SPOTLIGHT

Sponsored by: Imperva

To identify and protect business-critical and sensitive data, enterprises must rethink their approach to data security — including extending protection to all data no matter where it lives.

Effective Multicloud Data Security Requires a Unified Approach

February 2023

Written by: Jennifer Glenn, Research Director, Information and Data Security Products

Introduction

The digital economy is here. Accelerated by a global pandemic, organizations have refocused their efforts to mine and use data to fuel new applications, services, and tools that engage customers and increase business efficiencies. This data often contains critical business data as well as intellectual property and personally identifiable information (PII). As such, data has become incredibly valuable — to both businesses and cyberattackers.

Given this, organizations bear a very heavy responsibility for not only keeping that data available when and where it's needed but also keeping it safe from exfiltration and unauthorized access. Even a small breach can have a devastating impact on the organization's reputation and bottom line.

To identify and protect business-critical and sensitive data, enterprises will need to rethink their approach to data security. Cybersecurity teams need to evaluate their data protection initiatives from multiple perspectives including preventing a breach, proactively planning to limit risk, and adhering to data privacy and industry regulations. That protection must extend to all data no matter where it lives.

AT A GLANCE

KEY TAKEAWAYS

- 87% of organizations identified their business as primarily or somewhat digital first.
- This has resulted in data volumes increasing more than 25% or more over the next three years.
- To support these initiatives, data is stored and used in more infrastructures and applications, complicating security and compliance efforts.
- Data security and compliance requires unified visibility across all environments to comprehensively defend and protect sensitive information.

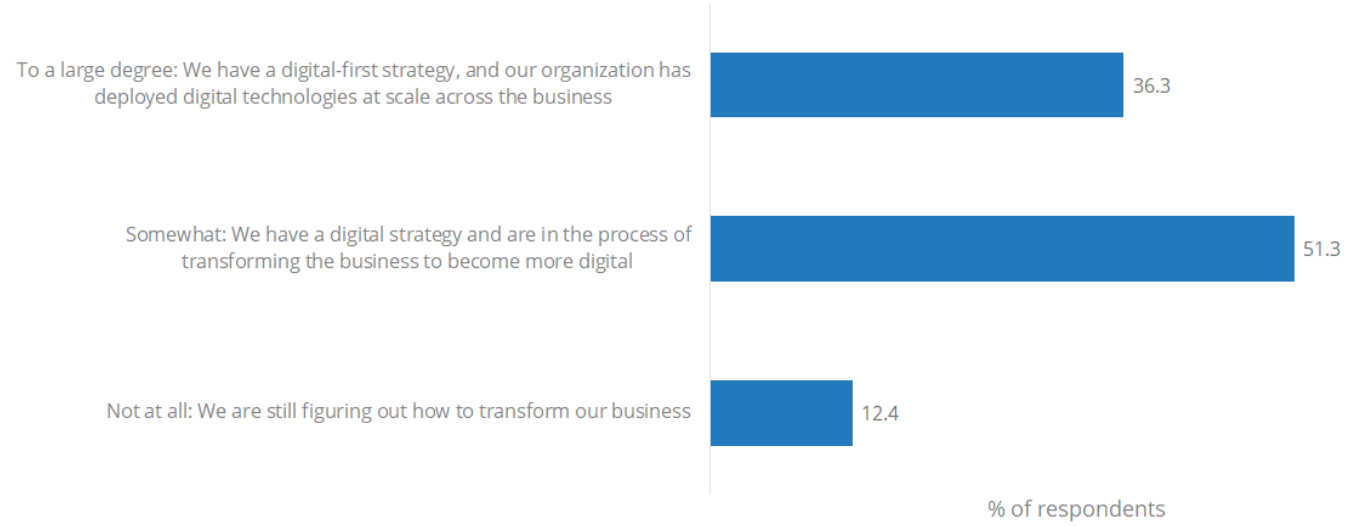
Data Spread and Multicloud Environments Complicate Security and Privacy Efforts

Enterprise data exists in multiple forms: in use, in transit, and at rest, each of which may reside within a cloud and/or an on-premises environment. This offers flexibility and reliability for digital-first strategies.

In IDC's August 2022 *Future Enterprise Resiliency and Spending (FERS) Survey,* 36% of respondents indicated they had moved to a digital-first strategy and deployed digital technologies at scale (see Figure 1). With this move to digital, organizations are storing and using more data in one or more cloud environments — and likely on premises as well. This distribution of data can be incredibly hard to secure consistently. Each cloud environment was likely set up with its own security controls, which may offer a measure of protection for that data. But for organizations with multiple clouds,

SaaS deployments, data repositories, and file shares, multiple silos of security mean less visibility — and likely inconsistency with how security policies are enforced.

FIGURE 1: ***Status of Digital Transformation***



n = 829

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 7, August 2022

Further, with data being used by more and more tools, the volume of data is increasing exponentially. According to IDC's December 2022 *Data Privacy Survey,* 40% of respondents expect to see their data volumes increase by 25% or more in the next three years.

Key Considerations for Building a Multicloud Data Security Strategy

Enterprise organizations are keenly aware of the security challenges presented by increasing amounts of data and mixed environments. As such, they've invested heavily in multiple data security tools to monitor and protect this data, including:

- **Database activity monitoring (DAM):** Traditional DAM offers a centralized way to manage user access and behavior across on-premises databases now in the cloud.
- **Data loss prevention (DLP):** Data loss tools are designed to identify, alert, and block sensitive or confidential data from leaving the organization.
- **Data encryption:** This involves anonymizing data in use by multiple applications or in storage, so that it's unreadable by unauthorized users.

However, to use data to its maximum potential for digital services, data must be available in various constructs, including structured elements such as databases, unstructured locations such as messaging applications and collaboration tools, or even semistructured forms such as file systems or devices. When securing data, often, these tools provide a measure of protection effective in only one of these constructs and are typically not orchestrated to effectively safeguard against vulnerabilities from the combined complexity of various data types, data stores, and topologies.

Further, with the move to more modern infrastructures, many security tools are designed to be cloud native. While this is helpful for securing data in cloud environments, they are not always backward compatible with on-premises legacy systems.

This has resulted in organizations having multiple data security tools that in totality may be addressing the problem — but are likely not offering consistent enforcement of policies and are not reporting in the same way. For teams that must report on integrity or security of sensitive data, this piecemeal visibility and control can make the job incredibly cumbersome, which slows time to respond.

Best Practices for Implementing a Multicloud Data Security Strategy

The best way to secure and protect data across multiple environments and constructs is with unified visibility and consistent enforcement of policies. Most organizations will need a solution for aggregating information from their current tools to understand where their most sensitive data is, including who is accessing it, what is being accessed, and if it is being used properly.

A data security platform (DSP) integrates security information from multiple data monitoring and protection sources. At its core, a DSP pulls this information together into a single view, to provide enterprisewide visibility and control over essential data so that it can be used to its fullest potential, while still being secure.

Benefits

- **Reduced workload for resource-strapped teams:** A growing skills gap continues to be a challenge for cybersecurity teams. According to IDC's July 2022 *FERS Survey, Wave 6,* 39% of the respondents stated that IT security professionals are in highest demand for the most important technology initiatives. If those initiatives involve digital sovereignty requirements, the skills gap also extends to data management (see Figure 2).

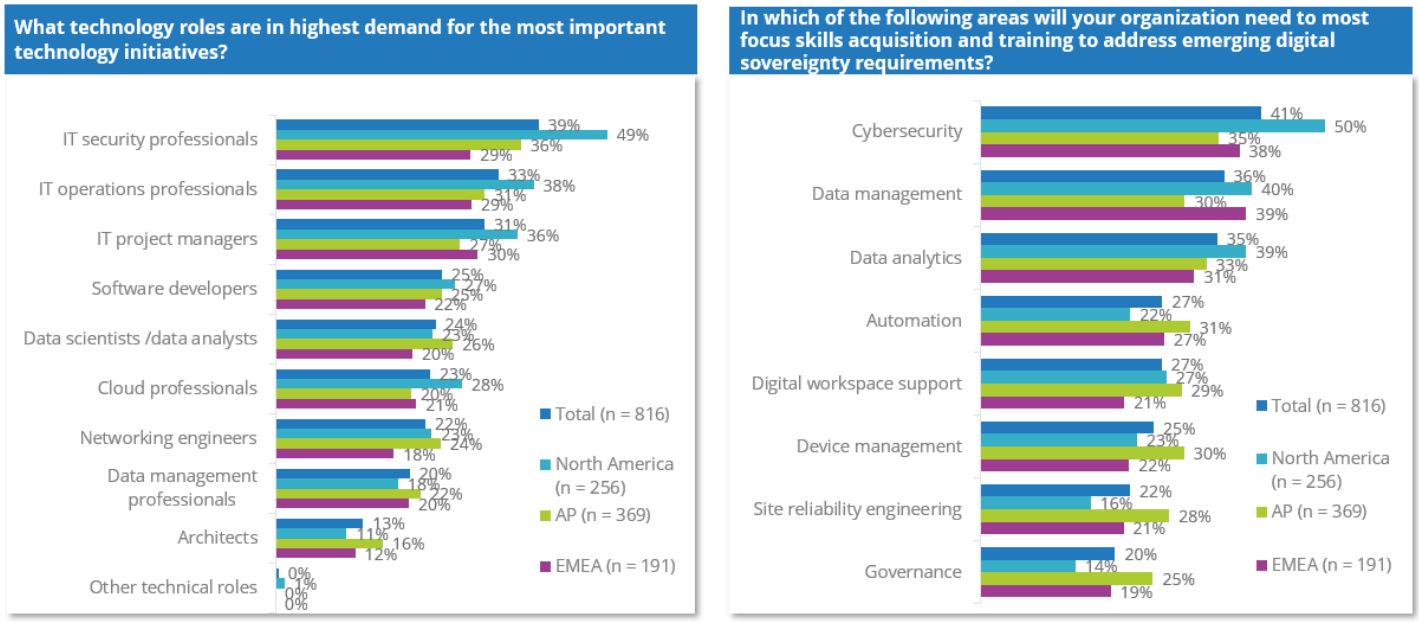
  Combining data security information into a single dashboard extends the capabilities of security teams by streamlining security tasks into a single view and providing self-service for different users including DBAs, IT, security, and SOC admins. Similarly, a unified view of data security information provides a solid foundation for implementing automated controls. Both these initiatives can reduce the stress and workload for security teams that may be struggling to find the right staff or skills.

- **Improved value from existing investments:** Most organizations don't have the desire or resources to replace the security investments they've previously made. However, economic uncertainty is prompting organizations to trim costs even more as well as get more functionality out of every purchase. Leveraging a data security platform for unified visibility and control enables organizations to use the tools and processes they already have in place.

- **Improved efficacy of security policies:** With so many data security tools covering different aspects of protection, it can be difficult to understand security alerts being presented. This is because different tools will report violation risks differently in varied formats and potentially using different parameters to identify problems. By aggregating all this information together in a single platform, it's much easier to analyze security information and consistently apply zero trust principles across access controls, entitlements, sensitive data management, and user rights management.

- **Better management of risks:** Pulling security data together into a unified view provides more insights about users, their behavior, and what data they have access to. Offering a clearer picture of each element that makes data vulnerable to compromise or unauthorized use gives organizations an easier way to ensure sensitive data is continuously prioritized, scored, monitored, and alerted based on automated controls and policies.

FIGURE 2: ***IT Security Professionals in High Demand***



Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 6, July 2022

Considering Imperva

Imperva, based in San Mateo, California, offers an integrated approach for securing digital data, with solutions that target application security, the network, and data itself. In April 2022, Imperva launched its Data Security Fabric (DSF), a multicloud data security platform. The DSF is designed to help customers simplify the process of data security by providing unified visibility across multiple data stores and consistent policy enforcement with core capabilities including Data Activity Monitoring, Data Discovery and Classification, Data Access Control, Data Risk Analytics, Threat Detection, Data Governance, Compliance, Automation, and Data Masking.

With the launch of DSF, Imperva offers a strong set of data security and compliance capabilities that customers ask for to meet today's dynamic and multifaceted threat landscape. Across all environments, DSF works with the existing ecosystem to integrate data protection capabilities, helping future proof customers' other investments.

When compared with internally developed solutions, Imperva DSF is helping organizations like Discovery Inc. save time and resources by making it easier to get the visibility it needs to extend compliance requirements to cloud data. Further, the Imperva DSF is designed to help customers maximize value from their data security initiatives in the following key areas:

- **Simplifying the user experience:** The DSF platform is designed for simple installation and onboarding to make it easier for IT professionals to quickly identify and address security and compliance risks.
- **Protecting all data and data types:** Imperva DSF was created to integrate with other data infrastructure investments and provide protection regardless of where data resides or how it is used.

- **Robust partner integrations:** The Imperva Technology Alliance Program offers a broad range of technology and business integrations, including data store vendors, cloud providers, workflow managers, and GRC, intended to address the needs of most data security initiatives.
- **Speed and scale in the cloud:** Imperva DSF extends performance and scalability across cloud environments including all major cloud service providers (AWS, GCP, Azure, OCI, Alibaba Cloud, and IBM Cloud) to help customers reduce their infrastructure footprint.
- **Maintaining compliance and passing audits:** With Imperva DSF, organizations can keep pace with numerous global regulations that specifically cite an organization's obligations to protect sensitive data with automated workflows to simplify compliance and audit reporting requirements.

Challenges

Data security vendors, like Imperva, will have to contend with an increase in competition from multiple security vendors. While the idea of aggregating data security capabilities onto a single platform is ideal, every organization is set up differently with their own unique applications, business needs, and desired outcomes. The challenge will be addressing these custom needs with the right solution. Certainly, integration with multiple security tools and environments will be useful, but if the management of the integration is perceived to be too complex, the value of a unified solution may not be clear.

The ability to protect data from unauthorized access and secure it from exfiltration will be the strategic differentiator for digital enterprises.

Conclusion

Data is the fuel for the digital economy. It is the information that feeds critical business applications. It can be used to build engaging customer experiences. It's shared through financial and healthcare portals. It's growing in volume, complexity, and location to keep businesses running smoothly. The ability to protect data from unauthorized access and secure it from exfiltration while maintaining compliance will be the strategic differentiator for digital enterprises.

About the Analyst

Jennifer Glenn, *Research Director, Information and Data Security Products*

Jennifer Glenn is Research Director for the IDC Security and Trust Group and is responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

More About Imperva

Imperva is the comprehensive digital security leader on a mission to help organizations protect their data and all paths to it. Only Imperva protects all digital experiences, from business logic to APIs, microservices, and the data layer, and from vulnerable, legacy environments to cloud-first organizations. Customers around the world trust Imperva to protect their critical applications, data, and websites from cyber attack at scale, and with the highest ROI. Imperva Threat Research and our global intelligence community keep Imperva ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into our solutions.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com