Global Edition

THALES
Building a future we can all trust

2024 DATA THREAT REPORT

Navigating New Threats and Overcoming Old Challenges

#2024DataThreatReport

cpl.thalesgroup.com

Table of Contents

Introduction

As economic uncertainty continues and the threat landscape grows more complex, enterprises are working to address increasing regulatory mandates while improving their security posture. The **2024 Thales Global Data Threat Report (DTR)** offers insights into new technologies, their security implications and the organizational changes for success ahead. The report analyzes global trends in threats to data and the underlying controls, regulations, risks and emerging technologies that need to be addressed. The report reflects insights from nearly 3,000 respondents at the individual contributor, managerial and executive levels from 18 countries across 37 industries and explores their data security experiences, challenges, strategies and outcomes.

S&P Global
Market Intelligence

Source: 2024 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

edvance value added distributor

EXCLUSIVE NETWORKS

netpoleon Network · Security

Securing Opportunities Ahead

The 2024 Data Threat Report (DTR) analyzes how core security practices have changed in response to or in anticipation of changing threats. This report also offers perspectives on what organizations can do to leverage data assets to expand opportunities to make their businesses more agile and build trust with their customers.

The diversity of internal and external stakeholders indicates that security initiatives must consider those parties that interpret, implement and live by policies, rules and controls. These initiatives span various contexts and may have multiple motivations, such as securing cloud environments to scale capacity or ensuring compliance with regulatory and data sovereignty requirements. This report offers perspectives on what is taking place and what is possible in regards to these challenges.

Market uncertainty, new regulatory requirements, and geopolitical tensions have added further stresses to what has always been a complex endeavor. In July 2023, the U.S. Securities & Exchange Commission announced rules requiring registrants, including both U.S. and foreign private issuers, to disclose material security events. In the same month, the EU adopted the EU-US Data Privacy Framework (DPF). The DPF faces similar EU legal challenges as its predecessors Privacy Shield Framework (2015) and US-EU Safe Harbor Framework (2000), adding greater uncertainty for enterprises.

Increases in threats and shifts in threat types have motivated these regulations. According to the findings in the 2024 DTR, the vast majority (93%) of enterprises reported an increase in threats. They identified malware, phishing and ransomware as the fastest growing attacks, respectively chosen by 41%, 36% and 32% of respondents, and they reported cloud assets such as SaaS applications, cloud-based storage, and cloud infrastructure management as the biggest targets for attack. Human factors are still a major cause of cloud data breaches, with user error as the leading cause at 31% and failure to apply multi-factor authentication (MFA) to privileged accounts also a significant factor at 17%.

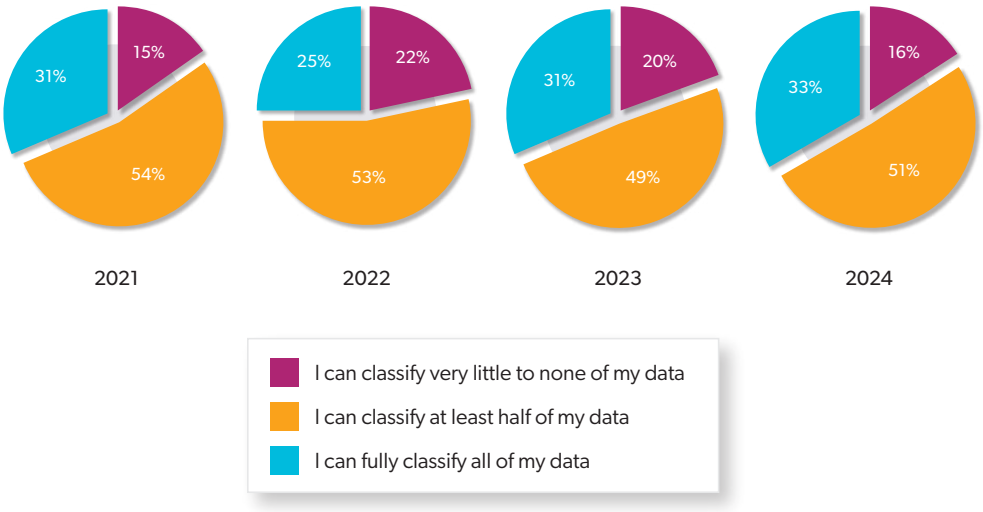
This year's report looks closely at these human factors by considering both workforce identity and access management (workforce IAM) and customer identity and access management (CIAM).

Because of these challenges, information security spending remains strong: 93% of respondents are increasing their budgets, according to 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2023.

Recent innovations in quantum computing, cloud computing, external user experience (UX), and generative artificial intelligence (GenAI) have captured the industry's imagination. This report considers both securing the use of GenAI and using GenAI to better secure the enterprise. Differing priorities from different functional leaders and external stakeholders will require security and risk management leaders to build stronger relationships.

While enterprises further pursue these new technologies, data security hygiene challenges are a barrier to better adoption.

Classification Issues Persist



Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

KEY STATISTIC

For the last 4 years, at least 1 in 6 enterprise respondents said that they have been able to classify very little or no data.

1 in 6

Fundamental understanding of what systems, applications and data are at risk from changing regulatory and threat landscapes continues to lag. For the last four years, at least one in six enterprise respondents said that they have been able to classify very little or no data. While sensitive data discovery and classification is the top-cited security technology that managers plan to implement in the next 12 months, according to 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2023 report, enterprises will need to improve their standing to better adopt new technologies in 5G/IoT and cloud among sovereign and external stakeholders.

This year's study also examines how and why technologies are chosen. These insights can better guide enterprises toward successful and secure adoption.

Key Findings

Data Breach Trends and Threats

49%

49% of organizations reported being breached sometime in their history, but recent breach history has decreased from 24% in 2021 to 15% in 2024.

28%

Ransomware attacks are more common, with 28% experiencing an attack (up from 22% last year), but planning is still poor, with only 21% saying they would follow a formal plan in the event of an attack.

Human factors are still a major cause of cloud data breaches; human error was the leading cause with 31%, and failure to apply MFA to privileged accounts constituted another 17%.

31%

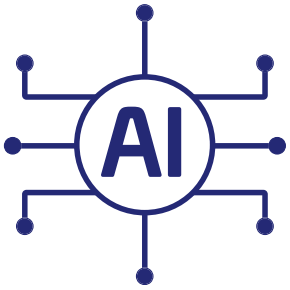
Multicloud growth is flattening, but financial services firms are now slightly more multicloud (2.03 cloud providers on average) than the average enterprise survey-wide (2.02 cloud providers).

Risks to Emerging Technologies

Prototyping post-quantum cryptography (PQC) is said to be the primary approach (52%) to address the future compromise of classical encryption techniques. "Harvest now, decrypt later" attacks (68%) are leading interest in PQC.

68%

The generative AI boom is underway: 22% plan to integrate GenAI into products/services in the next 12 months, and 33% are going to experiment with integrating the technology.



Security of data over 5G networks was the number one concern for nearly two-thirds (65%).

65%

Compliance and Sovereignty Concerns

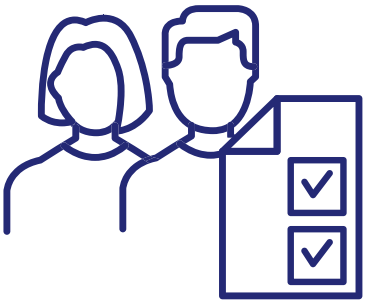
70%

Almost 70% of enterprises are able to classify only 50% or less of their sensitive data.

39%

Thirty-nine percent of all respondents said that **data residency would no longer be an issue** provided that external encryption, key management and separation of duties were implemented.

Identity Complexities and Compromise



16%

The **breadth of external customer identities accessing enterprise networks is high;** on average, one-sixth (16%) of all access is by customers.

62%

Achieving security consistency within CIAM initiatives was the number one cited challenge (62%).

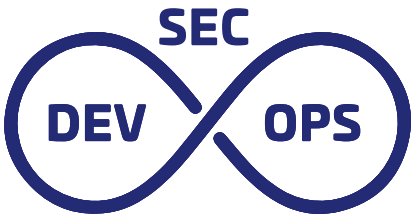
Increasing DevOps Challenges

56%

Secrets Management (56%) is the number one DevOps challenge, followed closely by workforce IAM challenges such as privileged user management (52%).

Over half (53%) have implemented a **formal security champions program** as part of a DevSecOps program.

53%



Operational complexity remains a security concern. While the number of respondents reporting five or more key management systems is down (53% versus 62% last year), the average number declined only slightly (from 5.6 to 5.4 key management systems).

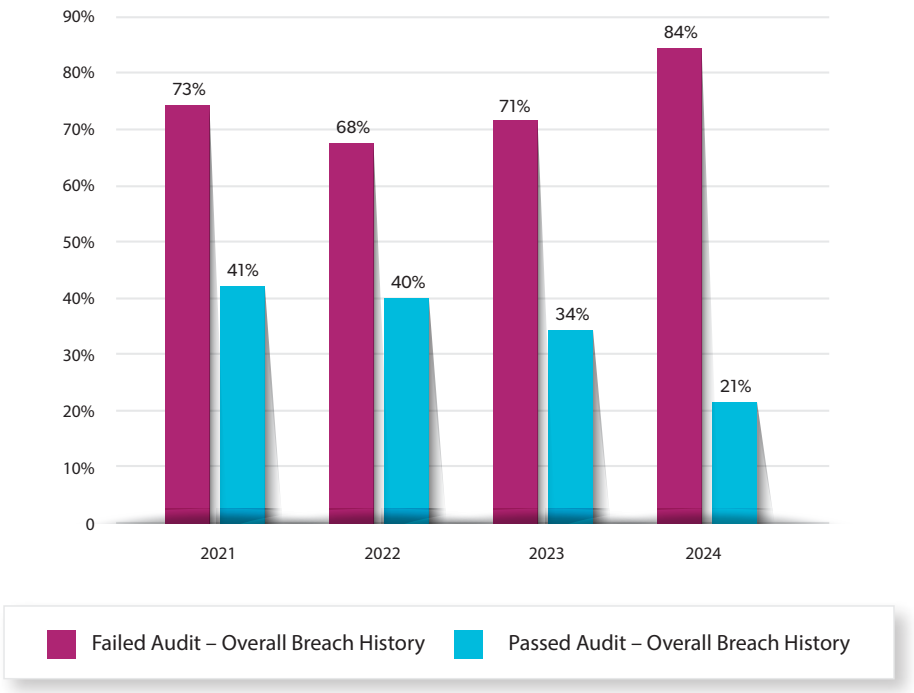
5.4

Enterprise Observations

This year's DTR provides additional insights into the internal enterprise organization. The need for data security as a discipline remains diffused throughout the enterprise. Functions such as compliance, go-to-market, supply chain and design all incorporate data security.

Security and compliance initiatives are converging as the two come together on inputs, processes and outcomes. Through the years, DTR findings have shown a stronger correlation between compliance achievement and reduced breaches. In 2024, of the respondents whose organizations failed a compliance audit, 84% reported having some breach in their history, with 31% saying they experienced a breach in the last 12 months. In contrast, for those that passed compliance audits, only 21% have a breach history and only 3% suffered a breach in the last 12 months.

Correlation – Compliance and Security Outcomes



Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

KEY STATISTIC

In 2024, of the respondents whose organizations failed a compliance audit, 84% reported having some breach history, with 31% saying they experienced a breach in the last 12 months.

84%

KEY STATISTIC

In contrast, for those that passed compliance audits, only 21% have a breach history and only 3% suffered a breach in the last 12 months.

21%

Compliance is arguably different than security, but many of the same techniques achieve beneficial outcomes in both. Regulatory oversight merges the distinctions between compliance and security diligence. Increasingly, compliance standards such as AICPA SOC2 Type 2 or ISO27K require that organizations demonstrate controls over time rather than at a single point in time. Automation will continue to drive improvement in this area. Among respondents prioritizing DevSecOps, 38% said that their configuration, compliance, and security controls were built into code. This report shares further insights on enabling developers and operators to achieve better security and service outcomes.

This year's key theme encourages security leaders to build stronger relationships by reconciling differences among internal and external enterprise stakeholders. Customers, developers and lines of business look to expand trustworthiness across new technologies and arenas such as GenAI, fintech, PQC, 5G and IoT. Study data shows progress is being made; greater demands and opportunities lie ahead. Internal pressures to manage costs conflict with efforts to mitigate attacks from more capable adversaries. Trust, safety, confidentiality, and privacy are now major factors in a business's brand, and security leaders can use the report insights to build stronger alliances across their organizations to achieve a more proactive, dynamic risk-based approach to security management.

38%

Among respondents prioritizing DevSecOps, 38% said that their configuration, compliance and security controls were built into code.

KEY STATISTIC

The Threat Landscape

The attack landscape remains vast and is growing: **93% of respondents said they experienced an increase in attacks, with malware, ransomware and phishing consistently being the largest growth categories for attacks.**

Top Threat Actors

	2021	2022	2023	2024
#1 Threat Actor	Malicious insiders	Human error	Human error	External attackers — hacktivists
#2 Threat Actor	Human error	External attackers — hacktivists	External attackers — hacktivists	Human error
#3 Threat Actor	External attackers	External attackers — nation-state actors	External attackers — nation-state actors	External attackers — nation-state actors

Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

Increasing Attack Types

	2021	2022	2023	2024
#1 Threat Source	Malware	Malware	Malware	Malware
#2 Threat Source	Ransomware	Ransomware	Ransomware	Ransomware
#3 Threat Source	Phishing	Phishing	Phishing	Phishing

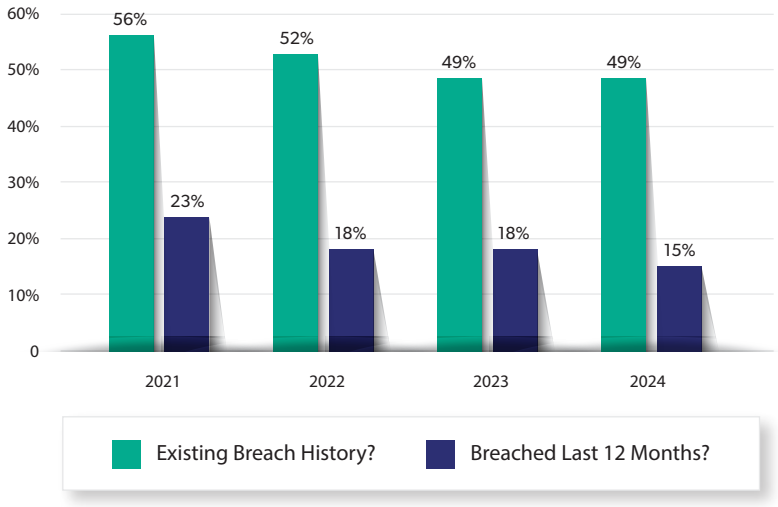
Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

Ransomware response remains a challenge. **For the last three years, less than 50% of respondents across all verticals and company sizes have a formal ransomware plan.** Overall, one in five respondents said that, in the event of a ransomware attack, they paid or would pay the ransom. Initial breach response is increasingly led by legal teams interfacing with regulators or law enforcement.

While some aspects of ransomware response have separate technical requirements, such as forensic isolation, continuous reliability and performance remain paramount concerns. Mutual beneficial opportunities in planning for incidents and responding to unplanned outages exist for both security practitioners and site reliability engineers (SRE). For security teams, partnering with SREs during the general design/architecture review process offers the chance to integrate security design. Explicit guidance, enablement and advice allow for SREs to definitively and proactively build in security best practices.

Overall Breach History and Recent Breach History

Trending down, but still high



Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

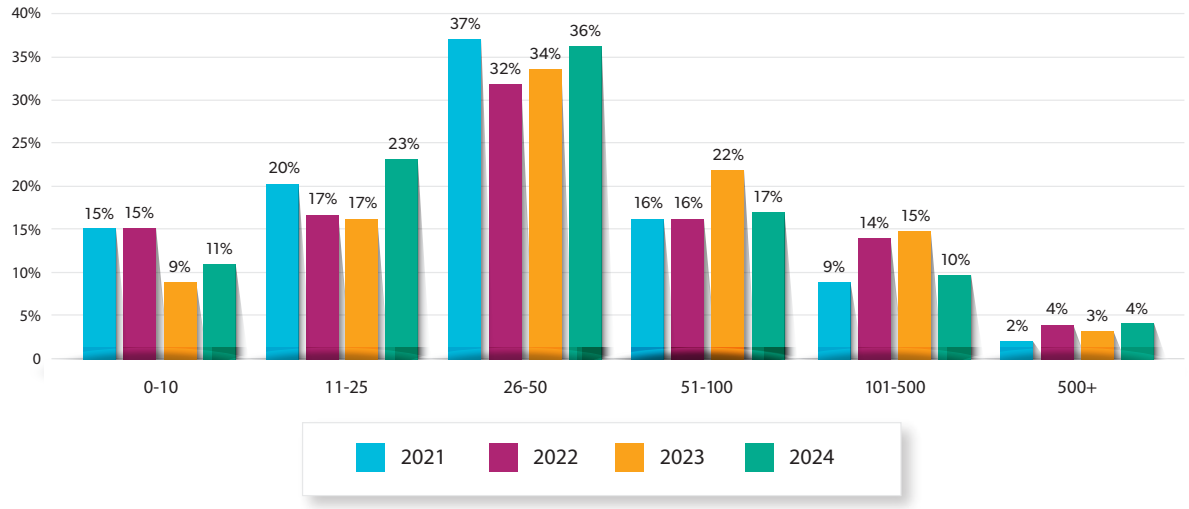
The complexity of cloud resources present among users, operators, and developers continues to grow. The percentage of enterprises saying they have 50 or more SaaS apps in use has grown from 27% in 2021 to more than 40% in the 2024 survey. The survey-wide average is now 84 SaaS applications in use. The percentage of enterprises that agree or strongly agree that managing security in the cloud is more complex than on-premises has consistently grown from 46% in 2021 to 55% in 2024 survey.

KEY STATISTIC

The percentage of enterprises saying they have 50 or more SaaS apps in use has grown from 27% in 2021 to more than 40% in the 2024 survey. The survey-wide average is now 84 SaaS applications.

84

Number of Enterprise SaaS Apps Used



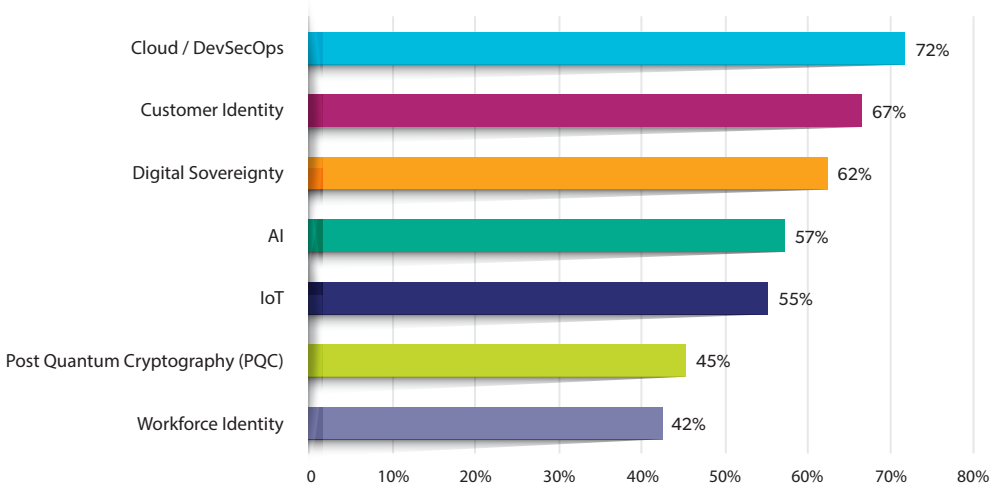
Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

When characterizing threat actors, internal human error remains a critical threat area, always ranking highly, if not the top category. In 2024, 22% of respondents said that human error was the single most concerning threat, and 74% of respondents placed some level of priority on threats from human error. The industry must continue redirecting its efforts to more secure and user-friendly approaches.

Innovations in cloud automation, developer experience, CIAM and workforce IAM reduce human errors and downstream consequences. Malicious adversaries are not only increasing the number of attacks but are also exhibiting growing sophistication in combining techniques. The ecosystems of ransomware creators, access brokers and criminal operators continue to evolve and adapt. While UX improves with new CIAM improvements such as passkeys and password deprecation, new challenges will arise such as deepfake attacks from generative AI. Simplifying this complexity reduces the missteps that adversaries can take advantage of and improves usability and engagement.

This year's DTR survey asked respondents to select their top four sources of security concerns among emerging technologies including cloud and DevSecOps, AI, Workforce IAM, IoT/5G, PQC and digital sovereignty. The results reflect broad concern in all emerging areas.

Greatest Sources of Concern for Security Programs



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

The 2024 DTR also examines why respondents are concerned and how they will address those concerns. In each of the following sections, the report shares insights on specific areas of emerging concern.

Developing Customer Trust - CIAM

For enterprises, safeguarding external users is essential for building trust with their customers. Enterprises must secure their data to meet consumer expectations of privacy and security.

According to the 2024 Thales Consumer Digital Trust Index Report, most customers (89%) are willing to share their data with organizations, but that comes with some non-negotiable caveats. More than four in five (87%) expect some level of privacy rights from the companies they interact with online.

In addition to high consumer expectations of privacy, DTR respondents reported that significant number of customers access their organization's internal systems or assets. **Respondents said up to 16% of those who access corporate cloud, network and device resources could be customers.** Similarly, external vendor and contractor access accounted for an average of 15% and 12% of users, respectively. With high consumer expectations of privacy and significant amounts of external user access, CIAM emerges as one of the top security priorities.

Broad Array of Personas Accessing Resources

Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

Respondents reflected in multiple ways on the diversity and volume of customers, external contractors, partners and vendors accessing corporate systems, and the resulting effects on security complexity. This year's study permitted write-in responses; two interesting responses to the prompt "Describe your specific CIAM challenges" addressed the complexity of trusting external users in the context of the organization's broader needs:

> **We have challenges adapting to changes in user consent dynamically."**
>
> – U.S., senior level, controller/CFO, federal government agency/dept, US$1.5B-US$2.0B revenue

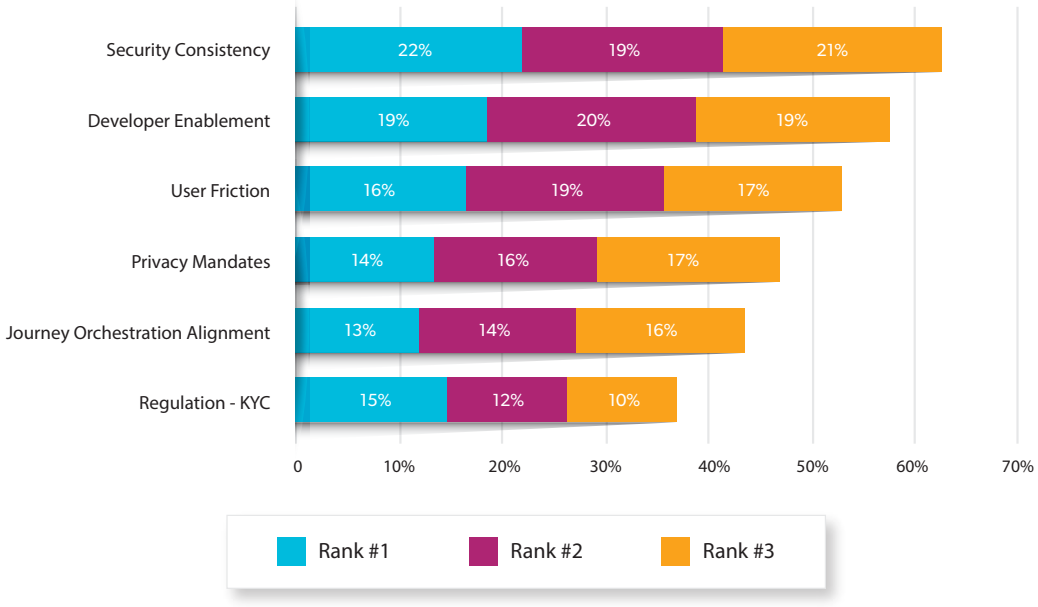
> **We have challenges managing data ownership responsibilities for external identities."**
>
> – Singapore, manager level, director, biotechnology industry, US$750M-US$1.0B revenue

Overall, security consistency was the greatest challenge, cited by 62% of respondents. The range of challenges to securely onboard external identities also matches the range of stakeholder involvement needed for successful CIAM initiatives. User friction, journey orchestration, privacy, anti-fraud know your customer (KYC), and developer experience challenges all reflect different stakeholders in UX, legal and development.

These CIAM challenges are compounding; high user friction or poor user experience makes identity verification (IDV) and KYC fulfillment more difficult. New threats such as GenAI deepfakes add new challenges to KYC, know your third party (KY3P) and IDV processes, and these threats further strain external identity management trust models based on user reputation rather than real-life identity. Challenging developer enablement leads to security inconsistencies. For example, inconsistent and arbitrary password complexity rules give a false sense of security while increasing user friction.

Given the compounding nature of CIAM challenges, security teams should look to enable improved developer experiences.

Challenges with Securely Onboarding Customer Identities



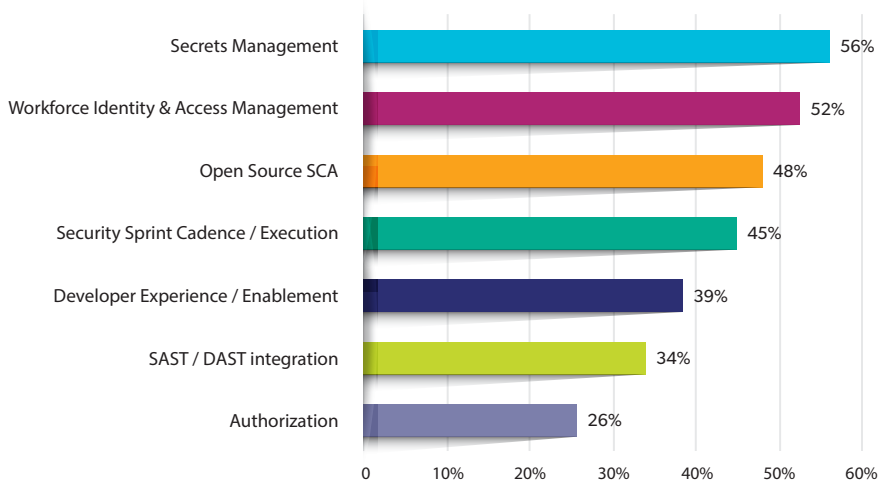
Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

Developer Journey - Cloud and DevOps

Given the trend toward building in external trustworthiness, DTR respondents also shared their insights for building in cloud and DevOps environments. The need for security to be flexibly integrated into digital product or service design has never been higher, given the adoption of new technologies. **This year, two-thirds of DTR respondents prioritized DevSecOps and cloud as their greatest emerging security concern.** Their insights revealed successes and areas for improvement.

Among emerging concerns, secrets management (56%) was the top challenge. Close behind was workforce IAM at 52%. Curiously, authorization (26%) was last on the list.

Top-cited Security Challenges in DevOps



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

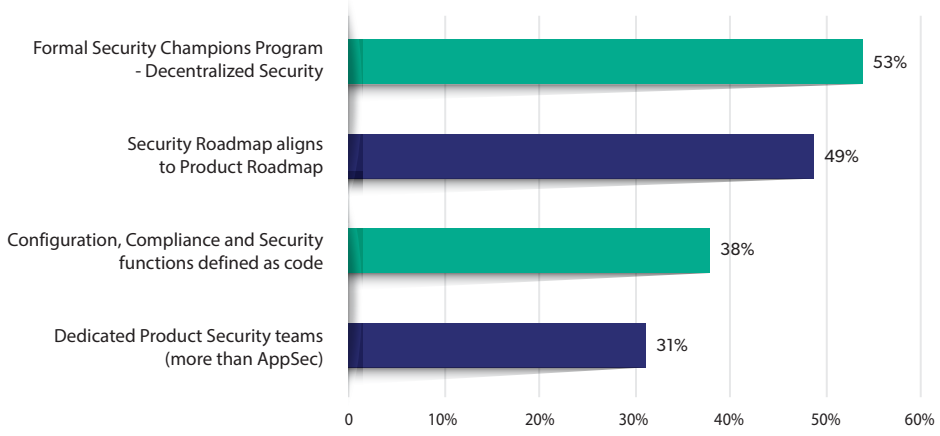
For developers, these three challenges are related. Secrets management, authorization, and workforce IAM are all interrelated tasks and disciplines for both privileged operators and the workload life cycle they manage. Tools and techniques that enable developers to proactively define and implement these controls maximize security and software publishing efficacy.

The difficulty with secrets is that they are frequently "bearer"-focused — that is, "bearer tokens" grant access to whoever bears or possesses, the token. When secrets are lost — written as cleartext environment variables in code, for example — consequences can be severe. Lost secrets such as signing keys used to authenticate downstream communications can have devastating consequences. If attackers can get a secret, they do not need to worry about impersonating an internal user.

As organizations mature their DevSecOps practices, dedicated security engineering and security champions will improve overall engineering performance in terms of quality and resilience.

As part of the process of gauging developer enablement, respondents characterized the maturity of their DevSecOps practices. Just more than half of all respondents reported having a formal security champions program. Successful security champions programs are proactive efforts at developer enablement. Providing clear, concrete, and repeatable security guidance for developers and operators is critical as security champions are frequently part of the development team, with only "dotted line" reporting to central security teams.

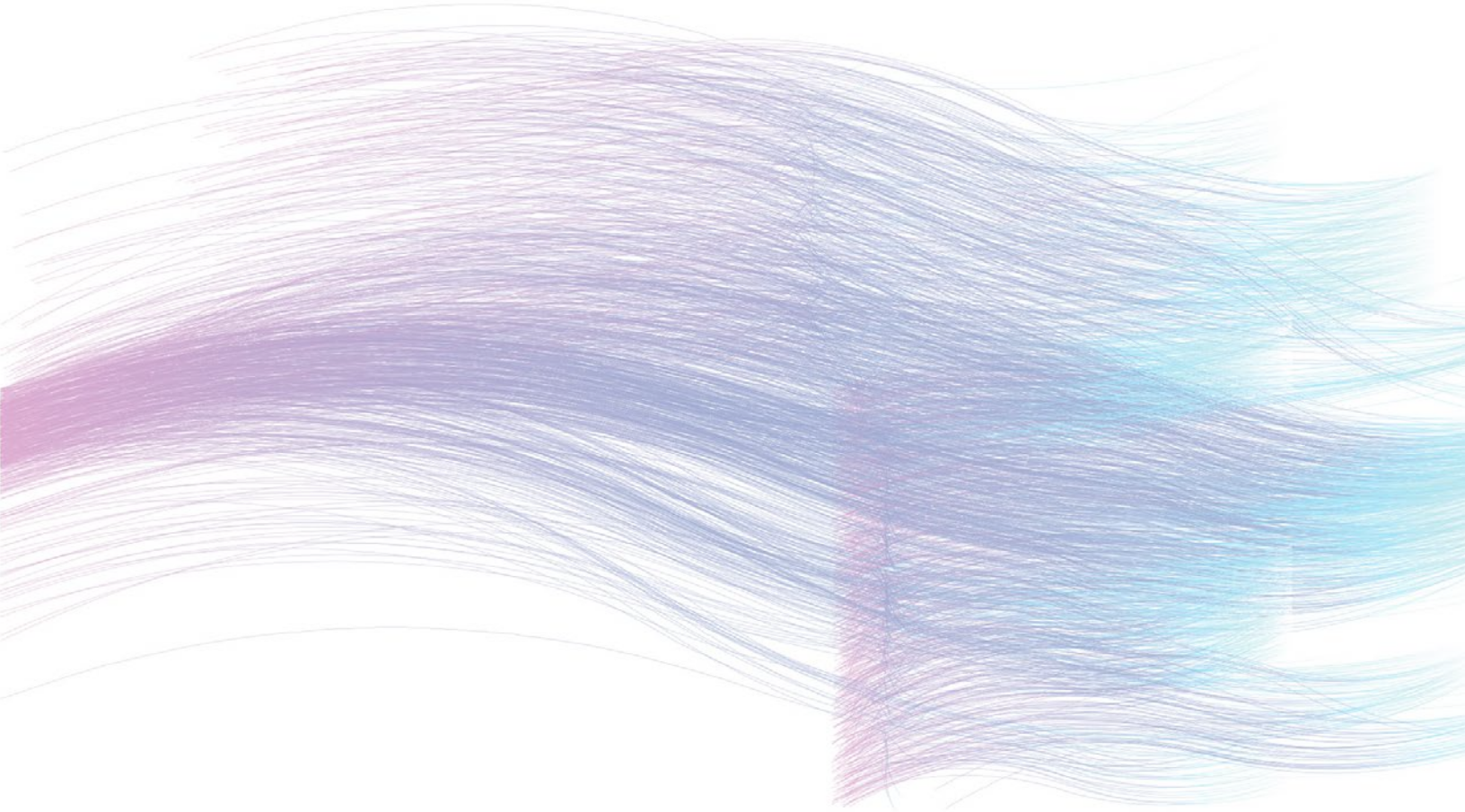
DevSecOps Organization Maturity



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

As organizations continue to mature, there will be greater concentrations of dedicated product security teams and more organizations defining their configurations, compliance and security functions as code. As application security continues to evolve from reactive to proactive functions and developers dedicated to security are formally allocated to product teams, the decentralization of security teams into the various branches of development will improve the organization's defenses. This integrated approach reduces brittleness between security and development initiatives, and success with technology components or adopting new technologies becomes easier to achieve.

Security leaders and embedded security champions will continue to focus their efforts to support DevSecOps improvements. Software delivery, operational, and reliability performance should be KPIs enabled and supported by security champions and teams alike. Best-in-class organizations deploy more frequently and have lower lead times for changes. Change failure rates and failed deployment recovery times are also reduced. As DevSecOps continues to mature and security teams branch further among development teams, CTO and CISO goals and objectives will continue to overlap better.



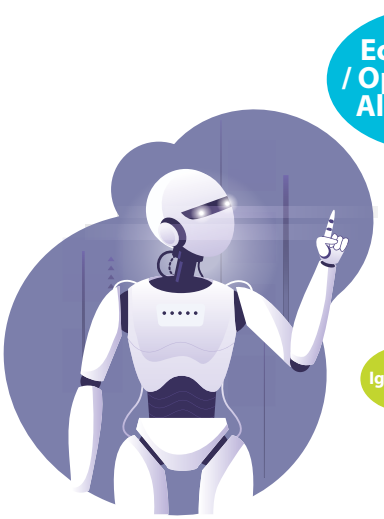
Developer Benefits and Concerns – GenAI

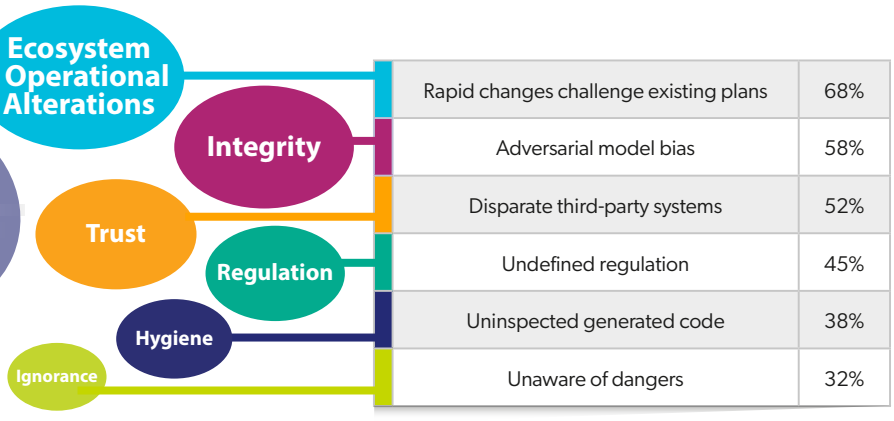
Very few technologies have captured the imagination as GenAI has since the launch of ChatGPT by OpenAI in November 2022. Surpassing 100 million users in a matter of weeks, its uncanny ability to converse is based on the billions of parameters incorporated in the underlying large language model (LLM). Trained with massive datasets to build transformer models that are capable of interpreting intention and meaning, generative AI does not just model written languages such as English. The underlying transformer models and parameters are now being applied for other use cases such as generating software code, speech, music, video and images. The potential commercial opportunities for new or improved services are unlimited.

All these innovations have spawned and accelerated other innovations. For example, LangChain, a framework to simplify the creation of applications with LLMs, can be used to create a series of AI agents that interface with each other. The extent of automation opportunities and how application interfaces will evolve are unknown. GenAI tools are further exposed through integration into other productivity tools. Microsoft Copilot in Office 365, Duet AI in Google Workspace and Firefly AI in Adobe Photoshop hint at how applications will continue to change.

With all this high-speed innovation in AI, respondents reported that the most concerning security risks with AI are rapid changes that challenge existing plans (68%).

AI Security Risks of Greatest Concern





Rapid changes challenge existing plans	68%
Adversarial model bias	58%
Disparate third-party systems	52%
Undefined regulation	45%
Uninspected generated code	38%
Unaware of dangers	32%

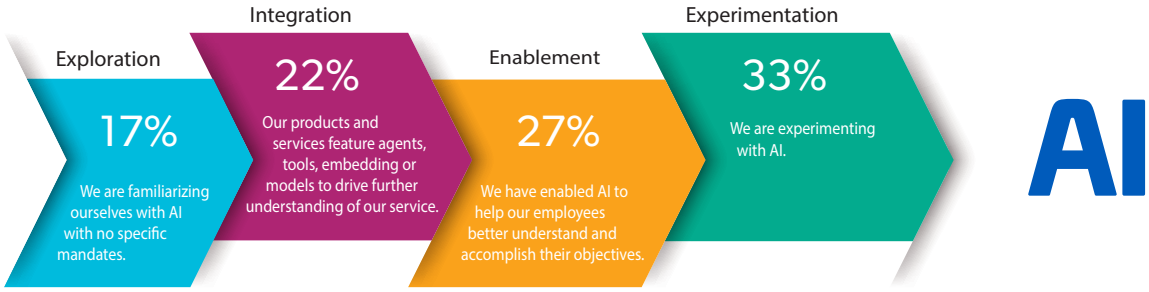
Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

In short order, two conversely related issues have arisen: using GenAI to improve security operations and improving security for GenAI. Addressing the former issue, the use of AI in security operations is not new. Machine learning techniques to identify outliers and better prioritize alerts have been evolving for a decade. LLM-based security operations that enable security operations center analysts to jointly explore security information to derive meaning have also emerged.

However, the latter issue of securing GenAI presents many unknowns. Within the most common chat use case, distinctive risk issues arise that may elude current security technologies such as data loss prevention (DLP) tools. For instance, chat interfaces may make no distinction between content and controls. Preventing a chatbot from generating or sharing personally identifiable information (PII) that was already part of its language model may be difficult to achieve. More education is required to understand the risks. On the one hand, adversaries employ GenAI by creating deepfake false identities to defraud individuals or organizations. On the other hand, depending on various factors, intellectual property and other sensitive data entered into a chatbot session may or may not become part of the LLM. Understanding where sensitive data resides and how it is accessed could prevent that data from being included in training data to augment an LLM.

While moving forward quickly, enterprises are still in the earlier adoption phases of AI. **When respondents were asked where they expect their enterprises to be in the next 12 months, 50% said they would still be in the experimentation or exploration phases in their AI journeys.**

Characterizing the AI Journey – Next 12 Months



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

Historically, security and privacy maturity have lagged behind new technology adoption. Surprisingly, the risks created by generative AI have also opened budgets, both in existing and new spending categories. **Just over half (52%) of respondents said they have invested in AI-specific security tools using existing budgets, reducing spending on other items.** An additional 20% of respondents said they have invested in AI-specific security tools using newly allocated budget. It is refreshing to see the prioritization of this type of security spending for enterprises that are still in their early stages.

With the shifting technology and ecosystem landscapes, leaders in all functional areas must continue to branch out to each other, anticipating and designing new use cases with potentially new business models that require a more inherent security design.

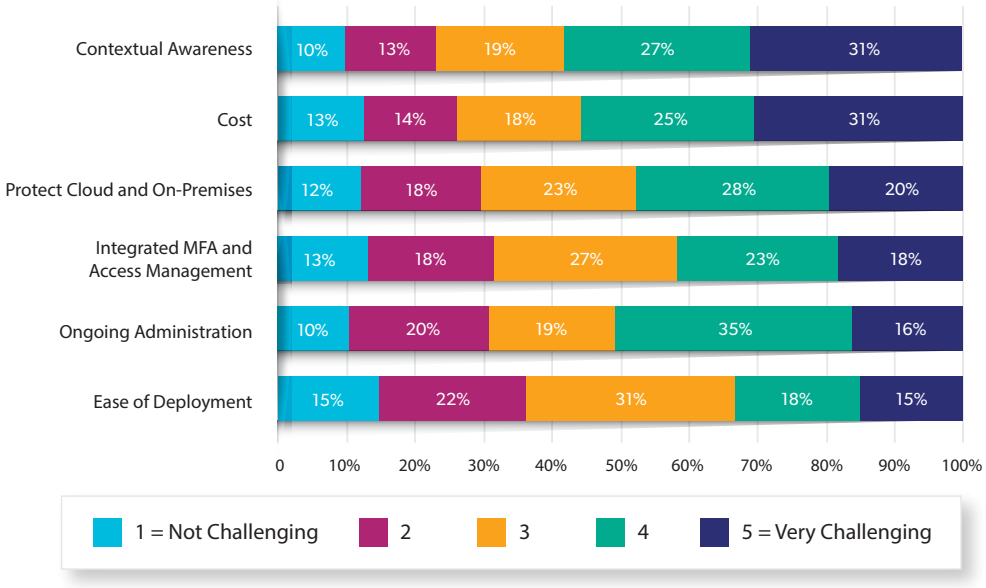
The User, The Perimeter – Workforce IAM

The adage "identity is the new perimeter" has been on the minds of security leaders and practitioners alike. The potential impacts on and implications for workforce identities are growing, given recent initiatives related to phishing resistance, distributed workforces and automated access requests for governance access. Workforce IAM initiatives must balance new and existing challenges.

Because it serves increasingly dynamic environments, workforce IAM faces renewed challenges with authentication and access. For privileged users or developers leveraging secrets management, understanding which controls need to be applied and ensuring those controls do not affect functionality is a massive challenge. Following security principles of "least privilege" — limiting access to only essential purposes in dynamic environments — requires diligence to keep track of the combinations of users, their respective groups, and the underlying roles of those users and groups within applications or datasets.

No wonder that our respondents said workforce IAM was the most pressing current discipline, prioritized by 71% of respondents. When respondents were asked about their challenges, they most frequently cited contextual awareness.

Challenges with Workforce IAM



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

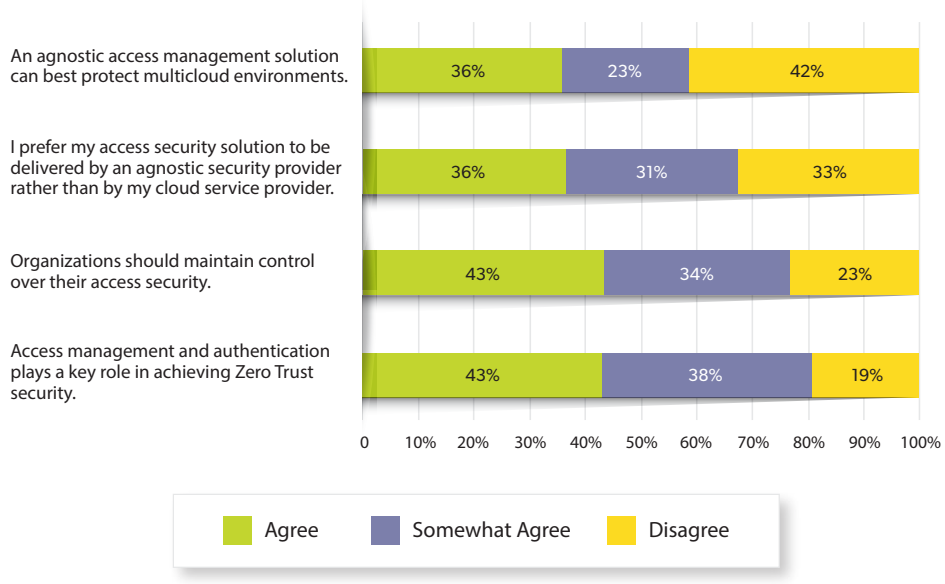
On the other hand, practitioners must acknowledge that existing legacy applications are not going away. Only 46% of respondents said that more than 40% of employees at their organization are using multi-factor authentication (MFA) for cloud-based applications. MFA usage for on-premises apps is even lower. Legacy applications, associated datasets and their users' burdens with passwords die hard. Legacy applications coupled with the growth in adoption of new apps means that the attack surface for credential stuffing is enormous. Newer innovations such as FIDO passkeys, which deprecate passwords and significantly reduce phishing, business email compromise and account takeover threats, are not universally supported by legacy apps.

KEY STATISTIC

Only 46% of respondents said that more than 40% of employees at their organization are using multi-factor authentication (MFA) for cloud-based applications.

46%

Workforce IAM Attitudes



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

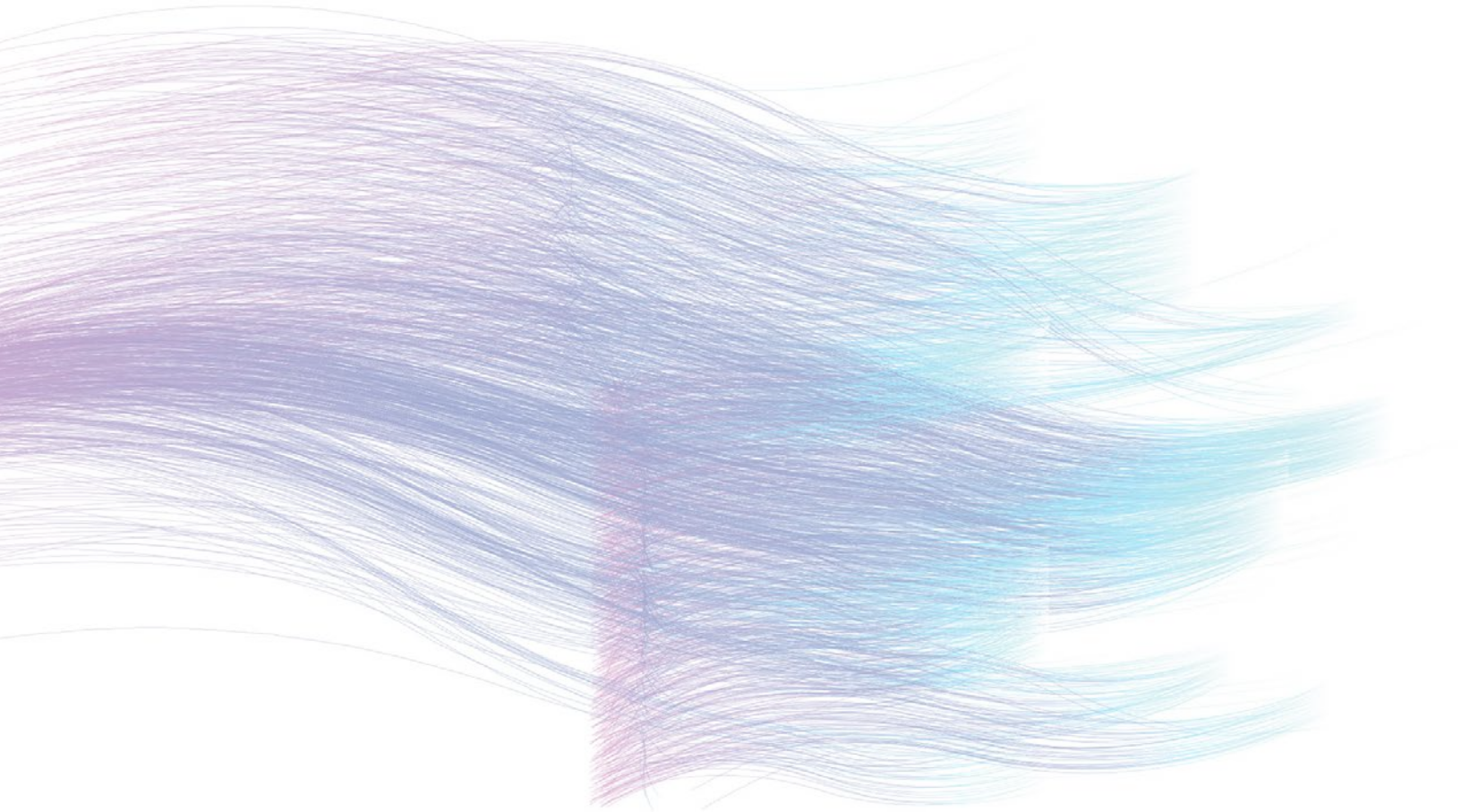
Respondents reported that workforce IAM is at somewhat of a crossroads. Spending on workforce IAM is high. **Among the selection of categories covered in the survey, workforce IAM is number two for spending.** It is also viewed favorably for effectiveness against attacks.

Identity infrastructure itself is increasingly under attack. Identity infrastructure, such as directories and directory services, has emerged as the number one cited target for attacks in the most recent survey. Cloud identities and privileged users are some of the more durable assets in a cloud environment.

Temporary and dynamic roles issued by authorization systems could mitigate some risks, but the loss of an identity can mean an attacker has a persistent hold of the environment. **The increasingly dynamic nature of authenticated and authorized users makes contextual awareness the number one reported challenge for workforce IAM.**

Demand for phishing-resistant MFA is gaining traction. For example, White House Executive Order 14028, the Cybersecurity and Infrastructure Agency and the National Institute of Standards and Technology (NIST) have called for the use of phishing-resistant MFA such as passwordless approaches that rely on public key encryption in lieu of shared secrets.

Beyond workforce IAM, new challenges to identify, authenticate and authorize processes, workloads, agents and devices lie ahead. The FIDO Alliance's Device Onboarding (FDO) initiative automates the onboarding of devices with secrets and configuration data to connect securely with cloud and edge management platforms.



Ubiquitous Connections – IoT / 5G

While operational technology (OT) deployments have sometimes been criticized for having little emphasis on security, this year's survey data saw IT security teams entering the OT realm as the number one way to defend against IoT threats (75%). OT devices such as power meters and "smart" sensors in a variety of distributed physical plants have been designed to be serviced with a minimum amount of oversight and a lower operational cost.

A proactive security approach is needed. With greater connectivity options and integrations, physical or network isolation ("air gapping") was the least-cited choice for securing IoT/OT environments. Perhaps reflecting the importance of zero-trust principles, respondents did not want to be dependent on carrier security. **When asked specifically about 5G technologies, only 33% said that the carrier's ability to secure the network was a concern.** 5G amplifies IoT/OT security challenges — challenges that carrier networks cannot solely address.

KEY STATISTIC

When asked specifically about 5G technologies, only 33% said that the carrier's ability to secure the network was a concern.

33%

Yet these devices have been plagued by security problems. Centralized defense teams often need help understanding the OT estates they have, with patching being the greatest concern. OT devices have also been plagued by weak default passwords that are never changed by operators. Further democratizing certificate authority deployments for private IoT and cloud environments could pay significant dividends to authenticate or repudiate IoT and OT devices. Patching and authentication are the second- and third-ranked answers, respectively, among this means to address IoT risks.

These proactive security approaches in security operations, patching, authentication and zero-trust principles will be essential as 5G and IoT initiatives converge. **Enterprises continue to look to 5G as a primary IoT connectivity option: 69% of enterprises aim to use 5G-IoT (public or private) to support their IoT deployments,** according to 451 Research's Voice of the Enterprise: Internet of Things, Connectivity and Security 2023 study.

IoT, OT and 5G environments are increasingly used for critical infrastructure, including smart city initiatives. New frameworks, such as the NIST Guide to Operational Technology (OT) Security Special Publication (SP) 800-82 and the ISA/IEC 62443 standards, should further encourage and guide device makers to tighten their security. Forty-four (44%) percent of public sector respondents already cite security concerns as the number one inhibitor of IoT initiatives, according to 451 Research's Voice of the Enterprise: Internet of Things, the OT Perspective, Use Cases and Outcomes 2023 survey. While IoT can deliver enhancements across various city outcomes, without security at its core, IoT deployments could present more risk than reward.

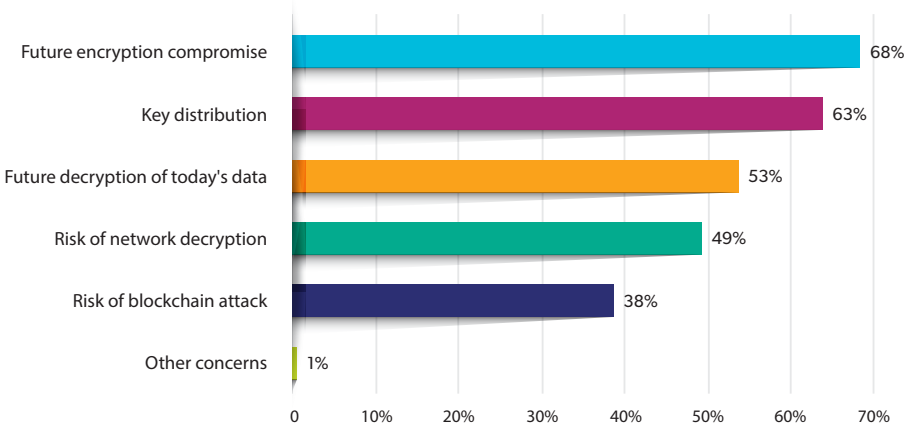
Taking the Quantum Leap – Post Quantum Cryptography

Since NIST approved four cipher suites in July 2022, post-quantum cryptography (PQC) addresses a future threat that moves closer to the present. While there has still been no confirmed or repeated quantum computing attack on any classically encrypted data, there is still cause for concern and action.

Crypto agility — the ability to readily switch cryptographic tools and ciphers — remains a challenge for enterprises when underlying infrastructure or other technology may not facilitate change. Certain OT and IoT technologies have a 5- to 15-year life span; maintenance patching for IoT/OT remains the greatest security challenge. Similarly, on-premises or legacy networks may also be unfeasible for currently approved PQC ciphers, or they may be difficult for operators to easily enable changes. Public key infrastructure (PKI), networks and long-life data all present broad challenges.

Respondents expressed less interest in retiring classically encrypted data that would be susceptible to quantum cryptographic attacks. **When asked to consider an 18- to 24-month time frame, only 23% of respondents said that retiring data would satisfy quantum security requirements.** There is a dual reality check for security teams regarding PQC, the first element being that classically encrypted data today may already be harvested for future decryption. "Harvest now, decrypt later" attacks are unsurprisingly the top concern for our respondents.

Quantum Computing Threats of Greatest Concern

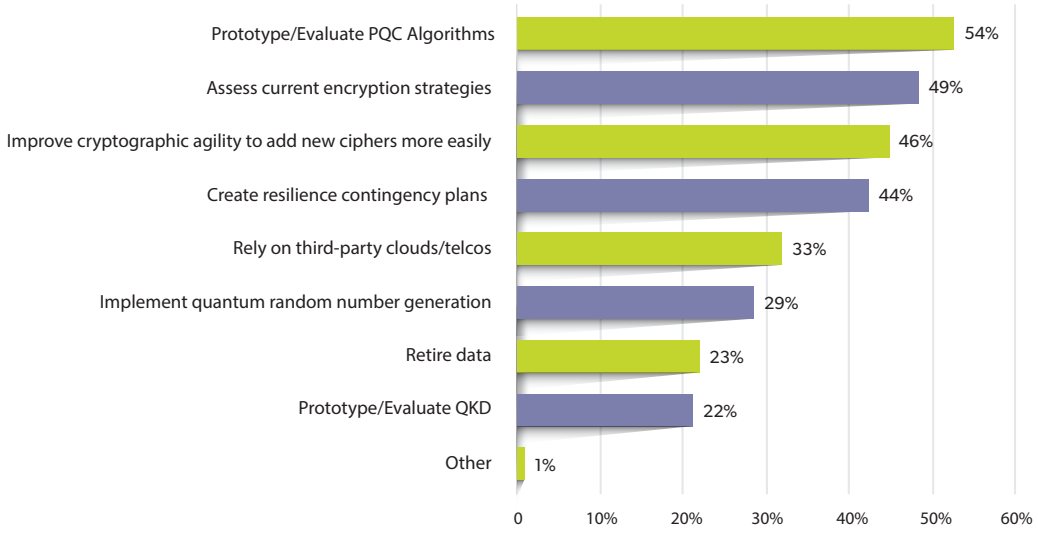


Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

The second reality check is that retiring information may not be permissible for technological or regulatory reasons. HIPAA (The Health Insurance Portability and Accountability Act) has records-retention provisions for up to six years. At an extreme, no personally identifiable information (PII) has been disclosed from the U.S. decennial census survey for 72 years; however, other datasets may reside in or be transported through systems that are difficult or unfeasible to upgrade.

The data does provide encouraging indicators of proactivity. Prototyping PQC was the most-cited choice when addressing quantum cryptography concerns, followed closely by enterprises assessing their strategies and further exploring crypto agility. Brittle or long-overlooked networks or other OT may finally be counted and strengthened thanks to a PQC prototyping or other strategic review. These improvements, catalyzed by PQC initiatives, may ultimately reduce operator burden or complexity.

PQC Security – Real Problems, Real Progress



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

PQC warrants continued attention for enterprises to prepare for or adjust to changing realities. While public clouds, carriers and content distribution networks are generally more capable of enabling PQC within their networks, enterprises must follow a shared responsibility model. While cloud provider and carrier networks may significantly reduce PQC attacks, it remains up to the enterprises to have sovereignty over their security controls, regardless of third-party involvement.

Choices and Checks – Sovereignty

Throughout this report, respondents reported more proactive approaches to security when embracing new technologies or addressing new technology trends. Enterprises have learned to operate under shared security responsibility models from their cloud operations; with new technologies such as PQC, 5G and GenAI, many enterprises are choosing to control their own security destiny.

The EU's General Data Protection Regulation (GDPR) has encouraged the launch of many other privacy regulations worldwide, including state and provincial laws such as the California Consumer Privacy Act. Coinciding with GDPR, sovereignty principles have arisen to enable enterprises to secure, store, operate and migrate citizen data and other non-public information with more explicit provisions to be self-sufficient from the nationality, location or future compatibility of any given environment.

Specifically for IaaS and SaaS, enterprises can make choices such as data security access controls, data residency, operator nationality and even full future software compatibility. Full future software compatibility allows for enterprises to withdraw from their cloud-based IaaS/SaaS provider and operate on the data with an open-source equivalent. **When respondents were asked what was driving their digital sovereignty initiatives, 31% selected full future software compatibility.**

Data residency concerns were somewhat softened with the preference for stronger, external encryption and key management. **Thirty-nine percent of all respondents said that data residency would no longer be an issue provided that external encryption, key management and separation of duties were implemented.**

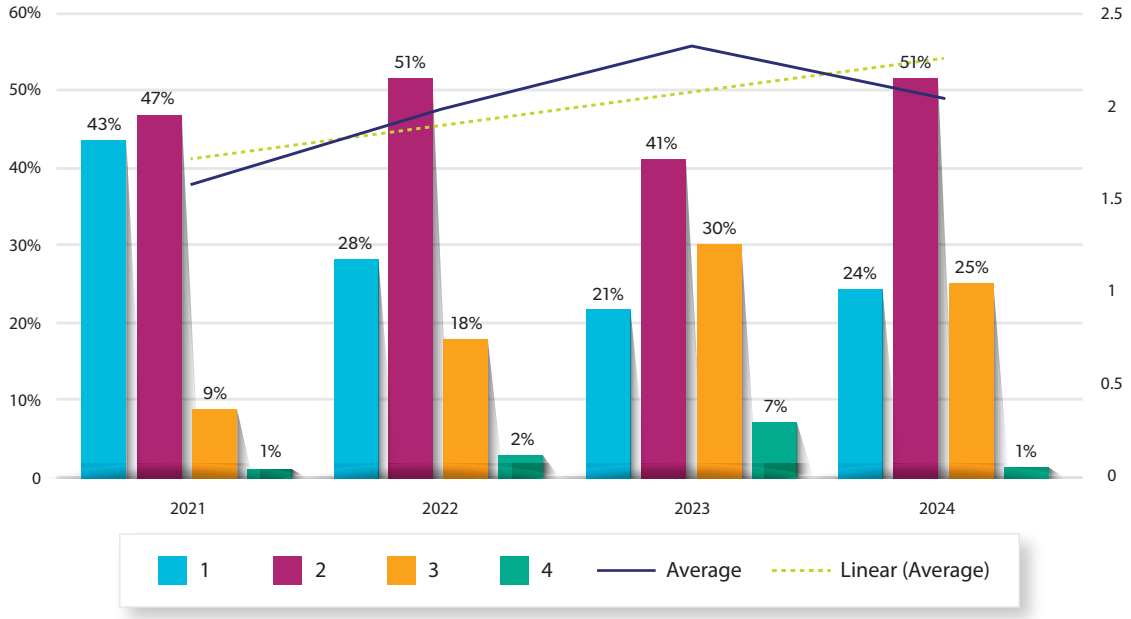
Yet just because enterprises can store, operate and migrate independently away from a particular cloud-based vendor doesn't mean they should. **Multicloud use is down slightly, with the average number of cloud providers declining to 2.02 from 2.26 last year.** Interestingly, banking, financial services and insurance respondents are now slightly more multicloud than the average enterprise survey-wide, with an average of 2.03 cloud providers versus 2.02.

KEY STATISTIC

Multicloud use is down slightly, with the average number of cloud providers declining to 2.02 from 2.26 last year.

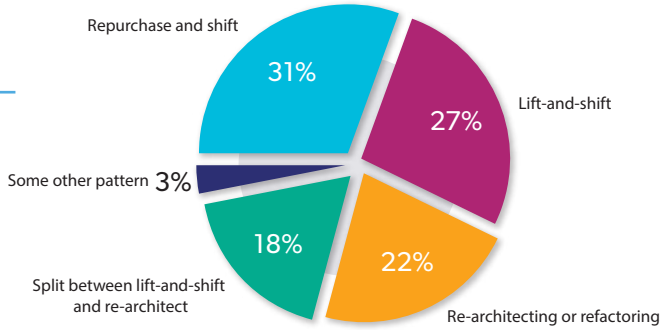
2.02

Multicloud IaaS Adoption Trending Higher Overall

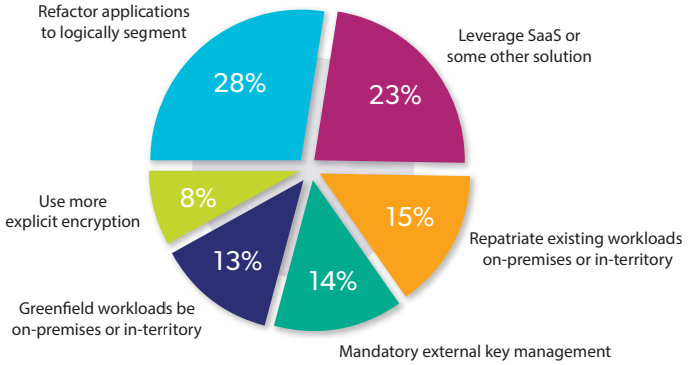


Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

Iaas and PaaS Cloud Migration Strategies



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey



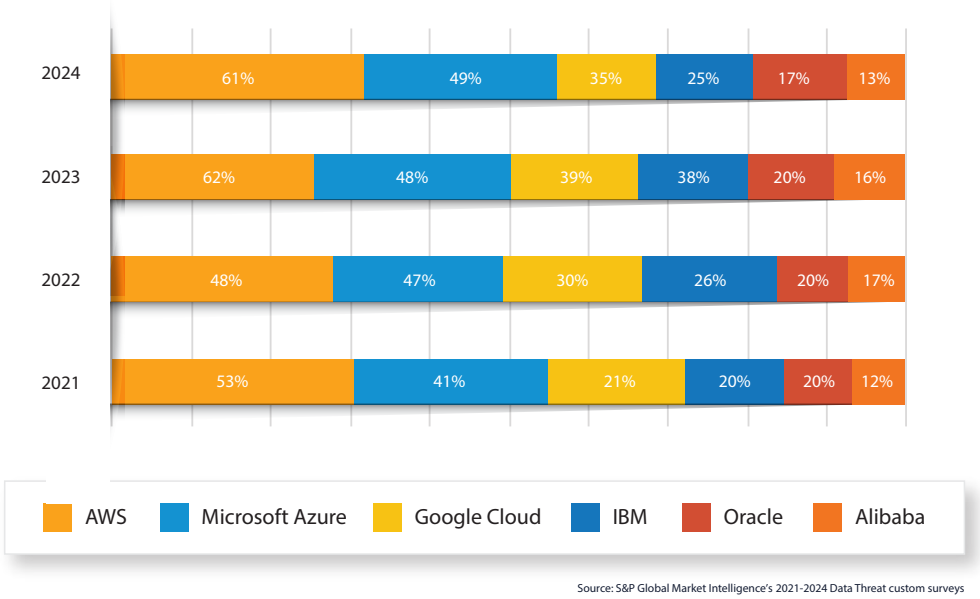
Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

Strategies of Sovereignty

Refactoring applications or workflows is a sizable challenge for enterprises. Rebuilding applications for specific clouds or PaaS is less popular or simple than lift-and-shift approaches or simply repurchasing a SaaS replacement.

As enterprises progress on their multicloud journey, significant switching costs remain between different cloud providers or to repatriate workloads back on-premises. While public cloud providers have many similar features in compute, storage, applications, networking or other services, significant differences in implementation details remain. Lower operating costs may only be attainable if the enterprise has the desire, skill or business incentive to switch.

Adoption Patterns - Public Cloud Providers



Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

With multicloud a fact of life, enterprises may not be able to swap out or consolidate infrastructures for consolidation's sake, but they can better abstract their controls so that they are more applicable to multiple jurisdictions and changing market requirements. Still, enterprises have ongoing complex challenges. **There has been a negligible decline in the number of key management systems in use, with the average declining from 5.6 to 5.4 in the last year. Still, over 53% have five or more key management systems in use.**

Enterprises must check the choices they make on their sovereignty journey. Ultimately, digital sovereignty provides for enterprise self-sufficiency to be able to better serve and build trust with their customers, consumers and other stakeholders. As such, digital sovereignty becomes strategic to an enterprise's design and a response to its relationships with outside stakeholders.

Conclusion and Next Steps

As enterprises grow, their design and adoption of technologies will continue to grow. Centrally defined security principles, built on the core tenets of advice and consent, have a greater opportunity for successful delegation and implementation. The rule of law is most successful in societies where citizens and institutions are aware of their rights and responsibilities, so enterprise data security risks will be reduced as other stakeholders are enabled and freely entrusted to follow those principles.

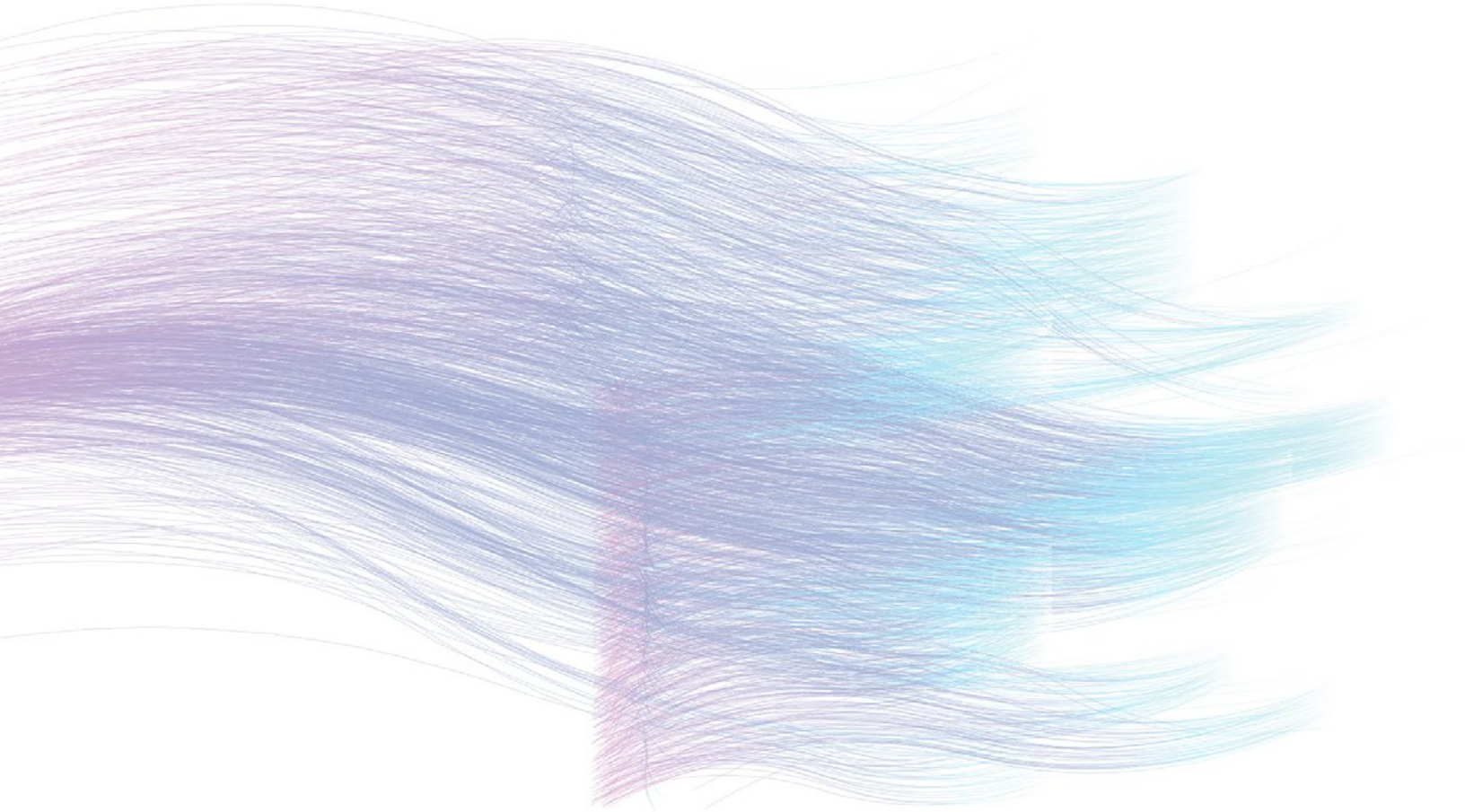
Based on the survey results reflected in this report, with respect to both current initiatives and emerging technologies, enterprises and security leaders could benefit from implementing the following principles:

- **Align targets, spending and effectiveness.** With phishing attacks and identity infrastructure attacks on the rise, for example, organizations should look towards robust program investments in Workforce IAM and CIAM for greater effectiveness.
- **Transition from reactive to proactive defenses.** Security program transformation is characterized by proactive defenses that enable operators, developers and other users to adopt new technologies safely. Respondents identified proactive measures in major emerging areas such as GenAI, cloud, IoT/5G and quantum computing.
- **Seek out stakeholder buy-in.** For security leaders, this means understanding and communicating the positive business impact that proactive security has for developers, auditors, users, lines of business and customers. Shared goals and outcomes begin with aligned activities.
- **Make it easier for stakeholders to buy-in.** For security leaders, this means enabling different stakeholders to secure themselves. Developers could choose simpler ways to onboard and authenticate customers, or security champion programs could encourage more developers to develop securely. Such initiatives can help security practices to spread and take root throughout the organization and beyond.

Increasing threat volume, complexity and severity, along with the proliferation of new technologies, will force enterprises to boldly prioritize and iterate on different initiatives such as:

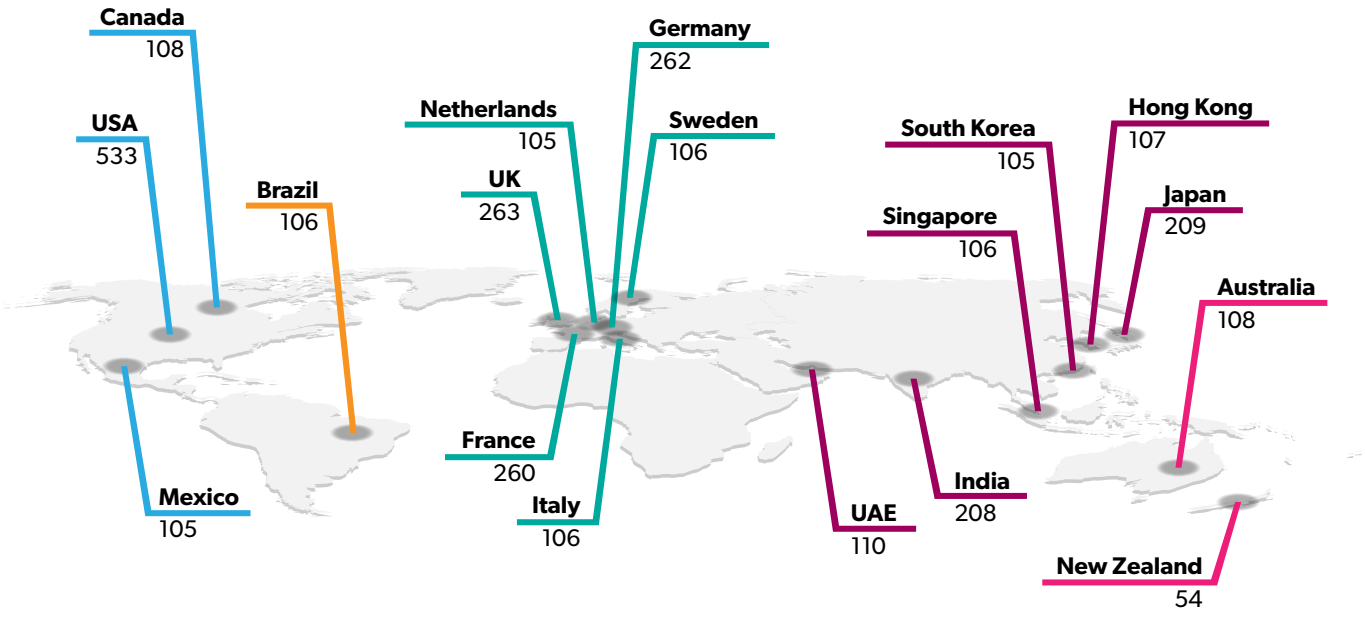
- **Growing customer trust.** Security can enable developers to build trustworthiness into better customer experiences.
- **Growing resilience.** Ransomware response is a coordinated responsibility with legal implications. Regularly exercising ransomware response plans will highlight addressable gaps in controls or procedures that prevent organizations from fully operating.
- **Growing readiness.** New cloud and GenAI technologies require a better understanding and control of data. Understanding what data exists, what protections are in place and what future protections can be implemented are critical precursors to further enterprise transformation.

Choosing singular, focused initiatives enables manageable collaboration across the many stakeholders involved. That collaborative quality is characterized by the hallmarks of proactive enterprise security — trust, safety, and privacy. Internal security teams have a singular advantage over their adversaries: knowledge of their roots. Understanding stakeholders, their applications, data, and support systems will allow enterprises to better defend against global threats to data.



About This Study

This research was based on a global survey of 2,961 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about the 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	138
$250m to $499.9m	847
$500m to $749.9m	773
$750m to $999.9m	704
$1 Bn to $1.49 Bn	216
$1.5 Bn to $1.99 Bn	103
$2 Bn or more	180

Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Retail	153	Financial Services	108
Manufacturing	150	Federal Government	106
Healthcare	144	Telecommunications	101
Technology	140	Automotive	96
Public Sector	110	Pharmaceuticals	86

THALES

Building a future we can all trust

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

cpl.thalesgroup.com/data-threat-report