THALES
Building a future we can all trust

#2025DataThreatReport

2025

Healthcare and Life Sciences DATA THREAT REPORT

AI, Quantum and the Evolving Data Threatscape

cpl.thalesgroup.com

Introduction

Healthcare and life sciences (HCLS) organizations — those involved in biotechnology, healthcare and pharmaceutical industries — encompass a wide variety of firms across the healthcare ecosystem, from research and development to regulatory oversight and patient care. Because much of the data they work with is valuable and sensitive, these firms are heavily regulated, and the information they steward provides an enticing target for cybercriminals. Top challenges for these organizations include compliance mandates, third-party risks, and a rapidly evolving threat landscape characterized by escalating malware, ransomware and phishing attacks plus additional emerging threat vectors.

In this executive summary, we share key findings from the **2025 Thales Data Threat Report (DTR)** focused on HCLS organizations and examine the differences between HCLS survey respondents and global responses across all industry verticals. Many of the HCLS DTR survey results are similar to overall responses, but we note key differences.

S&P Global
Market Intelligence

Source: 2025 Data Threat Report custom survey from
S&P Global Market Intelligence 451 Research, commissioned by Thales.

Sponsored by

ARROW Five Years Out

EXCLUSIVE NETWORKS

CLIMB

TD SYNNEX

Note: All charts displayed in this document are from S&P Global Market Intelligence 451 Research's 2021-2025 Data Threat custom surveys.

Key Findings

Tracking AI Development

HCLS organizations, like those in virtually all industries, are deploying advanced AI systems to remain competitive and improve employee productivity. Securing these systems is a priority:

69% cited the fast-moving AI ecosystem as their top concern, followed by concerns about lack of model and data integrity (65%) and trustworthiness (60%).

68% of HCLS respondents are investing in GenAI-specific security tools, and 18% are using newly allocated budget.

Right on 'Q'

HCLS respondents are concerned about the risk of future encryption compromise and quantum computing security threats:

67% are concerned about future encryption compromise, compared to 63% surveywide.

58% are concerned about key distribution, compared to 61% surveywide.

59% are concerned about future decryption of today's data, including harvest now, decrypt later, compared to 58% surveywide.

Cloud Platform Growth and Challenges Continue

HCLS organizations continued growing their cloud estates, according to the 2025 DTR, and security remains a top concern:

1.9 The average number of IaaS providers dropped slightly from 2.0 in the 2024 survey.

77 The average quantity of SaaS applications in use grew from 66 last year to 77 this year, lower than the survey average of 85 — a 14% increase in just one year.

IaaS/PaaS cloud security is the top security spending category for HCLS organizations, followed by identity and access management and security for AI.

Data Security Fuels Digital Sovereignty

Digital sovereignty remains a key concern of HCLS organizations, which are increasingly using data security to satisfy compliance requirements:

58% of HCLS organizations were driven to pursue digital sovereignty by specific customer, regional or global privacy mandates.

46% said that encryption and key management provide sufficient protection to achieve objectives.

Trends in Data Security

On average, nearly half of the data that HCLS organizations store in the cloud is characterized as sensitive, yet many fall short on leveraging basic data security controls:

27% have little or no confidence in identifying where their data is stored.

Only 4% of HCLS organizations have encrypted 80% or more of their sensitive cloud data.

HCLS organizations on average report that 47% of the data they store in the cloud is sensitive.

Application Security: Essential for Data Protection

32% of HCLS organizations use more than 500 APIs; 14% use more than 1,000 (compared to 34% and 16%, respectively, surveywide).

62% of HCLS respondents said code vulnerabilities are a major concern for application security, placing it as the top response, compared to 59% surveywide.

From Cloud DevOps to Platform Engineering

54% said secrets management is a leading DevOps security challenge, close to the surveywide result 55%.

Only 15% of HCLS respondents identified secrets management as most effective in protecting data, despite the devastating impact of compromised secrets, nearly identical to surveywide.

Healthcare and Life Sciences Observations

Structural and geopolitical changes in 2025 will likely prompt enterprises to rethink their security strategies. The HCLS DTR results suggest that organizations would be wise to focus on their most valuable asset: the data they collect, process, store and steward for stakeholders and customers. One sign of improvement is the number of HCLS organizations experiencing a recent data breach. In 2021, 37% of HCLS organizations had experienced a breach in the prior 12 months, but this number dropped to 12% in the 2025 survey — a significant 25-point decrease. The HCLS result is similar to the surveywide result, which went from 41% in 2021 to 14% in 2025. HCLS respondents indicated that credential theft/compromise, including misappropriated secrets, third-party vulnerabilities and infrastructure compromise, was the top area of increased cloud management infrastructure attacks.

In 2021, 37% of HCLS organizations had experienced a breach in the prior 12 months, but this number dropped to 12% in the 2025 survey — a significant 25-point decrease.

The Threat Landscape, Inside and Out

Rates of recent data breaches among HCLS respondents have steadily decreased, while breach complexity and sophistication continue to increase:

12% of HCLS respondents reporting a recent breach, down from 37% in 2021, due in part to increased use of strong multi-factor authentication (MFA), now used by 57% of employees on average (up from 21% in 2021).

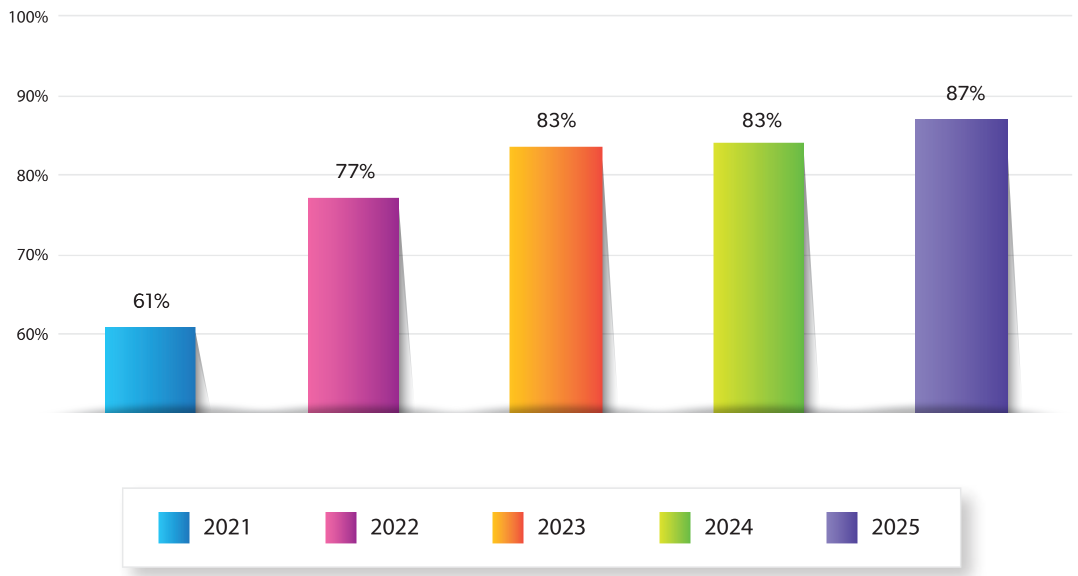
86% of respondents indicated that MFA is used by more than 40% of employees, up from 14% of respondents saying so in 2021.

The top root causes of breaches are misconfiguration or human error, exploitation of known vulnerabilities, and identity failure or compromise.

Data Security

Understanding data is critical to securing it effectively, and there are encouraging results in data classification: 87% of HCLS respondents reported that they can classify at least half of their data, a notable increase from previous years and similar to the surveywide result. The consistency and effectiveness of data discovery and data classification are less clear. Over half (59%) of HCLS organizations use five or more tools for data discovery and classification, which can lead to misalignment and conflicting protection policies. This misalignment might have contributed to the result that just 4% of HCLS organizations have encrypted 80% or more of their sensitive cloud data, which is half the overall result and quite low given HCLS data sensitivity. The 2025 HCLS DTR results show progress in key areas of data security, but much work remains as organizations mature their data security controls.

Proportion of HCLS respondents able to classify at least half of organizational data



Quantum Cryptography

There is better alignment regarding post-quantum cryptography risks in 2025, with 58% of HCLS respondents prototyping or evaluating new PQC algorithms, similar to the overall result. Deployment timelines are crucial, but early signs of this transition are promising. Regulatory focus on cryptographic protections is also notable: When asked about data sovereignty concerns, two in five HCLS respondents (43%) said they believe encryption could provide sufficient protections to meet sovereignty mandates.

Application Security

The complexity of application architectures is a key concern, necessitating improved application security. One-third of HCLS respondents reported having more than 500 application programming interfaces (APIs) in use, similar to the surveywide result. This proliferation raises broad concerns about vulnerabilities in code and in the software supply chain. While shift-left security controls are the top-cited priority for application protections, HCLS respondents also emphasized foundational production controls such as dynamic application security testing (DAST), API security tools and web application firewalls. Other application security concerns on the architecture side include secrets management, which leads among DevOps security concerns. However, only 15% of HCLS respondents identified DevSecOps secrets management tools among the top three most effective technologies for data protection, despite the high risk associated with secrets management failures, which can expose authentication data such as API keys. This concern is amplified given the high reported number of APIs in use.

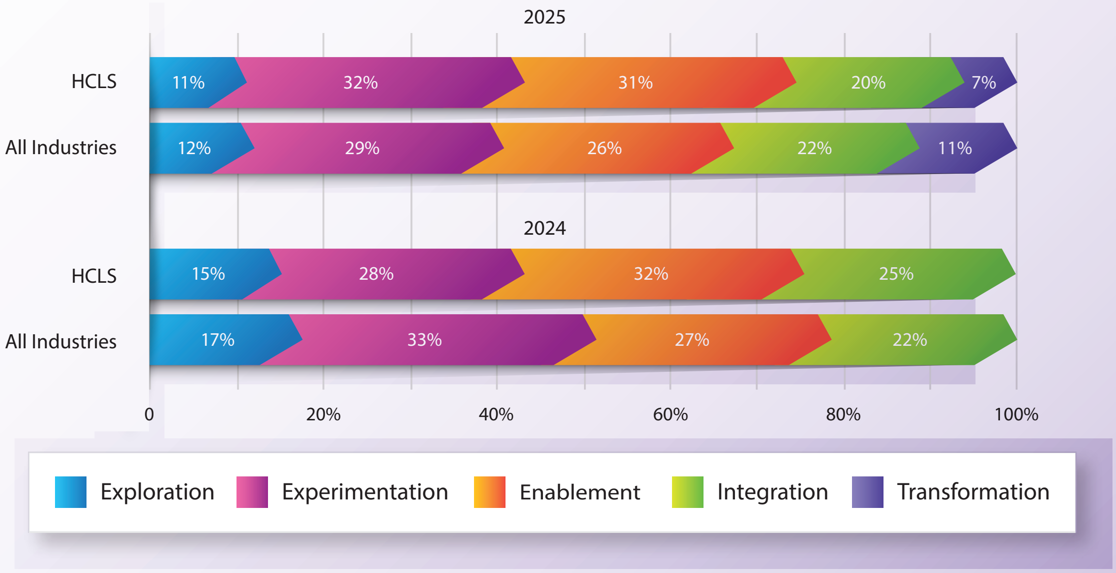
One-third of HCLS respondents reported having more than 500 application programming interfaces (APIs) in use, similar to the surveywide result.

Generative AI: Data Takes Center Stage

GenAI poses challenges to data security, but it can also be used to respond to security challenges. Increased GenAI integration reflects developing organizational maturity and progress beyond experimentation. An expanded and refined definition of GenAI among respondents reveals expectations for the transformational nature of GenAI as organizations continue their journey toward greater digital maturity.

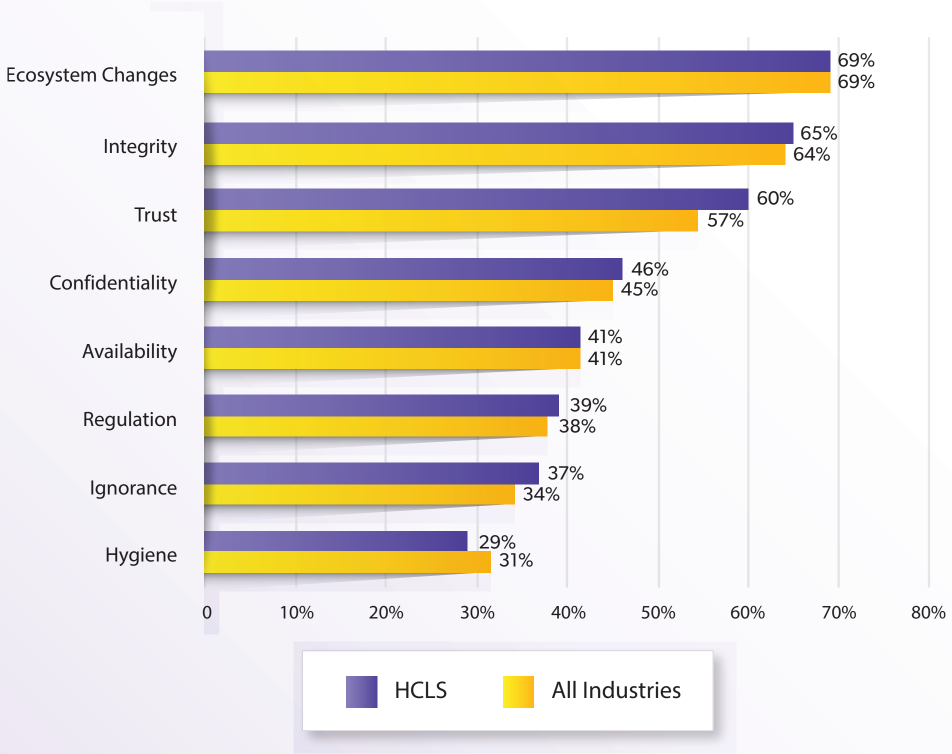
Organizations are under immense pressure to deliver GenAI capabilities, and the pace of adoption has shifted even more significantly for HCLS organizations. In 2024, HCLS was ahead of the general market in terms of AI deployment, with a 5-point lead in enabling employees to use AI. In 2025, 27% of HCLS organizations said they are in the "integration" or "transformation" phases of their GenAI journey, compared to 33% across the overall survey population. This trend is also reflected in AI-specific security spending, with 50% of HCLS organizations investing via existing budgets and 18% using newly allocated budget, compared to 53% and 20%, respectively, surveywide. GenAI's impact may further influence evolving data and privacy regulations, emphasizing the importance of maintaining confidentiality, trustworthiness and safety.

Stages of AI journey



Concerns about the risks of deploying AI are also growing, led by ecosystem and operational alterations forcing rapid changes to existing plans, followed by concerns about model integrity and trustworthiness of third-party systems.

Most concerning GenAI security risks



While GenAI is intensifying the focus on data security, hasty implementations raise the risk of data breaches. Vulnerabilities in the DeepSeek model reported shortly after its V3 release serve as a cautionary tale for security teams. Because GenAI architectures are new for most security teams, prioritizing data security efforts is crucial.

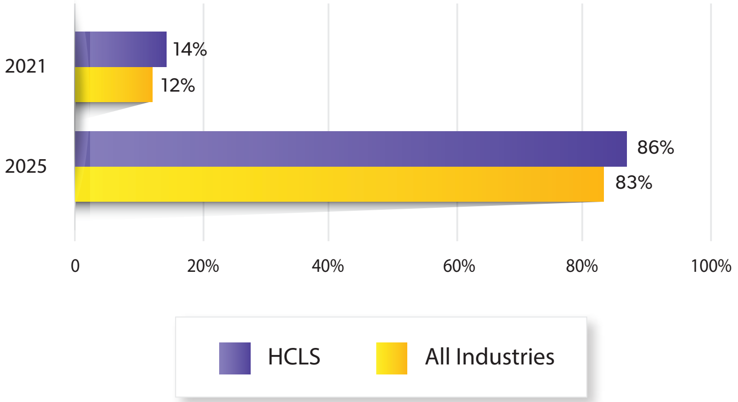
Conclusion

While many of the DTR results for HCLS organizations were similar to surveywide responses, key differences emerged. While HCLS organizations are not adopting technological innovations such as AI as aggressively as other organizations, the addition of generative and agentic AI to a foundation of mature machine learning techniques is a clear priority, with these technologies being widely deployed to aid in employee productivity and transform business processes. Securing AI systems remains a priority for organizations, driven by notable concerns such as the fast-moving ecosystem and lack of integrity and trustworthiness. This is also reflected in budget being directed toward AI, with a high percentage of respondents investing in GenAI-specific security tools, often using newly allocated budget.

Continual increases in technical complexity are the result of accelerated digital transformation, and a key indicator is the quantity of APIs in use. HCLS organizations use many APIs, reinforcing the need for application testing across the life cycle and intensifying concerns about software supply chain security. Another concern for HCLS organizations is secrets management, the leading DevOps security challenge.

Post-quantum cryptography continues to raise concerns regarding future encryption compromise, key distribution and future decryption of today's data, which are only partially being solved by assessing current encryption strategies and prototyping or evaluating PCQ algorithms. On a positive note, breach statistics continue to improve, with HCLS firms reporting a 26-percentage-point drop in recent data breaches since 2021, no doubt due to an astonishing 72-percentage-point increase in the proportion of organizations implementing strong MFA for 40% or more of employees.

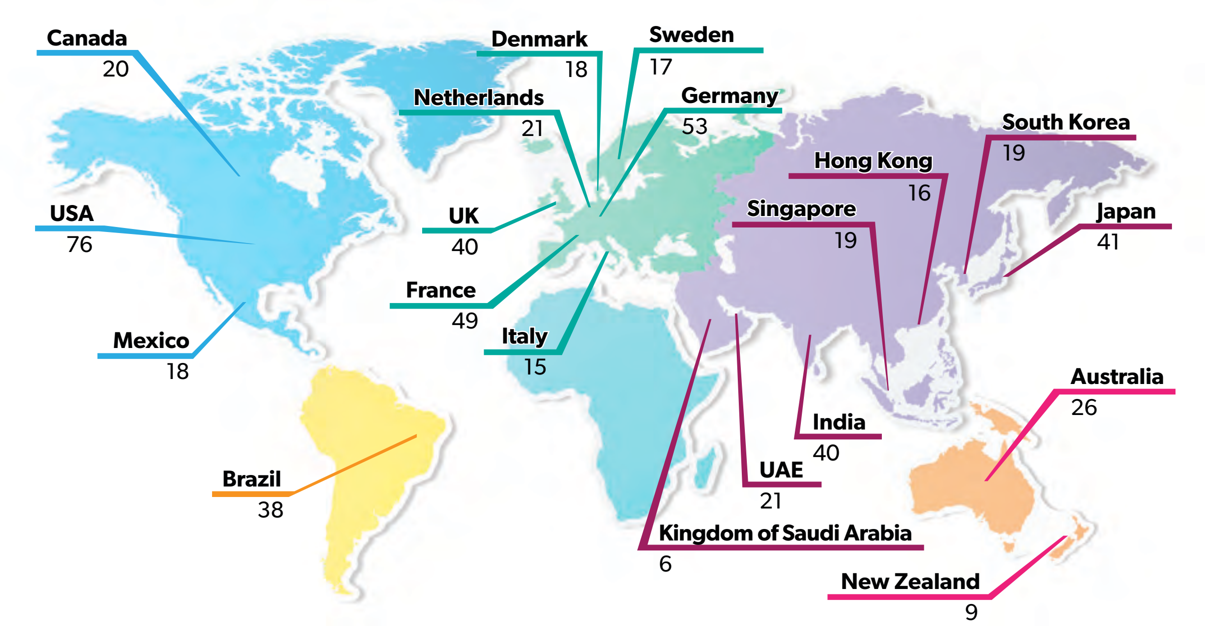
Organizations with 40% or more of employees using Multi-Factor Authentication



While this year's survey results indicate improvements in security posture, much more is needed to elevate operational data security to fully support the capabilities of emerging technologies such as GenAI and to pave the way for future innovations.

About this Study

This research was based on a segment of 562 healthcare, biotechnology and pharmaceutical industry respondents extracted from a global survey of 3,163 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria regarding 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	36
$250m to $499.9m	158
$500m to $749.9m	147
$750m to $999.9m	140
$1 Bn to $1.49 Bn	25
$1.5 Bn to $1.99 Bn	24
$2 Bn or more	32
Total	562

Industry Sector	Number of Respondents
Healthcare	274
Biotechnology	124
Pharmaceuticals	164
Total	562

THALES

Building a future we can all trust

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

cpl.thalesgroup.com/healthcare-lifesciences-data-threat-report