IDC

SPOTLIGHT

Sponsored by: Thales

Data is the foundation of business and, regardless of where it is, must be secure. A unified end-to-end approach offers the capabilities that help businesses confidently collaborate for efficiency, cost savings, and maintaining customer trust.

Improving Business Outcomes with Unified Full-Spectrum Data Security

September 2025

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

Introduction

Data is one of the most valuable assets for an organization. It serves as the foundation for business growth, enables competitive advantage, and drives informed decision-making. Among other things, it provides resilience against disruptive events, trains and sources AI models, and informs customer preferences. One could argue that data is *the* most valuable asset in the overall functioning and success of an organization. However, it is also an organization's biggest risk.

Organizational data and its use cases are also of tremendous value to malicious actors. Examples might include nation-state attacks intent on disrupting critical infrastructure or individuals determined to steal personal information for profit on the dark web. Organizations must be vigilant in identifying and proactively addressing attacks that threaten the integrity and availability of critical data.

AT A GLANCE

KEY TAKEAWAYS

- Compliance regulations, privacy requirements, and protection of intellectual property continue to drive the purchase of data security solutions.
- The use of multiple different point products to address all of these issues has resulted in complex and expensive security infrastructures.
- Unifying security technologies into a single platform offers practitioners better visibility and simplified remediation, resulting in reduced cost and better business outcomes.

Further, risks to data can arise from non-malicious actions. Users may unintentionally make errors that put data at risk, compromising the safety of sensitive information. For instance, misdirected emails can inadvertently send confidential data to the wrong recipient, or misconfigured access controls can expose critical systems to unauthorized users. These oversights jeopardize the integrity of the data and put the organization at risk of sensitive data exposure, privacy breaches, or compliance violations, potentially resulting in significant legal and reputational consequences.

Organizational Data Risk Comes in Many Forms

As the speed of data creation and distribution surges, organizations must leverage this resource to drive innovation, enhance customer experiences, and increase profitability. Prioritizing data management and security is nonnegotiable.

However, data exists in many forms: at rest, in motion, or in use. It can function in structured environments such as databases, data warehouses, data lakes, and storage devices, as well as unstructured environments such as file systems, SaaS applications, and messaging and email systems. In addition, data volume is increasing rapidly, much of it driven by AI initiatives that may replicate data for training or sourcing models. Finally, as business operations have evolved and moved to cloud infrastructure and applications, data now exists throughout the organization. These complexities make it challenging to effectively secure sensitive and confidential data.

The most significant risks include:

- **Exfiltration or loss of sensitive data:** Privacy or compliance violations around data exfiltration can be a significant risk to the organization, regardless of whether the threat is malicious or inadvertent. The fines for some of these violations can be significant. In addition, addressing violations and/or conducting audits takes time and pulls valuable resources away from regular tasks.
- **Exposure of sensitive data:** Loss is not the only concern in data security. Those same privacy and compliance regulations apply to data exposure. If data is not adequately encrypted, it may be open to exposure as it moves between applications and sources. It may also be possible to hijack keys and other credentials, potentially exposing sensitive data.
- **Availability of data for use or for applications:** In addition to data loss, many organizations are concerned about the availability of data for applications and other tools. Certificate expirations continue to disrupt businesses by making data unavailable for use or collaboration. When data is unavailable, businesses do not generate revenue and may also suffer damage to their brand reputation.
- **Misconfigurations/excessive privileges:** Insider risks are a significant threat to organizational data. Economic and workforce changes are creating an environment where some users can steal data as they move between jobs. However, most insider risks are not malicious but accidental, such as employees giving unauthorized application access to sensitive data stores.

Organizations are rushing to implement AI initiatives for efficiency improvements and staff augmentation. At the same time, AI itself is continuously changing. The combination of these two factors significantly increases security risks. In the race to harness AI's advantages, data security vulnerabilities may be overlooked. When data is inadequately or improperly secured, AI can potentially access and exploit these vulnerabilities. The result can lead to output that inadvertently reveals sensitive or confidential data. These incidents can negatively impact data quality and erode trust in the organization. According to IDC's March 2025 *Data Security and Privacy Survey,* data loss and data quality emerged as the primary concerns regarding AI deployments. When asked to rank their most pressing data security concerns, 24% of respondents highlighted the risk of losing sensitive or confidential data. Another 16% were concerned with the loss of data or ingesting sensitive data into an LLM. Finally, 20% of these respondents stated that data quality was their primary concern for AI initiatives.

Protecting Organizational Data Is Challenging

Maintaining effective data hygiene is complex, since data is continuously generated, transferred, and/or used across an organization's ecosystem by users, applications, remote/contract workers, and suppliers.

Strong data security requires addressing the contributing factors for risk, including:

- **Multiple uses:** Organizational data is multifunctional and underpins critical applications. Monitoring access privileges and user behaviors along with backing up application data helps in the recovery and availability of important workflows. Any restrictions on organizational data can significantly limit its use, disrupt operations, and/or interfere with the user experience.
- **Multiple forms:** The flexibility of data for all these uses means that organizational data exists in various forms: stored (e.g., backup or archives), in motion (e.g., email or migration to cloud workloads), and in use (e.g., to power applications). Each of these data forms requires specific security that balances productivity and protection.
- **Multiple locations:** Data exists in various locations, including (but not limited to) databases, files applications, cloud backups, endpoints, devices, and networks. Data sprawl is driven by the proliferation of cloud services and applications. When data is created, stored, and used in different locations, systems, and applications, it becomes harder to control, making it challenging to manage and secure. Mergers and acquisitions are also culprits, as are changes in the workforce ecosystem with remote or contract work. Without visibility into organizationwide data, businesses leave themselves open to exfiltration, data exposure, or disruptive attacks.
- **High volume:** Data volume is increasing and it's doing so at an exponential rate. A significant contributor to this volume comes from AI initiatives that also increase the risk of data duplication between files or applications. In addition, industries such as financial services or healthcare must retain data for a specific period to fulfill regulatory compliance requirements. High volumes of data increase the attack surface, putting organizations at risk as they manage vast amounts of information.

Data Breaches and Data Exfiltration Are Business Risks

Data security incidents are more than just a security issue. It is important for organizations to recognize the impact these security incidents have on the business. Top business risk concerns include:

- **Industry compliance and/or privacy violations:** Privacy and compliance are the primary drivers of data security implementations. In IDC's March 2025 *Data Security and Privacy Survey,* 20% of respondents cited local and regional privacy laws (e.g., GDPR and CCPA) as their top driver of data security initiatives. Another 17% cited industry compliance regulations (e.g., HIPAA, GLBA, NIS2, and DORA) as a primary driver. Industries that store and process a lot of regulated data are most at risk of violating these standards.
- **Loss of confidence in the brand:** Consumers are bombarded with media coverage of data breaches and notification letters. While there is some desensitization, repeated data breach notices from the same organization will eventually erode trust in the brand. In the same IDC survey question, 18% of respondents said that the primary driver of data security initiatives was addressing customer satisfaction and needs.
- **Financial impacts:** Breaches and security incidents can harm an organization's financial outlook. Resource costs for investigating and remediating these events, as well as any fines or fees paid for privacy or compliance violations, directly impact spending. Indirectly, the loss of business or secret information (e.g., trade secrets) can also negatively affect the overall bottom line.

Addressing Data Security Risks with a Unified Full-Spectrum Approach

A layered cybersecurity approach has been a best practice for more than a decade. While this approach uses tools that address security on several fronts — such as network, endpoint, and browsers — these tools are all designed for one thing: protecting the paths to data. However, protecting the data itself requires technologies that provide more granular security. This includes identity and access management, data activity monitoring, data access governance, data loss prevention (DLP), data security posture management (DSPM), and encryption solutions.

While protecting data is the common goal of these solutions, some of these technologies may have been purchased by separate teams. It is likely these tools were procured from different vendors and require purpose-built integrations to work effectively. This is true even for products designed specifically to protect data and may result in different, or even conflicting, policy creation, management, and enforcement. Each product requires specific product knowledge, experience, and skills. Consequently, teams need to allocate time and resources to build these integrations and then manage and adjust them following the release of new software versions.

Products that address a single element of data security, such as DLP, will remain relevant. However, individual solutions are often inadequate to meet the dynamic data needs for most organizations. There is a clear trend toward consolidating tools to proactively secure a wider range of use cases as they develop. This provides security teams with a broader visibility of incidents, a clear picture of malicious intent, and the information to respond appropriately.

Data security platforms that integrate different capabilities and share telemetry between them are ideal for helping organizations gain comprehensive visibility and important context about incidents that put the business at risk. Contextual understanding of all data access and usage (e.g., apps that rely on that data or who is using it) can improve remediations that keep data safe without sacrificing its availability for use. Context can also help organizations understand and manage their data risk while lowering their overall operating costs.

The Benefits of Full-Spectrum Data and Information Security

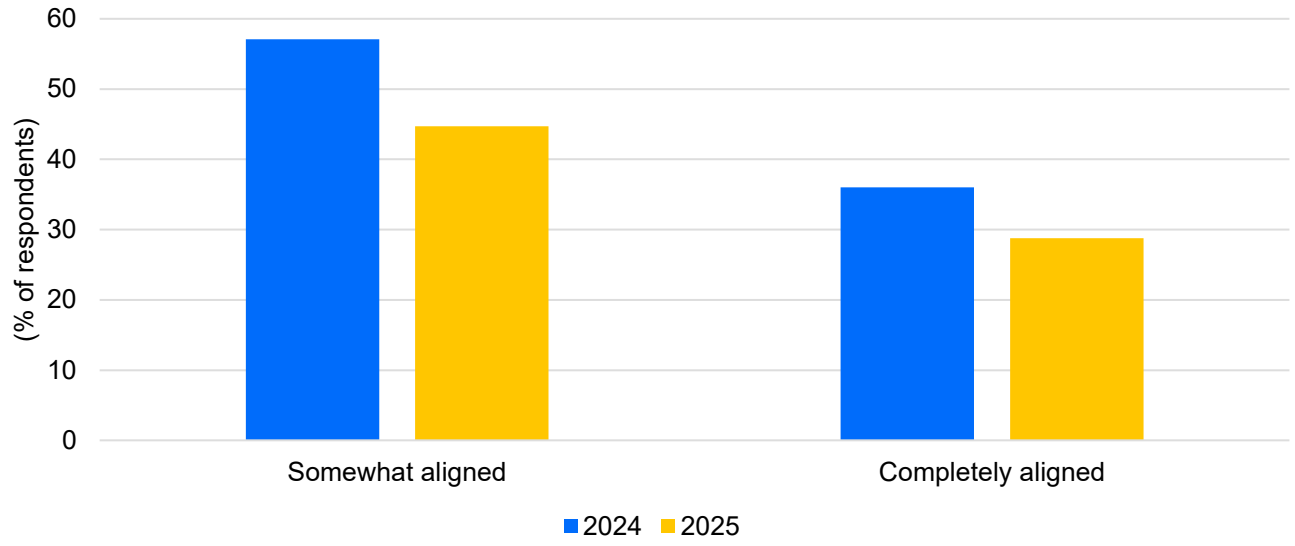
Unified security across multiple technologies offers a simpler approach to deployment and management. It also provides a number of benefits for security teams and the business as a whole. For example, for smaller teams, unified security can reduce the complexity of deploying and maintaining multiple solutions. A unified data security solution can also limit friction that may occur between multiple solutions, helping maintain an ideal risk posture.

Security teams must balance security with business objectives, which is not easy. AI is a great example of this. Implementing AI applications and assistants is a current top priority for most businesses. It promises faster critical data analysis, improved employee efficiency by eliminating minor tasks, and increased overall productivity. Security cannot hinder this progress. Responses to a question in IDC's March 2024 and March 2025 *Data Security and Privacy Survey* demonstrate how the alignment between security initiatives and business objectives is waning (see Figure 1).

FIGURE 1: ***AI Alignment Between Business and Security Teams Is Shrinking***

Efficiency and potential revenue generation are surpassing security objectives.

Q *How aligned are the company's business objectives and goals for GenAI with those of the security team?*



Notes:

IDC put this survey question to all global participants in both surveys.

The graphic shows the percentage of total respondents answering the question.

Source: IDC's Data Security and Privacy Survey, March 2024 and March 2025

While the misalignment between security teams and AI objectives is currently top of mind, it also tends to be true for other objectives, such as post-quantum cryptography preparedness. Unifying visibility and management can help security teams close the alignment gap and document priorities. Other benefits to security teams include:

- **Confident AI use:** Although AI initiatives appear to be taking priority over security, these teams can still make progress toward closing this alignment gap. Implementing a unified full-spectrum approach to data security provides security teams with visibility and better control over organizational data. Since AI relies on data for use, control can provide peace of mind about data being accessed — and protected — within AI applications.
- **Secure collaboration:** Collaboration tools are a critical part of every business. This includes file sharing, email, in-app messaging, and everything in between. Securing these tools is challenging, but data must move. Security solutions, such as masking, encryption, key management, and file activity monitoring, can protect data while ensuring it remains usable.
- **Consistent policy enforcement:** A single platform can enforce policies by applying uniform protection of sensitive data that includes monitoring violations across all data sources. Unified policy management makes it easier to improve overall security posture, accelerate time to compliance, and ensure audit readiness.

- **Faster time to compliance:** Compliance is not always challenging, but it is time-consuming. Unified dashboards can provide visibility across the data ecosystem, identify the whereabouts of sensitive data, and confirm security controls are active, offering faster proof of compliance.
- **Risk acceptance:** Armed with visibility and information about the use of and access privileges to data, practitioners can prioritize which remediations are urgent or important. This level of insight helps organizations define the acceptable level of risk associated with data source vulnerabilities, encryption status, and security incidents. Documenting risk levels ensures accountability and establishes a legal and compliance foundation.
- **Post-quantum readiness:** A full end-to-end data security solution also identifies data source vulnerabilities in the use of cryptography following NIST standards that underpin the corporate infrastructure. Seeing these vulnerabilities in context helps prioritize which business areas or applications should transition first and which can wait.

Security teams are beholden to the business. Given the importance of cybersecurity, most organizations are not likely to reduce overall spending on these tools. However, securing investment in a specific area is no longer just assumed. These teams have to continually demonstrate the value of their data security solutions to justify these purchases. Finding an approach that simplifies deployment across several fronts and offers seamless integration and broader visibility is essential. A unified data security platform has several benefits that help the business meet its objectives:

- **Faster time to value:** Bringing together context from different areas of security helps identify risks earlier by speeding the discovery, classification, and use of sensitive data. The ability to tie this to users, entities, and AI, as well as known compliance and privacy regulations, significantly accelerates the entire process. Deep context around sensitive data makes it easier to prioritize business risks and remediations.
- **Cost savings:** Reducing costs while still providing value is a top priority for organizations. Identifying, investigating, and remediating security incidents, including breaches, is time-consuming. Further, most security teams use different solutions to address the various threats and risks to the business. Bringing these solutions together on a single unified platform saves both costs and time. Adopting a platform approach helps reduce the licensing footprint and complexity, freeing up staff resources for other strategic priorities and improving operational agility. Also, a data security platform offers consistency for security teams with real-time visibility into system health, support issues, and dashboards.
- **Improved performance:** The rush to utilize AI in business operations and commercial products demonstrates the importance of efficiency and its impact on business performance. Security tools are not often considered to be helpful in this endeavor. In fact, it's quite the opposite; businesses see security as a speed bump for operations. However, by unifying data security tools into a single platform, security teams gain broader visibility across the organization. This makes it easier to proactively identify vulnerabilities and risks that can impact the organization's uptime and performance.

Considering the Thales Data Security Platform

Thales specializes in solutions that help make the world safer and sells technologies across three key areas: defense and security, aeronautics and space, and digital identity and security. The company's data security solutions aim to ensure that sensitive data is protected as it moves between databases, applications, and various systems.

In 2023, Thales expanded its data security portfolio by acquiring Imperva to further enhance its existing data protection offerings with Imperva's Data Security Fabric (DSF) platform. The Thales CipherTrust Data Security Platform (CDSP) consists of key management along with data protection capabilities such as encryption, tokenization, and secrets managements. The addition of Imperva's DSF delivers visibility and control functionalities, including data activity monitoring, vulnerability sensing, security analytics, and risk management. The company's latest CDSP integrates technologies from both organizations. The platform is designed to provide broad visibility into the various risks to organizational data and enable a faster, more informed approach to compliance, threat prevention, and remediation. Thales offers capabilities across the full data ecosystem, from discovering and classifying data across the business to enabling the integrity of organizational data with a modern approach to cryptography. These advanced capabilities leverage AI and machine learning technologies to support both current and emerging use cases for protecting data regardless of its location.

The Thales Data Security Platform seeks to address the complexity of securing and managing all types of data. Using a unified view of organizational data, such as personally identifiable information, intellectual property, and/or secrets, the platform is intended to prevent unauthorized data access and exfiltration. The platform features integrations with existing security vendors to offer a one-stop approach for protection. The product is designed with multidimensional vulnerability scanning, detection, and analytics systems offering comprehensive incident and business risk reports written in clear, nontechnical language. This approach facilitates effective communication and collaboration with departments beyond the security team, so essential information is shared with all relevant stakeholders.

The Thales CipherTrust Data Security Platform features include:

- The ability to address multiple use cases for data security, privacy, governance, and compliance in structured and unstructured data across on-premises and multicloud environments while simultaneously extending data security to cloud-native database-as-a-service (DBaaS) and file sharing technologies found in Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud, IBM Cloud, and popular NoSQL vendors such as Snowflake, DataStax, and Cloudera
- Protection of all data, both at rest and in transit, with modern key management, encryption, tokenization, ransomware, and secrets management
- End-to-end AI security with foundational capabilities, including data discovery, classification, data activity monitoring, and masking, as well as automated workflows and reporting with prompt/response safeguards
- Holistic risk prioritization and AI-based remediation capabilities to support the collection of massive amounts of machine- and user-created content, which is increasingly expanding the organization's attack surface
- Strong access controls with encryption for sensitive data and metadata that make it unreadable even if exposed while replacing high-risk data with tokens to prevent misuse
- Quantum-resistant encryption to counter quantum computing threats
- Flexible deployment and licensing options available to accommodate organizations of all sizes in all industries and support all data types in hybrid cloud and multicloud environments

The platform is designed to continuously discover, track, and analyze activity involving critical organizational data. In addition, the platform offers a range of detection and response capabilities. These include monitoring and blocking unauthorized activity by trusted insiders, as well as termination of local user activity and quarantining user accounts when a security policy is violated. Thales also offers data-at-rest solutions that deliver granular encryption, tokenization, masking, and role-based access control for structured and unstructured data residing in databases, applications, files, and storage containers. The goal is continuous awareness of where data lives, who is accessing it, how it is being used, and how it is encrypted, along with targeted remediation that doesn't disrupt business operations.

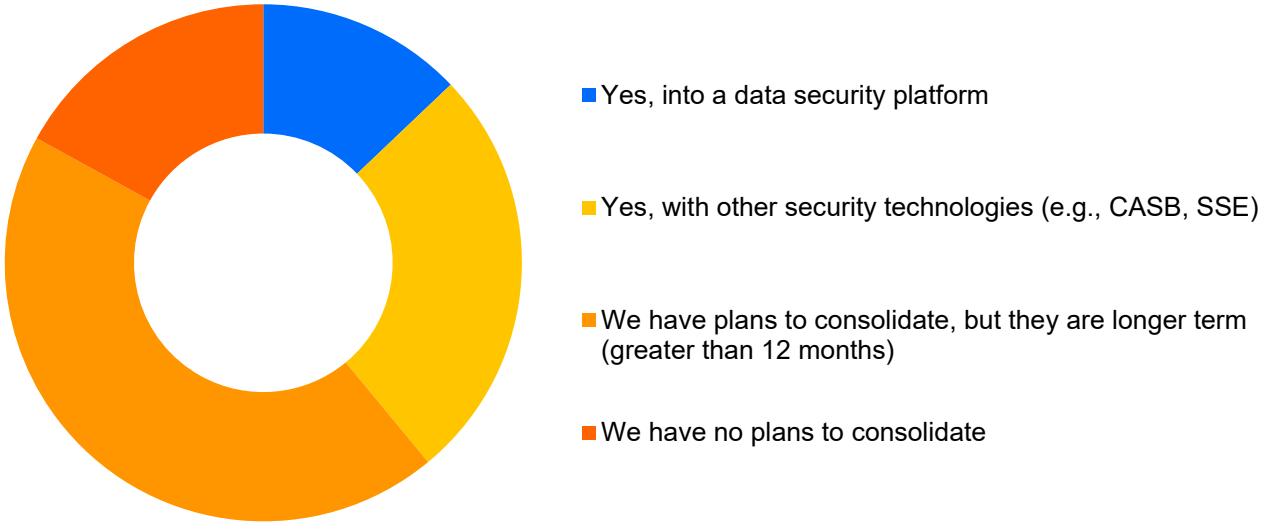
Challenges

As threats to organizational data have evolved, organizations have implemented multiple technologies and solutions to address these risks and protect sensitive data. According to IDC's March 2025 *Data Security and Privacy Survey,* organizations are actively relying on data loss prevention, data discovery and classification, data access governance, masking and tokenization, and encryption and key management. The same survey also shows 39% of organizations have already consolidated some of these technologies into a platform, with another 44% that have plans to do so within the longer term (see Figure 2). Adoption of data security platforms is growing as there is a need for a robust solution that encompasses not only protecting and safeguarding data but also minimizing risk. This is a crucial step toward enabling organizations to deliver valuable insight while they ensure the integrity and confidentiality of their sensitive data across all data assets and repositories.

FIGURE 2: ***Consolidation of Data Security Tools Is a Reality***

Most organizations are already consolidating or plan to within the next year.

Q *Do you plan to consolidate data security tools within the next 12 months?*



Notes:

IDC put this survey question to all global participants in both surveys.

The graphic shows the percentage of total respondents answering the question.

Source: IDC's Data Security and Privacy Survey, March 2025

IDC is seeing more acceptance and traction for the consolidation of data-centric security technologies. However, the financial and resource investment, acquired skill sets, and "best for us" technology selection may continue to be barriers to single platform consolidation for vendors like Thales and others. Further, integration with outside solutions is possible but not always easy or perfect, creating frustration for the security team.

Despite this, the consolidation of security tools is actively occurring. Smaller security teams and reduced overall budgets are driving organizations to move to a platform approach for simplicity and cost savings.

Comprehensive visibility and prioritization of data security risks enable proactive remediation, resulting in better business outcomes.

Conclusion

Data security has taken on new significance with AI advancement and the forthcoming migration to post-quantum encryption. Organizations must be agile and efficient to stay competitive. Integrated data security offers a number of benefits to security teams and the business as a whole, including cost and time savings and a less complex environment.

With comprehensive visibility and the prioritization of data security issues, organizations can proactively address risks to reduce the impacts of security incidents and improve business outcomes.

About the Analyst

Jennifer Glenn, *Research Director, Security and Trust*

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

Today's enterprises depend on the cloud, data, and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and datacenters to devices and across networks. As the global leader in security for a world powered by Applications, Data, Identities, and Software, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day. Thales Cybersecurity Products is part of Thales Group.

For further information, visit cpl.thalesgroup.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
blogs.idc.com
www.idc.com