SPOTLIGHT

Sponsored by: Data Dynamics

Data powers the business. Secure, self-serve data management balances privacy and compliance with data usability to confidently empower enterprise users to support customer needs, create new services, and improve processes.

Rethinking Data Security: Improving Privacy and Compliance with a Shared Approach

September 2024

Written by: Jennifer Glenn, Research Director, Security and Trust

Introduction

In IDC's June 2024 *Future Enterprise Resiliency and Spending Survey,* 53% of respondents identified as mostly a digital business or a digitally native business. This shift to digital business tremendously impacts the data that organizations use to keep running and engage with their customers.

Data is the most important asset for digital businesses and provides the foundation for customer-facing products and services and the internal systems used for operations. Digitizing data assets enables better collaboration with partners and suppliers, helps employees work more efficiently, and allows personalized customer engagement and support. This digital transformation demonstrates the value and flexibility of data, which laid the groundwork for generative AI (GenAI) to get a foothold.

While improving operational efficiency and customer engagement/satisfaction are critical business initiatives, these advancements can't come at the expense of privacy and trust. Organizations and their cybersecurity teams are responsible for ensuring the security and privacy of the data entrusted to them. This is required by industry and privacy regulations and is important for the company's longevity and brand health.

AT A GLANCE

KEY TAKEAWAYS

- Digital business has increased the volume and diversity of data used across the business.
- Rapid adoption of GenAI and data sovereignty requirements have made it critically important to have strict security controls on data in the business but with optimal usability.
- A new approach to data security privacy — led by self-service data management that ensures data ownership, control, and action down to the data owner layer — can help organizations confidently make the most of their data while ensuring privacy for AI and compliance with data sovereignty requirements.

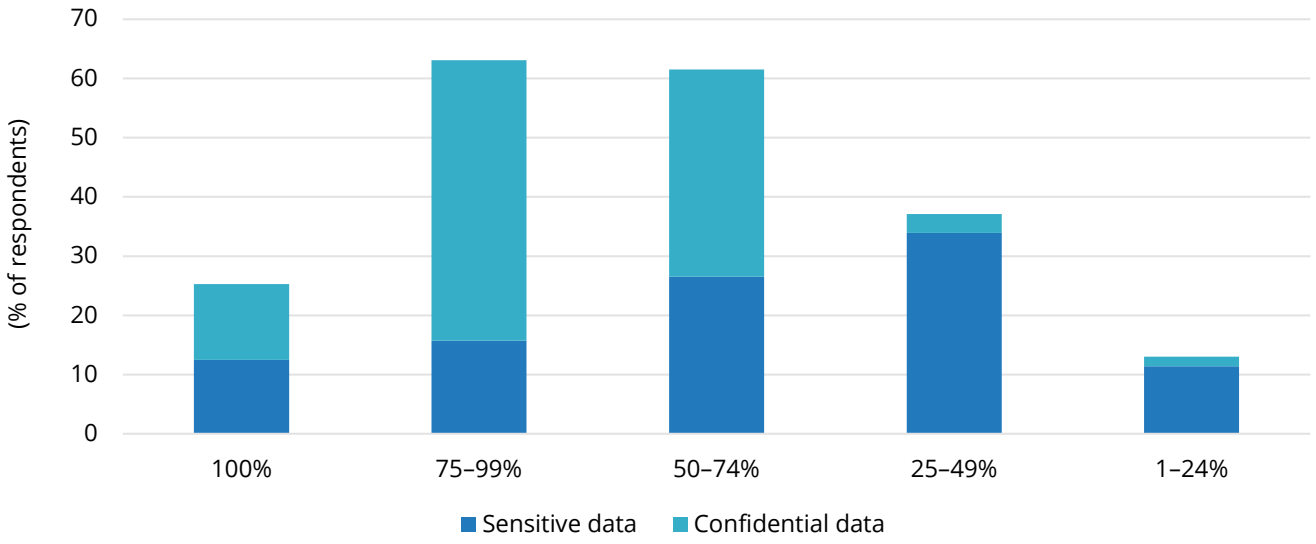
Data Volume and Sprawl Complicate Security and Privacy Initiatives

Data volume is becoming a significant challenge for enterprise IT and security teams, as organizations of all sizes collect and store massive amounts of data to support their customer satisfaction and GenAI initiatives. Many organizations, particularly those in healthcare and finance, have retention requirements for their data. Moreover, it is becoming common for these organizations to keep data for far longer than required. Finally, the volume of collected data is growing, and digital transformation efforts have made that data easily shareable. As a result, users and applications are collaborating and sharing data, leading to the creation of multiple copies of data artifacts in different locations.

In IDC's March 2024 *Data Privacy Survey,* 46% of respondents indicated that less than half of their sensitive data was adequately mapped, organized, and monitored (see Figure 1). When the respondents were asked about the barriers to achieving that level of data visibility, 41% cited data volume while 47% cited technology and system complexity.

FIGURE 1: ***Organizations Face Challenges in Organizing and Monitoring Sensitive Data***

Q *What percentage of sensitive or confidential data has visibility within the organization (is mapped, on a dataflow, organized, and monitored)?*



Source: IDC's Data Privacy Survey, March 2024

Enterprises are also struggling with visibility. Often data is siloed within different departments, applications, and users. Without a holistic view of enterprise data, security organizations are not able to react quickly to risks and/or compliance audits. Further, the multiple tools used to manage data in these silos make it even more challenging to gather and report data in a unified way.

Taken together, this growing volume of data and lack of visibility into confidential assets create multiple issues for the business, including:

- **Liability:** Too much data becomes onerous to secure effectively. First, intellectual property, trade secrets, sensitive data, and personally identifiable information (PII) can get lost in the deluge of assets. Second, it becomes even more challenging for organizations that must adhere to privacy regulations, including data subject access requests or the right to be forgotten, to find all the data for compliance. Finally, it increases the risk of accidental exposure to unauthorized users or machines and makes it a target for external attackers.
- **Expense:** With more data comes the need for more places to store it. The costs associated with storing and processing data in multiple cloud and on-premises environments can get expensive. Moreover, finding sensitive data will extend audit times and costs. The liabilities presented can increase costs if they are not properly managed.

» **Usability:** While many organizations are holding on to older data or duplicate copies to use, too much data makes it difficult to find needed information promptly. For GenAI initiatives, older, irrelevant, or redundant data to train or source AI models can skew outputs and affect quality.

Data security always requires a delicate balance between protecting data and keeping it usable. While too little control over organizational data exposes the organization, too much control creates a management challenge. It can cause delays for employees or customers with a legitimate need to access that information. While this balance has plagued the organizations for some time, the increased data volume and strategies GenAI has created will amplify these challenges.

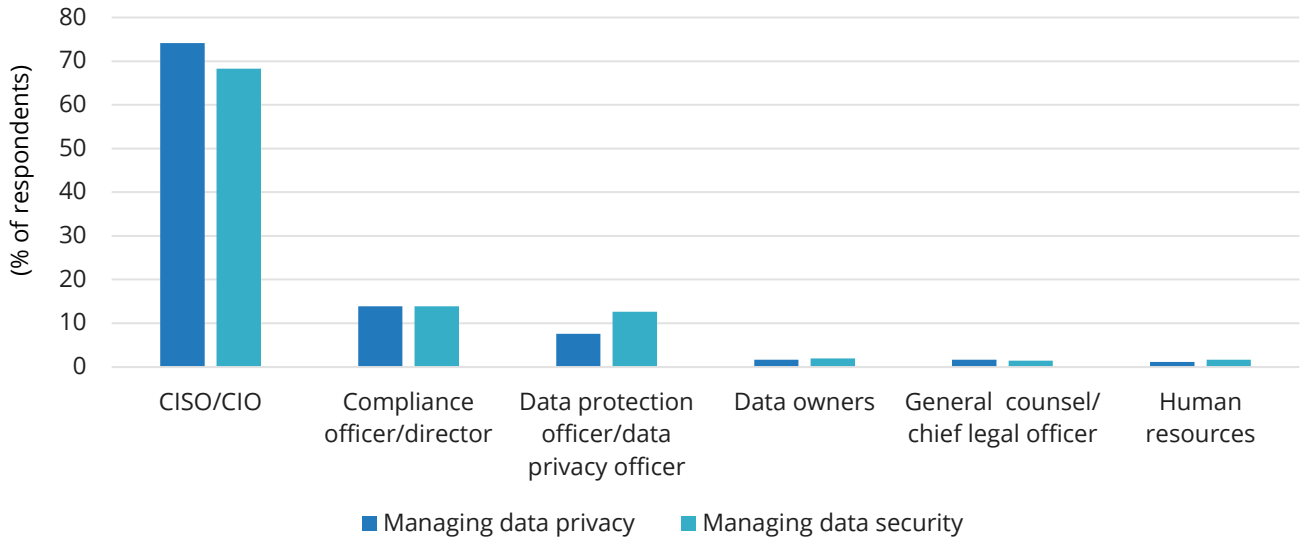
To effectively manage data security and privacy in the age of generative AI, organizations will need to rethink how they implement and enforce these policies.

Data Security and Privacy Should Be a Shared Responsibility

IDC's research shows that CISOs and CIOs are responsible for implementing and managing data privacy and security (see Figure 2). While this is common, the aforementioned challenges outlined indicate that this is not sustainable.

FIGURE 2: ***CISOs/CIOs Are Primarily Responsible for Implementing Data Privacy and Security Initiatives***

Q ***Which group is primarily responsible for implementing data privacy and data security initiatives in your organization?***



Source: IDC's Data Privacy Survey, March 2024

Effective data security starts with understanding the value of the data being used within the organization. Security and privacy teams are familiar with the consequences of not keeping confidential data (such as personal identifiers) safe from exfiltration and unauthorized viewing. However, knowing all the uses of enterprise data — and thus its value — is neither their job nor should it be. It is simply too big a responsibility for a single centralized team.

There are some data security and privacy responsibilities spread across the organization. Most security awareness and compliance training courses feature a section on using data responsibly. This serves to check one of the boxes for GDPR compliance. There is no question that this is an important task, as it raises awareness of the issue and provides a common definition of critical terms and policies to everyone in the organization. However, the responsibility and mechanics of controlling access and use of data still fall to the security team.

Unlike many other approaches to cybersecurity, data can't be easily categorized as "good," "bad," "known," or "unknown," rendering it challenging to make confident decisions about the controls placed on it. Data is merely an asset, and its characteristics are determined by how it is accessed and used. In other words, data is valuable based on its utilization and accessibility.

Data security teams are well-versed in protecting confidential data such as personal identifiers and account numbers, but sensitive data can be harder for these teams to manage for security. Sensitive data such as race, religion, or gender can be valuable or necessary for specific business processes or applications, making it difficult to put controls in place that don't impact business operations.

Conversely, data owners and business leaders are best positioned to determine the value of the data they manage, as they are accessing and using it every day. They should have influence over how the data is classified, categorized, and secured. They also should be responsible for ensuring that the usage of the data is appropriate and adequately protected.

Decentralizing security controls to data owners and the line of business (LOB) is not a simple or quick adjustment. For data owners and security teams, decentralization of security means changing how data is viewed.

- **For data security teams:** Sharing responsibility (and consequences) of information protection is difficult but necessary. Many of these teams are struggling with a lack of skilled resources and time. For these teams, the mindset shift starts by seeing data as a building block or an asset designed to be collaborated on and shared. This includes:
  - Continuing with security and privacy awareness training to keep data owners up to date on compliance standards and responsibilities
  - Creating security and privacy policies that provide the guidelines (and guardrails) for data owners to follow
  - Maintaining a data security risk dashboard to track open vulnerabilities and demonstrate progress in risk reduction
- **For data owners/LOBs:** Although taking responsibility for data security can be daunting, it is important. The rapid adoption of GenAI tools and strategies pushes the need for secure data procurement and use. Moreover, seeing data as a liability and a risk to the business is essential for these teams. This includes:
  - Understanding the data in the organization's control: What is the data? Who or what applications have access to it?
  - Knowing the responsibilities of handling that data, including any industry or privacy regulations, and the security expectations from customers, suppliers, and partners

- Acting on that data within the guardrails of defined security policies (The actions might include data retention or deletion, approving access, data quarantine, archival, transformation, and migration.)

The Benefits of Decentralized Data Security and Privacy

Despite the challenges of decentralizing security and privacy, the approach offers security teams several benefits, particularly as they aim to secure GenAI initiatives and address data sovereignty requirements, including:

- **Reduced management of data security policies:** As highlighted previously, data access and use are conditional. For security teams constantly creating data security policies, managing and updating these policies with necessary exceptions and rules to adapt to the changing nature of business can be overwhelming. By creating the guidelines and distributing the enforcement of these policies to the teams that manage the data, security teams can take a bit of a break from the constant adjustment.
- **Easier compliance with industry regulations:** Privacy and industry compliance is time-consuming. When sharing responsibility for data security with data and LOB owners, data security and compliance teams can maintain oversight to ensure policy is followed but still relinquish auditing activities, such as classification and remediation, to the teams that know their data best.
- **Improved security with fewer objections (operational barriers):** Security is strongest when it becomes part of the organizational muscle memory. When data teams are empowered to access the data they need, with the right security guidelines and guardrails, they are more likely to comply with critical policies instead of objecting to or ignoring them.
- **Demonstrable privacy for AI initiatives:** Enterprise organizations are actively implementing GenAI into their business processes and products. While many are opting for a private instance of GenAI models for better security, there is still a risk that sensitive or confidential data is inadvertently exposed to the wrong users or applications. When data teams within each LOB have control over their data, they are more in tune with the sensitivity of a particular data set and also the level of control required.
- **Provable adherence to data sovereignty requirements:** Global organizations need to know where all of their data originates from and where it is stored to comply with data sovereignty requirements in different locations. Decentralizing data management activities such as classification, as well as remediation actions such as data migration and access control to data owners in these regions, can help alleviate some of the complexity involved in these requirements.

These benefits extend to the business as a whole. When organizations decentralize data security and privacy and empower data owners to use data responsibly, they can confidently create data products that fuel new product innovations and operational processes.

Considering Data Dynamics

Data Dynamics has been helping enterprises manage their data since 2012. Its data management software can help companies democratize data across the business and promote ethical data use.

In 2024, Data Dynamics launched Zubin, its AI-powered, self-service data management software. This new software is designed to help data and application owners take a more active role in addressing the privacy, sovereignty, and security risks associated with the data they manage. The intention of the Zubin software is to offer a self-service framework that puts data ownership in the hands of data creators, enabling them to discover, classify, and act on the data they use every day. By unifying data management for all stakeholders, Zubin aims to make organizational data available to different users such as executives, LOB teams, technology managers, and data and application owners, so the data is secure, relevant, and appropriate for the users or applications.

The software uses AI to offer insights and information about sensitive/PII data. These insights can help organizations tackle GenAI initiatives and other data-driven projects with improved security, governance, and privacy. With Zubin's data insights, organizations are better positioned to demonstrate to customers how they are using and protecting their personal information.

Zubin includes multiple capabilities for helping manage and remediate risk to achieve privacy compliance and generate trust. These are all available through the CISO dashboard and include the following:

- **Data privacy in AI:** Zubin includes AI/ML content analytics and natural language processing capabilities that are designed to discover, classify, and protect sensitive data, including PII and PHI throughout its life cycle. The intention is to give organizations the ability to comply with the global privacy and industry regulations, such as GDPR, CCPA, and DPDP while enabling ethical AI-driven insights.
- **Risk access management:** The product integrates risk classification with role-based access control helping secure sensitive data based on least privileged access. Automated remediation workflows — including data quarantining, re-permissioning, and minimization — are intended to help strengthen organizational security.
- **Data sovereignty:** Zubin is designed to offer geoaware data governance, automated policy creation, and enforcement so organizations can comply with corporate and regional regulations. Capabilities that maintain control over data residency, usage retention, and access are intended to ensure data process and storage occur within the prescribed jurisdictions.
- **Data owner empowerment:** The software has user-centric controls that offer data owners observability and control over their data sets. A self-service interface is intended to empower data owners to enforce governance policies, track data usage, initiate risk remediation, and control access, as well as to migrate, archive, and transform data within predefined corporate policies.
- **Role-based unified visibility:** Zubin aggregates information from disparate sources into a unified dashboard. This centralized platform is intended to enhance decision-making by providing real-time data insights, compliance status, and storage optimization information based on individual roles and responsibilities.
- **Data management in a hybrid cloud:** Zubin is designed to enable seamless data mobility across on-premises and multicloud environments that adhere to corporate policies. Secure encryption, incremental updates, and data deduplication are intended to make data management efficient, compliant, and cost effective.

Challenges

Data management software is widely used by data infrastructure teams, but it is not well known by data security teams. Most organizations have a dedicated security team that has already invested a significant amount of time and money in multiple technologies and processes, such as data discovery, classification, data loss prevention, and data access governance. As a result, it can be hard for a company known for data management, such as Data Dynamics, to get its technology in front of these teams.

Further complicating the market is the intense focus on data and data-centric capabilities by other security organizations. Recent trends show endpoint and network security companies have started focusing on how they can protect data. This crowds the market and gives security teams the technologies and brands they are comfortable with.

However, this is not an insurmountable challenge for Data Dynamics. First, the market is shifting to focus on data as an enabler for the business — with a strong need to address data privacy and sovereignty risks. This opens the door for companies such as Data Dynamics to gain traction. Second, the organization has proven that it understands the value of data to the enterprise. This technology, combined with a clear message about the financial and time-saving benefits, will position Data Dynamics to meet the needs of the data security buyer.

Conclusion

Digital transformation changed how we see and value data. The true value of data manifests in how it is used and who has access to it. For most enterprises, this requires a new way of thinking about data management and security. Moreover, in the current enterprise environment where data collaboration initiatives like GenAI intersect with privacy regulations such as data sovereignty, it is imperative that organizations accurately balance usability and security. Self-service data management tools designed to integrate security capabilities and lead with privacy and protection functions will be a tremendous asset for organizations that want to get more out of their data without trepidation.

The true value of data manifests in how it is used. Data management tools that include privacy and protection functions will be an asset for organizations that want to confidently extract more value from their data.

About the Analyst

Jennifer Glenn, *Research Director, Security and Trust*

Jennifer Glenn is research director for the IDC Security and Trust Group and responsible for the Information and Data Security practice. Ms. Glenn's core coverage includes a broad range of technologies, such as messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

In an AI-driven world, effective data curation and transparency are critical to building digital trust between enterprises and their customers. At Data Dynamics, we understand that in order to achieve this, organizations need to treat data as a dynamic asset, which is why we created Zubin, our AI-powered, self-service data management software. Zubin revolutionizes how businesses address risk management, privacy, sovereignty, optimization, and sustainability through an industry-first "data democracy by design" approach that returns control to where it belongs—data owners. It enables organizations to centralize data governance while decentralizing data control, allowing central IT to set tailored data policies while giving stakeholders at all levels, from the C-suite to data owners, the power to discover, define, transform, and audit data through an intuitive, low-code, self-service interface. With Zubin, every data owner becomes a trusted champion, enabling your organization to fulfill its responsibility as a trusted data custodian, paving the way for a future built on digital trust and data democracy. Learn more at: www.datadynamicsinc.com.

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
blogs.idc.com
www.idc.com