IDC

SPOTLIGHT

Sponsored by: Egnyte

Enterprises need to put content and context-based guardrails in place and focus on the most sensitive data to make sure it is protected.

Unleashing the Value of Data with Content and Context-Aware Protection

April 2024

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

Introduction

Digital transformation is a reality for most enterprise organizations. In IDC's January 2024 *Future Enterprise Resiliency and Spending Survey,* nearly half of the respondents identified their organizations as either a mostly digital business or digitally native. The portable nature of digitized data has fueled more collaboration involving sensitive and/or confidential information, not only between different departments within the organization but also externally with suppliers and partners. While this collaboration offers several benefits to the organization, sharing this type of data increases the risk of data loss, leakage, or unauthorized exposure.

The amount of data that the organization is responsible for has also increased significantly. It is being stored in more locations and is being used for various business applications and processes.

AT A GLANCE

KEY TAKEAWAYS

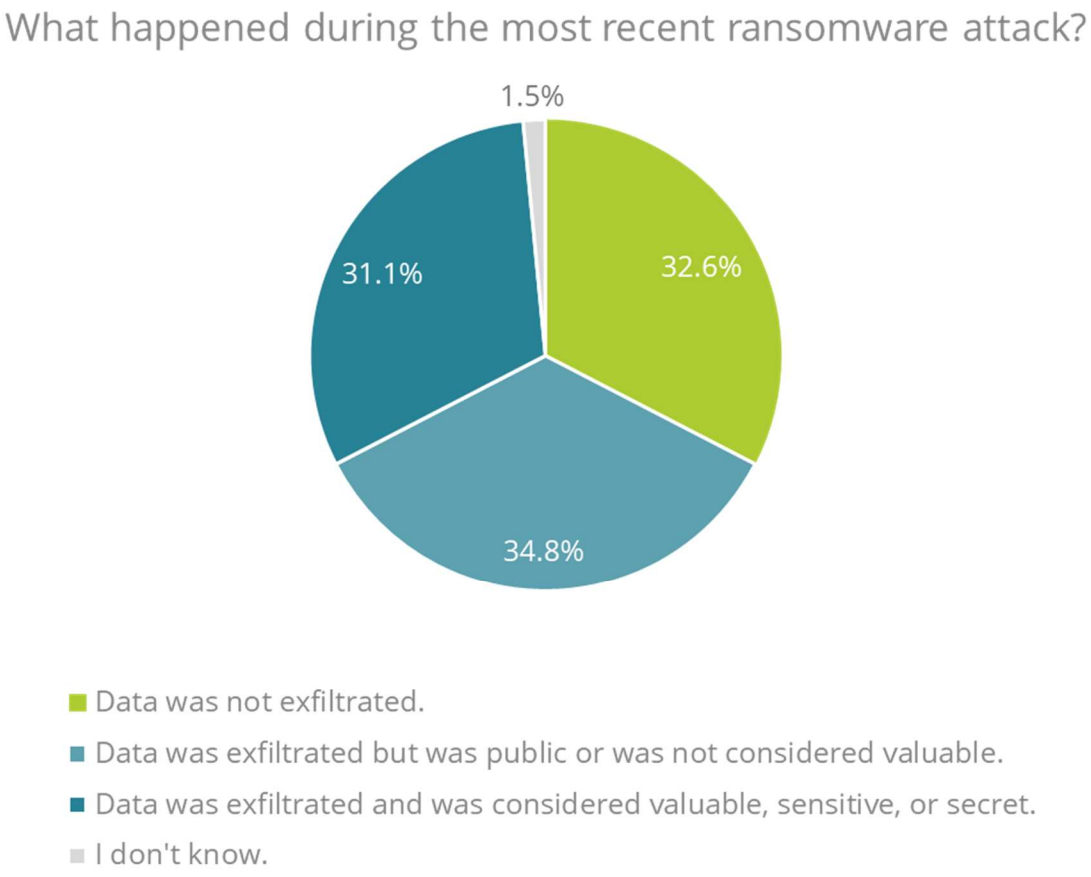
- Data volume is increasing, as data exists in more places and has more uses than it did just five years ago. This makes it difficult to balance availability and security — and attackers are taking advantage.
- Knowing what data exists in the enterprise, where it lives, how it's used, and who is using it offers valuable context to business information. Answering these questions provides the foundation for the granular control of data while maximizing its use.

Ransomware Continuing to Disrupt Enterprises

External threats, such as ransomware, add to the cacophony of data complexity and security noise. In IDC's December 2023 *Future Enterprise Resiliency and Spending Survey,* 63% of the responding organizations indicated they had been impacted by ransomware in the past 12 months, and 70% of those affected were disrupted for a few days or more. The research shows that ransomware primarily affected servers, web applications, and SaaS apps. Most (66%) of the organizations that ransomware affected indicated that data had been exfiltrated during the attack, with just under one-third (31%)of them stating that they considered the stolen data sensitive (see Figure 1). While the majority of exfiltrated data was not considered valuable, the total number of respondents indicating that the attacks exfiltrated data demonstrates that disruption is no longer enough — attackers are after the data.

FIGURE 1: ***Most Ransomware Attacks Are Also Exfiltrating Data***

Q ***For your most recent ransomware incident that blocked access to systems or data, which of the following occurred?***



n = 550

Note: This graph includes the percentage of worldwide respondents who indicated that their organization had experienced ransomware attacks in the past 12 months and had data exfiltrated.

Source: IDC*'s Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2023

Insider Threats and Risks of Data Exfiltration

In addition to the continued threat from external actors, security teams worry about insiders gaining access to sensitive data. This is a double-sided threat. On one side, the conditions of data access increase the risk of misconfigured policies or excess privileges that give trusted users access to information they shouldn't have. On the other side, workforce restructuring and employee dissatisfaction may also increase the risk of malicious insiders actively attempting to access data they have no authorization to view or use. The risks in this category also include stolen credentials and malicious actors posing as trusted users to access sensitive or confidential information without detection.

This category of risk — internal threats — is incredibly challenging to detect and address without upsetting the balance of business productivity and security. Users need to access data to perform their jobs. They need to collaborate on and manipulate data to make informed business decisions and inform products and processes that keep operations running. Preventing data access or use can break applications, introduce delays, and/or stop business processes altogether. This is why traditional data security technologies, such as data loss prevention (DLP) and data access governance (DAG), have become so challenging to manage. There are too many policies and exceptions to these policies to keep track of and too many alerts to keep up with.

Generative AI Exacerbating Existing Data Security Challenges

Generative AI's (GenAI's) rapid adoption exacerbates existing data security risks from internal and external actors, even though it offers clear benefits in terms of productivity, summarization, searchability, and efficiency. IDC's August 2023 *GenAI ARC Survey* shows that 80% of respondents are evaluating use cases for GenAI, testing proofs of concept, or investing significantly in GenAI technologies. For most organizations, GenAI offers a way to unlock the value of data to help address business goals. In the survey, 68% of respondents indicated that they expect GenAI to impact their competitive position or business operating model in the next 18 months. However, security — specifically data security — is a sticking point. In the same survey, 42% of respondents cited that concern over GenAI jeopardizing control over data and intellectual property was a significant factor limiting GenAI evaluation and testing in the organization.

Balancing Business Agility with Security by Protecting Where and How Data Is Used

The challenge that many organizations have with the increase in data volume and number of disparate data repositories is balancing the needs of the business with security. Business thrives when operations, applications, and processes run smoothly. Customer service flourishes when suppliers, partners, and users can collaborate on data assets without disruption. This data fluidity becomes even more important for organizations as they incorporate GenAI into their internal processes and external products.

Rather than put the brakes on data fluidity, enterprise organizations must put content and context-based guardrails in place and focus on the most sensitive content to make sure it is protected. They need to know who has access to that data, what they can do with it, and where the data is in use or who it is being shared with. This context is essential for the proper management of sensitive information to ensure security and meet privacy and compliance requirements.

These content guardrails follow a familiar path, including:

- **Gaining visibility:** The first step in securely managing sensitive data is simply knowing where it lives, which is easier said than done. In a digital enterprise, this could mean unstructured data in messaging and on team collaboration sites. It might also be data in a cloud database for a critical business application. An inventory of all data and its locations can help find shadow IT applications, duplicate data, and/or assets that are past their retention deadlines.
- **Identifying sensitive or confidential information:** Armed with a clear landscape of data, the next important steps are identifying and tagging the assets and information. This may include customer data, personally identifiable information, or intellectual property. With appropriate tagging for data type and classification, organizations can confidently take the next step.

- **Measuring and managing risk:** Once data tagging is complete, organizations can manage data. This can include managing the life cycle based on industry requirements for retention, managing privacy risks, or finding threats to sensitive or confidential information.
- **Taking action:** Knowing where sensitive data lives and how it is being used offers a license to take the best action. It can mean increasing security measures around that data to prevent access to unauthorized users or preventing data sharing and collaboration.
- **Reporting and adjusting:** Reporting on sensitive data risks is a task that most organizations perform out of necessity. However, rather than just providing risk reports, reporting can — and perhaps should — provide an important milestone for how well balanced an organization is with its data security and availability.

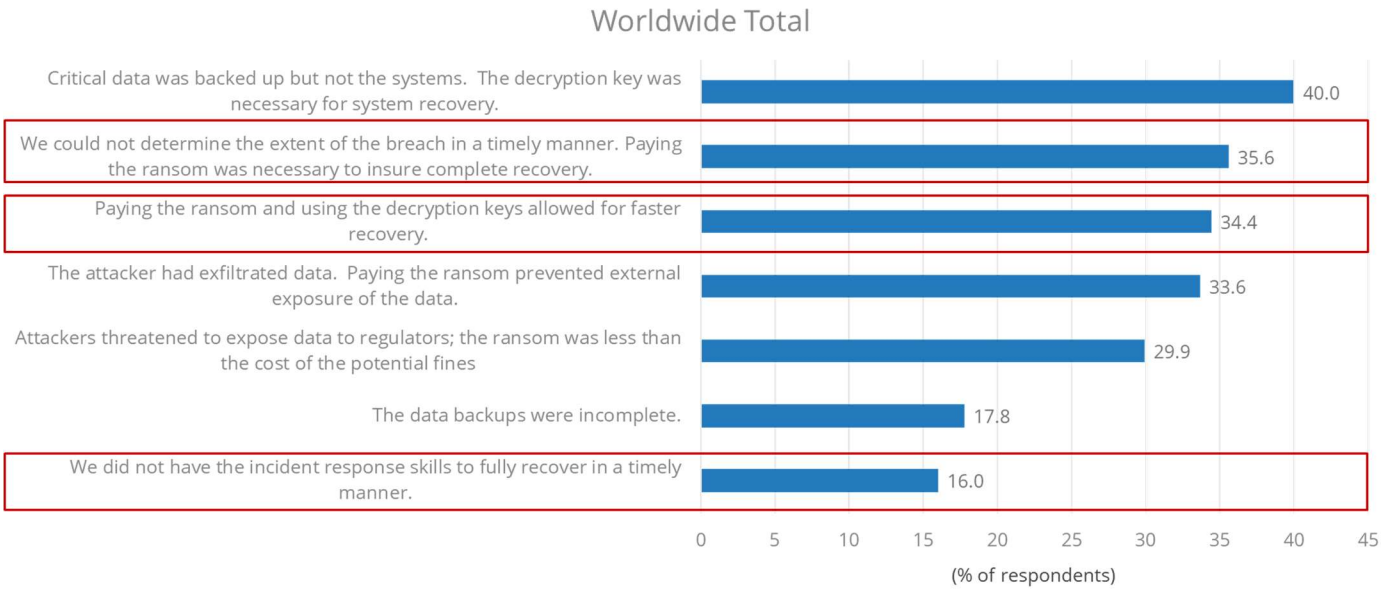
Benefits

Content and context-based guardrails offer many benefits to a business. Getting organizationwide visibility and clear reporting on data risks provides valuable information that multiple teams across the business can use. Privacy teams can leverage this information to demonstrate adherence to regulations such as the CCPA and the GDPR. Compliance departments can use the information to respond to audits and identify potential violations. Other lines of business may also find it useful for understanding their exposure points with third parties, including marketing firms. Other benefits include:

- **Reduced time on internal audits and consumer requests:** It's no secret that responding to audits is time intensive. Ongoing visibility, policy creation and enforcement, and reporting offer the information necessary to make it easier to answer audit questions and demonstrate compliance. Simplifying and shortening the compliance process can also allow more frequent audits of exposure points.
- **Better management of expenses:** The growing volume of data in organizations is also increasing data storage and management costs. Hardware and cloud costs are high, and finding the required staff to manage and secure data is also costly and difficult. Intelligent data platforms that find, tag, and help enforce data may decrease these costs and remove redundant or stale data. Proper tagging can enable the automation of enforcement controls.
- **Faster response and recovery from ransomware attacks:** IDC's December 2023 *Future Enterprise Resiliency and Spending Survey* asked respondents why their organization paid a ransom if it had a functional data backup (see Figure 2). Time was a common factor in many answers: 34% of respondents stated that paying the ransom was the fastest way to recovery, 36% of respondents cited that they couldn't determine the extent of the breach promptly, and another 16% said they didn't have the incident response (IR) skills to fully recover in a timely manner. Having a clear understanding of where important data is stored and how it is being used can help to not only assess the risks that ransomware poses but also be instrumental in quickly recovering the data that is most critical to the business.

FIGURE 2: ***Why Organizations Paid a Ransom Despite Having a Good Backup***

Q You indicated that your organization paid a ransom for your most recent ransomware incident to regain access to systems or data, and your organization had backups that either were not attacked or the attacker was unsuccessful in attacking. If your organization had backups, why did your organization pay the ransom?



n = 82

Notes:

This figure represents the reasons that respondents worldwide provided for paying the ransom. The responses outlined in red indicate that time was a factor in the decision.

Multiple responses were allowed.

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2023

Considering Egnyte

Egnyte, which is headquartered in Mountain View, California, has its roots in content collaboration and sharing. With an understanding of data needs, the company has added new capabilities in recent years to help ensure the protection of sensitive information. Its platform focuses on data enablement and is designed to help organizations address three key use cases:

- **Data security:** The Egnyte Content Intelligence Platform is designed to protect data from misuse by both malicious actors and careless behavior by well-intentioned users. The Snapshot Recovery capability takes frequent snapshots and keeps them for up to 30 days, helping to get important data back during a ransomware event or in the case of accidental deletion. The platform also includes real-time detection of unauthorized access as well as suspicious activity, including unusual user behavior or indirect artifacts (e.g., increased file entropy or file extensions). It aims to

reduce the risk to sensitive data by controlling permissions and limiting the number of people with editing access to shared files.

- **Data governance:** The goal of data governance is to unlock the value of data across the business, albeit with strict controls. Egnyte's platform offers critical capabilities for understanding not only where sensitive content lives but also how it is used and who is accessing it. This information is designed to inform, track, and measure data governance policies, which is important for managing remote and hybrid work environments and enabling secure collaboration with external vendors.
- **Privacy and compliance:** The Egnyte Content Intelligence Platform aims to make the management of organizationwide data easier and faster. It helps reduce exposure, which is an important proactive component of privacy and compliance regulations. The platform also includes capabilities such as prebuilt templates for making the process of demonstrating privacy and compliance regulation adherence less time- and resource-intensive and thus faster.

Challenges

Visibility and risk identification are so critical for data security, privacy, and compliance that many organizations have invested in multiple solutions that offer different pieces of these capabilities. Multiple enterprise security departments have deployed information-protection solutions, such as data loss prevention and data access governance and privacy. These technologies often include visibility, mapping, and/or classification offerings as a foundation for their enforcement tools. Although this space is relatively immune to spending decreases, economic uncertainty is fueling the need to consolidate resources. Enterprises will use the included offerings with their existing investments, even if the functionality isn't ideal. This could make it difficult for content management vendors, such as Egnyte, to gain traction.

Conclusion

In IDC's August 2023 *Future Enterprise Resiliency and Spending Survey,* 20% of respondents cited security risk and compliance as the area most immune to budget reductions, regardless of the economic environment. Even so, effectively balancing the security and availability of sensitive and/or confidential data assets requires input and coordination with data owners, compliance officers, and privacy teams. Furthermore, organizations must integrate data security and privacy into their daily activities and processes with employees, contractors, partners, and suppliers. Everyone has a responsibility to make sure data isn't used inappropriately, exposed to unauthorized users or devices, or, worse, leaked or stolen by malicious (internal/external) actors or clueless users. Visibility and granular control of data are essential for empowering the entire organization to store, use, and share data in a secure manner that supports privacy and compliance requirements.

Visibility and granular control of data are essential for empowering the organization to store, use, and share data securely.

About the Analyst

Jennifer Glenn, *Research Director, Security and Trust Group*

Jennifer Glenn is research director for IDC's 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, such as messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

Egnyte combines the power of cloud content management, data security, and AI into one intelligent content platform. With the threat landscape ever evolving and the data companies store growing rapidly, companies need solutions that reduce risk and improve business processes by controlling access to critical files quickly, easily and securely. More than 22,000 customers trust Egnyte to improve employee productivity, automate business processes, and safeguard critical data, in addition to offering specialized content intelligence and automation solutions across industries, including architecture, engineering, and construction (AEC), life sciences, and financial services.

Explore Egnyte's Content Intelligence Engine, which helps organizations unlock insights buried within their content. www.egnyte.com/product-tour

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