Europe and Middle East Report

THALES
Building a future we can all trust

2022 Thales Data Threat Report

Navigating Data Security in an Era of Hybrid Work, Ransomware and Accelerated Cloud Transformation

#2022DataThreatReport

cpl.thalesgroup.com

Introduction

Going on two years, the COVID-19 pandemic continues to dramatically impact IT teams worldwide. The 2022 Thales Global Data Threat Report looked at many aspects of those impacts, with insights found from topics such as ransomware, remote work, zero-trust security strategies and cloud data security trends. This report covers respondents based in France, Germany, the Netherlands, Sweden, United Arab Emirates and the U.K. This report analyses 1,070 respondents from midsize to large enterprises within many diverse verticals in the public and private sectors. Unless mentioned otherwise, respondents in this report are defined as those respondents from these countries.

451 Research

S&P Global
Market Intelligence

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

46%

of Europe and Middle East respondents reported an increase in the number of attacks.

73%

of respondents said they would trust their organization with their own personal data.

Contents

Breaches Still Disturbingly High

Despite substantial annual spending on cybersecurity, breaches are still being reported at a disturbingly high rate: In 2022, more than half (53%) of respondents reported that they have experienced a security breach at some point, and of these, 37% said they had experienced a breach in the last 12 months. The worldwide numbers were similar: 52% said they have a breach history, and of those, 35% experienced a breach in the last 12 months.

One possible reason breach history remains high is the lack of information on the location and classification of data. In this year's survey, only 19% of respondents said they have complete knowledge of where their data is stored, with only 26% of respondents being able to fully classify data. Safe harbour from breach notification processes also remains elusive, as 59% of those breached were unable to obtain it. In comparison, 61% of all U.S. respondents could not obtain safe harbour from encryption or tokenisation.

Breaches Reported by Europe and Middle East Respondents

HAS YOUR ORGANISATION EVER BEEN BREACHED?

Source: 451 Research's 2022 Data Threat custom survey

37%

of Europe and Middle East respondents reported that they had experienced a security breach in the last 12 months.

Only

19%

of Europe and Middle East respondents said they had complete knowledge of where their data is stored.

"Only 26% of Europe and Middle East respondents said they are able to fully classify data."

Security Threats

Forty-six percent of respondents reported an increase in the number of attacks. Of those respondents who saw an increase, 55% reported an increase in malware attacks, and 51% reported an increase in ransomware attacks. Among last year's respondents (2021), 55% ranked malware to be the leading source of increased security attacks, and ransomware came in second at 47%. The speed with which ransomware attacks occur and the increased economic impact will continue to alter the way organisations detect and respond to breaches.

Despite increased attacks, organisations remained confident. Seventy-nine percent of respondents said they would trust their organisation with their own personal data. Confidence was high at all levels, with 82% of senior leadership, 78% of management and 73% of individual practitioners reporting they would trust their organisation with their own data.

Among threat actors in ranked choice voting, 77% of respondents prioritised internal, incidental error, followed by 74% external adversaries motivated by ideology – "hacktivists." External adversaries with geopolitical goals, such as nation-state actors, came in third place at 74%. In another ranked choice vote, 34% of respondents said that their cloud storage is the greatest target for adversaries. Cloud databases and cloud delivered apps (IaaS-based) were prioritised as targets by 32% and 29% of respondents, respectively.

55%

ranked ransomware as the leading source of increased security attacks.

Ransomware Planning and Response

In 2022, the study had a new focus on ransomware planning and response. The speed and severity of ransomware, compared to "low and slow" data exfiltration attacks from most malware strains, impacts both data confidentiality and availability. Among respondents, 22% have suffered a ransomware attack. Of those attacked, 76% had some internal or external impact, and 28% suffered a significant internal or external impact. Of greater concern, only 48% of respondents said they have a formal ransomware response plan that they would follow. Twenty-two percent of respondents said they paid or would pay a ransom to recover from a ransomware attack. Given the severity and speed of ransomware attacks, a centralised and formal plan that ties together diverse stakeholders such as security operations, legal and senior leadership teams should be first when coordinating a coherent response.

Only

48%

of respondents said they have a formal ransomware response plan that they would follow.

Continued Era of Remote Working Security

Many organisations extended remote working for employees in the past year. Concerns about security risks of remote employees continued in 2022, with 31% "very concerned" and 49% "somewhat concerned." It was much the same story worldwide: 31% of global respondents said they were "very concerned" and 48% "somewhat concerned". Attitudes improved about their current remote access security solutions to effectively enable employees to securely work: 27% of respondents said they were "highly confident", 34% said "significantly" confident, 22% said "slightly confident and 16% said "not at all" confident in their secure remote access solutions.

When asked about remotely accessing applications, 58% of respondents said they use virtual desktop infrastructure (VDI). VPN came in second at 54%, followed by cloud-based single sign-on (SSO) and zero-trust network access (ZTNA) at 48% and 36%, respectively. These are similar to the worldwide numbers, at 59% for VPN, 55% for VDI, 51% for cloud-based SSO and 36% for ZTNA/software-defined perimeter.

In 2022, 80% of Europe and Middle East respondents were either "very concerned" or "somewhat concerned" about security risks of remote employees."

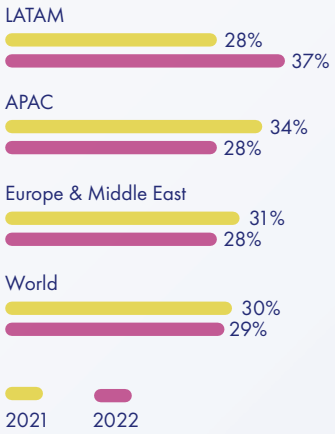
Zero-Trust Strategies Gaining Momentum

The principle of zero trust is based on the recognition that identities, networks, devices, applications, and data are no longer confined within traditional corporate networks. In general, zero-trust principles mean that there are no implicit or assumed levels of trust between identities, networks or even sets of data. As such, perimeter-based approaches to security that rely on outdated notions of "trust" that are largely rooted in physical location (i.e., which network data exists on) have become less effective. In contrast, zero-trust approaches rely primarily on identity as a central means of granting access to resources. Perhaps because zero-trust security strategies cover so much ground, fewer respondents said they have a formal zero-trust strategy.

This is an area where Europe and Middle Eastern respondents are closely aligned with the global percentages. In 2021, 31% of respondents said they had a formal strategy, while in 2022 only 28% said they have embraced a formal strategy. At the time of this study, another 29% of respondents were still in research and planning to develop a formal zero-trust network access (ZTNA) strategy. Forty-six percent of all respondents said they rely on "some concepts" of zero-trust security strategy to shape their overall cloud security strategy, and another 36% of respondents said that zero trust shapes their cloud security strategy to a great extent.

Formal Zero-Trust Strategy/Policy Among Europe and Middle East Respondents

WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?



Source: 451 Research's 2021 and 2022 Data Threat custom surveys

"In 2022, Europe and Middle East respondents who said they had a formal zero-trust security strategy was down by 3% against 2021."

Cloud Momentum, Cloud Coverage Gaps

Organisations worldwide place increasing amounts of data in the cloud, and Europe- and Middle East-based organisations are no exception. In 2021, 30% of respondents stated that 41-50% of their data was stored in external clouds. Nearly a quarter (24%) of respondents said over 50% of their data was stored in external clouds. In 2022, 54% of respondents said they have at least 40% of their data in the cloud and 22% reported over 60% of their data in the cloud. Worldwide, 55% of respondents said they have at least 40% of their data in the cloud, and 23% said they have at least 60% in the cloud.

Gaps in protection are shrinking. In 2021, only 29% of respondents said 41-50% of their sensitive data stored in the cloud was encrypted, and only 17% of respondents said that more than 50% of their sensitive cloud data was encrypted. In 2022, 51% of respondents said at least 40% of their sensitive cloud data is encrypted, and 23% said at least 60% of their sensitive cloud data is encrypted. Recent breach history remains high, but the rate is declining slightly. In 2021, 46% of respondents experienced a breach or failed an audit involving cloud data and applications in the last 12 months. In 2022, this improved to 37% of respondents.

Despite growth in the cloud and cloud-first strategies, last year, 45% of respondents "agreed" or "strongly agreed" that it was more complex to manage privacy and data protection regulations in a cloud environment compared to on-premises networks within their organisation. In 2022, 51% of respondents said that they "strongly agreed" or "agreed" that cloud privacy and data protection regulations are more complex to manage than on-premises environments. Worldwide respondents in 2022 reported the same, with 51% "agreeing" or "strongly agreeing." Adding to some of this complexity, different personas are responsible for cloud security strategy. In 2022, 50% of respondents said that policies are centrally defined by a security team, but defining technical standards and enforcing them is up to the individual developer or application owner. Another 36% said that policies and standards are centrally defined and enforced by the security team.

Policy Definition and Implementation Stakeholders

HOW DO YOU DECIDE AND ENFORCE POLICIES AND STANDARDS FOR CLOUD SECURITY?

- Policy defined and enforced by central security team — 36%
- Policy defined by security team, implemented by cloud delivery team — 50%
- Policy defined & implemented by cloud delivery teams — 14%

Source: 451 Research's 2022 Data Threat custom survey

37%

of Europe and Middle East respondents said they experienced a breach or failed an audit for cloud applications or cloud data in the last 12 months.

Most Firms Are Using a Multicloud Strategy

The status of encryption in the cloud is further complicated by the fact that most organisations in our survey are using multiple cloud providers, across all "flavours" of cloud: IaaS, PaaS and SaaS. In 2022, we found near-parity among respondents employing AWS and those using Azure: 47% use AWS and 46% use Azure for production workloads. This is a significant change compared to 2021, when 54% of respondents used AWS and only 39% used Microsoft Azure. The most varied cloud usage, not surprisingly, is with SaaS. The greatest percentage of respondents (35%) use more than 50 SaaS applications, and 19% are using more than 100 SaaS apps. A small proportion (4%) of respondents reported using more than 500 SaaS apps. As more SaaS is delivered in API form, the expected "heterogeneity" of cloud usage certainly increases concerns (and challenges) about managing encryption keys and identities across multiple providers.

Multiple Clouds and Key Management Options Driving Complexity

Given the diversity of IaaS and SaaS, existing on-premises infrastructures, as well as security mandates requiring consistent controls throughout agencies, it's no wonder that organisations have a mixture of encryption and key management solutions. Specifically, our 2022 survey found that the largest percentage (42%) of Europe- and Middle East-based organisations employ between five and seven separate key management products, while a smaller number (10%) have as many as 8-10 key management products. These typically include a mix of key management software, hardware security modules, homegrown solutions and spreadsheets or flat files.

Organisations not only have a variety of cloud providers and key management technologies to choose from, but they can also choose the types of controls for encryption and key management from cloud providers. To illustrate, over half of respondents indicated that their cloud provider controls most or all their encryption keys, and another 38% said their organisation controls most or all the encryption keys deployed for cloud data. Only 8% of respondents in 2022 reported a "shared" key-generation/key-control arrangement, where the agency controls key-generation material, but the cloud provider furnishes key control.

Many cloud services and platforms may offer data encryption as a feature, yet underlying key management is not as well emphasised or understood, which may add further complexity to cloud data protection. When asked what security technologies are prioritised to protect sensitive data in the cloud, 56% of respondents chose data-at-rest encryption, whereas only 52% chose key management. Organisations would be better served taking a holistic look at the different encryption and key management solutions to identify further gaps in implementation and safety.

Cloud Encryption Drivers

WHAT IS THE PRIMARY DRIVER FOR DECISIONS ON WHERE AND HOW ENCRYPTION IS USED IN CLOUD?

- Internal security architecture decisions — 43%
- Regulatory compliance requirements — 41%
- Customer or partner requirements — 12%
- Other requirements — 3%

Source: 451 Research's 2022 Data Threat custom survey

42%

of Europe and Middle East organisations employ between five and seven separate key management products.

Moving Ahead

This study can serve as an indicator of potential paths that organisations in the Europe and Middle East region may choose to follow on their security journey. One of the key lessons learned from the pandemic was that security strategies must be sufficiently agile to respond to a rapidly changing world, but also flexible enough to deal with the hybrid nature of our infrastructure, applications, data and users as both hybrid work and cloud become permanent fixtures in the security landscape.

The study reinforced the need for organisations to better understand and inventory data throughout its lifecycle across both on-premises and cloud infrastructure. A better understanding of the risks will shape security incident response and resilience, especially with ransomware attacks that aim to seize and extort as much of the enterprise as quickly as possible. Understanding the risks as they pertain to zero-trust architectures for data, devices and identities provides visibility and delivers assurance to governance and regulation.

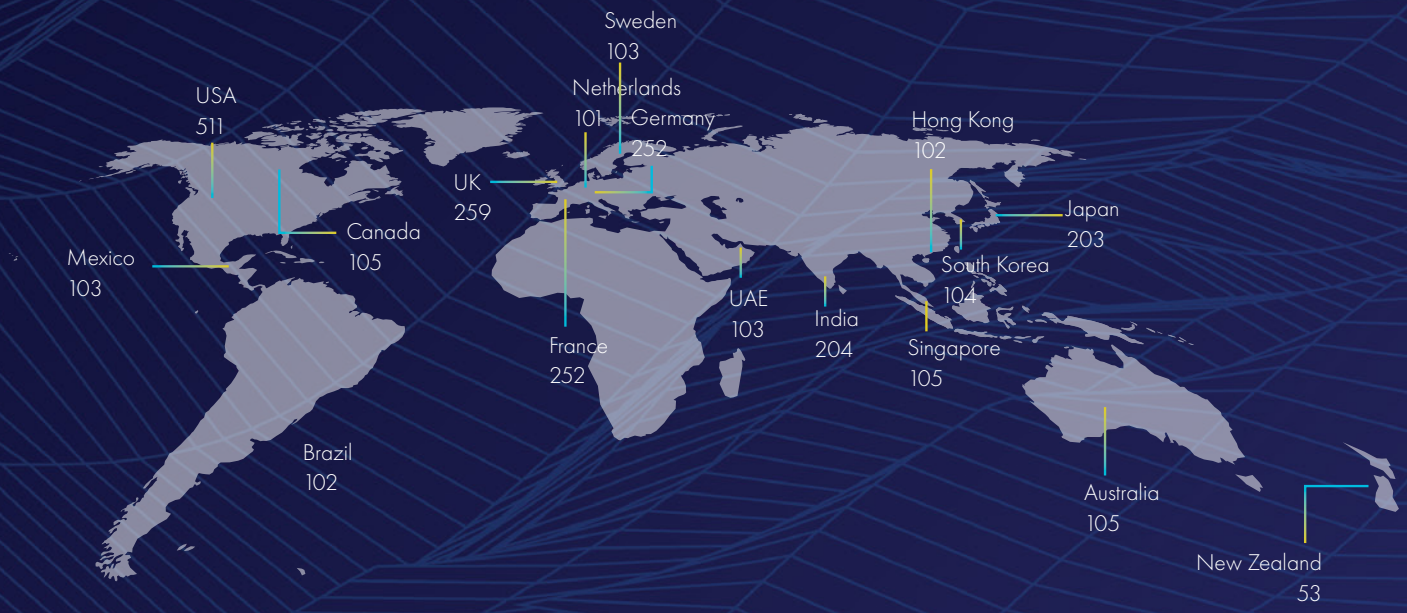
For all their benefits, cloud computing and hybrid environments have also layered on considerable complexity, an issue that is reported more significantly in Europe and the Middle East. We know that complexity is the enemy of good security. This means that both security controls and security management will need to extend to cloud in ways that keep each cloud environment from being an isolated operational realm, as well as leverage service-based offerings and automation to reduce manual burdens.

Cloud computing and hybrid environments have layered on considerable complexity, and we know that complexity is the enemy of good security."

About This Study

The COVID-19 pandemic has had an immediate and dramatic impact on IT teams around the globe, and its long-term effects are still evolving. The Europe and Middle East edition of the 2022 Thales Data Threat Report study looked at various aspects of those impacts in a wide-ranging survey of security professionals and executive leadership that touched on issues ranging from COVID-19 and work-from-home strategies to quantum computing.

The 2022 Thales Data Threat Report is based on a survey of almost 2,800 security professionals and executive leaders, including 1,070 respondents from Europe and the Middle East.



Industry Sector

Manufacturing	157
Retail	154
Technology	127
Financial Services	120
Healthcare	115
Public Sector	109
Consumer Products	107
Computers/ Electronics/Software	106
Engineering	104
Federal Government	103

Revenue

$100 million to $249.9 million	162
$250 million to $499.9 million	802
$500 million to $749.9 million	865
$750 million to $999.9 million	458
$1 billion to $1.49 billion	254
$1.5 billion to $1.99 billion	58
$2 billion or more	168

THALES
Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/data-threat-report