study commissioned by IBM, June 2023.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
November 2023