IDC

ANALYST BRIEF

Sponsored by: LightBeam AI

Privacy and security are converging. Disparate tooling and vendor fatigue are crushing stakeholders. If privacy and security are converging, then the tooling should as well.

With Privacy and Security on a Path to Convergence, Tools Should Be Too

April 2024

Written by: Ryan O'Leary, Esq., Research Director, Privacy and Legal Technology

Introduction

Data sprawl and growth are becoming a serious challenge for organizations. Data privacy regulations around the globe require organizations to find and produce data related to specific individuals on request. As data grows and spreads out among hundreds of enterprise applications, the sheer volume of legacy systems, data, and newer cloud-based systems is challenging to manage. Data governance is taking center stage in data privacy and security strategies, while security, privacy, and governance are converging on one another. By and large, traditional data governance vendors focus on structured data, and privacy regulations impact both unstructured and structured data. Organizations need tools that can handle it all.

Currently, enterprises manage data security and privacy with many tools. Modern-day demands on efficiency, budget constraints, and security requirements will put pressure on the volume of tooling currently deployed. They will need to shift from a multitude of tools across security and privacy. Organizations are leveraging data discovery and classification solutions with deep capabilities to better understand compliance and risks to their data estates. Data privacy and other compliance challenges are driving an information governance revolution and shifting more toward continuous data intelligence. Creating an accurate understanding of an enterprise's data estate is an essential foundation for privacy compliance and security.

AT A GLANCE

KEY STATS

According to IDC research:

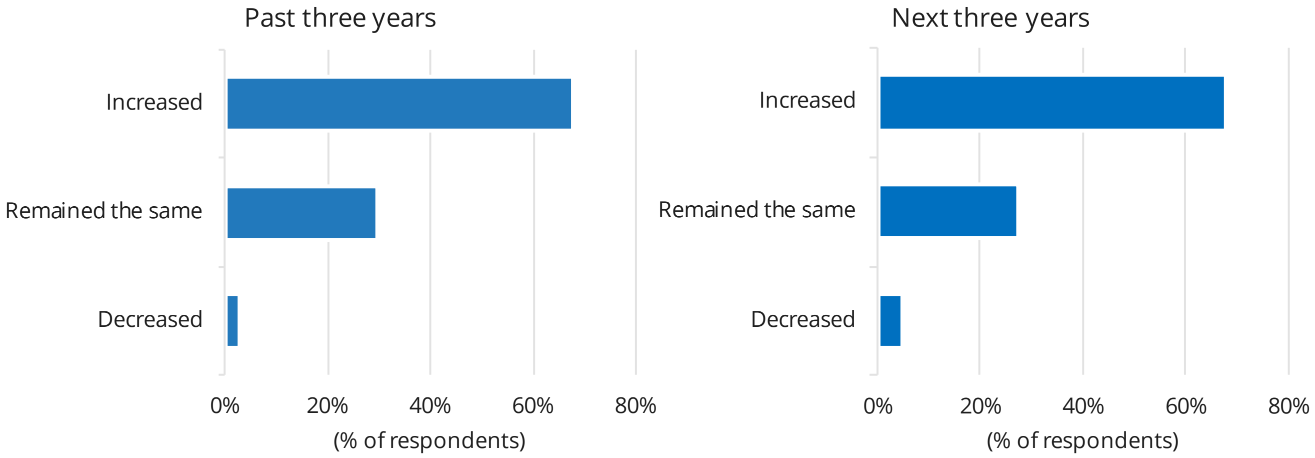
- 68% of organizations believe that their data volumes will increase in the coming years.
- Organizations were successfully breached by attackers 6.15 times within a 24-month period. The average fine under the EU's GDPR is €1.67 million.
- Organizations spend ~$200,000 a month to comply with data subject access requests.

Benefits of an Integrated Platform

Data volumes are exploding. Organizations create new data every second of the day, and most expect that data volumes will continue to increase over the next few years with no sign of slowing down (see Figure 1). The world has entered the zettabyte era, where hundreds of zettabytes of data are created every year.

FIGURE 1: ***Data Volume Growth: Comparison of Past Three Years and Next Three Years***

Q *How has the volume of data at your organization changed in the past three years, and how do you expect it will change in the next three years?*



n = 316

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Multiple responses were allowed.

Use caution while interpreting small sample sizes.

Source: IDC's Data Privacy Survey, December 2022

It's not just the volume of data that compounds the issues but the variety and location of data as well. Work has changed drastically in recent years, and data is sprawling all over the globe depending on the work culture of an organization. Data is no longer contained on premises but in the cloud, at individual endpoints, and on devices. Security and privacy teams need to manage the data no matter where it is. Many organizations have legacy technology essential to their business, which may be a bit of an oddity. Organizations must protect their data across different applications and file types while applying privacy compliance controls.

Data in the digital business era is more portable and usable in different applications and operations. Most enterprises rely heavily on data to create engaging customer experiences and support internal operations. Traditionally, data had been siloed into different departments and tools, making it easier to know where critical IP or personally identifiable information was kept. However, digital transformation has spread data to SaaS applications, collaboration tools, and other enterprise applications, including IT tickets, logs, chat messages, video, and audio. The data is now connected and flowing through the organization, making it difficult for organizations to answer basic questions such as: Where is the organization's data? What type of data is the company responsible for? Who can access that data? Is the data protected? The problem is complex and challenging even without factoring in the sophistication and tenacity of threat actors.

There are also industry-specific regulations that govern security and privacy, like the Health Insurance Portability and Accountability Act , Payment Card Industry Data Security Standard, and Gramm-Leach-Bliley Act.

According to IDC's *CIO Sentiment Survey,* an average organization was successfully breached by attackers 6.15 times within a 24-month period, accounting for a breach every four months. Those attacks came from individuals, organized ransomware gangs, insider threats, and state-sponsored attackers. Threat actors are more sophisticated and have access to better technology more cheaply. Generative AI can be used as an attack vector in many ways. The sophistication and tenacity of threat actors are again compounded by data privacy regulations that regulate breaches and breach responses.

Many jurisdictions have implemented data privacy regulations. The most famous of these are Europe's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act. These regulations give data subjects specific rights, such as the right to have their data deleted or the right to access it. These regulations punish insufficient data security measures and untimely notification of breaches. Since the GDPR came into force in 2018, the average fine issued under it has been €1.67 million, according to IDC research. There are also industry-specific regulations that govern security and privacy, like the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard, and Gramm-Leach-Bliley Act. Organizations in specific industries must comply with general data protection and industry-specific regulations. Noncompliance comes with great risks, as breaches and privacy violations can cause fines to organizations and reputational damage. Often, the reputational damage a company sustains by being in the headlines is much more devastating than a simple fine and can have a long tail. Protecting the organization's data and complying with privacy regulations are paramount but difficult to do. The regulations have some overlap but are not mirrors of one another, which creates tool sprawl. The same can be said for privacy and security.

Organizations deploy a broad category of technologies across security and privacy, including data access governance, data loss prevention (DLP), and privacy and compliance. These technologies approach information protection by evaluating the value of the content and enforcing rules on access and use. Enterprise organizations have evolved in the past 20+ years, and so have the solutions required to secure them. Since business operations don't change overnight, securing the organization has begat a multipronged approach that has resulted in a "Frankenstein" of a toolset. A significant number of security tools are used to solve multiple different attack scenarios and information theft. Many organizations have cited the need to consolidate tools to save on licensing and/or staff to run them.

A significant number of security tools are used to solve multiple different attack scenarios and information theft. Many organizations have cited the need to consolidate tools to save on licensing and/or staff to run them.

First, enterprises have invested heavily in tools that work for their specific environment. These investments include the cost of the technology, the research and trial to get the best fit for their needs, staff training, and custom policy or creation. Even if the existing tools offer a less-than-ideal experience, many organizations are not keen to rip and replace them and start over. Second, the "best fit" for the organization varies from product to product, so while one technology in the platform might be a great fit, another may not be. Enterprises deploy DLP, encryption, data discovery, privacy compliance, and endpoint detection and response tools around the data. However, this leads to significant tool fatigue.

Negotiating, contracting, deploying, and maintaining tools have to be done on an individual basis for every tool. Multiply this over many vendors, and it adds up. When you look at the typical tooling across privacy and compliance, there is a significant overlap in tasks. Both privacy regulations and data security management mandate strong encryption, data loss prevention, and data discovery capabilities. In fact, data discovery and classification are the foundations of data privacy compliance. Data security practitioners need to know where and what data is to protect, produce, or delete in conjunction with data subject access requests (DSARs). Organizations indicated that they are averaging 135 DSARs per month and spending around $200,000 a month to fulfill them (source: IDC's *Data Protection and Privacy Survey,* December 2020). Respondents to the same survey indicated that data discovery was the second-biggest challenge to subject rights request fulfillment, just behind identity verification. Some organizations deploy two separate data discovery tools, one for privacy and one for security.

The synergies between privacy and security are too great to ignore. Organizations can limit their vendor fatigue, save money, and increase the efficiency of their operations by looking for platforms with deeper functionality. With the disparate systems that security and privacy tools need to connect into, having one tool with one connection to each data source is safer than creating a patchwork of connections, as there will be one provider to negotiate with, contract with, maintain, and manage. The overlap between security and privacy allows enterprises to consolidate their tooling, which is necessary as both departments do not drive revenue directly. Dollars are at a premium, and any cost that can be saved is welcome. Cost savings with tooling consolidation, "a single throat to choke" model for vendor accountability, and time saved by having a single pane of glass can be a great starting point for building an internal business case. Compliance and security are necessary, but they are not the main mission of most organizations. Unified tooling will also cause the breaking down of silos. While security and privacy often share responsibilities, they can oftentimes be siloed. Forcing them to share tools can improve an organization's culture of collaboration.

Considerations

Investment in security and privacy expertise will be necessary for the effective deployment of unified tooling. Investment will need to happen in technology as well, which can be difficult as security and privacy often have fixed budgets. The soft costs and savings provided by security and privacy are hard to quantify, and those looking to upgrade to a unified stack will need to find a way to make the case internally.

When upgrading to a unified tool, organizations will need to carefully weed out obsolete technology from their stack and limit the mishmash of vendors that they currently rely on. Effective information protection and privacy operations require privacy-aware data discovery and classification for cloud and on-premises architectures, devices, and applications, so careful consideration of organizational tech stacks is needed.

Conclusion

The escalating challenge of data sprawl and growth necessitates a strategic overhaul in how organizations manage data privacy and security. With data spreading across numerous applications and locations, traditional data governance methods are becoming inadequate, particularly as privacy regulations increasingly focus on unstructured data. Enterprises are currently juggling multiple tools to address security and privacy, but there's a pressing need to shift toward integrated solutions that offer comprehensive data discovery and classification capabilities. This approach promises to enhance compliance and risk management and addresses the burgeoning volume and variety of data generated. The convergence of security, privacy, and governance into unified tooling is essential for efficient and effective data management. This consolidation will mitigate vendor fatigue, reduce costs, and foster a more cohesive organizational culture around data management. In the face of sophisticated threats and stringent regulations, adopting a unified platform for data governance is paramount for organizational resilience and compliance.

About the Analyst

Ryan O'Leary, *Esq., Research Director, Privacy and Legal Technology*

Ryan O'Leary is a research director in IDC's Security and Trust research program covering privacy and legal technology. In this role, Mr. O'Leary leverages his legal experience to provide perspective on changes in laws, shifting regulation, and other market forces that affect technology decision-making today for both law firms and corporations. He also provides thought leadership that technology suppliers and technology buyers may use to develop effective strategy for the future. Mr. O'Leary's core research coverage includes the evolution of ediscovery and legal technology as well as the evolution of privacy compliance technology and impacts of new and emerging data privacy regulation.

MESSAGE FROM THE SPONSOR

LightBeam.ai converges data security, privacy, and governance, helping businesses unify data protection across cloud, SaaS and on-prem locations. Leveraging generative AI, LightBeam ties together sensitive data cataloging, control, and compliance across structured, unstructured, and semi-structured applications. LightBeam enables you to start down the road of your zero-trust data protection journey.

Customers use LightBeam for three organizational initiatives:

- **Accelerate Growth:** Unblock your sales into new markets by accelerating compliance with local privacy and security regulations. Win your customers' confidence by eliminating or limiting the impact of any unfortunate data breaches and exposure events.
- **Contain Costs:** Automate sensitive data discovery, classification, labeling and lifecycle management, helping your team focus on strategic tasks.
- **Contain Risks:** Understand WHAT sensitive data you have, WHERE it is, and WHO it belongs to; ensuring compliance with PCI-DSS, GDPR, CPRA, Quebec Law 25, HIPAA, SOC2, GLBA, FERPA among other regulations.

To learn more, visit LightBeam.ai.

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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.