Overcoming data security challenges in a hybrid, multicloud world

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

IBM **Security**

IBM

Contents

Deploying in a hybrid, multicloud environment

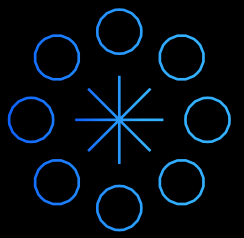
Let's face it, cloud computing is evolving at a rapid pace. Today, there's a range of choices for moving applications and data to cloud that includes various deployment models, from public and private to hybrid cloud service types.

As part of a broader digital strategy, organizations are seeking ways to utilize multiple clouds. With a multicloud approach, companies can avoid vendor lock-in and take advantage of the best-of-breed technologies, such as artificial intelligence (AI) and blockchain. The business benefits are clear: improved flexibility and agility, lower costs, and faster time to market.

According to an IBM Institute for Business Value survey of 1,106 business and technology executives, by 2021, 85% of organizations are already operating multicloud environments. 98% plan to use multiple hybrid clouds by 2021. However, only 41% have a multicloud management strategy in place.[1]

When it comes to choosing cloud solutions, there's a plethora of options available. It's helpful to look at the differences between the various types of cloud deployment and cloud service models.

85%
of organizations are already operating in multicloud environments.[1]



98%
of organizations plan to use multiple hybrid clouds by 2021.[1]

Understanding cloud deployment models

Over the past decade, cloud computing has matured in several ways and has become a tool for digital transformation worldwide. Generally, clouds take one of three deployment models: public, private or hybrid.

Public cloud
A public cloud is when services are delivered through a public internet. The cloud provider fully owns, manages and maintains the infrastructure and rents it to customers based on usage or periodic subscription, for example Amazon Web Services (AWS) or Microsoft Azure.

Private cloud
In a private cloud model, the cloud infrastructure and the resources are deployed on premises for a single organization, whether managed internally or by a third party.

With private clouds, organizations control the entire software stack, as well as the underlying platform, from hardware infrastructure to metering tools.

Hybrid cloud
It offers the best of both worlds. A hybrid cloud infrastructure connects a company's private cloud and third-party public cloud into a single infrastructure for the company to run its applications and workloads.

Using the hybrid cloud model, organizations can run sensitive and highly regulated workloads on a private cloud infrastructure and run the less sensitive and temporary workloads on the public cloud. However, moving applications and data beyond firewalls to the cloud exposes them to risk.

Whether your data is in a private cloud or a hybrid environment, data security and protection controls must be in place to protect data and meet government and industry compliance requirements.

The hybrid cloud market is estimated to be a **USD 1.2 trillion opportunity**.[2]

But concerns remain about data protection and compliance.

The cost of data breach is rising.

On average, companies take **279 days** to detect and contain a data breach.[3]

Types of cloud service models

Data security differs based on the cloud service model being used. There are four main categories of cloud service models: infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), and database as a service (DBaaS), which is a flavor of PaaS.

IaaS allows organizations to maintain their existing physical software and middleware platforms, and business applications on the infrastructure provided and managed by the service provider. Organizations benefit from this approach when they want to quickly take advantage of the cloud while minimizing impact and using existing investments.

PaaS allows companies to use the infrastructure, as well as middleware or software provided and managed by the service provider. This flexibility removes a significant burden on a company from an IT perspective and allows it to focus on developing innovative business applications.

DBaaS solutions are hosted and fully managed database environments by a cloud provider. For example, a firm might subscribe to Amazon RDS for MySQL or Microsoft Azure SQL Database.

SaaS is a service model that outsources all IT and allows organizations to focus more on their core strengths instead of spending time and investment on technology. It offers SaaS to the end users. In this cloud service model, a service provider hosts applications and makes them available to organizations.

With each step, from IaaS to PaaS to SaaS to DBaaS, organizations give up some level of control over the systems that store, manage, distribute and protect their sensitive data. This increase in trust placed in third parties also presents an increase in risk to data security.

Regardless of the chosen architecture, it's ultimately your organization's responsibility to ensure that appropriate data security measures are in place across environments.

Cloud service models: Key differences

IaaS	PaaS	SaaS	DBaaS
Maintains complete control of the infrastructure management	Enables outsourcing of infrastructure, middleware and software maintenance	Avoids capital expenditure on software	Avoids capital expenditure on database infrastructure and hardware
Is platform independent	Frees IT staff to focus on application development	Turns complete management over to the service provider	Turns complete management over to the service provider
Offers a pay-as-you-go pricing model	Lacks complete control over IT infrastructure	Lacks control over data and security	Reduces control over data and security

Data security challenges to your cloud environment

Chances are, you're already on your journey to the cloud.

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.

Research by the Ponemon Institute has found that insider threats are significantly increasing in frequency and cost. According to the institute's findings, "the average global cost of insider threats rose by 31 percent in two years to $11.45 million and the frequency of incidents spiked by 47 percent in the same time period."[4] The surveyed organizations had a global head count of 1,000 or more employees.

$11.45M
is the global average cost of an insider threat.[4]

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.

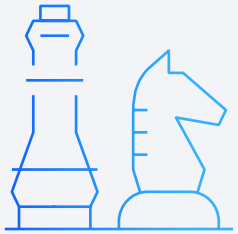
Even as the expense of acquiring storage drops, it can be expensive in the long term due to increased business use and the number of personnel managing the storage systems. However, while putting data storage in the hands of third-party service providers can help save money and time, it can also pose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

Cloud deployments work on a shared responsibility model between the cloud provider and the consumer. In the case of an IaaS model, the cloud consumer has room to implement data security measures much like what they would normally deploy on premises and exercise tighter controls.

On the other hand, for SaaS services, cloud consumers for the most part have to rely on the visibility provided by the cloud provider 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, 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 security controls need to go wherever your data goes.

Determining how best to store data is one of the most important decisions an organization can make.



Keep your sensitive data safe essentially everywhere

Who has access to sensitive data in your organization? How sure are you that your staff or privileged users haven't inappropriately accessed sensitive customer data?

In other words, you can't protect what you don't know. Simply locking down network access may not serve the purpose. After all, employees rely on this network to access and share data. This access means that the effectiveness of your data security is largely in the hands of your employees, some of which may no longer work directly for your company but still maintain access. Automated discovery, classification and monitoring of your sensitive data across platforms is crucial to enforce effective, in-context security policies and to help address compliance with regulations.

Generally, in cloud environments, cloud service providers (CSPs) have the ability to access your sensitive data, which makes CSPs a new frontier in insider threats. Additionally, cybercriminals know that CSPs store vast amounts of important data, making such environments prime targets for attacks. To counteract these threats, sophisticated analytics-based tools that verify authorized and normal access must be utilized.

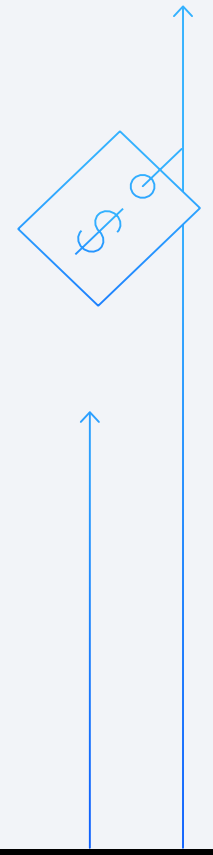
Learn more →

95% higher

average data breach cost in organizations without security automation in 2019.[3]

$5.16M

was the cost **without automation**.[3]



$2.65M

was the cost **with fully deployed automation**.[3]

Consider encryption for cloud storage

With cloud storage, your data may move to a different place, on a different media, than its location today. The same is true of virtualization. Not only cloud-based data, but also cloud-based computing resources might shift rapidly in terms of both location and hardware underpinnings. The shifting nature of the cloud means that your security approach needs to address different kinds of cloud-based storage. Your approach also must account for copies, whether long-term backups or temporary copies, created during data movement.

To address these challenges, you should deploy cross-platform solutions and employ strong encryption to help ensure that your data is unusable to unauthorized persons in the event that it's mishandled.

Even if your data is not primarily stored in the cloud, both the form in which data leaves and returns to your enterprise and the route data takes are important concerns. Data is only as secure as the weakest link in the processing chain. So, even if data is primarily kept encrypted and behind a firewall onsite, if it's transmitted to an offsite backup or for third-party processing, the data may be exposed.

Malware detection or behavioral analysis that's designed to spot suspicious activities can help prevent an internal or external data breach—and serve valuable functions in their own right.

Encryption, however, helps protect data wherever it exists, whether it's at rest or in motion.

Effective cloud storage security is more than simply backing up files. It's about guarding your data with preventive measures against unauthorized use.

Cloud storage security best practices

- Blocking access over non-approved ports
- Proactively assessing for vulnerabilities
- Continuously scanning for suspicious data access
- Encrypting your sensitive data, maintaining good encryption key hygiene, and storing the keys on premises on a separate network from the encrypted data
- Using a unified platform that integrates security information across hybrid, multicloud environments

Organizational challenges to your cloud environment

With data growing at an exponential rate, organizations are facing a growing list of data protection laws and regulations. What are 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 security solution, organizations should adopt a risk-based approach to protecting customer data across environments.

Here are five challenges that could impact your organization's security posture:

- Ensuring compliance
- Assuring privacy
- Improving productivity
- Monitoring access controls
- Addressing vulnerabilities

IBM Security™ Guardium® data protection platform is designed to help your organization meet these challenges with smarter data protection capabilities across environments.

Keep up with 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 European Union (EU) General Data Protection Regulation (GDPR), information that reveals a person's racial or ethnic origin are considered sensitive and could be subject to specific processing conditions.[5] 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 also help with demonstrating compliance with regulations, such as:

- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Security Content Automation Protocol (SCAP)
- Federal Information Security Management Act (FISMA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act (HIPAA)
- California Consumer Privacy Act (CCPA).

IBM Security Guardium solutions are designed to monitor and audit data activity across databases, files, cloud deployments, mainframe environments, big data repositories, and containers. The process is streamlined with automation, thus lowering costs and time for compliance requirements.

Learn more →

"Guardium has a lot of built-in reporting and features now, focusing on things like GDPR. So, we can take advantage of that built-in functionality to give us a faster start, without having to build up things from scratch."

A senior governance specialist, insurance organization, in a Forrester Total Economic Impact (TEI) Study.[6]

Read the Guardium TEI Study →

Address privacy issues

With the proliferation of smartphones, tablets and smart watches, 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, as well as advanced analytics based on proprietary machine learning (ML) technology to help them uncover hidden threats within large volumes of data across hybrid environments.

Learn more →

Hear from Kevin Baker, Chief Information Security Officer at Westfield, on the data privacy challenges facing his organization, and his approach to addressing them through the necessary insights and automation while scaling to support innovation with IBM Security Guardium Insights.

Watch video →

Improve productivity

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.

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

According to Ponemon Institute, IBM Guardium solutions can help make IT security teams more efficient.[7] Prior to deploying the Guardium solution, about 61% of the surveyed IT security teams' time was spent identifying and remediating data security issues. Post deployment, the average percentage of time spent on such activities was 40%, a decrease of 42%.

Prior to deploying Guardium solution

61%

of the time was spent annually on identifying and remediating data security issues.[7]

Post-Guardium deployment

40%

of the time was spent annually on identifying and remediating data security issues.[7]

Monitor access controls

The lifecycle of a data breach is getting longer, states a study by the Ponemon Institute. In fact, the institute's research found that 49% of the data breaches studied were due to human error, including system glitches and "'inadvertent insiders" who may be compromised by phishing attacks or have their devices infected or lost/stolen."[3]

Cybercriminals could range from individuals to state-sponsored hackers with disruptive intentions. They could be rogue computer scientists trying to show off or make a political statement, or they may be tough, organized intruders. They could be disgruntled employees or even foreign state-sponsored hacker 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 end 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 make protection of data at its source crucial.

A layered data security solution can help administrators examine data access patterns and privileged user behaviors to understand what's happening inside their private cloud environment. The challenge is to implement security solutions without hampering the business' 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.

49%

Nearly half of the data breaches caused were due to inadvertent breaches from human error and system glitches.[3]

Address vulnerability assessments

When it comes to defending against attackers, what worked in the past may not work today. Many organizations rely on diverse security technologies that could be operating in silos. According to a study by Forrester Consulting, on average, organizations are managing 25 different security products or services from 13 vendors.[8]

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 could 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 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 cloud services 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 there be coding changes 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 wherein security strategies are built into the fabric of their hybrid, multicloud environments.

Unlike a point solution, IBM Security Guardium Insights supports heterogeneous integration with other industry-leading security solutions. Guardium data protection also provides best-of-breed integration with IBM Security solutions, such as IBM QRadar® SIEM for proactive data protection.

Learn more →

"Guardium takes all of the different database management systems and consolidates it into one tool versus us needing to use separate systems for Oracle, for SQL server and the like. We can look at all the information in a single pane of glass."

VP, cyber security management, financial services, TEI Study[6]

Read the Guardium TEI Study →

A smarter data security approach

As cloud matures and scales rapidly, we must realize that **effective data security isn't a sprint, but a marathon**—an ongoing process that continues through the life of data.

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

What constitutes an effective cloud security strategy?

Discover and classify your structured and unstructured sensitive data, online and offline, regardless of where it resides and classify sensitive IP and data that's subject to regulations, such as PCI, HIPAA, Lei Geral de Proteção de Dados (LGPD), CCPA, and GDPR.

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 should help keep your sensitive data protected.

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.

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 security 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 suspicious 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 multiple, disjointed consoles.

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 data security and audit data. Data security and compliance reporting must be comprehensive, accounting for your entire data environment.

Encrypt data in hybrid, multicloud environments

Since 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 essentially 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 customers who 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 will be able to meet regulations, such as the PCI DSS, SOX and HIPAA.

Discover more →

IBM Security Guardium platform was named a Leader in the Forrester Wave: Data Security Portfolio Vendors, Q2 2019. According to the report, the Guardium platform is a "good fit for buyers seeking to centrally reduce and manage data risks across disparate database environments."

Read the report →

Discover a new approach to data security

At the core of protecting a hybrid, multicloud environment is the need for organizations to adopt solutions that offer maximum visibility and business continuity and help meet compliance and customer trust.

IBM Security Guardium platform is centered on the overarching value proposition of a "smarter and more adaptive approach" to data security. Further, the solution supports a wide array of cloud environments, including private and public clouds, across PaaS, IaaS, and SaaS environments, for continuous operations and security.

The Ponemon Institute conducted a survey of organizations that use the Guardium solution to monitor and defend their company's data and databases. It found that 86% of respondents said the ability to use the Guardium solution to manage data risk across complex IT environments, such as a multicloud or hybrid cloud ecosystem, is very valuable. Similarly, ML and automation is a significant benefit in managing data risks across the enterprise.[7]

With the Guardium solution, your security team can choose the system architecture that works for your enterprise. For example, your team can deploy all of the Guardium components in the cloud, or choose to keep some of those components, such as a central manager, on premises. This flexibility allows existing customers to easily extend their data protection strategy to the cloud without impacting existing deployments.

Learn more →

IBM Security 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.

Conclusion

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

- 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 protection 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 will provide an efficient platform for data security and privacy delivery, helping you manage costs by reducing resources and providing greater agility and flexibility.

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

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. Visit ibm.com/security/data-security/guardium

The Forrester TEI Study shows these key business benefits enabled by IBM Security Guardium platform:[6]

343% ROI

$3.3M in overall benefits

Payback in **<6 months** on average

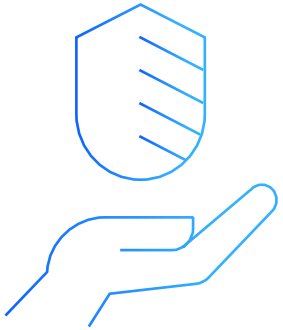
Read more →

Why IBM Security solutions?

IBM Security solutions offer one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications. It offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more.

These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures.

IBM operates one of the world's broadest security research, development and delivery organizations, monitoring greater than 60 billion security events per day in more than 130 countries, and the corporation holds more than 3,700 security patents.



For more information, please contact your IBM Business Partner:

K&P Computer

+4961227071205 | koehler@kpc.de

www.kpc.de

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2020

1 "Assembling your cloud orchestra." *IBM Institute for Business Value*, October 2018. ibm.com/thought-leadership/institute-business-value/report/multicloud/#

2 Jim Comfort, "How a Hybrid Multicloud Strategy Can Overcome the Cloud Paradox." *IBM*, November 5, 2019. ibm.com/blogs/think/2019/11/how-a-hybrid-multicloud-strategy-can-overcome-the-cloud-paradox/

3 "Cost of a Data Breach Report 2019." *IBM Security.* databreachcalculator.mybluemix.net/executive-summary

4 "2020 Cost of Insider Threats Global Report", *Ponemon Institute, ObserveIT*. observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

5 "What personal data is considered sensitive?" *European Commission*. ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

6 "The Total Economic Impact Of IBM Security Guardium." *Forrester*, April 2018. ibm.com/downloads/cas/QA8XWPBA

7 "Ponemon Report: Client Insights on Data Protection with Guardium." *Ponemon Institute*, August 2019. ibm.com/account/reg/us-en/signup?formid=urx-40683

8 "Complexity In Cybersecurity Report 2019." *Forrester Consulting*, May 2019. ibm.com/downloads/cas/QK1YD49A

GWB3E8ZV