IBM Security

Comprehensive data protection for physical, virtual and cloud infrastructures

Keeping data secure in the age of cloud computing

IBM

1

Virtualization

Virtualization lowers total cost of ownership, improves business agility and provides a gateway for cloud computing, but it also raises new security concerns.

2

What does it mean to deploy a "Cloud" environment?

Organizations are rapidly moving to the cloud, even though cloud systems represent a new vulnerability that may be easily exploited.

3

Organizational challenges

Challenges when protecting data in the cloud include: ensuring compliance, monitoring access controls, assuring privacy, improving productivity and addressing vulnerabilities.

4

Data protection approach

Data security technologies should operate in multiple environments (physical, virtual and cloud) at the same time. Make sure the data security solution is dynamic and adaptive.

5

Conclusion

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

Virtualization: A fundamental change in the data center

Virtualization is the creation of a logical rather than an actual physical version of something, such as a storage device, hardware platform, operating system, database or network resource. The usual goal of virtualization is to centralize administrative tasks while improving resilience, scalability and performance and lowering costs. Virtualization is part of an overall trend in enterprise IT towards autonomic computing, a scenario in which the IT environment will be able to manage itself based on an activity or set of activities. This means organizations use or pay for computing resources only as they need them.

Forrester defines data virtualization as: An integration platform that orchestrates data in real time or near real time from disparate data sources, whether on-premises or cloud, into coherent self-service data services to support various use cases and workloads including extreme transactions, analytics and predictive analytics.[1]

By inserting the level of abstraction provided by data virtualization, organizations can decouple consumers from resources. Virtualization enables previously hard-coupled elements of the IT stack to be taken apart and recombined in ways that easily enable new combinations and use cases. This fundamentally changes the data center and raises numerous questions about security and privacy.

In fact, per Forrester, one of the key benefits of virtualization is real-time data sharing across lines of business, partners and the enterprise. With growing data volumes and silos in most organizations, data sharing and collaboration is a major challenge. In large environments, widespread data movement is impractical, especially when dealing with hundreds of terabytes and petabytes of information. Data virtualization allows any application, process, use or tool to access any business data, regardless of its physical or logical location and data format.[2]

While sharing business data on this scale can have a very positive impact on the business, by reducing the boundaries and setting this (often sensitive) data free, you can also create a significant data security exposure. Examples of frequently occurring new behaviors that create significant exposure in this virtualized world include doing things such as copying virtual loads without notice, relying on SP administration personnel, leaving clear sensitive data on cloud resources, allowing SP tools to mine your data, etc.

Virtualization: A fundamental change in the data center

In fact, security concerns are one of the largest barriers to cloud adoption. For example:

- How do existing data security and compliance strategies translate in this new computing model?
- Can sensitive data be properly secured in cloud environments?
- Do compliance mandates specify requirements for virtualization?
- What types of new threats are introduced?
- What are the key sources of risk?

Virtualization has been rapidly deployed, and, according to Gartner, "cloud service providers (CSPs) are beginning to offer stronger network and infrastructure security environments than many organizations are able to offer on premises, but such efforts do not prevent cyber security risks such as hacking or insider malicious behavior."[3]

Also as part of the Gartner Predicts 2016 report, Gartner goes on to state that "Despite the urgent need for organization-wide DSG [Data Security Governance] for compliance or data protection", there are gaps on both the SaaS side of virtualization and on the on-premises (or private cloud) side of virtualization.[4]

So, even though virtualization has been around for more than a decade, and has been increasingly deployed, fundamental data security issues remain unanswered. It's easy to see that data security issues need to be very carefully planned for and addressed as organizations elect to deploy virtualized environments.

What does it mean to deploy a 'Cloud' environment?

Just a few years ago, many organizations were looking to private cloud environments alone to help improve business flexibility and help control costs—largely because of the immaturity and lack of control in public cloud environments. The decision to 'go cloud' has become less of a binary decision and more of a "spectrum of choices, and private cloud or public cloud has also become a spectrum of opportunities. Doing one or the other is a choice made for use cases, not for enterprise IT as a whole."[5]

A private cloud is an IT infrastructure operated solely for a single organization. It can be managed internally or by a third party. With private clouds, organizations control the entire software stack, as well as the underlying platform; metering tools, hardware infrastructures and so forth. When workloads move to private clouds, securing data in virtual environments becomes more important than ever.

Data centers must become more flexible, especially as workloads of different trust levels are combined to run on the same physical hardware.

Enterprises are increasingly turning to public cloud computing to enable faster, frictionless services, which 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 through 2019.[6] Private cloud computing has the attributes of public cloud computing, except that the services are not shared with other enterprises; they are for the use of a single enterprise's business units (or shared only with its partners).[7]

Gartner research shows that there will continue to be significant use and investment in private cloud computing, but that nearly all enterprises that Garner surveyed want to leverage a hybrid cloud model — where both private and public cloud will be used. The figure 1 on page 6 shows the breakout of Gartner respondents, with a weighted average of 64 percent private and 36 percent public cloud.

When it comes to private cloud environments, data security controls must accomplish two objectives. The first is to respond to the need to protect sensitive data in the private cloud or virtual environment. The second is to validate compliance with the growing requirements of regulatory mandates.

What does it mean to deploy a ‘Cloud’ environment?

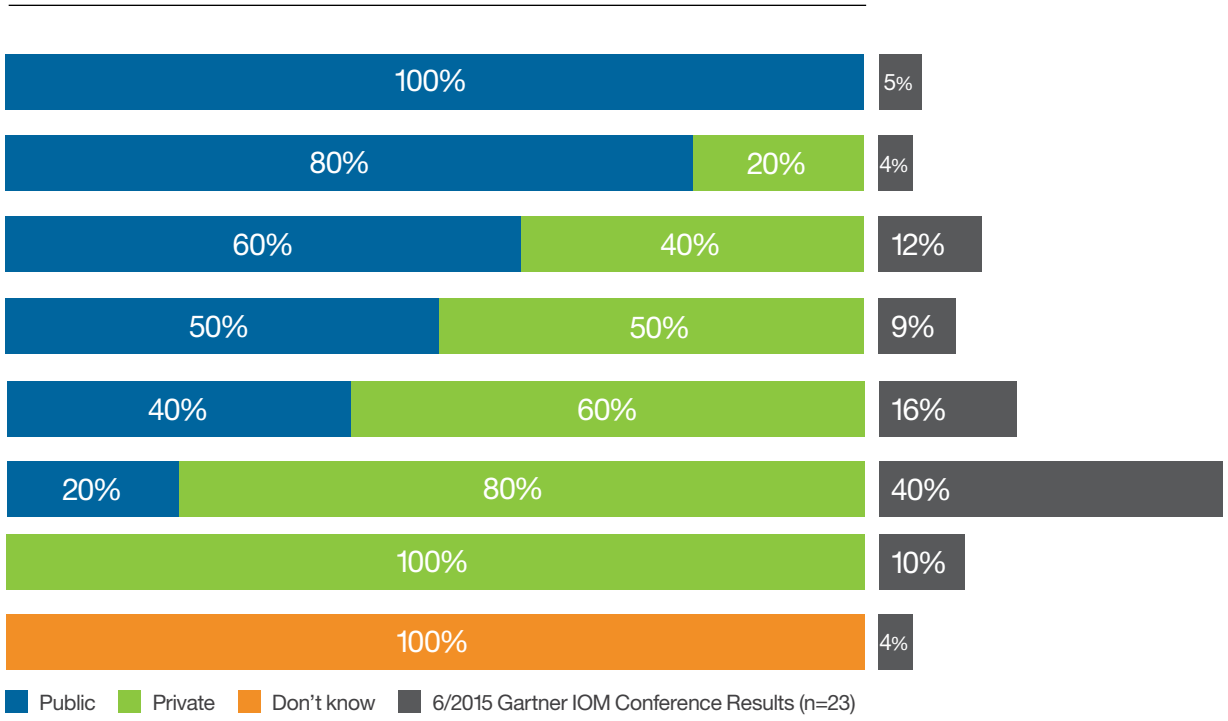


Figure 1: Polling Question: How much of your enterprise’s cloud service aggregate capacity will operate in the public cloud versus the private cloud in 2018?[8]

It is important to realize that whatever environment is being secured — a physical data center, a virtual data center or a private cloud, the fundamental data security principles don’t change. What does change is the fact that controls must become more flexible to support a paradigm where workflows are decoupled from the physical hardware underneath.

This means security controls need to scale across physical, virtual and cloud environments. When evaluating data security technologies, select solutions which operate in multiple environments at the same time. Make sure the data security solution is dynamic and adaptive.

Organizational challenges

Organizations are still highly challenged when trying to safeguard their sensitive data. 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."[9]

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 addressing: compliance requirements, access control needs, privacy requirements, vulnerability requirements and productivity needs.

Virtual and private cloud data protection challenges

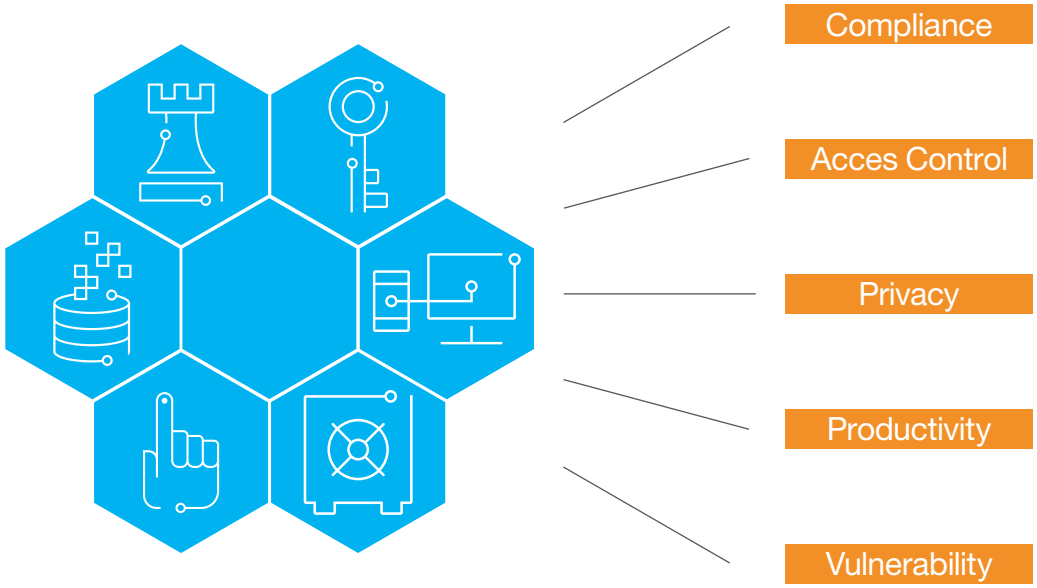


Figure 2: Virtual and private cloud data protection challenges.

Organizational challenges

Compliance

Think about where sensitive data resides in a cloud environment. It's important to identify sensitive data types and establish policies for use of this data in the private cloud. If data is in a public cloud, you need to understand how the provider of the cloud infrastructure is going to protect any sensitive data that will be residing in the cloud. In either case, understanding where data resides, what domains of information exist, and how it's related across the enterprise will help organizations define the right policies for securing and protecting that data and demonstrating compliance to regulations such as SOX/COBIT, PCI DSS, data privacy laws, SCAP, FISMA and HITECH. The number and variety of compliance regulations keeps growing. Organizations are still accountable even as the data moves to the cloud.

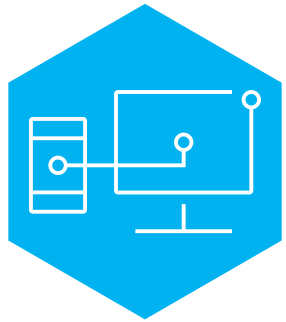
Access controls

Hackers are individuals or groups with 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 cyber criminals. Foreign states have even sponsored hackers to collect intelligence and the sensitive data on people in other government organizations. Hackers might even be disgruntled employees upset about internal policies or other issues. 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 privileged users and end users with "least possible privilege" to prevent abuse of privileges or errors. It is important to note that organizations should protect data from both internal and external attacks in physical, virtual and private cloud environments.

Perimeter defenses are very important, but it's equally important to protect the sensitive data itself. If and when the perimeter is breached, sensitive data needs to be secure with real-time reaction to minimize the impacts of the breach and ensure the hacker does not have free reign. Organizations need layers of defense that include data security solutions so they are able to understand what's happening inside the private cloud, for example, understanding privileged user behaviors.

Privacy

Another challenge around data access is ensuring that only those with a valid business reason have access to privacy information. For example, physicians need to see sensitive personal information such as symptoms and prognosis data, whereas a billing clerk only needs the patient's insurance number and billing address.



Organizational challenges

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.

Productivity

Security and privacy policies should enable and enhance, not interfere with, business operations. Security and privacy policies should be built into everyday operations and work seamlessly in private cloud environments so user productivity is not impacted. For example, many private clouds are put in place to facilitate application testing. Consider masking sensitive data to mitigate the security risk of exposed data.

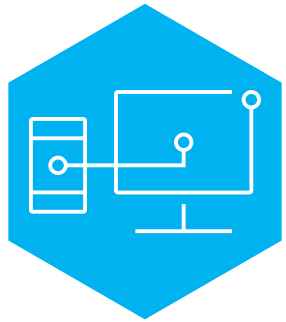
Vulnerability

The number of database vulnerabilities is vast, and hackers 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 database vulnerabilities include: missing patches, misconfigurations and default system settings. This complexity is increasingly difficult to keep track of and manage as database servers become virtualized.

Today, organizations have diverse security technologies in place to protect enterprise data and ensure compliance. As organizations move toward private clouds, for example, these solutions might not scale. For example, some encryption approaches are tied to a particular hardware or network resource. In the private cloud environment, no dependencies on the network or infrastructure are possible.

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

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 home-grown solutions. Ideally, as new databases are added, security processes and procedures should be carried out without manual intervention. In short, security strategies should be built into the fabric of the private cloud.



Data protection approach

Organizations should look to centralize data security controls in private cloud environments, as well as in the rest of the enterprise, and ensure a separation of duties so that the data administrator doesn't also become the security administrator or auditor. Key elements of a private cloud security strategy include:

- Understanding where sensitive data exists and who has access to it. Organizations can't protect sensitive data 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 pre-built reports for auditors and with automated workflow so you can get the right reports to the right people at the right time for signoff

Comprehensive protection strategies for private cloud environments should provide alerts of 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 private cloud environments need to continuously track data across the private cloud and provide insight into who is accessing the data across applications, databases, warehouses and file shares, big data environments and more.

Such an approach ensures a 360-degree lockdown of all sensitive organizational data, no matter where it resides.

Conclusion

To ensure 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 they can demonstrate compliance. Protections should be built into virtual and cloud environments from the start with a phase-one goal of helping organizations demonstrate compliance.

When choosing data security solutions, select those data security solutions that are scalable and unified 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 virtual and 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.

IBM® Security Guardium® solutions can help support your cloud and virtualization strategy with:

- Virtualized database activity monitoring, database vulnerability assessments, data redaction and data encryption
- Automatic discovery and classification of data in the cloud
- Static and dynamic data masking to ensure a least privileged access model to cloud resources
- Audit and compliance reports, customized for different regulations, to demonstrate compliance in the cloud

Conclusion

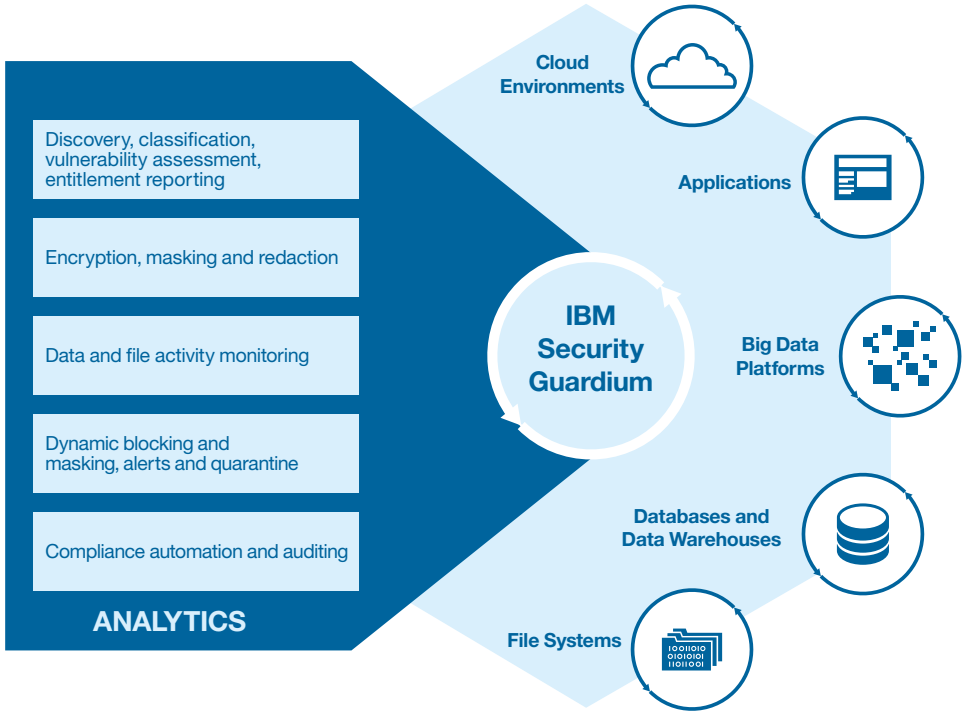


Figure 3: IBM Security Guardium

Guardium software provides a single comprehensive solution for physical, virtual and cloud infrastructures through centralized, automated security controls across heterogeneous environments. Guardium helps streamline compliance and reduce risk.

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.

IBM security solutions for data help organizations rest assure that their data is protected in complex smarter planet virtualized and cloud environments.

Additional resources

Why 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
February 2016

1. Forrester webinar, Enterprise Data Virtualization: The Next-Generation Data Integration Technology, Noel Yuhanna, Principal Analyst.

2. The Forrester Wave™: Enterprise Data Virtualization, Q1, 2015, An Evaluation of Nine Data Virtualization Vendors, Noel Yuhanna with Leslie Owens and Elizabeth Cullen.

3. Gartner, Predicts 2016: Application and Data Security; (3 December 2015).

4. Gartner, Predicts 2016: Application and Data Security; (3 December 2015).

5. Gartner, Internal Private Cloud Is Not for Most Mainstream Enterprises, Published: 22 May 2015; Analyst(s): Thomas J. Bittman.

6. Gartner, Internal Private Cloud Is Not for Most Mainstream Enterprises, Published: 22 May 2015; Analyst(s): Thomas J. Bittman.

7. Gartner, Internal Private Cloud Is Not for Most Mainstream Enterprises, Published: 22 May 2015; Analyst(s): Thomas J. Bittman.

8. Gartner, Internal Private Cloud Is Not for Most Mainstream Enterprises, Published: 22 May 2015; Analyst(s): Thomas J. Bittman.

9. The Forrester Wave™: Enterprise Data Virtualization, Q1 2015 by Noel Yuhanna, March 11, 2015.

NIB03013-USEN-01