2026 EDITION

THALES
CYBERSECURITY

DATA THREAT REPORT

Data Sheet
Hong Kong

cpl.thalesgroup.com

#2026DataThreatReport

Introduction

Data security has taken center stage as the success of enterprise AI initiatives increasingly hinges on consistent, controlled access to proprietary organizational data sources. The **2026 Thales Data Threat Report** examines the complex calculus that organizations must undertake to enable innovation while securing their most valuable asset — their data.

The proliferation of AI and agentic operations is compounding stress on data management and security, as reflected in a 50% year-over-year increase in the proportion of respondents allocating new security budgets specifically for AI. Organizations are struggling with data quality and security as they work to safely deliver access to the raw material from which AI value is built. As agentic applications gain access to greater volumes of data, organizations must improve data security and management practices to ensure that AI does not become a new insider threat.

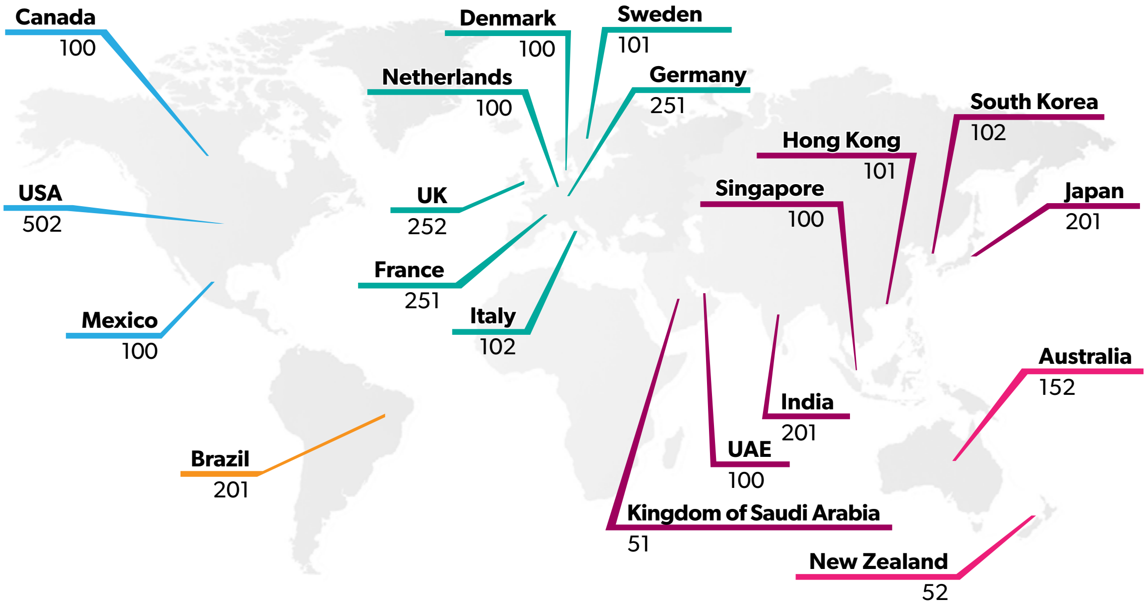
Organizations face pressure to accelerate their operations, but these efforts are challenged by complexity in security operations exacerbated by sprawling security toolsets and increasingly complex hybrid and multicloud IT infrastructure. AI is forcing the integration of new elements, such as chat interfaces and Model Context Protocol servers, that security teams are wrestling to secure. The threat landscape is also shifting as attackers employ AI and quantum computing risks loom ever larger. Further complicating matters, the AI ecosystem is constantly shifting under security teams' feet.

While there are positive trends in this year's Data Threat Report, much more must be done to secure organizations' most sensitive data. The report captures the insights of more than 3,100 respondents from 20 countries. Most have a fully multicloud operating model, with data and applications located across different cloud provider venues, although not all can be said to have actively embraced this reality.

Comparing this year's survey results with previous years reveals notable areas of concern. Significant volumes of sensitive data in the cloud remain unencrypted. Cloud-based applications and cloud management infrastructure remain key targets for attackers. The complexity of security operations in the cloud can be challenging, particularly given staffing constraints. As the name suggests, cloud security demands expertise in both cloud operations and security applications, and both capabilities are in short supply. Added to this is the pressure to deliver ever greater data volumes and computational power for AI applications. As we enter the age of agentic operations, security practitioners will need to address access, authentication and authorization on an even greater scale.

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

Key findings - Hong Kong

Security priorities are changing with AI

Spending on AI security is rising –

39% of organizations now have a dedicated budget for AI security (up from 22%), but **42%** still fund AI security using their existing security budgets.

74% The speed of AI change within AI ecosystems is top of mind when it comes to AI security with 74% citing rate of change as the top AI risk.

56% report their AI applications are being targeted by attackers, with sensitive data being the leading target.

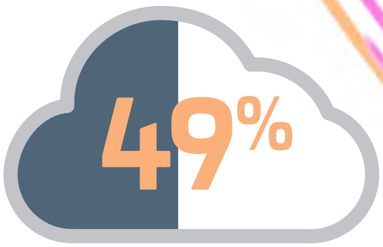
AI-fueled attacks emerge as a prominent threat - **59%** have seen deepfake attacks and

45% **have experienced reputational damage, as a result of AI-generated misinformation.**

69% report AI generated misinformation and deepfakes showed the second highest attack increase.

Data protection is critical in the AI age

60% regard identity and access management as the most pressing security discipline, as attackers exploit credentials.



49%

Only about half of sensitive data in the cloud is encrypted.

Only 36%

have complete knowledge of where their data is stored.

55%

rank secrets management as one of the leading concerns in application security.

Complexity limits clear insight into data security posture

Security complexity creates greater risk –

tool counts are high with

72% having five or more data protection tools.

45% have five or more key management systems

42% are confident in their understanding of data security tools

41% cite Human error as the leading cause of breach, but 54% rank nation state attackers as one of the top three greatest concerns.

Cloud is a significant attack target

Cloud assets are the top three attack targets – as respondents cited

32% cloud storage, 49% cloud applications and 37% cloud management infrastructure as the top three attack targets.

Credential theft is one of the leading attack technique against cloud infrastructure –

44% are seeing credential theft and misappropriated secrets increasing.

Rising geopolitical risk is reshaping data sovereignty

47% are pursuing reworking and refactoring of application and data architectures as their main focus in achieving sovereignty objectives.

29% believe cryptographic protections such as encryption and key management are sufficient to achieve data sovereignty.

Future risks are here today

Quantum concerns shift to the reality of harvest now, decrypt later (HNDL),

59% cited as top concern.

Organizations are moving to mitigate quantum risk

62%

are prototyping and evaluating Post-Quantum Cryptographic (PQC) algorithms.

THALES

CYBERSECURITY

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

cpl.thalesgroup.com/data-threat-report