IBM Security

xelere Making IT better

IBM

# Overcome the challenges of protecting data that is here, there and everywhere

Keeping sensitive data secure in the age of Cloud computing

Click on a circle to jump to chapter


## Deploying a cloud environment

Organizations are rapidly moving to the cloud, leveraging infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) as new ways to optimize their business, even though these environments present new risks to sensitive data.


## Cloud security challenges

Cloud deployments often mean sensitive data is kept in locations you can't control and managed by third parties that may have unfettered access to it.


## Organizational challenges

Challenges when protecting data in the cloud include ensuring compliance, monitoring access controls, assuring privacy, improving productivity, and addressing vulnerabilities—all while leveraging your on-premises data and your cloud-based data together to drive your business forward.


## Data protection approach

Data security and protection technologies should operate in multiple environments (physical, cloud and hybrid) at the same time. Your data security solution should be automated, dynamic and adaptive, and should provide consistent, flexible encryption capabilities.


## Conclusion

As cloud computing becomes pervasive, security fundamentals remain the same: secure and protect data and support compliance.

# 1.1 Deploying a cloud environment

Just a few years ago, many organizations turned to private cloud environments to help increase flexibility and control costs—largely because of the immaturity and lack of control within the public cloud environments then available. Today, however, the decision to "go cloud" is less of a binary, and more of a spectrum of choices, spanning different deployment models (public, private and hybrid) and service types, including IaaS, PaaS and SaaS.

With more granular options, cloud deployment has become fragmented according to line of business, rather than being a standardized IT decision. And while the list of new cloud options is plentiful, most enterprises will adopt a mixed, hybrid environment to leverage their existing investments in mainframes, on-premises databases, big-data distributions, file systems and more.[1]

A private cloud is an IT infrastructure operated solely 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. Private-cloud services are dedicated for the use of a single enterprise's business units (or shared only with its partners).[1] Nonetheless, when workloads move to private clouds, securing data in virtual environments becomes even more important, especially as workloads with different trust levels are combined to run on the same physical hardware.

Gartner research shows that there will continue to be significant use and investment in private cloud computing. Nearly all enterprises that Gartner surveyed, though, want to leverage a hybrid cloud model—with both private and public cloud elements. Enterprises are employing turnkey public cloud computing options to enable faster, frictionless services and to increase business agility and spur innovation. Public cloud computing fills a key role for innovation and, as a result, is forecast to grow at 15.2 percent annually through 2019.[1]

When it comes to cloud environments, whether in the public cloud or a privately hosted environment, data security and protection controls must protect sensitive data—and support constantly growing government and industry compliance requirements.

# 1.2 Deploying a cloud environment

The most common service types are IaaS, PaaS and SaaS. The easiest way to visualize the difference is to consider your IT stack. At the bottom, you have your infrastructure—which includes your hardware, servers and networking—that acts as your IT foundation. Above this infrastructure you have your software or middleware platforms that provide the tools your developers need to deploy business applications. And at the very top you have your business applications that interface with internal employees and customers.

IaaS allows organizations to maintain their existing physical software and middleware platforms and business applications, but outsource the management of their underlying infrastructure. Companies do this with the intention of quickly taking advantage of the cloud, while minimizing impact and leveraging existing investments.

PaaS allows companies to outsource the infrastructure as well as middleware or software. This removes a significant burden on a company from an IT perspective and allows it to focus on developing innovative business applications.

SaaS is the most extreme option, which outsources all IT and allows organizations to focus more on their core strengths (e.g., healthcare, financial services) instead of spending so much time and investment on technology that can be left to the technology experts.

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

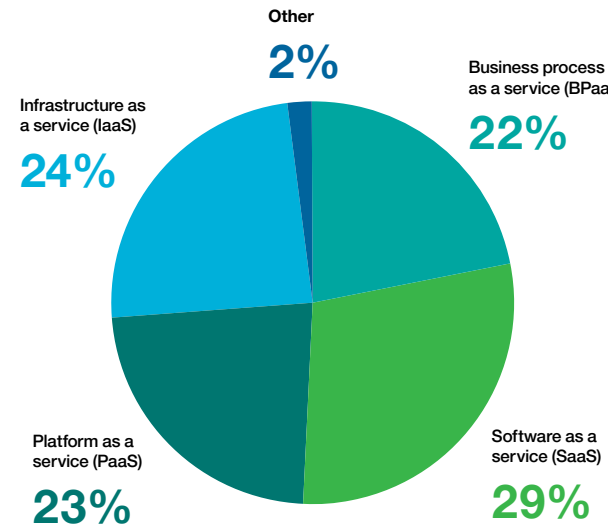



Figure 1: Polling question: "How is the budget currently allocated to 'public' cloud services divided between the following types of cloud?"

Source: Ed Anderson and Sid Nag, "Market Trends: Cloud Adoption Trends Favor Public Cloud With a Hybrid Twist," Gartner, August 4, 2016. ID: G00294424.

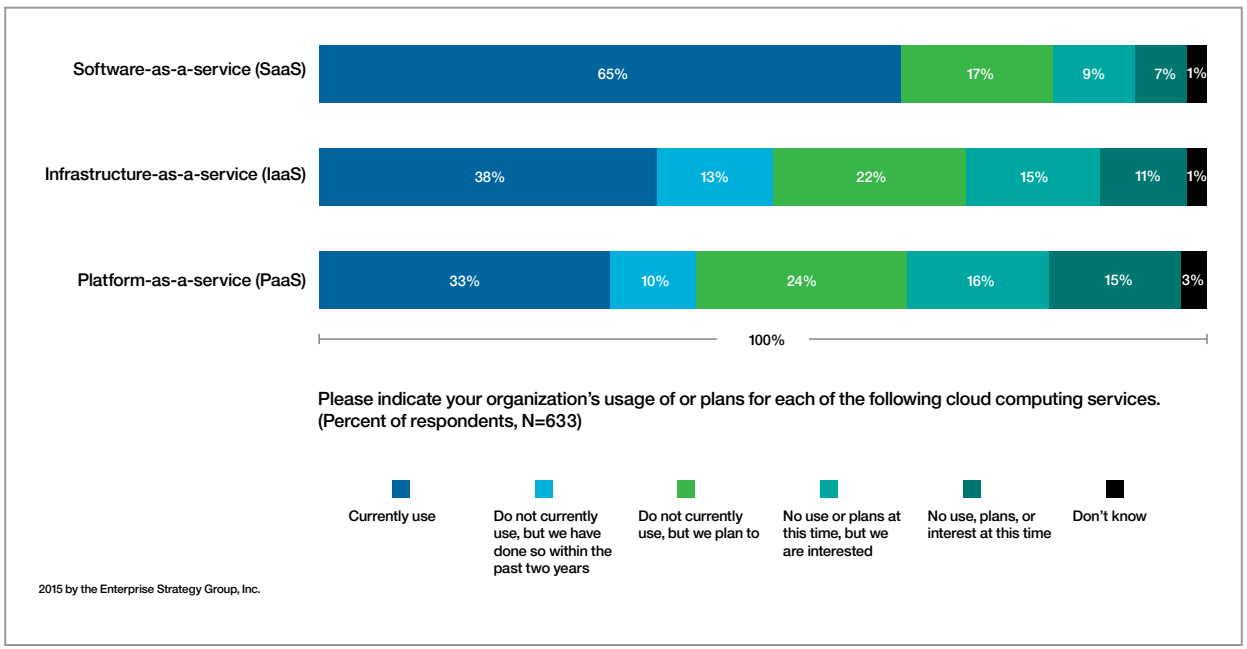
# 1.3 Deploying a cloud environment

"Using the cloud" isn't a binary. A study of more than 600 enterprise IT decision makers shows that most firms surveyed have adopted at least some SaaS applications; fewer than 20 percent of respondents had no plans or interest in employing SaaS.

PaaS deployment, which demands deeper commitment to off-premises data storage and computing, understandably lags behind piecemeal cloud applications, but 67 percent of respondents used, had used, or planned to adopt PaaS.

Adoption of cloud infrastructure—IaaS—which moves the burden of installing and maintaining physical infrastructure from an enterprise to a dedicated provider, lies statistically between PaaS and SaaS. At the time of this survey, 73 percent of respondents used or planned to use some form of cloud infrastructure, or had already experimented with it.

**Virtual and private cloud data protection challenges**



# 2.1 Cloud security challenges


The cloud is especially well-suited for long-term, enterprise-level data storage—with economies of scale in both equipment and administration that can make cloud-based data centers a smarter place to store business-critical information than a stack of servers down the hall. That's because even as the expense of acquiring storage drops, the costs of increased business use and of personnel to manage storage continue to rise. However, while putting data storage in the hands of dedicated administrators can help save money and time, it can also pose serious security challenges and create new levels of risk.

It is important to realize that whatever the deployment model or service type—the fundamental data security principles should not change. What does change is that your sensitive data now sits in many places, both within your company's walls and outside of them. This means security controls need to go where your data goes. When evaluating data security technologies, select solutions that operate in multiple environments transparently and simultaneously. Make sure the data security solution is dynamic and adaptive across a full range of environments so that you don't need to haphazardly 'bolt on' additional data protection pieces.

### Keeping data safe everywhere, from everyone

The most important of these challenges is obvious: sensitive data is now everywhere, inside and outside of your firewalls, and is being managed in some way by people on your payroll as well as by third parties. You can no longer protect your sensitive data by simply locking down network access. In fact, you rely on the network to access and share your data. This leaves data security largely in the hands of many more people than in the past and many people who no longer work directly for your company. Generally, in cloud environments, cloud service providers (CSPs) have the ability to access your sensitive data, which makes CSPs the new frontier in insider threats. Additionally, cybercriminals know that CSPs store vast amounts of important data. Both of these risks make capabilities such as data encryption and data activity monitoring an especially valuable part of your security strategy.

# 2.2 Cloud security challenges

Data portability is one reason that cloud storage is an economical choice to start with. Infrastructure expenses (from real estate to energy costs) vary hugely by geography and even by time of day. Likewise, storage costs and performance among media types shift. Tape, spinning disk and solid-state storage all are advancing in capacity, speed and reliability, and the most economical mix of storage technologies for a given enterprise can change rapidly. With cloud storage, therefore, your data may live tomorrow in a different place, on 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—transparently and rapidly—in both location and hardware underpinnings.

The shifting nature of the cloud means that security approaches for cloud-based storage need to address different kinds of storage. Your approach also must account for copies, whether long-term backups or temporary copies created during data movement. To address these challenges, select cross-platform solutions and employ strong encryption.

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. Even for data primarily kept encrypted and firewalled on-site, if portions of it are exposed when transmitted to an off-site backup or for processing by a third party, the sensitive data is only as safe as the weakest link in the data processing chain.

Effectively guarding your data when it is in the cloud takes both passive, preventive measures (such as blocking access over non-approved ports) and active ones, such as continuously scanning for suspicious data access. Chief among the measures you can take is to employ encryption for your sensitive data. While malware detection or behavioral analysis designed to spot suspicious access can help prevent an internal or external data breach—and serve valuable functions in their own right—encryption helps protect data wherever it exists, whether it is at rest or in motion.

# 2.3 Cloud security challenges

### Administrative and regulatory implications

The realities of cloud-based storage and computing mean that securing sensitive data across cloud and hybrid cloud systems is rarely as seamless as administrators would hope. Security tools that offer unified interfaces across cloud endpoints—from a dedicated off-site server farm to virtual machines in a public cloud infrastructure—are a good start toward realizing the promise of efficient remote administration.

Just as important are regulatory requirements and data sovereignty—in other words, the rules that address data security and protection when sensitive data is stored physically in a particular place. Storing data in the cloud may result in sensitive data being stored in locations where stricter laws are in force than those in the data's original home. Stricter protection for the personal data of individuals within European Union (EU) countries, for instance, is mandated in the terms of the EU's General Data Protection Regulation (GDPR). These requirements apply even to companies located in other regions of the world that hold and access EU residents' personal data.

***Know who's accessing your data: IBM® Security Guardium® can help secure your cloud and hybrid cloud infrastructure with monitoring and assessment tools that reveal anomalies and vulnerabilities.***

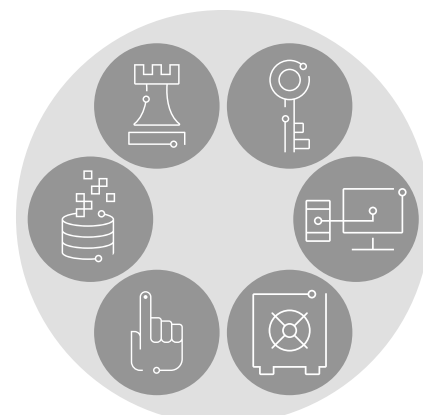
# 3.1 Organizational challenges

3

Organizations are still highly challenged when trying to safeguard their sensitive data, and complex regulations are one reason why. Forrester points out that today, "most enterprise architects and security professionals struggle to improve data security or meet compliance requirements, due to growing data silos and increasing data volumes. Applying uniform access control polices across databases, data warehouses, Hadoop, NoSQL and files has become extremely challenging."[2]

Virtualization has the potential to make applying security controls and compliance mechanisms easier, but only if the virtual or private cloud environment is able to support securing sensitive data by uniformly addressing compliance requirements, access control needs, privacy requirements, vulnerability requirements and productivity needs.

**Virtual and private cloud data protection challenges**



Compliance
Productivity
Access control
Vulnerability
Privacy

Figure 2: Protecting cloud-stored data still requires administrators to pay attention to security aspects from security and privacy to regulatory compliance across several domains.

# 3.2 Organizational challenges

### Compliance

Think about where sensitive data resides in a cloud environment. It's important to identify and classify sensitive data types and establish policies for its use, whether in the public cloud or in a private cloud environment. If data is in a public cloud, you need to understand how the provider of the cloud infrastructure plans to protect your sensitive data.

In either case, understanding where data resides, what domains of information exist, and how these relate across the enterprise will help organizations define the right policies for securing and encrypting that data and for 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 Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH). Compliance regulations continue to emerge, and organizations remain accountable even as data moves to the cloud.

### Privacy

Another challenge for data access administrators is ensuring that only those with a valid business reason have access to personal information. For example, physicians need to see 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.

# 3.3 Organizational challenges

### Access controls

Cybercriminals have unscrupulous and disruptive intentions. They could be rogue computer scientists trying to show off or make a political statement, or they may be tough, organized intruders. Foreign states have sponsored hackers to collect intelligence from government organizations. Attackers might even be disgruntled employees. Breaches can also be accidental—for example, when permissions are set incorrectly on a database table, or when an employee's credentials are compromised. Best practices suggest 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 it's equally important to protect the sensitive data itself. If the perimeter is breached, sensitive data needs to already be secure (and unusable to a thief) to minimize the impact of the breach and ensure that the hacker does not have free rein. Defenses should include a layered data security solution, so administrators can understand what's happening inside the private cloud—for example, by understanding data access patterns and privileged user behaviors.

The challenge is to provide the appropriate access and data protections while meeting business needs and ensuring that data is managed on a "need-to-know" basis—wherever it resides.

### Productivity

Security and privacy policies should enable and enhance, not interfere with business operations. They should be built into everyday operations and work seamlessly within and across all environments—in private cloud environments, public cloud environments, on-premises environments and hybrid environments—without impacting user 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.

# 3.4 Organizational challenges

### Vulnerability

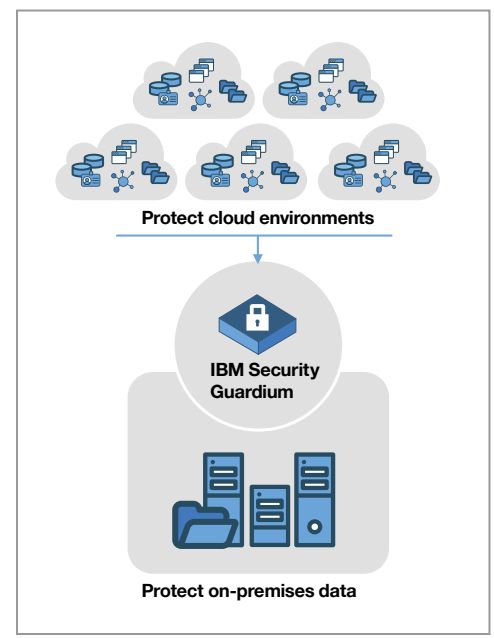
Today, organizations have diverse security technologies in place to protect enterprise data and support compliance. But the number of data repository vulnerabilities is vast, and criminals can exploit even the smallest window of opportunity. It's important to understand vulnerabilities from all angles and develop an approach to address them. Common vulnerabilities include missing patches, misconfigurations and default system settings. This complexity is increasingly difficult to keep track of and manage as data repositories become virtualized.

As organizations move toward private as well as public clouds, for example, these solutions don't always scale. In addition, some encryption approaches are tied to a particular hardware or network resource. In a cloud environment, administrators cannot depend on access to the low-level hardware infrastructure.

Another issue often arises when a private cloud is used for application testing or development. New databases are regularly created and decommissioned. Data needs to be protected as these databases are dynamically created to support testing and development. A scalable data security approach for such a private cloud environment means that as these new databases are created, they are automatically discovered and the data that lives in them is automatically classified, monitored and protected.

Finally, think about the use of homegrown tools in place today for data security—for example, data masking routines or database activity monitoring scripts. Are there coding changes required to make them work on a virtual database? Chances are, a significant investment will be required to update these homegrown solutions—and then you will still face significant challenges. Ideally, as new databases or other data sources are added, security processes and procedures should be carried out without manual intervention. In short, security strategies should be built into the fabric of any cloud environment.

### Data protection approach



# 4.1 Data protection approach


Organizations should look to centralize data security and protection controls in private and public cloud environments, as well as in the rest of the enterprise, and ensure a segregation of duties so that data administrators don't also become security administrators or auditors. Key elements of a secure cloud strategy include:

- Understanding where sensitive data exists and who has access to it. Organizations can't protect sensitive data with encryption or apply tough access controls unless they know where it resides and how it's related across the enterprise.
- Safeguarding structured and unstructured sensitive data, online and offline, with the appropriate technologies and establishing the right access requirements.
- Protecting data beyond production, in development, testing and quality assurance environments.
- Securely and continuously monitoring access to sensitive data—wherever it resides.
- Demonstrating compliance to pass audits with prebuilt reports for auditors and with automated workflow so you can get the right reports to the right people at the right time for sign-off.

Comprehensive protection strategies for all cloud and hybrid cloud environments should provide alerts on suspicious behaviors to security administrators. Organizations should also consider data security solutions that provide automated compliance support to streamline the compliance process.

Data security processes for cloud environments need to continuously track data and provide insight into who is accessing the data across applications, databases, warehouses and file shares, big-data environments, and more. Such an approach can help ensure 360-degree protection for sensitive organizational data, no matter where it lives.

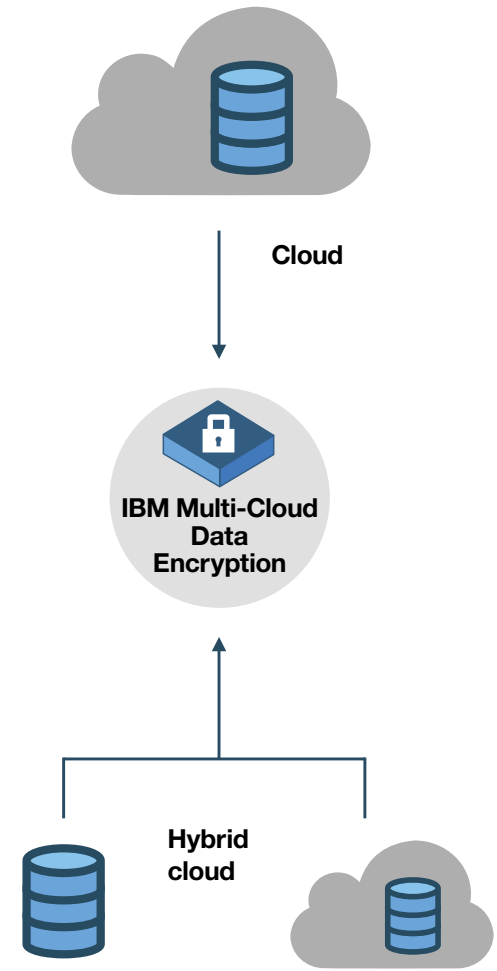
# 4.2 Data protection approach

Regulatory burdens on data holders (as well as the risks of a breach) can make enterprises considering new or expanded cloud-based storage wary. Strong encryption is the most obvious answer to the challenge of securing sensitive data, on-premises or off, but 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 Multi-Cloud Data Encryption protects cloud (and hybrid-cloud) data, and does so with portability and compliance requirements in mind. To keep encryption keys accessible and reliably available, it can be integrated with an advanced key manager.

Additionally, IBM Security Key Lifecycle Manager can help customers who require more stringent data protection, based on hardware-encrypted storage, to simplify and centralize the management of encryption keys, without fear of data exposure in virtual cloud environments.

*Key management is the heart of a secure encryption environment.*



# 5.1 Conclusion


To ensure that data is protected in virtual and cloud environments, organizations need to understand what data is going into these environments, how access to this data can be monitored, what types of vulnerabilities exist and how compliance can be demonstrated. Protections should be built into cloud environments from the start with a phase-one goal of helping organizations demonstrate compliance.

When choosing data security and protection solutions, select those solutions that are scalable and extensible across 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 any special setup, configuration or added expense. Such an approach will provide an efficient platform for data security and privacy delivery, help manage costs by reducing data security resources and provide greater agility and flexibility with self-services for security and privacy.

Guardium can help support your cloud strategy with:

- Data and file activity monitoring, vulnerability assessments, data redaction and data encryption, dynamic blocking, quarantining and alerting
- Automatic discovery and classification of sensitive data in the cloud
- Static and dynamic data masking to ensure a least-privileged-access model for cloud resources
- Prebuilt audit and compliance reports, customized for different regulations, to demonstrate compliance and automate compliance workflow—in on-premises and cloud environments

# 5.2 Conclusion

Guardium software provides a comprehensive solution for physical, virtual and cloud infrastructures through centralized, automated security controls across heterogeneous environments. Guardium helps streamline compliance and reduce risk, and offers install-ready images for IaaS deployments on major cloud platforms, such as IBM SoftLayer®, Microsoft Azure, and Amazon Web Services, and operating across Microsoft Windows, UNIX and Linux environments.

The flexible Guardium architecture allows for several different deployment models. You can choose the system architecture that works for your enterprise: Guardium components can all be deployed in the cloud, or you can choose to keep some of those components, such as a central manager, on-premises.

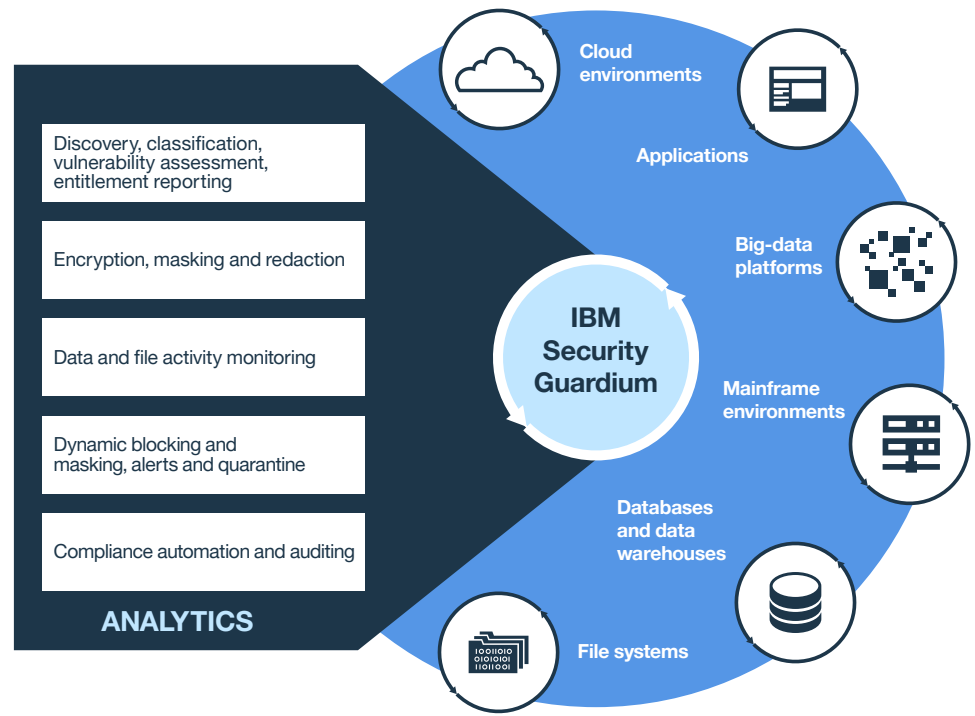



Figure 3: Guardium provides end-to-end data protection across a broad range of environments and technology platforms.

# 5.3 Conclusion

This flexibility allows existing customers to easily extend their data protection strategy to the cloud without impacting existing deployments.

Input-monitoring collectors deployed in the cloud can easily feed their data to the central manager, ensuring a single, consolidated view of your data protection threats, no matter where the data resides.

Security controls that keep cybercriminals out of a data store—or quickly detect a successful intrusion—are important tools. But in the era of portable data, shifting workloads and virtualization, keeping data safe with encryption is just as important.

IBM data security solutions help protect sensitive data so that organizations can rest assured that their data is protected in complex virtualized and cloud environments.

## 5.4 Additional resources

### About IBM Security solutions

IBM Security offers 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, offering 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, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information on data security, compliance and cloud, visit **ibm.com**/guardium.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589, U.S.A.

Produced in the United States of America
May 2017



1. Thomas J. Bittman, "Internal Private Cloud Is Not for Most Mainstream Enterprises," *Gartner*, May 22, 2015.

2. Noel Yuhanna, "Enterprise Data Virtualization, Q1 2015," *The Forrester Wave*, March 11, 2015.



WGM12362-USEN-00