FORRESTER®

A 2026 Snapshot On The State Of Data Security

How Modern Data Protection Unlocks Operational Resilience And Business Value

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CAPITAL ONE SOFTWARE
APRIL 2026

Better Protection Means Greater Payoffs For The Business

Traditional data security focuses on static perimeters, but in a world of cloud and AI, data is constantly in motion. Beyond mere protection, organizations must implement security strategies that secure data across all hosting models while enabling the data to unlock greater value for the business.

To successfully compete, organizations must leverage their data security to enable operational flexibility and ease of use, achieve data sovereignty, and support emerging agentic and generative AI use cases.

In February 2026, Capital One Software commissioned Forrester Consulting to evaluate the state of data security. We fielded a survey of 211 North American decision-makers with responsibility for their organization's security and risk technology strategy to explore this topic.

Key Findings

Security leaders struggle to keep pace. Seventy-two percent said that data security has never been more critical — but investments in traditional network and perimeter security tools impede adequate data protection.

Legacy siloed solutions hold back organizations. More than half of respondents lack full visibility of vulnerabilities. A lack of modern solutions stymies data protection scalability, flexibility, and new use cases (e.g., with AI).

Creating value with data must be the key motivator to protect it, and tokenization can help. Two in three decision-makers don't use tokenization solutions, underscoring opportunity. Tokenization reduces risk and expands data use so organizations can maximize their data ROI.

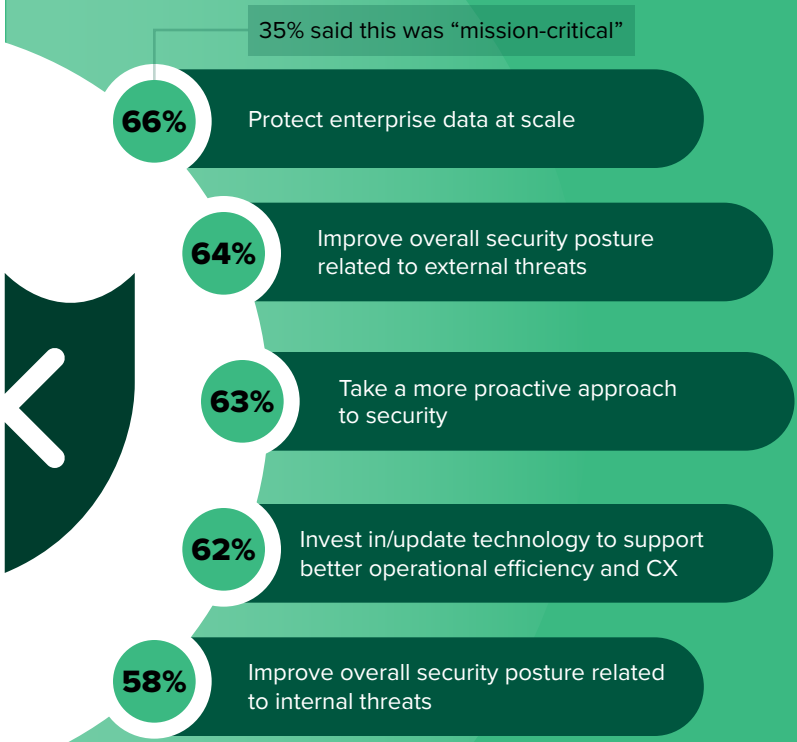
Leaders Are Prioritizing Data Protection, Resilience, And Operational Agility ...

Data security remains a top priority for security decision-makers; however, this extends beyond pure defenses. Respondents report that data protection must also support operational efficiency and customer experience, signaling an important shift in how organizations approach data protection.

Importantly, these priorities dwarf the attention paid to AI capabilities within data security. In other words, organizations seek to get their data foundations and data sovereignty right before turning to the promise of AI.

This is consistent with Forrester Research, which says rather than viewing AI as a silver bullet, organizations must first get their people, processes, and data in order before relying on emerging technologies to fuel transformative change.[1]

Security Priorities Over The Next 12 Months



Note: Showing top five combined “High priority” and “Mission-critical” responses
Base: 211 North American director-level and above decision-makers in IT and data and analytics who are responsible for their organization’s security and risk technology strategy
Source: Forrester’s Q1 2026 Data Tokenization Survey [E-66642]

… But Their Tools Can't Keep Pace With Modern Demands

Security leaders know they need to do better. Nearly half admit that their organizations can't successfully compete given current data security processes. Forrester's Zero Trust data security research agrees, finding that organizations must evolve beyond traditional security approaches.[2]

Decision-makers today slog through a fractured environment, relying on familiar tools that fail to satisfy the current business landscape:

- Network security technologies, such as firewalls, VPNs, and intrusion detection systems.
- Identity and access management systems, which centralize control over access to cloud resources.
- Vulnerability management tools, which scan for vulnerabilities and misconfigurations.

Organizations Use Multiple Solutions To Enable Their Data Security Goals

Network security technologies (e.g., SASE, firewalls, VPNs, intrusion detection system/ intrusion prevention system [IDS/IPS])

Identity and access management (IAM) systems

Vulnerability management tools

Note: Showing top three responses
Base: 211 North American director-level and above decision-makers in IT and data and analytics who are responsible for their organization's security and risk technology strategy
Source: Forrester's Q1 2026 Data Tokenization Survey [E-66642]

Silos And Slow Decision-Making Impede Progress And Business Performance

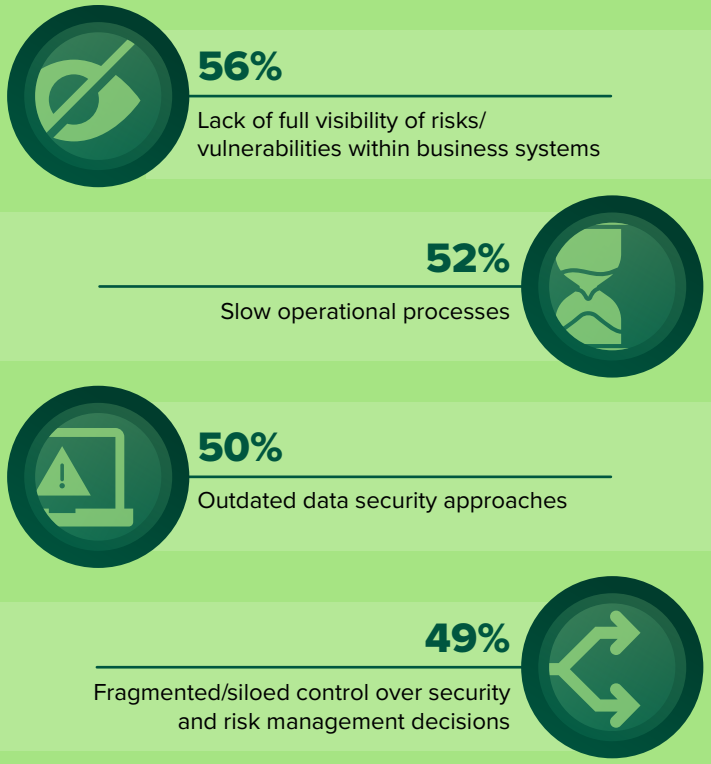
While many organizations believe their current tools adequately protect their data, legacy solutions lack the speed, flexibility, scalability, and AI readiness required today.

Leaders struggle with visibility gaps, as 56% lack a full view of risks and vulnerabilities within business systems. Operational friction also hinders success: 52% are slowed by lack of automation, nonstandard processes, and siloed decision-making. Half cite technical debt, relying on outdated data security approaches that no longer scale or function in modern cloud/AI-driven environments. And fragmented governance plays a role: 49% deal with siloed control over security and risk management decisions.

The consequences are critical: As data security challenges mount, downstream business performance suffers, scalability weakens, breaches and regulatory problems rise, and overall risks to the business surge.

Forrester research supports these findings, underscoring how data breaches and added risk interrupt core business processes.[3]

“What process challenges does your organization face with its data security?”



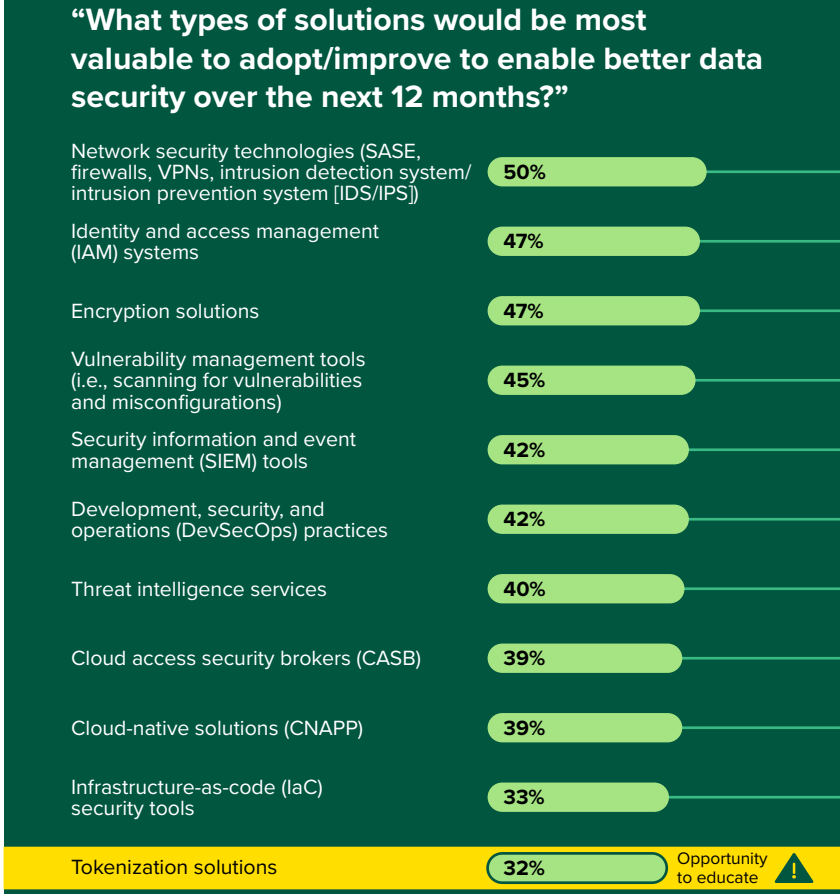
Note: Showing top four responses
Base: 211 North American director-level and above decision-makers in IT and data and analytics who are responsible for their organization’s security and risk technology strategy
Source: Forrester’s Q1 2026 Data Tokenization Survey [E-66642]

Leaders Need Help Modernizing Their Data Security Solutions

With volatility normalized, security leaders require more guidance during budget decision-making.[4] While survey respondents know they need to improve, current investments skew toward familiar categories and do not meet organizational needs. Their investment plans sprawl across the usual suspects — network security technologies (50%), access management systems (47%), and encryption solutions (47%).

Just one in three leaders see tokenization solutions enabling better data security over the next 12 months. This oversight suggests opportunity and first-mover advantages.

Tokenization represents a strategic shift from locking down data to actively securing it for use. Unlike traditional methods that often force a trade-off between protection and accessibility, tokenization keeps data protected while maintaining the format and function required for modern AI and analytics.[5]



Base: 211 North American director-level and above decision-makers in IT and data and analytics who are responsible for their organization's security and risk technology strategy
Source: Forrester's Q1 2026 Data Tokenization Survey [E-66642]

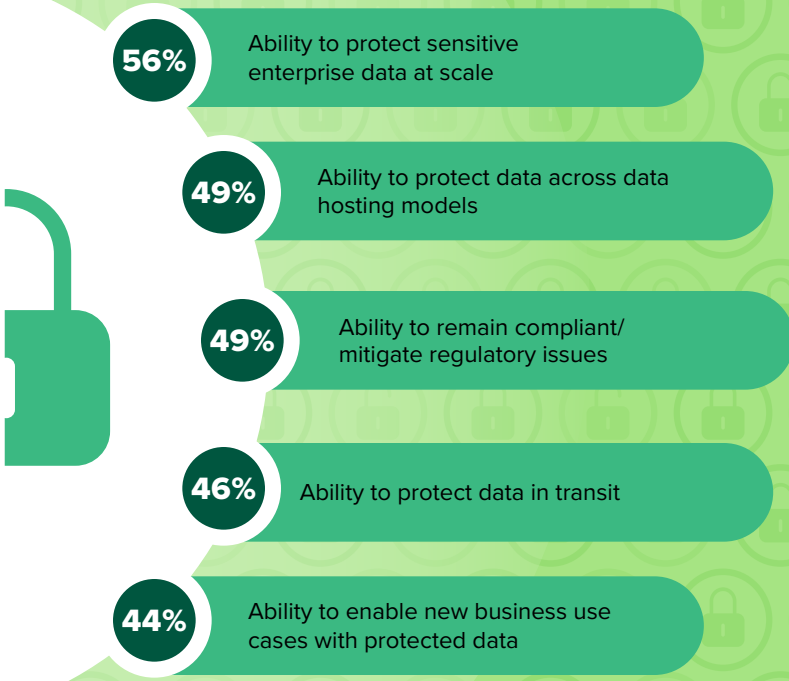
Decision-Makers See Competitive Value In Tokenization

Tokenization solutions equip organizations to protect data in use, in transit, and at rest without sacrificing utility for downstream systems, users, and third parties. This versatility is why forward-thinking leaders are pivoting to tokenization. Rather than solving a single pain point, they are looking to tokenization to deliver multiple benefits:

- Resilient security and governance: 56% of organizations prioritize safeguarding sensitive data at scale, while 49% aim to neutralize regulatory risks.
- Operational agility and growth: Nearly half require consistent protection across hybrid hosting models and transit. Meanwhile, 44% see these safeguards as a launchpad to unlock new business use cases with their protected data.

Early adopters who recognize this multifaceted value gain a competitive edge. By removing the friction between security and usability, tokenization allows them to use their highest-value data to fuel innovation.

Expected Benefits From Adopting Tokenization Solutions



Note: Showing top five responses
Base: 68 North American director-level and above decision-makers in IT and data and analytics who are responsible for their organization's security and risk technology strategy
Source: Forrester's Q1 2026 Data Tokenization Survey [E-66642]

Organizations Expect AI To Drive Security Workflows Going Forward

Security leaders are increasingly looking to AI to modernize their defensive posture. While just 34% of decision-makers said genAI capabilities are paramount to data security today, that figure balloons to 64% as they look two years ahead. Respondents expect genAI to help their organizations keep pace with proliferating threats, incident response, and privacy risk assessments — among other growing use cases.

However, these use cases create a data paradox: To detect threats or predict attacks, AI models require deep access to sensitive organizational data. Without a secure foundation, this creates new vulnerabilities, expanding the very attack surface AI is meant to protect. This underscores the need for secure, trusted, and usable data foundations. According to Forrester research, weak data and IT foundations not only hamper AI readiness but risk costly failures and reputational risk.[6]

Ultimately, emerging AI functionality across genAI and agentic AI will empower leaders to fortify their data security and harness new use cases so they can maintain agility, create more payoffs for the business, and safeguard their organizations into the future.

"Which generative AI use cases do you expect to be most valuable to your organization's data security over the next one to two years?"

Note: Showing top six responses
Base: 211 North American director-level and above decision-makers in IT and data and analytics who are responsible for their organization's security and risk technology strategy
Source: Forrester's Q1 2026 Data Tokenization Survey [E-66642]

Conclusion

Data security is undergoing a massive change driven by the following factors:

Legacy data protection isn't enough. While traditional data security protections like encryption, data leak prevention, and malware/ransomware detection remain essential to a defense-in-depth strategy, they can't meet the demands of the AI era. Integrated, 360˚ data protection across on-prem, cloud workloads, and data repositories is critical.

Data protection must enable usability, not hinder it. Data protection is the glue binding data to business processes. Users must never notice it and should be able to seamlessly use business systems. Data protection measures should be comprehensive (cover all surfaces), granular (offer fast, easy access to protected data), and integrated (offer seamless human user and AI agent data processing and interaction).

AI adoption is impossible without rethinking data protection. AI agents autonomously operate at speed and scales that bypass human oversight, elevating the risk of unintended data exposure. Modern data protection solutions must embrace reliable and scalable data protection methods like tokenization to ensure data is secure, regardless of an agent's autonomy. This offers opportunity to support overall scaling of enterprise AI use by decoupling data utility from data risk.

Resources

Related Forrester Research:

Top Recommendations For Your Security Program, 2026, Forrester Research Inc., March 4, 2026

Top Emerging Technologies For 2025: Quantum Security, Forrester Research Inc., September 9, 2025

Related Blogs

Andras Cser and Heidi Shey, Think Hardware Security Modules Aren't Exciting? Think Post-Quantum Migration!, Forrester Blogs, January 30, 2026

Katie Linford and Audrey Bond, Build Your Foundation First: The Hard Truth About Successful AI Deployments, Forrester Blogs, October 2, 2025

Project Team:

Jason Daniels,
Senior Market Impact Consultant

Contributing Research:

Forrester's Technology Architecture & Delivery research group

Endnotes

[1] Source: Unlocking Process Efficiency With AI, Forrester Research Inc., April 29, 2025.

[2] Source: Data Security: The Time Is Now To Pioneer A New Strategy, Forrester Research, Inc., September 25, 2024.

[3] Source: The State Of Data Security, 2025, Forrester Research, Inc., October 22, 2025.

[4] Source: Budget Planning Guide 2026: Security And Risk, Forrester Research, Inc., July 10, 2025.

[5] Source: Hardware Security Module Requirements For The Post-Quantum Era, Forrester Research Inc., January 21, 2026.

[6] Source: The CIO's Guide To AI Readiness, Forrester Research, Inc., January 23, 2026.

Methodology

This Opportunity Snapshot was commissioned by Capital One Software. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 211 decision-makers in IT and data and analytics responsible for their organization's security and risk technology strategy. The custom survey began and was completed in February 2026.

Demographics

COUNTRY	
US	74%
Canada	26%

ANNUAL REVENUE (USD)	
$5B or more	29%
$1B to $4.9B	71%

TOP TWO INDUSTRIES	
Financial services	43%
Life sciences	17%

DEPARTMENT	
IT	70%
Data and analytics	30%

TOP THREE ROLES WITHIN IT	
Cybersecurity	41%
Information management	14%
Application development	10%

POSITION	
C-level executive	20%
Vice president	36%
Director	44%


FORRESTER®