EUROPEAN EDITION

THALES
Building a future we can all trust

EXECUTIVE SUMMARY

2021 Thales Data Threat Report

Data Security in the Era of Accelerated Cloud Transformation and Remote Work

#2021DataThreat

cpl.thalesgroup.com

Contents

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 European edition of the 2021 Thales Data Threat Report looked at different 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 (WFH) strategies to quantum computing.

The 2021 Thales Data Threat Report is based on a survey of more than 2,600 security professionals and executive leaders, including more than 950 in Europe.

451 Research

S&P Global
Market Intelligence

Source: 2021 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Our sponsors are:

Key Findings

"Half (49%) of European organisations reported an increase in the volume, severity and/or scope of cyberattacks in the past year."

Good News and Bad News for Security Professionals

Overall, the survey results offered a mix of both positive and not-so-positive findings. The bad news is that breaches are still being reported at a disturbingly high rate: 58% of European respondents claimed to have experienced a security breach at some point, and of these, 42% said they had experienced a breach within the last 12 months. Indeed, nearly half (49%) reported an increase in the volume, severity and/or scope of cyberattacks in the past year, particularly malware (54%) and ransomware (47%). Clearly, as attackers get better at their job, it gets harder for security professionals to do theirs. Further complicating matters is that most organisations don't have a solid grasp of what data they have and where it is located: three-fourths of respondents (75%) don't have full knowledge of where their data is stored, and less than one-third of European respondents claimed to be able to fully classify all of their data.

FIGURE 1

Breaches Reported by European Respondents

Q: Has your organisation ever been breached?

Source: 451 Research's 2021 Data Threat custom survey

On the plus side, nearly half of respondents were able to avoid a breach notification process because the stolen or leaked data was encrypted or tokenised; however, 53% of respondents saying 'no' (meaning that many firms were likely subject to fines) is an indication that there is clearly work to be done. In terms of spending priorities, data loss prevention was ranked first at 38%, with encryption a close second at 37%. Similarly, 37% of respondents selected tokenisation as the most effective option for protecting sensitive data, followed by data discovery and classification (36%) and encryption (34%).

COVID-19 Ushers in Permanent Changes to the Workforce, Accelerates Cloud Adoption

The effects of the COVID-19 pandemic are manifesting through changes in the nature of the workforce – particularly remote working arrangements and changes to the composition of branch offices. They are also hastening the pace at which enterprises have shifted resources to the cloud. A large portion of European respondents were ill-prepared for both COVID-19 and the related WFH phenomenon: More than three-fourths of respondents said they were unprepared to some degree (just 22% were 'very prepared'). Additionally, 38% of respondents are 'somewhat' concerned about the security risks/threats of employees working remotely, while nearly half of respondents (46%) indicated that privacy and security were the most important investments during the pandemic, ahead of investment in infrastructure/cloud (34%) and investment in distributed (hybrid) cloud (21%).

> "A large portion of European respondents were ill-prepared for both COVID-19 and the related WFH phenomenon."

FIGURE 2

Security Infrastructure Preparation Reported by European Respondents

Q: How prepared was security infrastructure to handle the range of risks associated with the new business operating environment caused by the pandemic?

22% Very prepared
32% Somewhat prepared
29% Somewhat unprepared
17% Not at all prepared

Source: 451 Research's 2021 Data Threat custom survey

Zero Trust Strategies Gaining Momentum

The principle of Zero Trust is based on recognition that applications, resources, devices and users are no longer confined within traditional corporate networks. 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 a user is on) have become less effective. In contrast, Zero Trust approaches rely primarily on identity as a central means of granting access to resources and data, and with the increased WFH and cloud usage driven by COVID, Zero Trust has, not surprisingly, become one of the hottest 'buzzwords' in security over the past several years, and perhaps for good reason: 32% of European respondents on average said they have a formal strategy and have actively embraced a Zero Trust policy, while 44% rely on some concepts of Zero Trust to inform their cloud security strategy. Sweden (38%) and Germany (36%) specifically showed some of the highest adoption rates for Zero Trust amongst all countries, and well ahead of the US at 25%. Perhaps most noteworthy is that our survey found that those organisations with a formal Zero Trust strategy are less likely to have been breached.

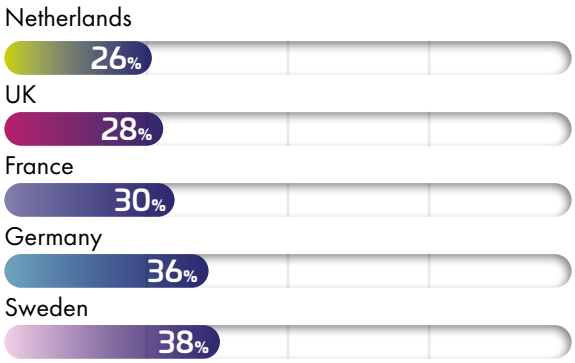
> **"32% of European respondents on average said they have a formal strategy and have actively embraced a Zero Trust policy."**

FIGURE 3

Number of IaaS/PaaS/ SaaS Vendors

Q: Where are you on your Zero Trust journey?

Response: Execution: We have a formal strategy and are actively embracing Zero Trust policy



Source: 451 Research's 2021 Data Threat custom survey

44%

rely on some concepts of Zero Trust to inform their cloud security strategy

WFH and Zero Trust Driving Increased Interest in Identity-Based Access Controls

With respect to the pandemic specifically, respondents were less than confident in their existing remote access security products to effectively enable employees to work remotely in a secure and easy manner – just 36% of respondents were 'somewhat' confident. By contrast, 43% selected conditional access (defined as a method for granting access based on certain conditions, such as contextual indicators like time of day, device status, etc.) as the leading technology they planned to deploy during the pandemic, followed closely by Zero Trust network access, software-defined perimeter and cloud-based access management (access management service that offers policy-based access, authentication and single sign-on (SSO) delivered from the cloud), selected by 42% each.

One positive response to increased WFH and Zero Trust has been a greater willingness to adopt multi-factor authentication (MFA) and other identity-related techniques. After years of languishing behind other security tools such as network and endpoint security in terms of enterprise adoption – existing 451 Research data points to enterprise adoption levels hovering just over 50% – nearly two-thirds (64%) listed MFA as a new technology to invest in, while 62% cited access management (SSO) and MFA as one of the security technologies most effective in protecting sensitive data.

64%

nearly two-thirds listed MFA as a new technology to invest in

62%

cited access management (SSO) and MFA as one of the security technologies most effective in protecting sensitive data.

Encryption, Key Management and MFA Top Choices to Protect Data in the Cloud

The value of encryption to protect sensitive data is even more pronounced in the cloud, particularly as the cloud is increasingly used as a repository for sensitive data – more than half of respondents (55%) indicated that 31-50% of their data that is stored in an external cloud is sensitive. Nearly two-thirds (63%) of respondents selected encryption as the primary tool to secure sensitive data stored in the cloud, followed by key management (56%) and multi-factor authentication (53%). However, there is a significant disconnect between interest levels and practice, as few firms encrypt a large percentage of their sensitive data – only 17% of respondents stated that more than half of their sensitive data stored in cloud is encrypted. In other words, the vast majority of respondents encrypt less than half of their sensitive cloud data. This is despite the fact that 43% of respondents said they have experienced a data breach, and nearly half (46%) have experienced a breach or failed an audit involving data and applications residing in the cloud. Part of the reason may be that encryption and key management can be complex, and skilled personnel with both cloud platform and security expertise are in high demand.

Most Firms Using a Multi-Cloud Strategy

The status of encryption in the cloud is further complicated by the fact that the majority of companies in our survey are using multiple cloud providers across all 'flavors' of cloud: IaaS, PaaS and SaaS. For example, just over half (54%) of respondents employ AWS, while 39% use Microsoft Azure, in line with global averages. The same holds true for PaaS, with the lion's share of respondents (42.9%) using two PaaS providers and nearly one-quarter (23%) using three. The most varied cloud usage, not surprisingly, is SaaS, with the vast majority of respondents (38%) using 26-50 SaaS applications, while 28% use more than 50 SaaS apps. The 'heterogeneity' of cloud usage certainly raises concerns about the challenges of managing encryption keys across multiple providers.

40%

of organisations have between five and seven separate key management products currently employed

33%

preferred keys controlled 'all' or 'mostly' by the cloud provider

Multiple Clouds and Key Management Options Driving Complexity

An additional challenge is that many firms are dealing with a multitude of key management systems, often inherited via mergers and acquisitions. Specifically, our survey found that nearly 40% of organisations have between five and seven separate key management products currently employed, while 15% said that that their company employs 8-10 key management products. These typically include a mix of key management software, hardware security modules, homegrown solutions, and spreadsheets or flat files.

In addition to a variety of cloud providers and key management technologies, firms also have choices in the types of encryption and key management they can obtain, either directly from their cloud provider, bring-their-own or some combination. To illustrate, in their IaaS/PaaS environments, 37% of respondents indicated a preference for using 'all' or 'mostly' encryption from their cloud provider, while only 22% indicated they would use 'all' or 'mostly' their enterprise encryption offerings. Similar results held for key management – 33% preferred keys controlled 'all' or 'mostly' by the cloud provider, compared to 24% selecting 'all' or 'mostly' enterprise control.

Quantum Computing Concerns Growing, but Less So in Europe

The much-anticipated arrival of quantum computing has significant long-term implications for cybersecurity, given its potential to break current cryptographic methods, particularly those related to asymmetric cryptography.

Not surprisingly, the study found that 44% of European respondents are 'very concerned' about the security threats of quantum computing, slightly lower than the global average of 47% (and considerably lower than most countries in APAC that averaged comfortably north of 50%). This level of awareness should translate into increased interest in post-quantum cryptographic techniques and efforts to improve crypto agility.

> **"44% of European respondents are 'very concerned' about the security threats of quantum computing."**

Moving Ahead

This study can serve as an indicator of potential paths organisations may choose to follow on their security journey. One of the key lessons learned from the pandemic was that security strategies have to 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 WFH and cloud become permanent fixtures in the security landscape. Thus, for all of their many benefits, cloud computing and hybrid environments have also layered on considerable complexity – and 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.

THALES

Building a future we can all trust

Contact us

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

To download the full report, including 451 Research recommendations visit

cpl.thalesgroup.com/data-threat-report