

Europe and Middle East Edition

THALES
Building a future we can all trust

2024 DATA THREAT REPORT

Navigating New Threats and Overcoming Old Challenges

#2024DataThreatReport

cpl.thalesgroup.com

SUPPLEMENT TO GLOBAL EDITION

In this report, we share key findings from the **2024 Thales Data Threat Report (DTR)**, focused on the **Europe and Middle East (EME) region**, and we briefly discuss differences between EME and global responses, along with enterprise observations and a summary of the threat landscape. Many of the EME DTR results were close to the global responses, but we call out key differences.

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

Key Findings

Data Breach Trends and Threats

The proportion of EME organisations that have ever been breached remains high (49% Global, 51% EME). However, the percentage that have experienced a recent breach has decreased. Globally, that figure fell from 24% in 2021 to 15% in 2024. **In EME, recent breach history decreased from 30% in 2021 to 15% in 2024 — a 15 percentage point difference.** Compliance success is strongly correlated with a lower incidence of recent breaches. Among EME enterprises that had passed all compliance audits, less than 4% reported a recent breach history.

51%



Ransomware attacks are increasingly common, with 28% Global and 27% of EME respondents experiencing an attack, up from 22% Global and 21% EME in the prior survey. Planning remains poor, with only 19% of EME respondents saying they would follow a formal incident response plan in the event of an attack, slightly lower than the global percentage.

27%

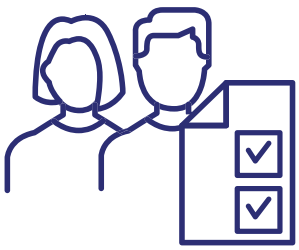
Human factors remain a major cause of cloud data breaches; human error was the leading cause of breaches, at 31% for both Global and EME respondents. Failure to apply multi-factor authentication (MFA) to privileged accounts constituted another 17% both Global and in EME.

31%

Identity Complexities and Compromise

On average, customers account for one-sixth (16%) of all external access to respondents' IT systems and resources. This figure is similar among both EME and global respondents (16%).

16%



Among respondents who cited external identity as an emerging security concern, achieving security consistency across workforce and non-workforce identities is the most frequently cited challenge in enabling external identities both in EME (59%) and Global (62%).

59%

Increasing DevOps Challenges

55%

Among respondents who cited Cloud/DevSecOps security as an emerging security concern, **the greatest proportion cited secrets management (56% Global, 55% EME) as a top DevOps challenge,** followed by workforce IAM issues such as privileged user management (52% Global, 51% EME).



Operational complexity remains a security concern. The results reflect incremental improvement. The proportion of respondents with five or more key management systems in use declined by 9 percentage points both Global (53% versus 62% a year ago) and in EME (55% versus 64% a year ago). The average number of key management systems also declined slightly year over year, from 5.8 to 5.7 Global (a 2% reduction) and from 6.0 to 5.8 in EME (down 3%). **This suggests that EME organisations and their Global counterparts need to further simplify operations.**

5.8

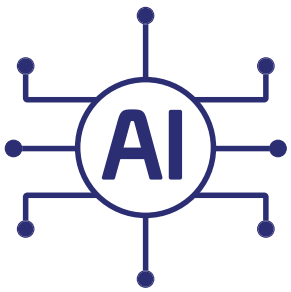
Risks to Emerging Technologies

Regarding threats from quantum computing, future compromise of classical encryption techniques, enabling "harvest now, decrypt later" (HNDL) attacks, is leading interest in post-quantum cryptography (68% Global, 70% EME). Among respondents who identified post-quantum cryptography as a source of emerging security threat, more than half said they would likely prototype or evaluate PQC algorithms in the next 18-24 months (52% Global, 55% EME). **While EME organisations and their Global counterparts are equally concerned about HNDL attacks, EME respondents are slightly more likely to deploy PQC than the Global average.**

70%

The generative AI boom is underway: 22% of Global and 23% of EME respondent organisations plan to integrate GenAI into security products and services in the next 12 months, while 33% of Global and 31% of EME plan to experiment with integrating the technology. **These percentages suggest that EME organisations are proceeding with AI for security at a similar pace to their Global counterparts, albeit with a slight variance in integration versus experimentation.**

23%



Enterprise Observations

This year's DTR provides additional insights into the enterprise IT and security organisation. 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 on common inputs, processes and outcomes. Through the years, DTR findings have shown a stronger correlation between compliance achievement and reduced breaches. In 2024, of the EME respondents whose organisations failed a compliance audit, 85% reported having some breach history, similar to the global result. In contrast, for those EME organisations that passed all compliance audits, only 23% reported a breach history (slightly lower than global), and only 4% experienced a breach in the past 12 months (similar to global results).

KEY STATISTIC

In 2024, of EME respondents whose organisations failed a compliance audit in the past 12 months, 85% reported having some breach history, with 29% saying they experienced a breach in the last 12 months.

85%

KEY STATISTIC

In contrast, for those that passed compliance audits, only 23% have a breach history and only 4% suffered a breach in the last 12 months.

23%

Compliance is arguably different than security, but both disciplines use many of the same techniques. Increasingly, regulatory oversight blurs distinctions between compliance and security diligence. For example, compliance standards such as AICPA SOC2 Type 2 and ISO27K require organisations to demonstrate controls over time (a characteristic typically associated with security) rather than at a single point in time. Automation will continue to drive improvement in this area, such as through the application of security as code. Among EME respondents prioritizing DevSecOps, 39% said their configuration, compliance and security controls were defined as code, similar to the global result (38%). This report shares further insights on enabling developers and operators to achieve better security and service outcomes.

The Threat Landscape

In EME as in the rest of the world, the attack landscape remains vast and growing, and EME organisations are faring similarly to their global counterparts. **Nine out of 10 EME respondents (92%) said they experienced an increase in attacks, similar to global results (93%).** The three fastest-growing types of attacks reported in EME were malware, phishing and ransomware, similar to global results. In particular, 42% of EME respondents prioritized malware as one of the fastest-growing attack types, followed by 37% prioritizing phishing and a further 31% citing ransomware. Global figures were similar at 41%, 36% and 32%, respectively. Meanwhile, the most common root cause of cloud data breaches was human error (31% Global, 31% EME), with failure to use MFA for privileged user accounts (17% Global, 17% EME) also a significant factor.

When we examined the top attack root causes by attacker type within EME, the top "toxic combination" was accidental incidents (caused by human error) where a known vulnerability was exploited. This is the typical recipe for a phishing attack. The number two and number three most-mentioned attacker types, external attackers with ideological goals and external attackers with geopolitical goals, typically used a misconfiguration to gain access, which is also caused by human error. As in past years, humans remain the top threat vector, and with attacks increasingly performed at machine speed, it is becoming necessary to counter these attacks at machine speed as well.

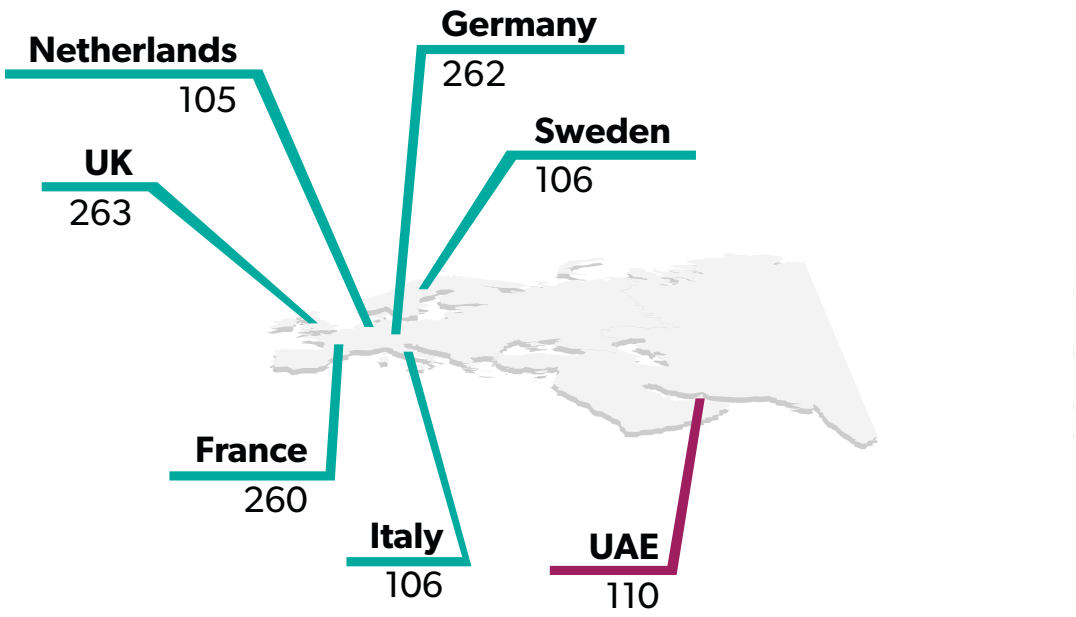
Ransomware response remains a challenge. For the last three years, less than 50% of global respondents across all verticals and company sizes have reported having a formal ransomware plan — and only 19% of EME respondents have one. Overall, 18% of EME respondents said that, in the event of a ransomware attack, they paid or would pay the ransom, similar to global responses. Initial breach response is increasingly led by legal teams interfacing with regulators or law enforcement.

The complexity of cloud resources present among users, operators and developers continues to grow. The percentage of EME enterprises saying they have more than 50 SaaS apps in use has increased from 27% in 2021 to 32% in the 2024 survey, similar to global results (27% in 2021 growing to 31% in 2024). The survey-wide average is now 84 SaaS applications in use, with EME reporting an average of 90. The percentage of EME enterprises that agree or strongly agree that managing security in the cloud is more complex than on-premises has grown slightly from 53% in 2021 to 55% in the 2024 survey.

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 identity and access management, IoT/5G, post-quantum cryptography and digital sovereignty. **EME responses differed from those global, with cloud security and DevSecOps the top choice, followed by digital sovereignty, customer identity and post-quantum decryption.**

About This Study

This research is based on a subset of the global DTR survey of 2,961 respondents that was fielded in November and December 2023 via a web survey aimed at professionals in security and IT management. This subset comprises targeted populations in select European and Middle Eastern countries for a total of 1,212 respondents across 36 industries. 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 organisations with annual revenue of less than US$100 million. The majority of respondents (85%) were affiliated with organisations reporting annual revenue between US$100 million and US$999.9 million. This research was conducted as an observational study and makes no causal claims.



Revenue	Number of Respondents
$100m to $249.9m	14
$250m to $499.9m	357
$500m to $749.9m	335
$750m to $999.9m	320
$1 Bn to $1.49 Bn	79
$1.5 Bn to $1.99 Bn	39
$2 Bn or more	68

Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Retail	65	Telecommunications	41
Healthcare	62	Automotive	38
Manufacturing	61	Transportation	37
Technology	52	Food & Beverage	36
Public Sector	47	Consumer Products	35
Financial Services	44	Advertising/Marketing	32
Energy & Utilities	43		

THALES

Building a future we can all trust

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

cpl.thalesgroup.com/euro-data-threat-report

© Thales - August 2024 • GHv4