2026 EDITION
DATA THREAT REPORT

THALES
CYBERSECURITY

QUANTUM & AI TRENDS

Protecting data at the crossroads of two revolutions

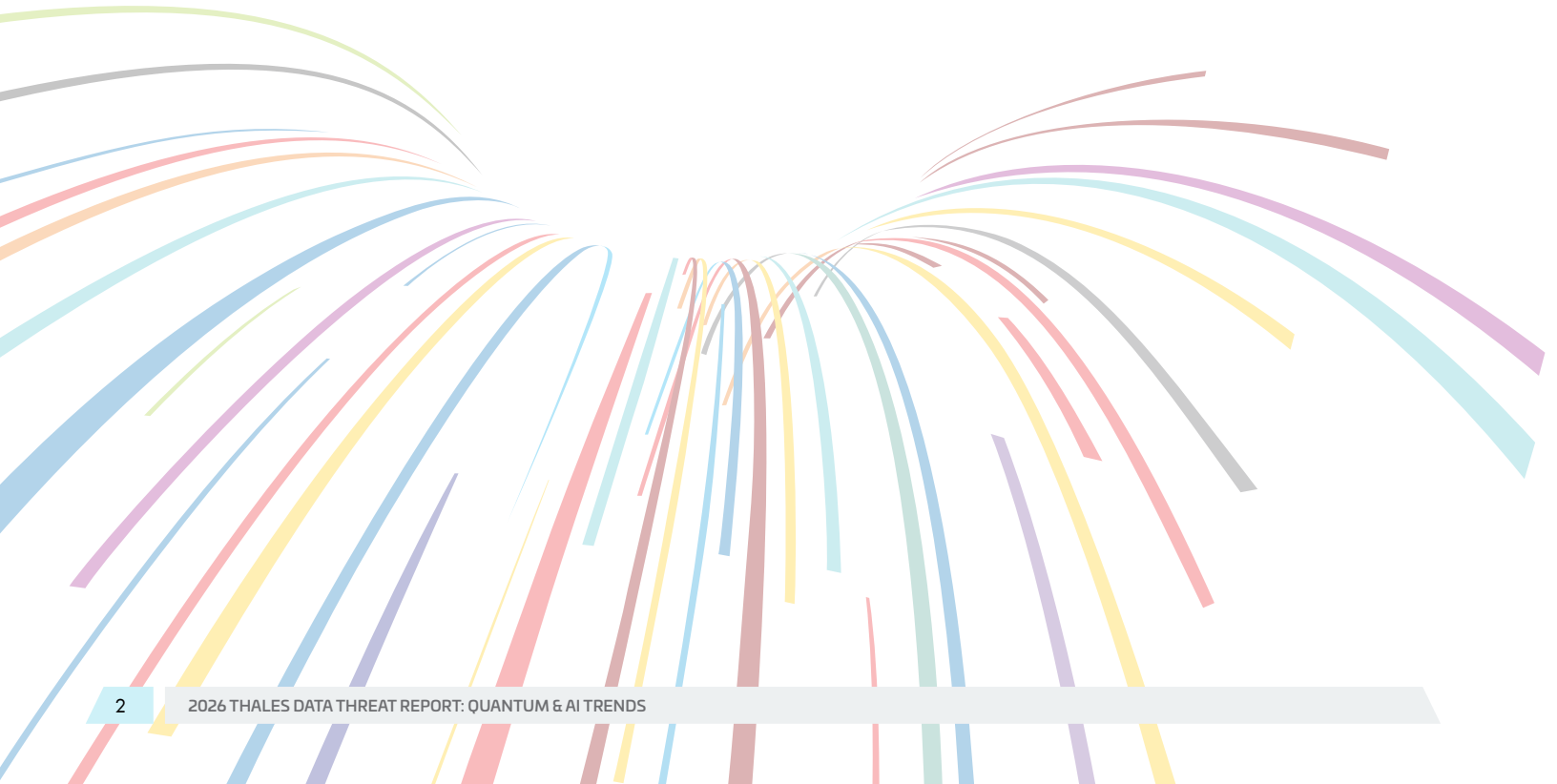


cpl.thalesgroup.com

#2026DataThreatReport

Table of Contents

Introduction	04
Key findings	06
AI, quantum and the future of computing	08
Quantum and AI leaders and laggards	10
AI imperatives strain security efforts	12
Security pressures expand with AI and agentic operations	14
Quantum risk realities	19
Cloud infrastructure under attack	23
Data sovereignty, quantum and AI risks	25
Conclusions	26
Methodology	27



Conducted by

S&P Global
Market Intelligence

About the authors



Justin Lam, Senior Research Analyst

Justin Lam is a senior research analyst at 451 Research by S&P Global, leading data security research within the Information Security channel since October 2021. He leverages his years of industry experience and his unique understanding of both how customers buy and why sellers sell to help investors, practitioners and entrepreneurs understand and contextualize industry trends.



Eric Hanselman, Chief Analyst

Eric Hanselman is the chief analyst at 451 Research by S&P Global. He coordinates industry analysis across the broad portfolio of technology, media and telecommunications research disciplines, with an extensive, hands-on understanding of a range of subject areas, including information security, networks and semiconductors and their intersection in areas such as AI, 5G and edge computing.



Mark Ehr, Principal Research Analyst

Mark Ehr is a principal research analyst at 451 Research by S&P Global, focused on cloud security, security operations and AI within the 451 Research information security practice. He has more than 20 years of cybersecurity experience, a decade in software development and many years working in product marketing, product management and sales enablement.

Introduction

Technology transitions always present challenges to security strategies. AI and quantum computing are creating new and profound strategic imperatives. One of the most difficult aspects of managing security risks is understanding the nature and timing of threats. Risks related to AI are here today in the early stages of its deployment. Quantum risks might seem more distant, but they could loom larger and advance more rapidly. The **2026 Thales Data Threat Report: Quantum & AI Trends** presents a new look at two revolutionary technologies and their impacts on data security. This report examines where those risks are materializing and explores the measures that enterprises are taking to mitigate them, as well as their expectations for future developments.

Quantum- and AI-driven threats to critical data assets must be addressed in the near term, and many organizations are already implementing protections. Enterprises are broadly aware they must build trust in how data is collected, processed, analyzed and leveraged to fulfill business goals. However, AI and quantum, progressing on distinct and tough-to-predict timelines, pose dual threats to data trust. AI radically changes how quickly and unpredictably data is discovered, accessed, reused and exposed. Meanwhile, quantum computing risks threaten core cryptographic systems used to protect data and authenticate identity over time.

The Data Threat Report: Quantum and AI builds on the long history of the Thales Data Threat Report, specifically examining quantum and AI security considerations through the insights of more than 3,100 respondents from 20 countries. In addition to exploring broad trends, this report models behaviors and outcomes for distinct classes of respondents characterized as leaders and laggards in quantum and AI technology, with lessons to be learned from each. Much as the technologies are intertwined, leaders in both areas show that they've achieved better outcomes in data security.

The rapid proliferation of AI has caught security teams by surprise. GenAI is inherently non-deterministic. Risks include loss of confidentiality, integrity and authenticity. Risks from newer harms such as AI-generated deepfakes may be easy to recognize but difficult to define. New layers of models, agents and skills have boosted expectations for innovation while adding further risks for security leaders to manage.

Sufficiently powerful quantum computers could compromise both the root of trust in identity and the cryptographic protections that businesses and individuals rely on. The time when such a powerful quantum computer becomes available is referred to as "Q-Day." The Cybersecurity and Infrastructure Security Agency has issued guidance for government agencies and private-sector enterprises to complete their migrations to quantum-safe systems by 2035. Organizations must begin diligent transition commitments today if they have not already. Cryptography is foundational within and among modern enterprises, and transition efforts require planning to ensure future compatibility and security.

These are not future threats. AI is already affecting data security as training initiatives risk exposing poorly understood data resources and agentic applications hunt down and integrate data to build more comprehensive and detailed catalogs. With many AI workloads hosted in the cloud, enterprises' challenges securing their cloud environments raise additional concern. Moreover, today's data is already at risk from future quantum attacks based on harvest now, decrypt later and harvest now, forge later attack strategies. The survey results indicate there is much to be done to effectively and efficiently secure sensitive data, and that work should be underway.

AI security leaders are succeeding at critical data security tasks

This year's research reveals that AI security leaders (those that have invested in AI-specific security and identify as leading their peers in AI) are succeeding at critical data security tasks.

Better data knowledge – 36% have complete knowledge of where data is stored, versus 28% for AI laggards.

Better data classification – 43% can classify all of their data, versus 35% for laggards.

More likely to have full control of encryption keys for data in cloud (12% versus 6%). This is also true for quantum leaders, outpacing laggards by 13% to 10%.

Interestingly, AI security leaders are also ahead in some areas of quantum resilience.

Only 1% don't have a formal plan for addressing quantum threats, but three times as many (3%) of laggards are lacking a formal plan. Lacking a formal plan for addressing quantum threats could leave them exposed to quantum exploitation.

AI leaders are implementing quantum random number generation at a greater rate than laggards (31% versus 24%). Improving the robustness of cryptographic protections is a key part of improving post-quantum security postures.

Quantum security leaders are also moving forward

At the same time, Quantum computing leaders (those that are experimenting with or surveying quantum use cases) are also further along in their post-quantum computing security work:

22% report being further ahead in securing PKI (versus 14% of quantum laggards). 16% are ahead on certificate lifecycle management (versus 11% of laggards).

22% are ahead on enterprise key management (EKM) (versus 18% of laggards).

19% are ahead on code signing (versus 11% of laggards).

12% are ahead on interoperation with their ecosystems (versus 7% of laggards).

Both AI and quantum security leaders are less likely to see budgets as a leading inhibitor to tools consolidation – 39% versus 49% for AI and 37% versus 43% for quantum for laggards. This is an indicator that they may be able to work more quickly to reduce operational complexity for security teams.



Key findings

Protecting data at the crossroads of two revolutions

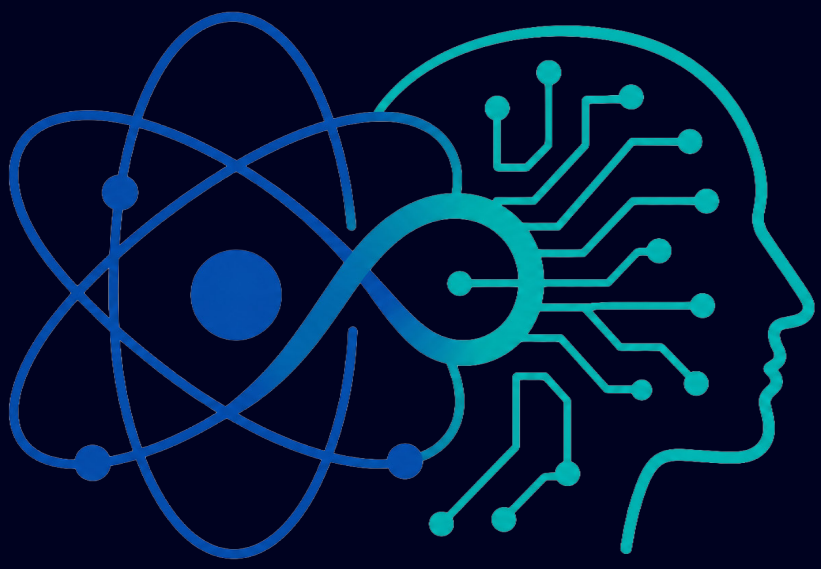
AI and quantum futures are intertwined

98% of respondents are considering the impact of Quantum and AI on each other

Quantum computing will help improve AI:

57% believe it will enhance machine learning; and

54% believe it will lead to advanced simulation of complex systems



AI has created security pressures

25% ranked AI security spending as the second highest spending category after cloud.

30% said their security budget, specifically for AI, increased significantly.

Quantum risks are impacting security today

32% have either identified quantum projects or started experimenting with quantum computing as quantum concerns shift to the reality of harvest now, decrypt later (HNDL) as 61% regarded it the top concern.

59% of organizations regard prototyping and evaluating Post-Quantum Cryptographic (PQC) algorithms as their top path to becoming quantum safe.

52%

said competitive advantage was the number one factor driving interest in quantum computing.[1]

36%

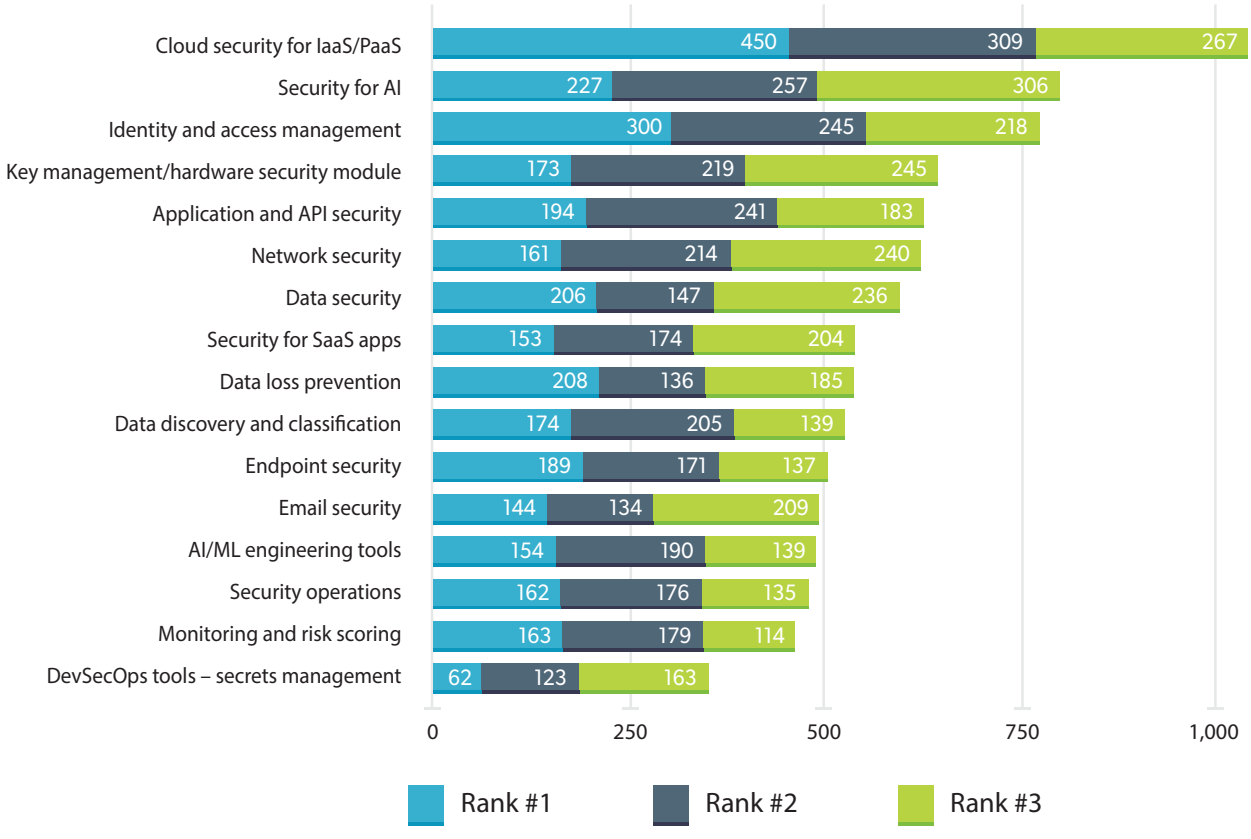
of enterprises believe they will realize material value in 1-3 years, with an additional 28% expecting in 3-5 years from now.[3]

[1] From 451 Research's VoTE Digital Pulse, Quantum computing study (April 2026)

AI, quantum and the future of computing

Science fiction writer William Ford Gibson is frequently quoted as saying, "The future is already here — it's just not very evenly distributed." While the AI and quantum computing technology landscapes are rapidly progressing, indications of the enterprise's future are visible today. Both quantum and AI security issues have critical, overlapping implications for the confidentiality and integrity of the same datasets. While these threats are evolving on distinct and unpredictable timelines, enterprises must avoid the pitfall of focusing solely on their own timelines to achieve business goals.

SECURITY SPENDING PRIORITIES



Note: All charts displayed in this document are from S&P Global Market Intelligence 451 Research's 2021-2026 Data Threat custom surveys.

The collection, processing, analysis and application of data drives decisions, leading to business outcomes. Despite ongoing efforts to aggregate and act on early indicators and key data signals, security challenges posed by AI came as a shock to many organizations, and the resulting disruption has rapidly accelerated, elevating AI security (25%) to the second-highest prioritized security spending category after cloud security (33%). To ensure that this disruption is not repeated with quantum computing, organizations must invest in understanding the technology's risks and move proactively to mitigate them.

"The future is already here — it's just not very evenly distributed."

In our analysis of the survey results, we modeled respondents' characteristics to classify them as technology leaders or laggards. The characteristics of the respective groups offer useful insights into security operations and posture across AI and quantum technologies. Those categorized as AI leaders are more forward-looking in their AI security strategies and identified that they are using AI to gain competitive advantage. Those characterized as leaders in quantum computing have begun to formally explore quantum applications and technology. Leaders in both areas show greater attainment of key data security metrics, including their ability to classify and protect data. Interestingly, AI leaders tend to be further along in their journey to adopt quantum computing, and quantum computing leaders are more likely to be investing in AI-specific security. Leadership spills across disciplines, with each reinforcing the other.

AI leaders reported higher levels of data insight, with greater proportions reporting that they know where all their organization's data is stored (36%, versus 28% for laggards) and that they are able to classify it (43% can fully classify, versus 35% of laggards). This also appears to translate into better breach outcomes, with a slightly higher proportion of leaders reporting no history of data breaches: 54% of leaders versus 49% of laggards reported no breaches in the cloud, while 60% of leaders versus 56% of laggards reported no breaches on-premises.

Quantum and AI leaders and laggards

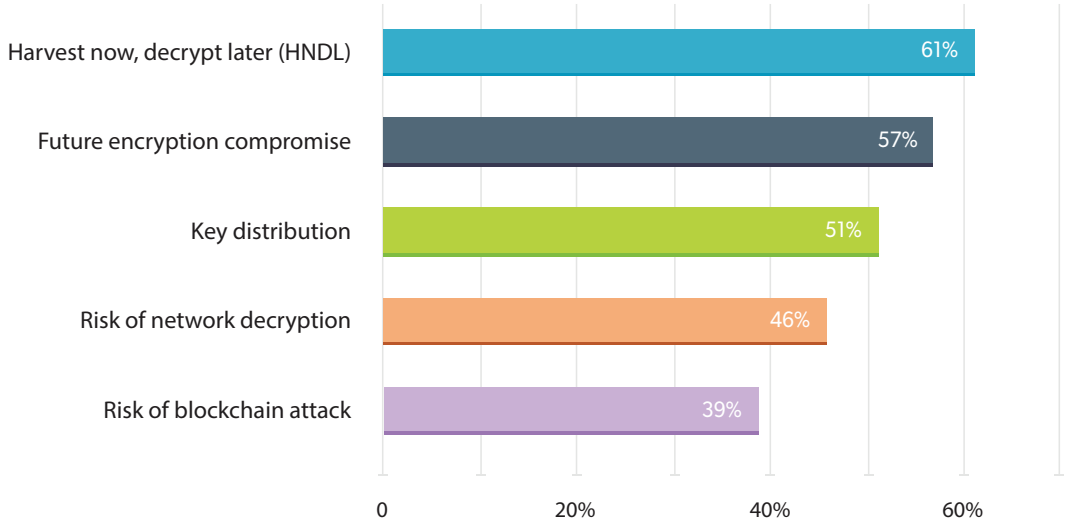


AI Leaders	• Invested in AI-specific security tools • Identified as leading peers in AI use
Quantum Leaders	• Experimenting or surveying quantum computing

As one might expect, organizations with more quantum computing experience reported a stronger post-quantum security posture across all the initiatives surveyed, including public key cryptography, certificate life-cycle management, enterprise key management, code signing and interoperability with broader computing ecosystems. Notably, while there may be a stronger one-way correlation between leadership in quantum experimentation and advancement in post-quantum cryptography (PQC), there is also correlation between AI leadership and PQC achievement. This supports the view that AI and quantum computing adoption are not isolated maturity markers but reflect an organization's deeper strategic and cultural emphasis on safely leveraging data to achieve business outcomes.

Enterprise understanding of quantum computing risks is maturing. This year's results have shifted from the prior year's broad concerns about encryption compromise toward the more specific and immediately relevant risk of harvest now, decrypt later as the top concern (61%). There is also growing awareness of the real risk of data exposure and loss of trust through harvest now, forge later attacks as projections for the arrival of Q-Day draw nearer.

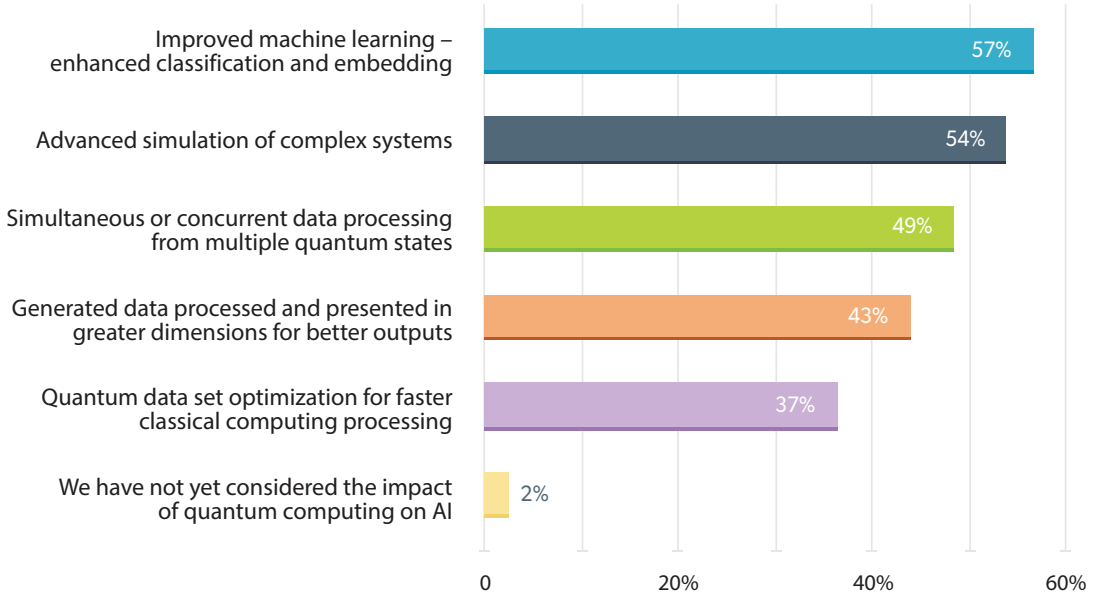
MOST CONCERNING QUANTUM RISKS



Trust is at risk not only for data,
but also for cryptographically protected identities.

The survey also explored potential benefits of combining quantum capabilities with AI. We have already seen AI used for applications such as error correction in quantum computing, and survey respondents indicated that quantum computing could further augment AI functionality. The top anticipated impact is improving machine learning through enhanced classification (57%), followed closely by the ability to perform advanced simulations of complex systems (54%). This is an area of active and widespread investigation: 98% of respondents have considered quantum computing's potential to accelerate AI processes.

QUANTUM IMPACTS ON AI

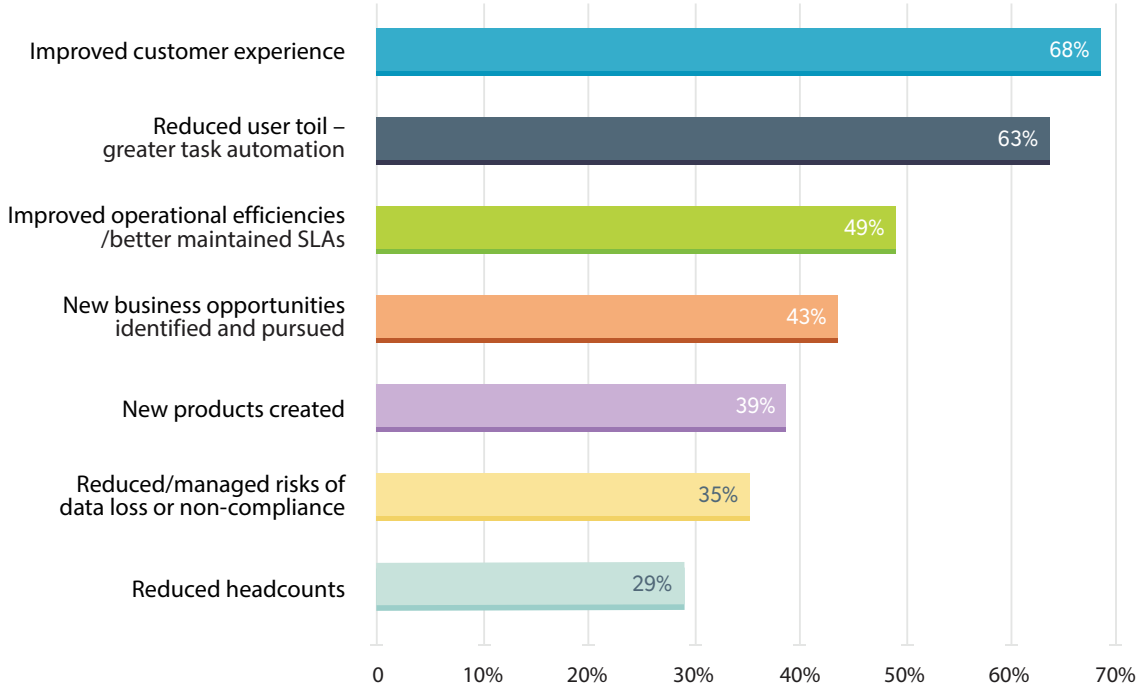


This report encourages technology and security leaders to view the looming threats of AI security and quantum security through the same lens as the underlying data. The challenges of data security are no longer confined to on-premises, cloud-hosted or SaaS-driven workloads. Principles and practices of data classification, access control, detection and response must extend seamlessly across all elements of modern infrastructure to address these new risks. As such, the same enterprise data faces two simultaneous waves of change stemming from AI and quantum developments, and data security controls must protect against both.

AI imperatives strain security efforts

In many cases, the imperatives driving AI projects are pushing data security concerns into the background. That means security teams must ensure effective protections are built into AI infrastructure up front to avoid the risk of safeguards being swept aside in the rush to capitalize on AI's promise. Respondents indicated that AI projects are moving ahead and that security is not the priority — indeed, risk mitigation (35%) ranks second to last among seven potential success criteria for AI initiatives. Organizations are scrambling to enhance customer experience and improve automation and employee efficiency. That places a burden on security teams to ensure they understand what data is being used and how it is secured.

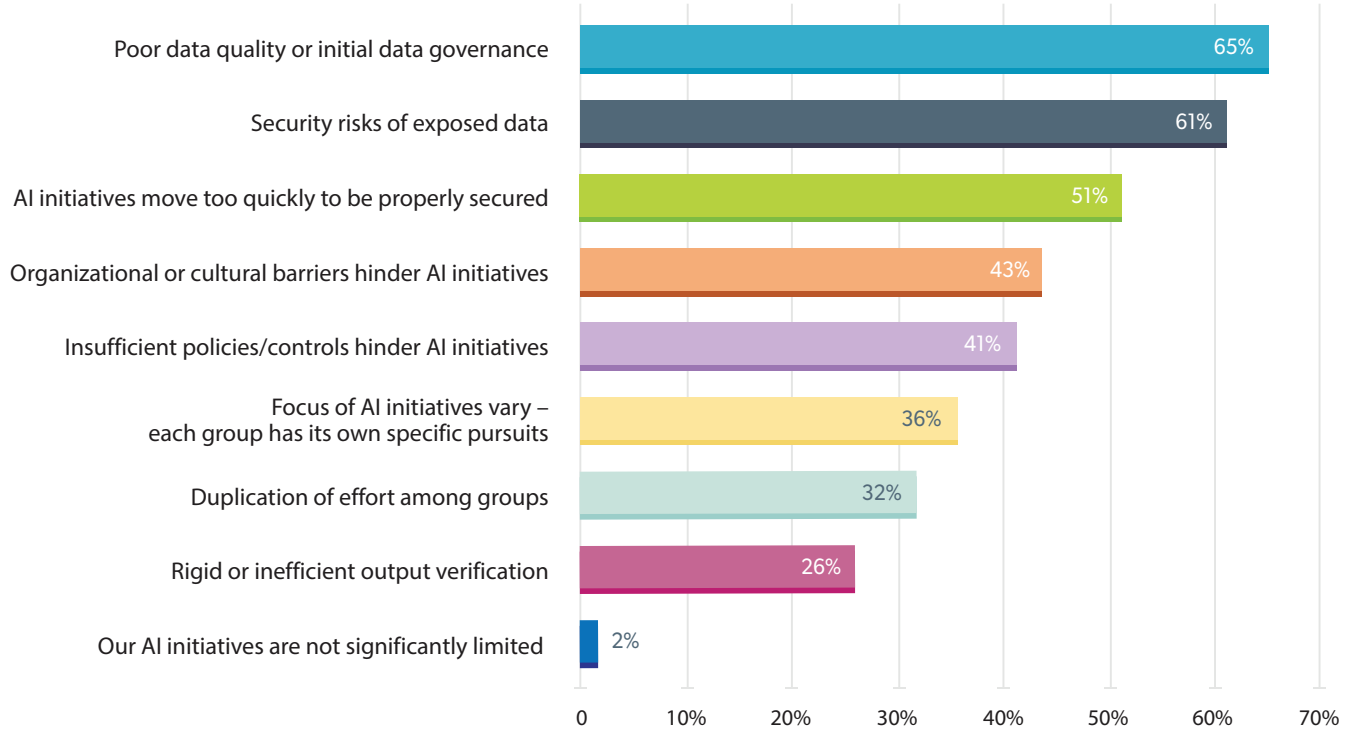
AI PROJECT SUCCESS FACTORS



That places a burden on security teams to ensure they understand what data is being used and how it is secured.

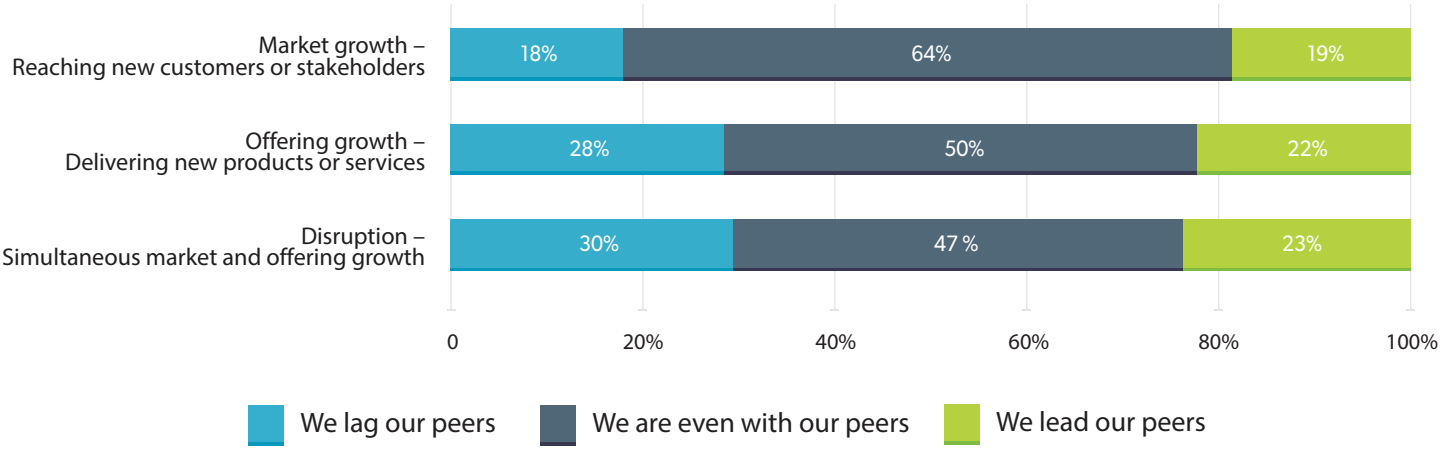
When we asked about AI project inhibitors, data came to the forefront. Respondents cited concerns about data quality and governance (65%) as the leading inhibitor, followed by risk of data exposure (61%). This illustrates the positive impact of effective data security in accelerating AI initiatives. Data classification and protection can reduce the risk of data exposure by helping organizations better understand the data used in AI projects. In two industries with long-standing regulatory imperatives for data management — financial services and pharmaceuticals — the results differ slightly. Among pharmaceutical organizations, data exposure risk (60%) narrowly leads data quality concerns (58%), while in financial services, the top two responses match the surveywide result, but with lower percentages (59% and 53%, respectively). This suggests that controls established to meet regulatory requirements may have eased data concerns in advancing AI projects.

AI ADOPTION INHIBITORS



Another key aspect the survey explored is relative competitiveness in AI. Respondents are reasonably upbeat, with less than a third saying they lag peers in using AI to drive market growth (18%), expand offerings (28%) or both (30%). The proportion self-classified as leading their peers is more consistent across the three categories (19%, 22% and 23%, respectively), while in each case the greatest share place themselves on par with their competitors. The ability to leverage AI as a competitive differentiator is growing in importance and can support greater operational efficiency in business and security operations.

CLOUD AND SECURITY PROVIDERS SUPPLY AI-PROTECTION TOOLS

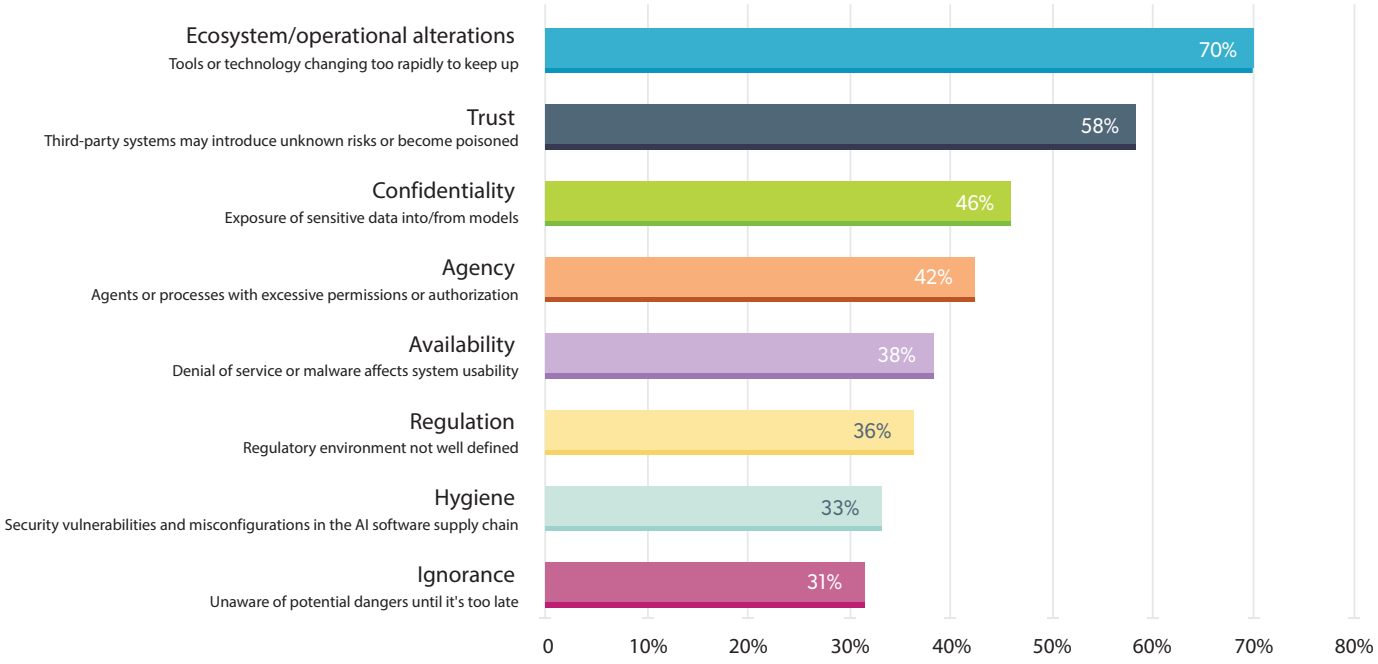


While improved data governance accelerates AI initiatives, tensions remain. Previous security strategies relied on known identities, applications and datasets working deterministically. In contrast, the pathways for AI to retrieve, augment, train and infer across different datasets are greatly variable; these pressures are described further in the next section.

Security pressures expand with AI and agentic operations

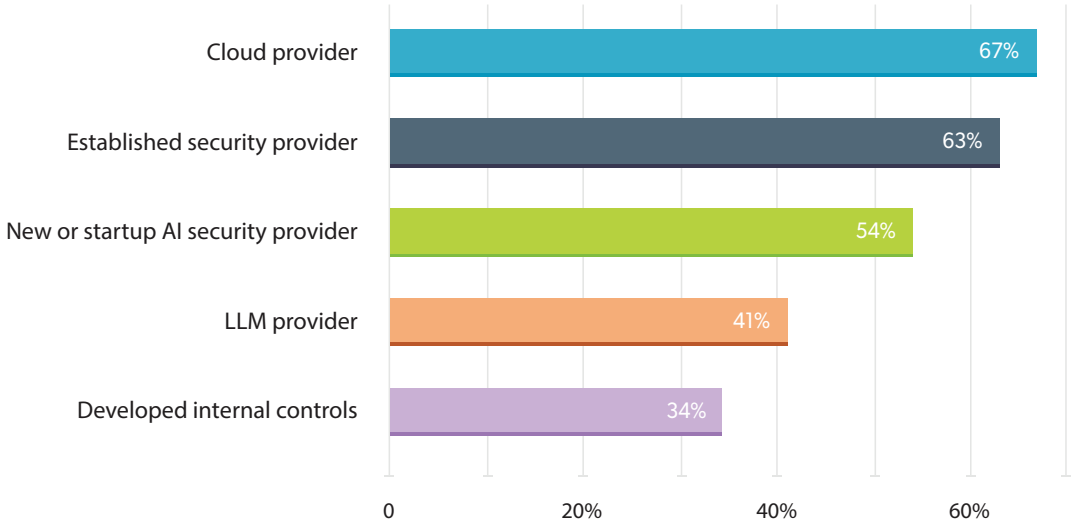
The rapid advent of agentic AI in organizations is drastically increasing the velocity and volume of data use. Rapid IT ecosystem changes driven by AI adoption and development are also amplifying risk: 70% of DTR respondents ranked this among their top three security concerns, placing it as the top concern overall.

MOST CONCERNING RISKS REGARDING THE SECURITY OF AI



Unsurprisingly, attackers are also rapidly adopting AI, leveraging fully automated attack tools that run at machine speed and scale, and forcing security teams to counter with scalable, machine-speed defenses. Complicating the situation is the tumultuous state of "AI for security" technologies, presenting organizations with myriad alternatives, including solutions from cloud providers, established security vendors, specialized security startups and large language model providers.

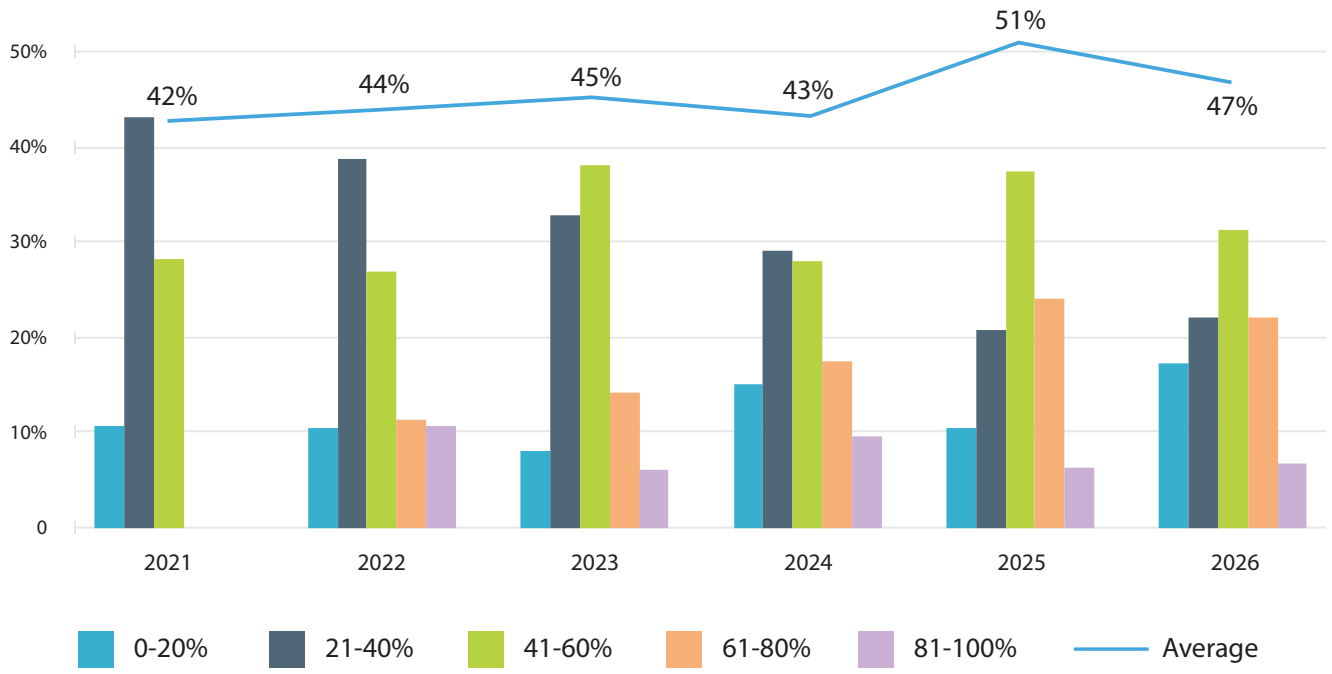
CLOUD AND SECURITY PROVIDERS SUPPLY AI-PROTECTION TOOLS



This also highlights the need for mature foundational security controls, including data discovery, classification and encryption. If organizations cannot find, classify and protect their sensitive data, attackers will readily find and exfiltrate it. This year's survey shows a slight drop in the average proportion of sensitive data encrypted: Only 7% of organizations reported that over 80% of their sensitive data is encrypted, and less than a third (29%) reported more than 60% encrypted.

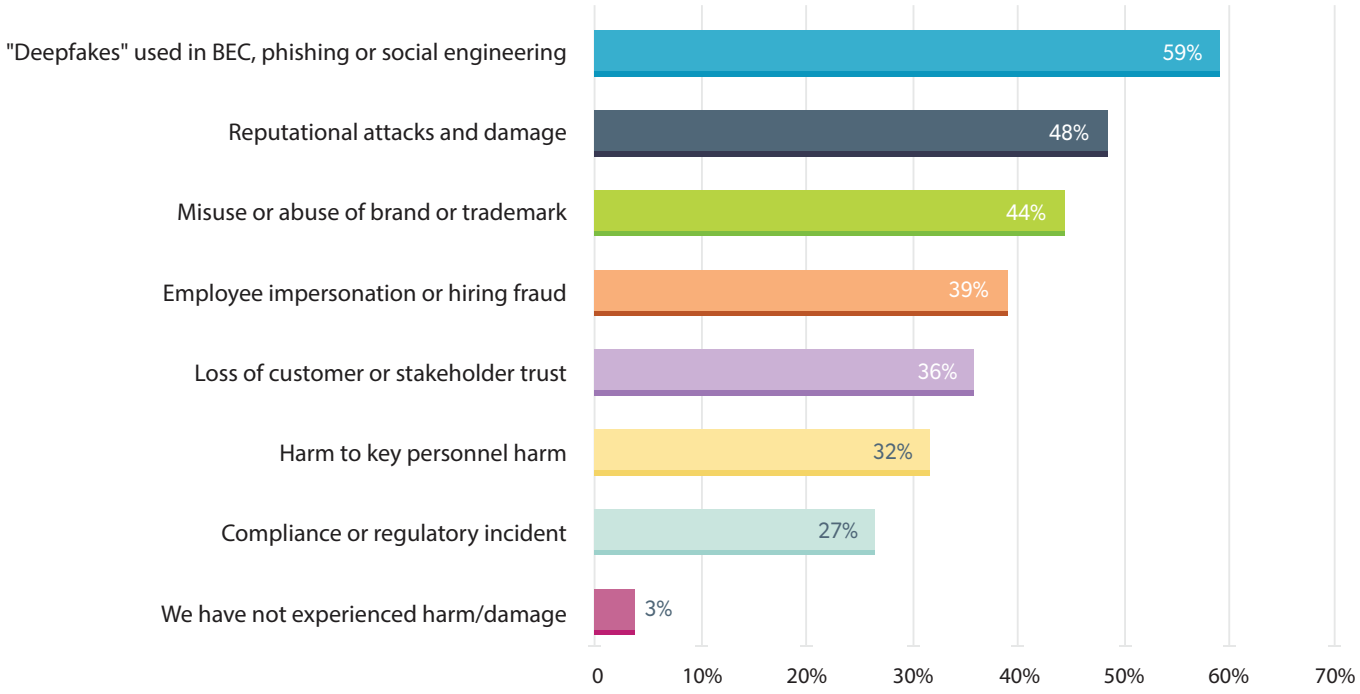
While the fast-moving ecosystem is cited as the greatest AI-driven security concern, it is worth noting the difficulty of ranking related, interdependent concerns. Excessive machine agency in IT systems may lead to greater data exposure. Growth in third-party connections and dependencies also multiplies potential avenues for data oversharing, and changing regulations may not clearly delineate how providers and operators should define their shared responsibilities. On the other hand, AI for security is already discovering new vulnerabilities and providing guidance for remediation. Anthropic's Mythos and Google Big Sleep are powerful examples of recently released tools.

PROPORTION OF SENSITIVE CLOUD DATA ENCRYPTED



Respondents reported organizational damage from a wide variety of AI-generated risks, and only 3% reported no resulting harm. Human error is again the top cause of data breaches, while AI-generated "deepfakes" are participants' top source of concern. Rapid advances in image, video and audio generation yield accurate facsimiles, created in minutes from minimal source data. Only a few seconds of audio or video can be used to create believable email, text messages, and video or audio. Deepfake detection technologies are also advancing, but in the meantime, security teams must rely on a combination of user education and technology such as behavioral anomaly detection to prevent deepfakes from causing harm at an unprecedented rate.

MOST COMMON SOURCES OF HARM FROM AI-GENERATED MISINFORMATION/DISINFORMATION



More recently, risks from AI-powered vulnerability discovery and exploitation have increased with the release of more powerful frontier models. Both Google Deep Sleep and Anthropic's Glasswing initiative have increased the rate and depth at which new vulnerabilities can be discovered and improved the ability to automate exploitation. These advances should be expected to continue, and this recognition reinforces the need for better data security protection. When applications and systems become easier to compromise, identity and data security become the last lines of defense.

When applications and systems become easier to compromise, identity and data security become the last lines of defense.

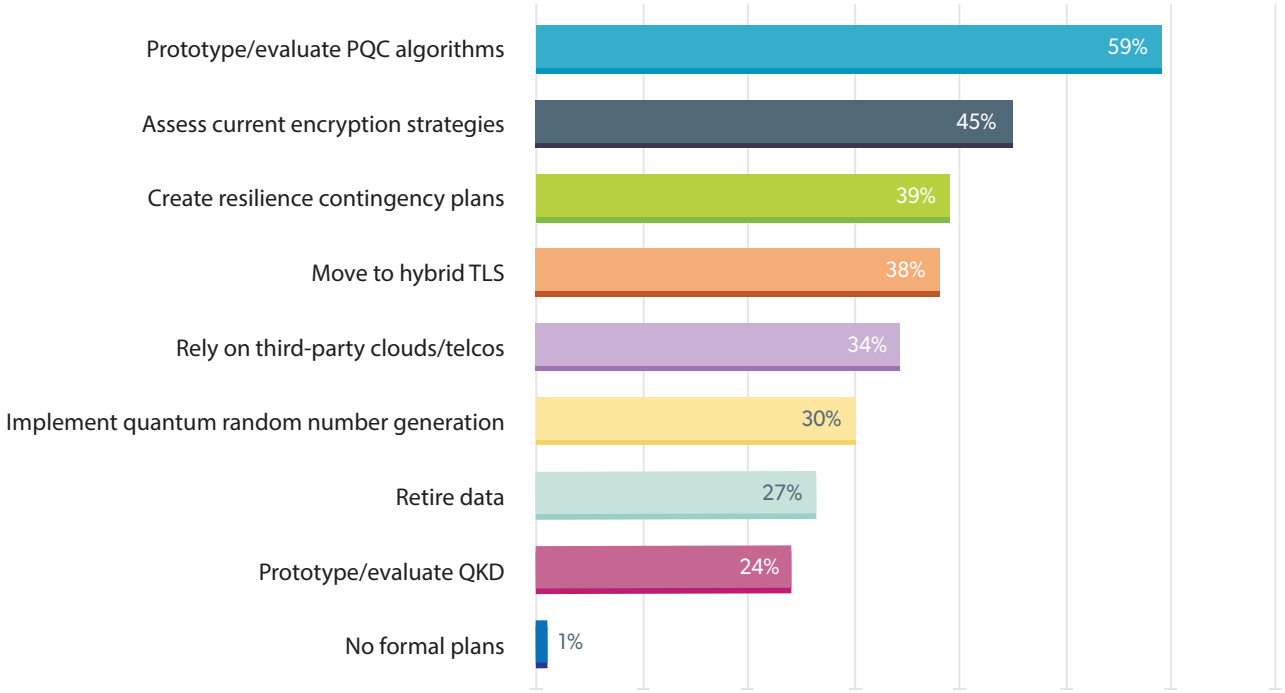
Quantum risk realities

The key promise of quantum computers is to solve difficult problems faster, cheaper or more efficiently than classical supercomputing methods. In some cases, quantum computers may solve problems that would be impractical to ever solve on classical computers. The survey explored plans to protect against quantum-driven risks and efforts to put quantum computing to work.

While classical computing solves problems sequentially, quantum computers can consider the state of a variable in dual or multiple conditions simultaneously, drastically reducing the amount of time required to solve previously unsolvable problems. Nondeterministic polynomial (NP) time problems in operations research and mathematics, such as the traveling salesperson problem, are well-suited to be solved on quantum computers. Quantum computing use cases will profoundly affect industries such as pharmaceuticals, materials science and finance. These same quantum capabilities can also be applied to attack the foundation of data security and identity: encryption. NP problems form the core of classical encryption, making public key cryptography algorithms such as RSA and ECC susceptible to quantum attacks. Public key cryptography underpins data confidentiality and authenticity for key exchange, identity, certificates, digital signing and trust chains. The ability to rapidly solve NP problems could effectively break many forms of encryption.

Recent improvements in qubit error correction and accuracy, in some instances augmented by AI, have also reduced the estimated resources required to build a relevant quantum computer, raising critical security concerns. A recently submitted, peer-reviewed **journal article**, written by researchers from the California Institute of Technology, University of California Berkeley and quantum computing company Oratomic, estimates that a system with as few as 10,000 qubits could be used to break 256-bit elliptic curve cryptography.

TOP PLANNED QUANTUM SECURITY MEASURES



This underscores the urgency to move from current encryption technologies to quantum-resistant ciphers and systems. More than half of respondents (59%) expect to prototype or evaluate post-quantum cryptography in the next 18 to 24 months. That is a positive first step, but with Q-Day anticipated by some as early as 2030, that leaves little time for implementation and deployment.

The survey dug deeper to gauge progress in five key areas of PQC adoption: public key infrastructure (PKI), certificate life-cycle management (CLM), enterprise key management (EKM), code signing and interoperability with broader IT ecosystems. Some of these efforts are showing significant progress. PKI, EKM and code signing have more than 50% on schedule or ahead of implementation plans. However, it is concerning that CLM is not at the same level of achievement. There are additional pressures on improving CLM processes, including certificate inventories, interrelated dependencies and shortened time durations. The CA/Browser Forum, a consortium of certificate authorities and browser developers, is in the process of dramatically reducing certificate lifetimes from over a year to 47 days by 2029. This should drive enterprises to improve their certificate management practices through automation, and it represents an opportunity to set the stage for PQC transitions.

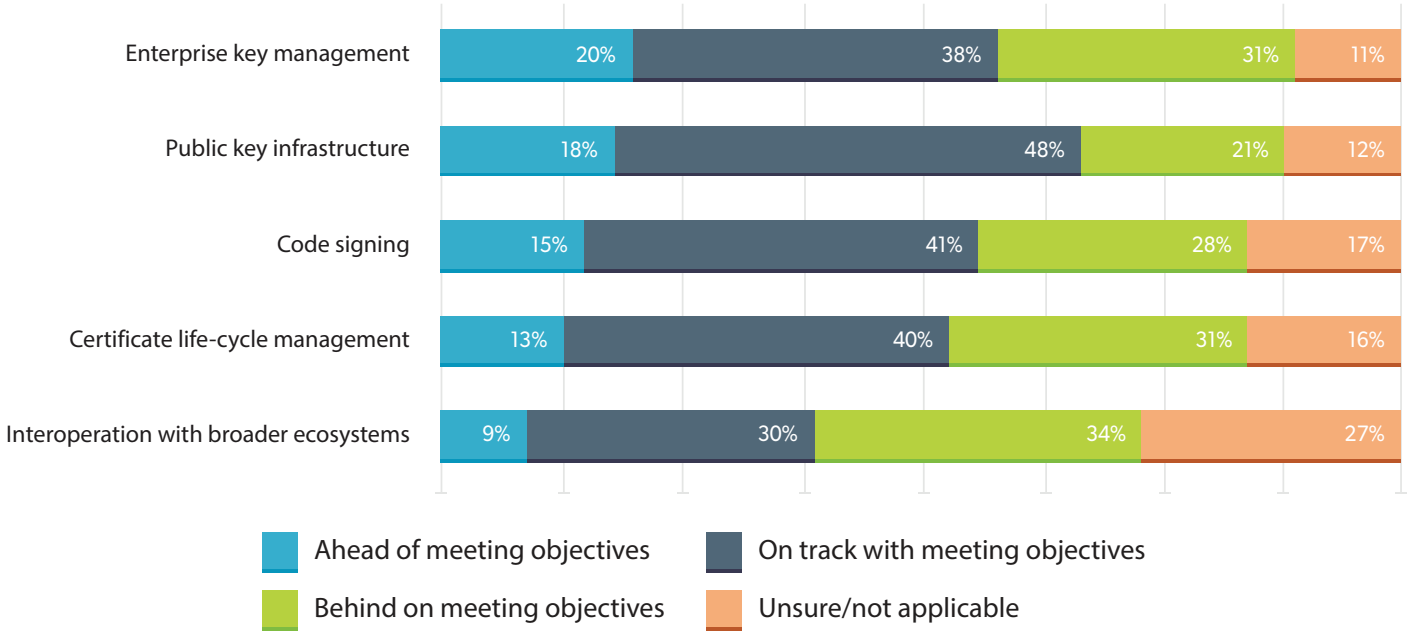
PQC transitions require deliberate, measured changes because susceptible algorithms such as ECC and RSA are built into computing infrastructure — networks, storage, cloud, identity and even code creation. An outcome of any successful PQC transition is to achieve a state of crypto-agility, meaning that enterprises can flexibly incorporate new quantum-resistant cryptography algorithms into infrastructure without jeopardizing operations or security. Crypto-agility could be likened to the ability to change out the door locks on a moving car.

New PQC algorithms cannot necessarily be adopted into existing components. Transport Layer Security (TLS) is used to encrypt a large proportion of internet traffic. More than 99% of internet traffic publicly accessed through major browsers such as Google Chrome is encrypted with TLS. Yet, older versions of TLS, such as TLS 1.2, are still required for certain network operations. Many load balancers, proxies and VPNs terminate TLS transmissions to inspect and direct network traffic based on the content. These disassembled TLS transmissions are then reassembled and re-encrypted for transmission to the recipient. Newer versions of TLS, such as TLS 1.3, incorporate forward secrecy so that any interruption or termination of a TLS transmission cannot be reassembled. PQC algorithms such as ML-KEM have key lengths that are larger than what TLS 1.2 can handle. In this scenario, any preexisting network service requiring or performing TLS 1.2 termination would not function with a PQC algorithm. Upgrading to TLS 1.3 would significantly change the way many load balancers, proxies and VPNs operate.

Similarly, there are challenges in authentication, identity and even building code. Three recent PQC algorithms proposed by the National Institute of Standards and Technology in 2022 involve digital signatures, reinforcing their importance. Existing authentication processes built on Kerberos or RADIUS are also susceptible. Yet these authentication processes may be deeply embedded in existing infrastructure, making PQC transitions even more brittle. In addition, the authenticity of code-signing processes may be susceptible to quantum attacks.

For developers and security leaders, changes to cryptography have taken a long time. The developer experience for OpenSSL, one of the leading cryptographic libraries, **is complex**, as it can be used for everything from stand-alone file encryption to creating new certificate authorities. According to the **2025 OWASP Top 10 list of web application security risks**, cryptographic failures remained at No. 4.

ORGANIZATIONAL PROGRESS IN MEETING PQC OBJECTIVES



While PQC raises a technically complex set of issues, the basic challenges remain for security leaders: to know what infrastructure, cloud or development processes are at risk, and to diligently plan for a transition that minimizes disruption while increasing flexibility, allowing enterprises to minimize risk and maximize rewards.

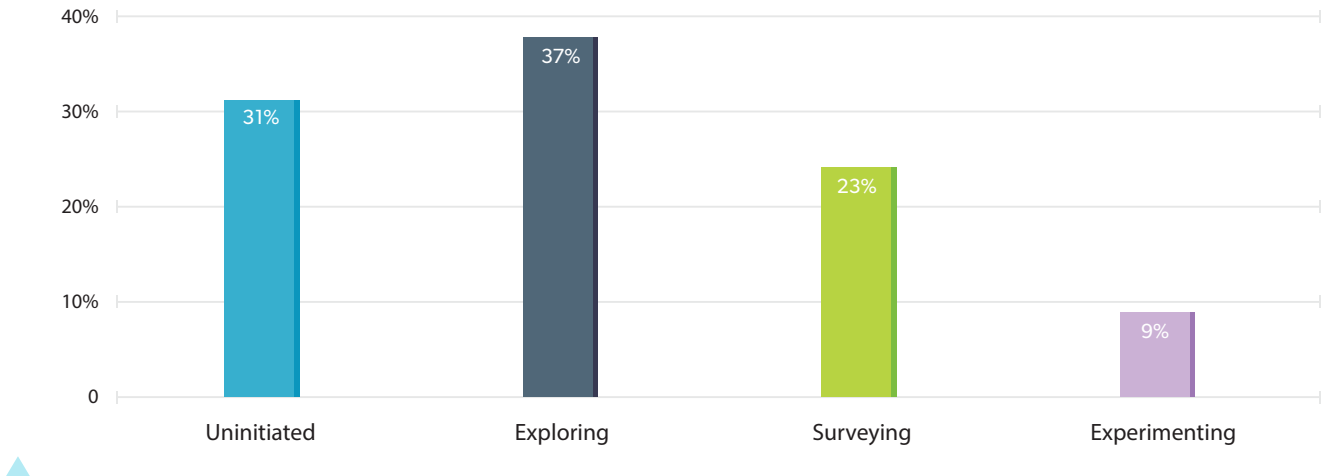
Notwithstanding the challenges of the transition to PQC, quantum computing offers major promise. Quantum computing will significantly change how enterprises operate, given the ability to solve entirely new classes of problems.

According to 451 Research's Voice of The Enterprise: Digital Pulse, Quantum Computing 2026 study, advances in quantum computing are expected to bring the following results:

- *36% of enterprises believe they will realize material value in 1-3 years.*
- *28% of additional enterprises believe they will realize material value in 3-5 years.*
- *52% said competitive advantage was number one factor for driving interest in quantum computing.*

Almost a third (32%) of quantum and AI survey respondents have started on their quantum journey, either experimenting with or surveying quantum computing applications. As we have pointed out, this segment of the survey population is also leading in AI and data security, another benefit of forward-looking security thinking.

QUANTUM PROGRESS



Cloud infrastructure under attack

Cloud security has been the top information security pain point in 451 Research's Voice of the Enterprise surveys every year since 2020. Given that many AI workloads run on public and private cloud infrastructure, securing these environments is a key concern. Attackers are focusing on cloud-based assets with an eye toward gaining access to the large volumes of data that reside there. AI training activity demands ever-larger datasets, and the rapid pace of AI infrastructure build-out may leave gaps susceptible to exploitation.

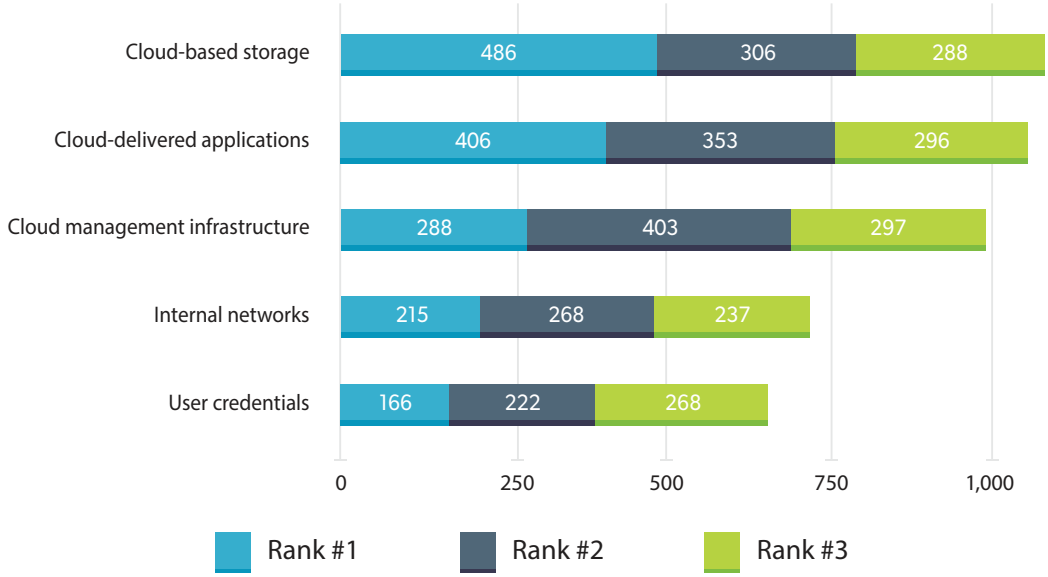
TOP INFORMATION SECURITY PAIN POINTS, 2020-2025

Year	No. 1	No. 2	No. 3
2025	Cloud Security	Data Privacy	Generative AI
2024	Cloud Security	AI/ML Implementation	Generative AI
2023	Cloud Security	Data Privacy	Threat Detection
2022	Cloud Security	User Behavior	Data Privacy
2021	Cloud Security	User Behavior	Changes in IT architecture (cloud, SaaS)
2020	User Behavior	Cloud Security	Visibility across the full IT architecture

Voice of the Enterprise: Information Security, Budgets & Outlook 2021-2025; Voice of the Enterprise: Information Security, Workloads & Key Projects 2020.
Source: 451 Research by S&P Global.

According to the 2026 Data Threat Report: Quantum and AI, the top three asset types targeted by attackers are cloud-related: cloud-based storage (35%), cloud-delivered applications (34%) and cloud management infrastructure (32%). Meanwhile, organizations struggle to recruit and retain cloud security talent: Cloud security is cited as the second most pressing security discipline after identity and access management (IAM). The issue is further complicated by IAM coverage having to span multiple cloud providers: Most organizations are multicloud, with an average of 2.3 cloud providers in use, and 39% use more than three. Combine these challenges with the automation and speed of AI-driven attacks, and defenders must not only respond with equal speed, but they must also have a thorough understanding of data location and classification. Given that much AI infrastructure is deployed via containers in cloud-based venues, it is unsurprising that two-thirds of respondents reported investing in their cloud provider's AI-specific security tool.

TOP TARGETS FOR CYBERATTACKS



Given that many AI workloads run on public and private cloud infrastructure, securing these environments is a key concern.

Data sovereignty, quantum and AI risks

Data sovereignty concerns take on new significance in the face of quantum computing and AI risks. AI's appetite for data, coupled with the challenges of meeting computing demands, adds pressure to the process of establishing sovereign infrastructure. The addition of agents dramatically increases data exposure risk as it becomes more complicated to manage and control data movement. Meanwhile, AI data collection, training and inference occur at different locations and under varying circumstances.

Two elements of the survey results offer particularly important insights about sovereignty initiatives. First, the primary cited driver for sovereignty initiatives is to establish full control over software and data to achieve portability. More than a third of respondents prioritize this factor, significantly ahead of the second choice, regulatory compliance. Portability brings specific benefits for AI applications, where access to the latest models or training environments may be critical to maximize returns.

The second key aspect concerns how sovereignty is achieved. While physical location is the traditional path to sovereignty, the leading choice in the results is cryptographic: The greatest proportion of respondents said encryption and key management would give them sufficient protection for their sovereignty goals (36%). This reinforces the importance of encryption for data security, even though implementation levels still leave room for improvement. Various levels of sovereignty are achieved by differing levels of control, with strong data encryption as a foundation. For example, full digital sovereignty also involves ensuring that data can be accessed by open-source equivalents to commercial software and platforms.

Portability and encryption considerations are increasingly relevant since AI frontier models, inference locations and training data collection venues may be highly distributed. This is also an area where quantum computing risks come into play. Is the current focus well-founded in a post-quantum world? To achieve the level of trust needed for sovereign protection, quantum-resistant protection will need to be in place. This is one more reason for enterprises to prioritize PQC deployments.

To achieve the level of trust needed for sovereign protection, quantum-resistant protection will need to be in place.

Conclusions

Sovereignty, AI and PQC crypto-agility require increased flexibility. Ultimately, strong controls governing AI, quantum computing and sovereignty initiatives will enable leading enterprises to minimize opportunity costs from investing in any single new technology. As more enterprises realize gains from quantum computing and AI, both leaders and laggards will have chances to build or rebuild competitive leads.

While the implementation timelines for quantum computing and AI technologies differ, the risks they pose are immediate and should motivate organizations to act today to mitigate their impacts. If organizations want to spare their security teams the kind of unwelcome surprises that arose with the rapid adoption of AI, they must understand quantum risks and take proactive steps to prepare for when those threats arrive.

Organizations are already spending on AI-specific security measures, but these must be accompanied by broader data protection efforts. Many of the data protection mitigations needed for AI can also aid in preparing for quantum threats. With the gaps in data classification, many enterprises cannot be sure that necessary protections are optimally placed. Actions must address both quantum and AI risks:

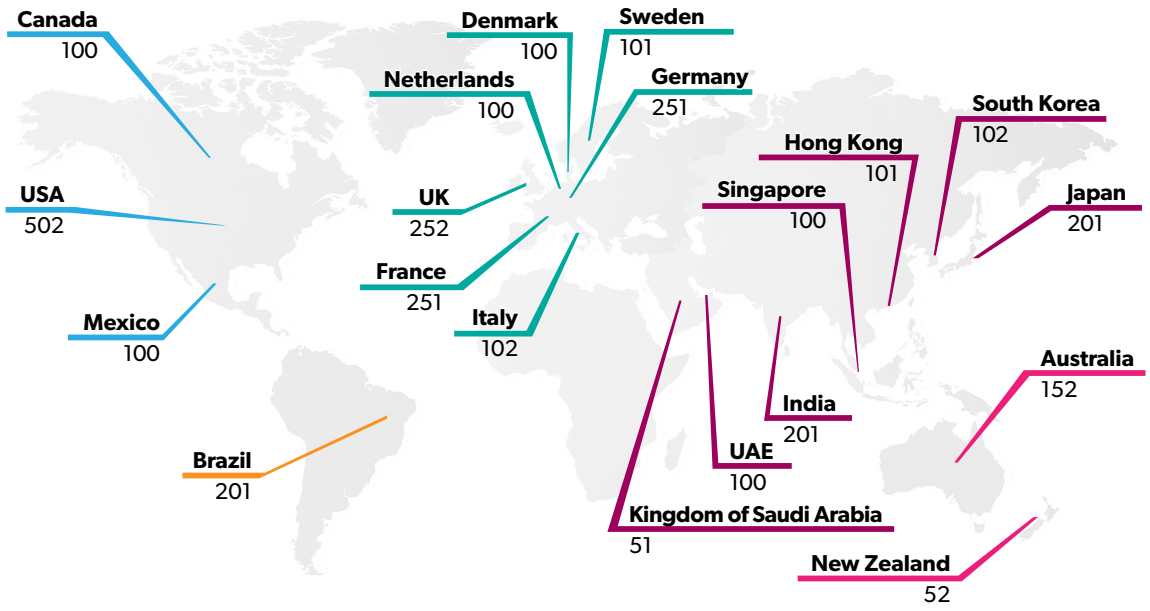
- Data discovery and classification must be more effective.
- Security management must deliver a unified set of controls that can operate at AI speed and span the hybrid nature of modern infrastructure.
- Post-quantum cryptographic ciphers and protocol deployments must accelerate.
- Security tooling and operations must be simplified, and PQC updates present an opportunity.

There are encouraging signs for security teams. The potential benefits of quantum computing and GenAI for enterprises also represent opportunities to advance security and trust. For AI and quantum leaders, opportunities to innovate faster are increasingly within reach. For laggards, these benefits should provide ample motivation to work toward becoming a leader. Business agility has never been more essential or more rewarding; amid the ongoing change, strong data stewardship can provide a solid foundation as technology shifts across cloud, AI, digital sovereignty and quantum computing platforms.

What we understand about quantum and AI risks today represents only the first stage of their impacts. However, by implementing approaches that enable greater scalability and flexibility, efforts to address the full range of today's security challenges can help to establish resilient and responsive security infrastructure for the future.

Methodology

This research was based on a global survey of 3,120 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million and with US$100 million-$250 million in selected countries. This research was conducted as an observational study and makes no causal claims.



Revenue	Number of Respondents
$100m to $249.9m	213
$250m to $499.9m	701
$500m to $749.9m	799
$750m to $999.9m	774
$1 Bn to $1.49 Bn	265
$1.5 Bn to $1.99 Bn	137
$2 Bn or more	231
Total	3,120

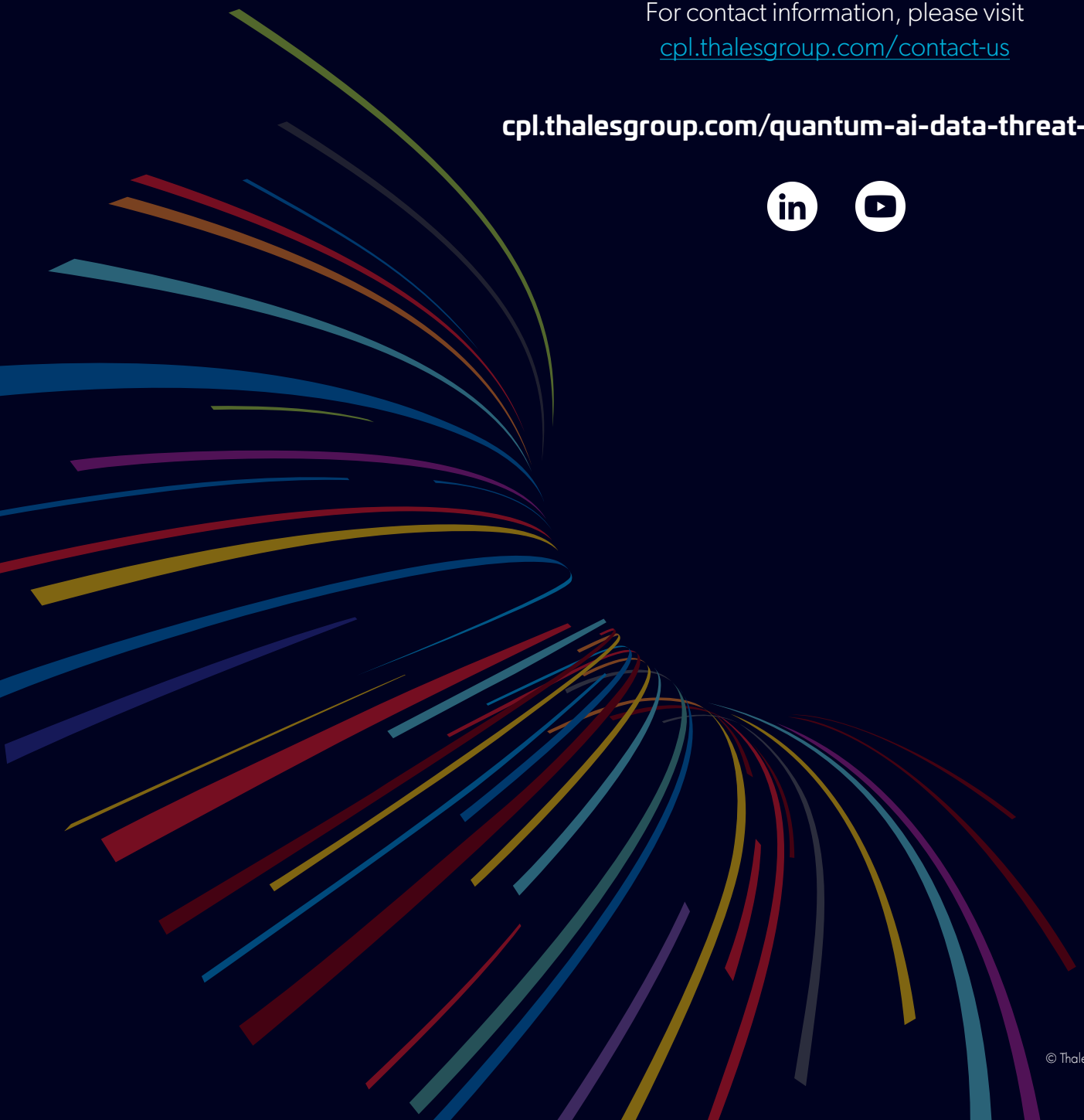
Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Healthcare	263	Travel / Hospitality	181
Retail	255	eCommerce	171
Manufacturing	251	Automotive	166
Financial Services	237	Education	141
Technology	222	Biotechnology	124
Energy & Utilities	213	Defense	115
Government	207	Aerospace	80
Transportation	189	Telecommunications	79
Pharmaceuticals	187	Other	28
Total			3,120

THALES

CYBERSECURITY

For contact information, please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/quantum-ai-data-threat-report



© Thales - July 2026 • GHv5