Security Leader's Guide to Data Security

Published 7 September 2023 - ID G00787538 - 8 min read

By Analyst(s): Andrew Bales

Initiatives: Security of Applications and Data; Demonstrate Value and Collaborate With Business Partners

Many approaches can ensure the security of data on-premises and in the cloud. Security and risk management leaders must identify the complex business and security concerns and build a multidisciplinary program that combines technology innovation with business-centric processes and policies.

Strategic Planning Assumptions

By 2025, 30% of Gartner clients will protect their data using a "need to share" approach, rather than the traditional "need to know" approach.

By 2027, at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation.

Analysis

Data is the cornerstone of digital business and includes a wide spectrum of sourced and derived data. It can include information needed by service employees, partners and customers. This data may be sensitive, such as personally identifiable information (PII), personal health information (PHI), payment card information (PCI) or other regulated data, internal and external communications. It may also include intellectual property, other sensitive or confidential information, and the continually growing use cases for data and analytics, including widespread adoption of AI.

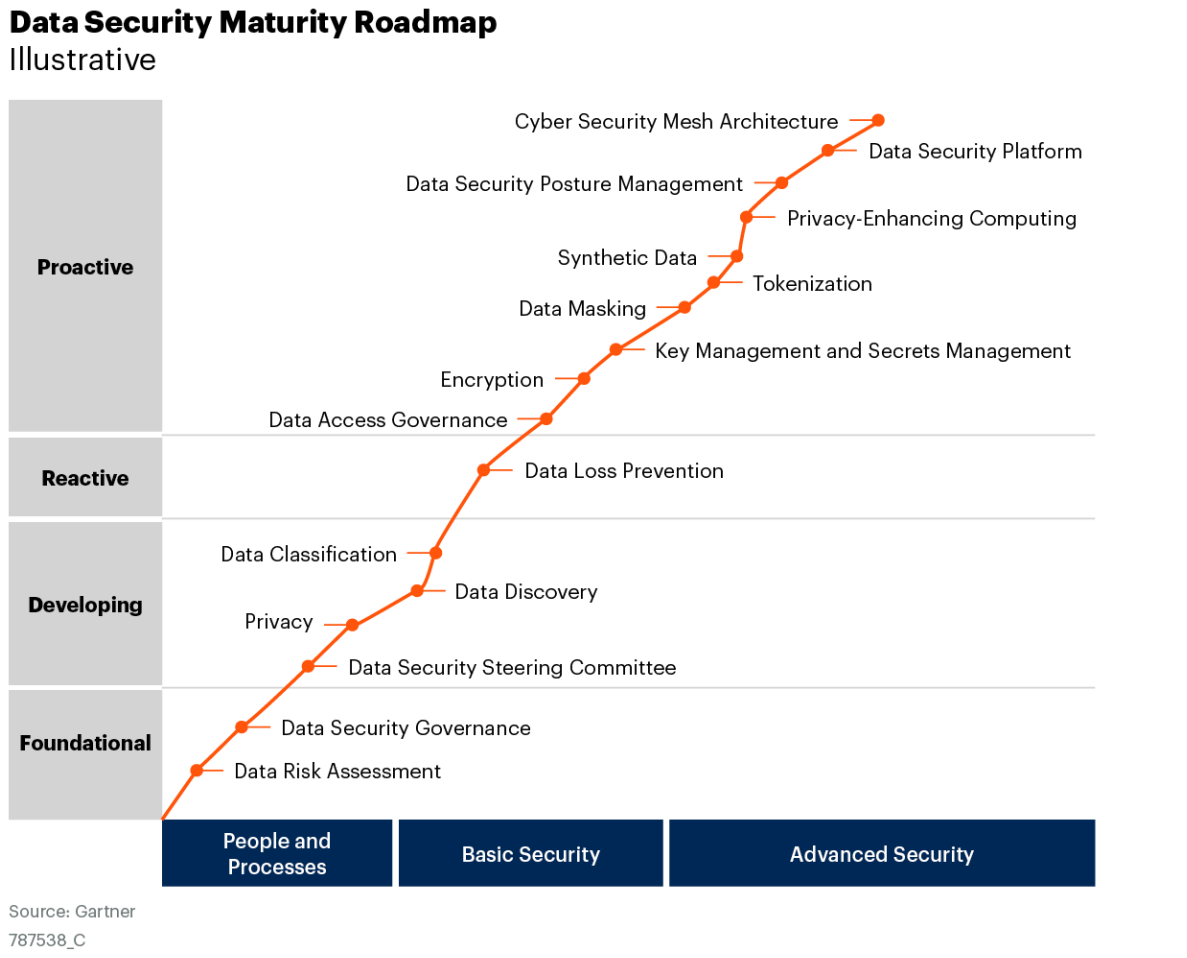
Many organizations are exploring the use of AI for their business strategies, and an evolution of AI use cases (such as LLM applications) is just beginning. Organizations are also undergoing cloud migration journeys, adopting multicloud and hybrid IT architectures. Naturally, data is subject to these developments, which is causing an increase in organizational data sprawl. An expansive geographic footprint can introduce data residency risks for personal and regulated data, leaving it susceptible to threat actors eager to take advantage of misconfigurations and vulnerabilities in the cloud. To avoid these negative outcomes, organizations need to prioritize the protection of data across all of their technology assets, including IaaS, PaaS and SaaS.

Privacy is increasingly relevant to security and risk management (SRM) leaders who have been tasked with developing a data security program to address privacy concerns. As a result, consistent, business-driven data security is top of mind. This is especially important to avoid some of the negative impacts associated with data residency risks, such as monetary losses from privacy noncompliance, reputational damage and loss of competitive advantage. Data is pervasive, valuable and easy to use across the organizational ecosystem. As a result, data security is more complex than merely implementing tools to understand, secure and protect data from loss or exposure.

Many data security projects have unforeseen roadblocks. Reacting to these roadblocks, rather than preparing for them, can extend the data security project timeline and cause delays in addressing business continuity impacts. Roadblocks can include business disruption, difficulties garnering business buy-in, or unforeseen implementation costs. Failing to engage the business in data security initiatives can cause significant business disruption, such as preventing completion of timely sales initiatives, or keeping data and analytics (D&A) teams from engaging seamlessly with the data they need. If data security policies and controls are developed independent of the business needs, policies and controls will be perceived as oppressive and disruptive rather than being directive and educational.

As the common element for so many aspects of technology and business, securing and ensuring appropriate access to data can be a daunting task. Many organizations lack a meaningful data security program that includes process, governance and technology. Gartner clients often struggle to understand where to start or to accurately assess the maturity of their data security program. This must start with a foundation of people and processes, basic security hygiene across the organization and advanced data security tools and technologies (see Figure 1).

Figure 1: Data Security Maturity Roadmap



Adequate preparation around policies and processes, technology and threat mitigation, all done with the business insight and buy-in, will help break through typical data security roadblocks. This research will help SRM leaders understand the scope of a data security program, and the elements that must be considered. Specifically, it provides insights to:

- Address impending privacy regulations
- Engage the business in gathering requirements and developing shared responsibilities for decisions around data security
- Understand technology and market trends
- Develop organizational management strategies
- Choose among options to meet technology needs to start a data security program

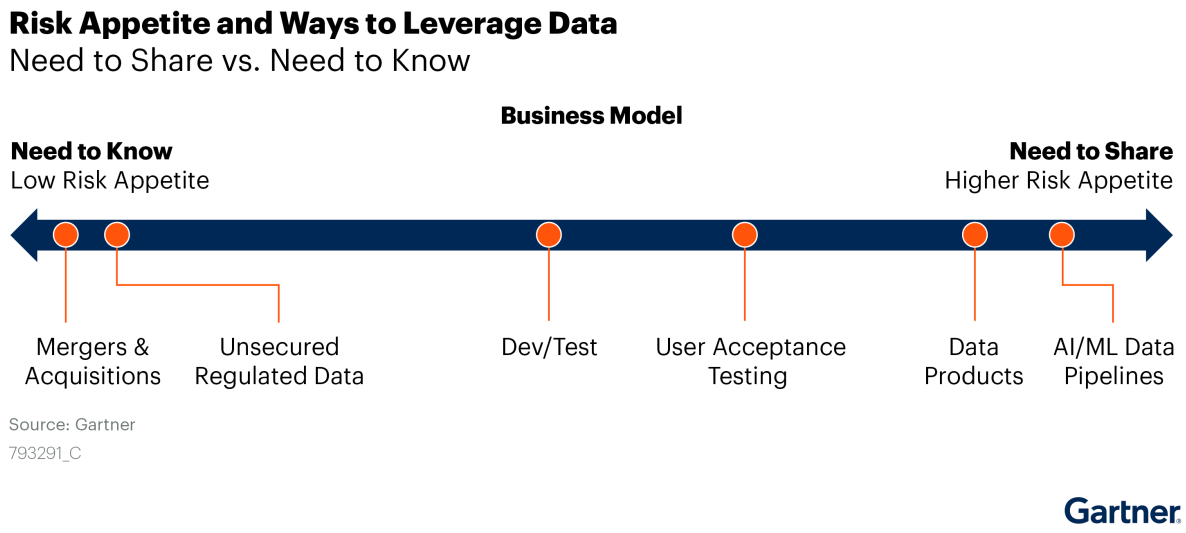
Research Highlights

Some recommended content may not be available as part of your current Gartner subscription.

The Business Is the Foundation for Data Security

The foundation of data security must be the business. Risk appetite and business needs drive risk prioritization in data security programs (see Figure 2). To understand the business needs, SRM leaders should develop a data security governance (DSG) process using a data risk assessment for risk identification and prioritization (see 4 Critical Steps to Accelerate the Adoption of Data Security Governance). They must also continue to engage the business after developing a DSG program (see Use a Data Security Steering Committee to Realize Data Security Governance Objectives). Because they frequently have the most complete understanding of organizational data risk, SRM leaders should communicate the identified data risks to the organization (see How to Communicate Data Risk to the Business).

Figure 2: Risk Appetite and Ways to Leverage Data



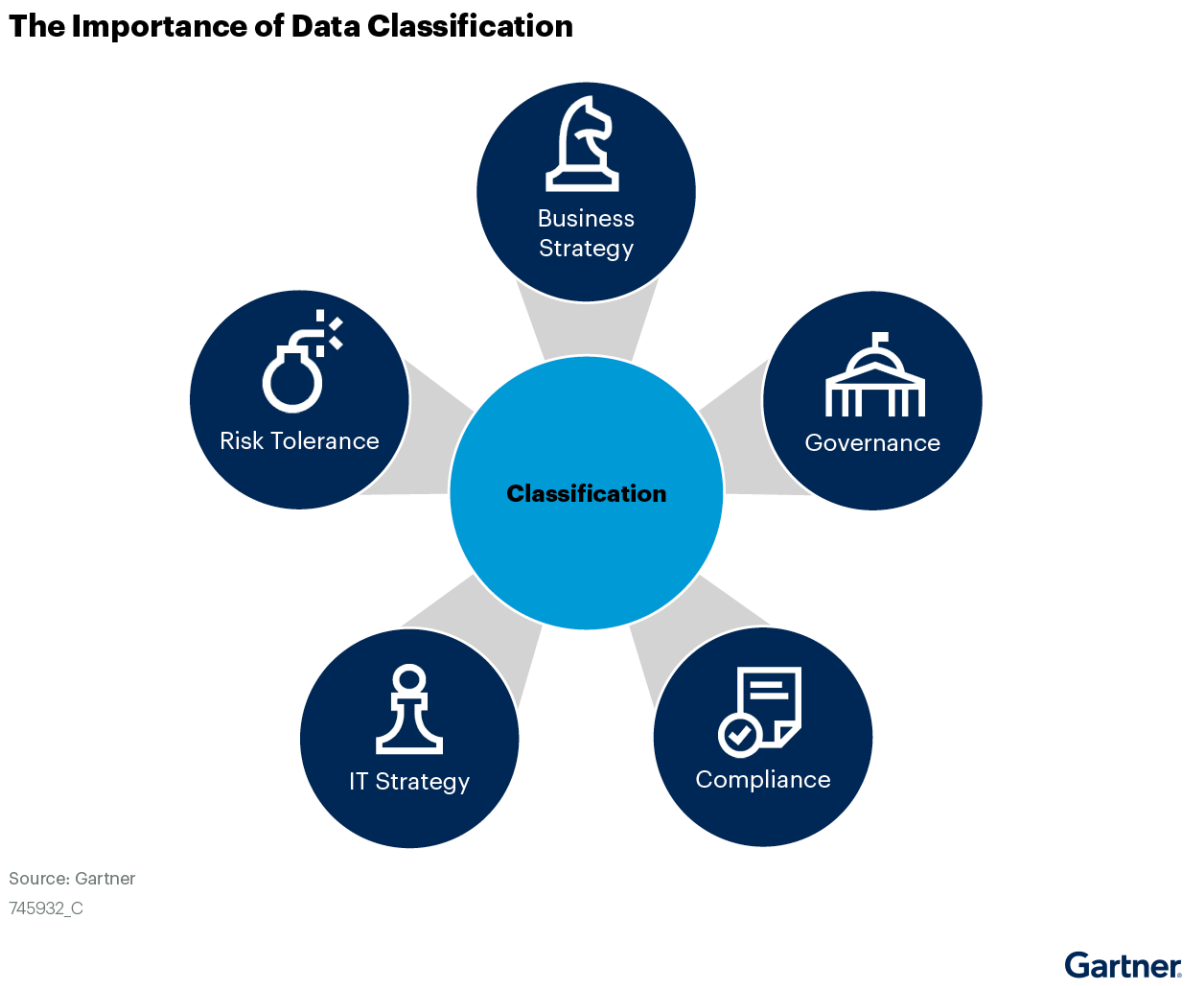
Evaluate the Implications of Privacy Regulations on Data Security

Following the publication of GDPR in 2016, privacy regulations have increased globally (with the likes of CCPA, LGPD, PIPL and others). Many jurisdictions (e.g., countries, U.S. states) have passed data protection legislation, often in similar and overlapping fashion. This rapid evolution of the global privacy landscape demands that organizations set up a modern and comprehensive privacy program. To gain necessary insights into what the organization needs to do to have a comprehensive data protection regime, and retention and backup best practices, see Practical Privacy — Managing Data Retention and Backups. To prioritize investments to align to top trends, see Top Trends in Privacy Driving Your Business Through 2024.

Understand Your Data

Data discovery and classification are foundational to data security (see Figure 3). If deployed effectively, they can be instrumental in driving business engagement in data security. Classification policies and data handling documents establish clear objectives and requirements and connect the data classification to the overall organizational security framework (see Building Effective Data Classification and Handling Documents). A modern, phased approach to data classification shifts the focus from user awareness and training toward automation and metadata enrichment (see How to Succeed With Data Classification Using Modern Approaches). Once the organization is data literate (see Note 1), it's important to understand how that data is being used and identify risks posed by the data (see Innovation Insight: Data Security Posture Management).

Figure 3: The Importance of Data Classification



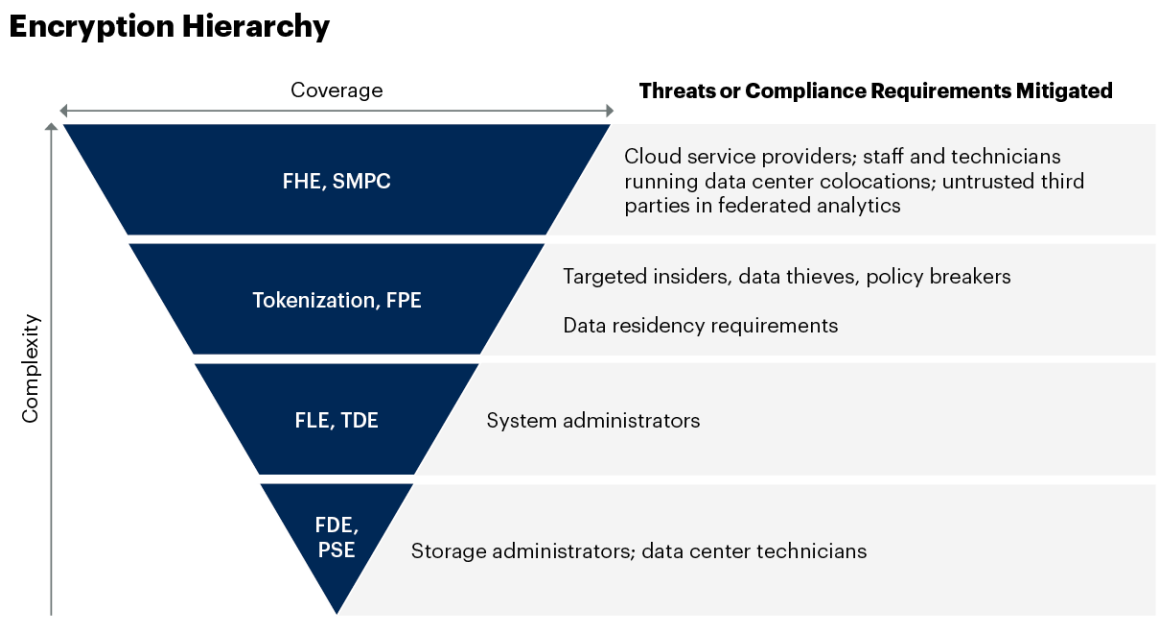
Prevent Data Loss

Data loss prevention (DLP) is frequently considered the program of choice for an organization tasked with building a data security program. Due to inefficiencies in DLP implementation and program development, and its reactive nature, organizations often struggle to develop an effective program, viewing success as unattainable. SRM leaders must focus on business objectives, identify data risk factors, decrease DLP violations and address stakeholders' frustrations to optimize chances of successfully developing a DLP program (see Getting DLP Right: 4 Elements of a Successful DLP Program). Programmatic optimization is one facet, technology is the other. The market for DLP-focused technology solutions, though mature, continues to evolve, with emerging alternatives to the traditional approaches (see Market Guide for Data Loss Prevention).

Protect Against Data Loss

Reactive controls (DLP) are only as good as their detection accuracy. Proactively securing data through encryption and key management can mitigate internal and external threats, because the data is secured at rest, rather than only once the data transverses the corporate boundary (see Figure 4). To mitigate growing security threats, data residency requirements and privacy impacts to data, SRM leaders should use enterprise key management to create strong data protection policies across a variety of cryptographic technologies (see Use Enterprise Key Management to Provide Stronger Data Security and Privacy). These technologies include tokenization, privacy-enhanced computation or other data encryption approaches (see Getting the Most Out of Your Investment in Encryption).

Figure 4: Encryption Hierarchy



FHE (Fully Homomorphic Encryption); SMPC (Secure Multiparty Computation); FPE (Format-Preserving Encryption); FLE (File-Level Encryption); TDE (Transparent Data Encryption); FDE (Full Disk Encryption); PSE (Primary Storage Encryption)

Source: Gartner

772811_C

Gartner

Mitigate Threats of Sensitive Data Exposure From AI Usage

Recent acceleration of AI in D&A use cases and general accessibility to generative AI chatbot applications (such as ChatGPT, Bard and others) have introduced the threat of organizational data exposure. To mitigate these threats, SRM leaders should:

- Apply security controls to the AI pipeline, supporting a systematic view of data security (see Securing Your AI Data Pipeline)

- Leverage synthetic data (see Embrace Synthetic Data to Improve R&D Product Development and Optimize Processes)
- Mask sensitive data (see Market Guide for Data Masking)
- Limit data exposure by setting clear organizational policies for the use of AI services until controls are implemented (see Quick Answer: How Can Executive Leaders Manage AI Trust, Risk and Security? and Quick Answer: How to Use ChatGPT and Generative AI Securely With Minimal Data Loss).

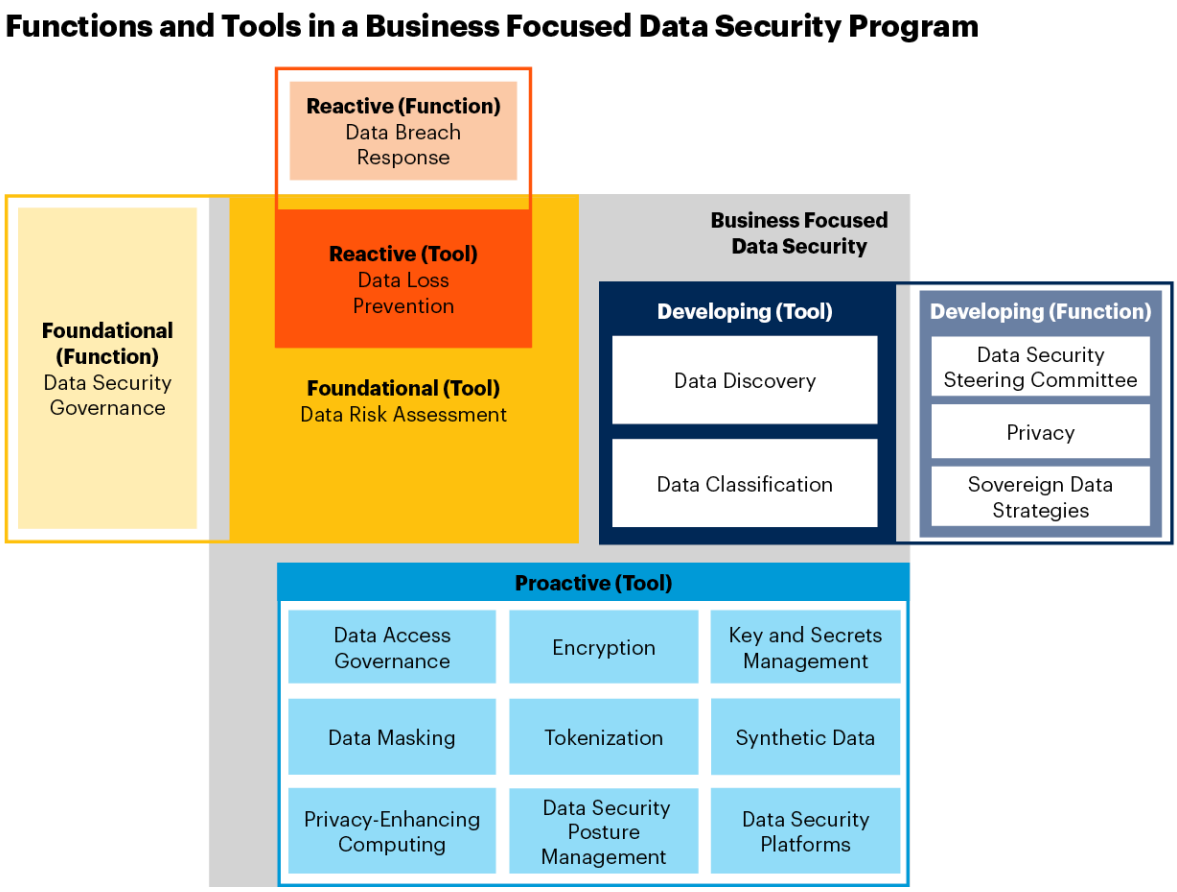
Integrate Disparate Security Capabilities for Increased Efficiency and Cost Reduction

Implementing efficient and effective data security controls requires more than just an array of siloed products (see Figure 5). SRM leaders tasked with developing a security program should integrate siloed data security controls, where feasible, to help reduce complexity and costs (see 2023 Strategic Roadmap for Data Security Platform Adoption). Take advantage of platform controls by:

- Drafting policies to standardize controls across silos
- Accommodating business need to share data
- Enhancing governance and security posture
- Discovering and classifying unknown data across cloud service platforms
- Identifying security and privacy risks associated with data sprawl

Organizations with a vendor consolidation strategy may look to build data security controls into their cybersecurity mesh architecture, aligning disparate technologies to a cohesive security vendor architecture (see How to Start Building a Cybersecurity Mesh Architecture).

Figure 5: Functions and Tools in a Business-Focused Data Security Program



Note 1: Data Literacy Defined

Data literacy is the ability to read, write and communicate data in context, including an understanding of data sources and constructs, analytical methods and techniques applied, and the ability to describe the use-case application and resulting value.