



EUROPEAN EDITION

THALES
Building a future we can all trust

EXECUTIVE SUMMARY

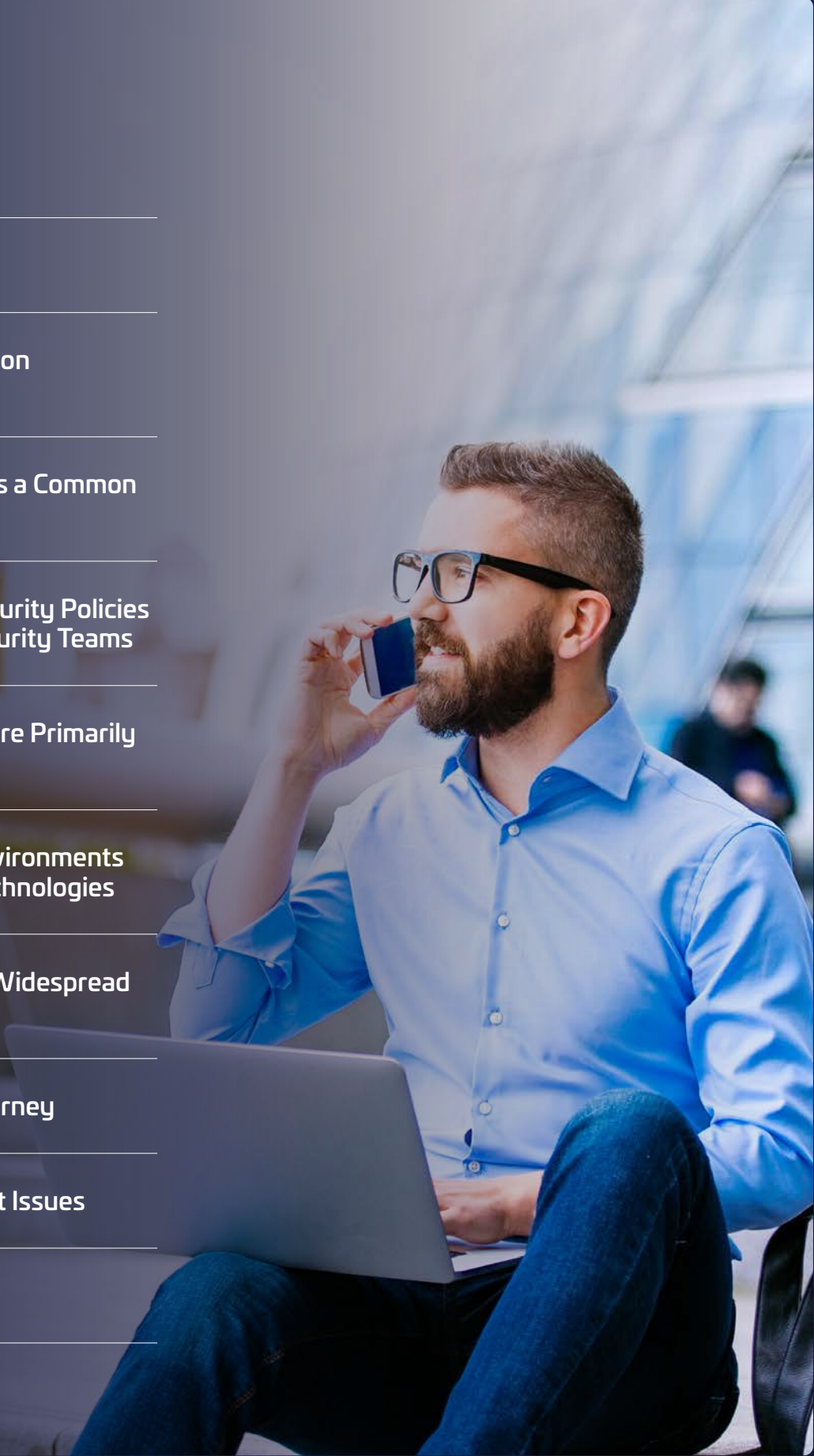
2021 Thales Cloud Security Study

The Challenges of Cloud Data Protection and Access Management in a Hybrid and Multicloud World



#2021CloudSecurity

cpl.thalesgroup.com



4	Introduction
5	Key Findings
5	Multi-Cloud Adoption Is Widespread
6	Cloud Complexity Is a Common Concern
6	Defining Cloud Security Policies Is Squarely for Security Teams
7	Cloud Migrations Are Primarily 'Lift & Shift'
8	Securing Cloud Environments Centres on Key Technologies
9	Encryption Is Not Widespread in the Cloud
10	The Zero Trust Journey
13	Breaches and Audit Issues
13	Moving Ahead

About this study

The pandemic has pushed organisations into many changes in the last year, but the move to greater use of cloud-based infrastructure was already underway. The demands of increased remote work and expanded digital delivery were just some of the imperatives that accelerated cloud use. The 2021 Thales Cloud Security Report, based on data from a survey of more than 2,600 respondents in more than 10 countries across the globe, looks to identify the depth of that change, as well as the current state of and plans for how organisations across a range of industries manage access to enterprise applications, cloud services and networks. This executive summary looks at the European segment of the results and compares and contrasts it with the global perspective. (The study includes the UK in European results for geographic continuity alongside France, Germany, the Netherlands and Sweden.) The insights in this report were gleaned from the survey data, and it explores the impacts on security strategy and planning.

The results of the survey show that, while a strong movement to cloud is in progress, there are limited security controls in place for what is a new infrastructure element for most. Respondents reported significant levels of data breaches, notably higher in Europe than the global average. Organisations have an opportunity to accelerate cloud utilisation by strengthening cloud security through tactics such as greater use of encryption to enable cloud use by a wider range of workloads.

451 Research

S&P Global Market Intelligence

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

Our sponsors are:



Introduction

“ Organisations need to extend and adapt their capabilities to manage security efficiently and effectively in these new, dispersed environments.”

Key Findings

- Stronger data privacy and governance requirements in Europe create a greater need for effective and efficient data management, but many organisations lack required capabilities.
- Europeans reported greater use of cloud consoles for key management, a practise that has increased risk.
- Respondents are slightly less emphatic in their identification of cloud management complexity than the global average.
- There is greater focus on the importance of multi-factor authentication (MFA) for data protection in cloud.
- While there is limited use of encryption for sensitive data in the cloud, European respondents reported greater use of bring-your-own (BYO) encryption.
- Europeans reported slightly higher levels of cloud-related data breaches.

Multi-Cloud Adoption Is Widespread

As organisations addressed the various challenges presented by the pandemic over the last year, they turned to cloud-based infrastructure to give them scale and reach. Cloud capabilities can bring applications closer to employees and customers faster than other options. However, that shift can create its own challenges because this is a new operating mode, and organisations may not understand its characteristics well, and procedures may not directly align with on-premises models. Organisations need to extend and adapt their capabilities to manage security efficiently and effectively in these new, dispersed environments, but survey results show that can be tricky.

Few organisations are working with a single cloud provider for infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS). This mix of providers can create operational complexity because each can have unique capabilities and controls. While European averages are close to global numbers, there are some outliers, an indication that the bloc isn't uniform in all aspects. Regarding PaaS providers, 73% of European respondents indicated that they have two or more, in line with global numbers. However, there is greater variability in the number of SaaS applications; while the largest percentage (38%) indicated that they have 26-50 on average, the Netherlands skewed lower (43 average) and Sweden much higher (78). The number of SaaS apps grows with organisational complexity as measured by revenue.

Cloud Complexity Is a Common Concern

The diversity of environments may also be contributing to operational complexity. Almost half of European respondents (45%, close to the 46% global average) agreed or strongly agreed that it is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks. Individual countries reported higher levels of concern, with the UK at 55% and the Netherlands at 56%. This should prompt organisations to look at ways to simplify their operations with security management capabilities that can span the various operating environments and standardise their operational processes across them.

FIGURE 1

Managing Cloud Security is Complex

To what extent do you agree with the following statement: It is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks within my organization.



- **19%** Strongly Agree
- **26%** Agree
- **19%** Disagree
- **19%** Strongly Disagree
- **16%** Don't Know

Source: 451 Research's 2021 Cloud Security custom survey

Defining Cloud Security Policies Is Squarely for Security Teams

Organisations need to have policies for defining and enforcing security policies that can cut through the complexity of the environments they have to manage. The survey looked at decision-making processes, and 84% of respondents indicated that security teams are involved in cloud security decisions, with roughly an even split between security teams running cloud security independently and those running security in collaboration with cloud engineering teams. However, there is some discrepancy in perception across job roles. Senior leadership views security teams as having greater responsibility, while staff have the perception that there is more collaboration. The same discrepancy exists when looking at roles in the purchase process as another lens into organisational hierarchy.

84%

of respondents indicated that security teams are involved in cloud security decisions

Cloud Migrations Are Primarily 'Lift & Shift'

There are many paths to cloud, and the survey looked at how organisations expect to transition to cloud environments. Just over half (53%) indicated that they expect to 'lift and shift' workloads, taking existing workloads and moving them to cloud with minimal change. Lift & shift is generally quick for workloads that can easily make the transition, but it can open gaps in protection if not carefully planned, and it may not make the most efficient use of cloud resources. Just 22% of respondents said they expect to do some level of re-architecting of applications. That's a path that can put native cloud capabilities to work more directly but can take more resources to implement. To protect workloads that have been shifted to cloud, organisations have to ensure not only that the controls that existed in on-premises environments can be delivered in their new surroundings, but also that they can be operated effectively and efficiently.

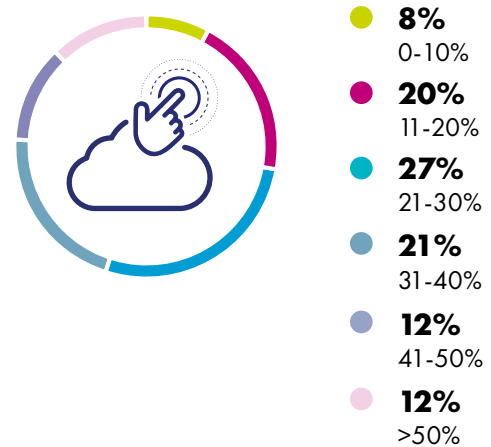
Securing Cloud Environments Centres on Key Technologies

Protecting applications and data in the cloud requires a new set of skills and potentially new technologies. The survey asked respondents to list the technologies they are using to protect data in cloud environments; 63% of European respondents cited encryption, followed by key management at 56% and MFA at 53%. Individual countries differed in the extent of their use of the various technologies. Sweden showed the highest level of encryption use, at 67%, but the lowest level of key management use, at 45%. The Netherlands showed consistently high use of all three technologies (encryption at 62%, key management at 65% and MFA at 57%). This variability underscores the complexity involved in cloud security management; these three leading technologies should all be in place to effectively secure cloud deployments. They should be in place to provide a secure foundation for cloud operations.

The survey looked at access management for cloud-based applications and found that organisations are using modern authentication technologies like MFA in a selective manner rather than broadly implementing them. Only 16% of European respondents (in line with the global average) are protecting more than 50% of their cloud-based applications with a modern authentication technology, which leaves the door open to an attack risk that has been growing considerably. This is clearly an area where additional investment is needed.

FIGURE 2
Cloud Applications Protected by MFA

What percentage of employees use MFA for cloud applications/SaaS applications?



Source: 451 Research's 2021 Cloud Security custom survey

Regional considerations on access management appear to align between European and global respondents. Similar to the global numbers of only 16% of respondents indicating they use MFA to secure more than half of their cloud applications, Europeans are also at 16%. Similar results occur when considering MFA access to more than half of their on-premises applications: 11% globally, 12% for Europe.

When considering complexity of securing both on-premises and cloud services with their access management capabilities, 67% of Europeans (compared to 66% globally) listed the issue as 'challenging' or 'very challenging'.

Encryption Is Not Widespread in the Cloud

Data protection is another area that showed considerable underinvestment. Respondents said that encryption is important for data protection, but their responses indicate limited implementation. Only 17% of European respondents said they encrypt more than 50% of their sensitive data in cloud environments. While that was in line with the global average, these organisations are leaving themselves open to considerable risk. And it's not a matter of limited cloud use: almost a quarter (24%) of European respondents reported having over 50% of workloads with an external cloud provider, and they said that 22% of the data residing in cloud is sensitive.

The other aspect of data protection effectiveness in cloud is key management. On average, European respondents were similar to the global average regarding the control of their keys (36% indicated that they control most or all of their keys), but they rely more heavily on cloud provider consoles for that control (57% vs. 52%). Organisations that aren't in control of their own keys face not only the security risk of potential data exposure, but they also create management complexity in the handling of their key material because they have to coordinate their activities across different environments for the on- and off-premises key management systems. That's a situation that is not only more resource-intensive, but it is also more prone to operational errors. Investing in a key management system that spans the breadth of an organisation's infrastructure can reduce staff workloads and improve the security posture.

Only

17%

of European respondents said they encrypt more than 50% of their sensitive data in cloud environments.

63%

of European respondents cited encryption as the technology they are using to protect data in cloud environments

“ Organisations that aren't in control of their own keys face not only the security risk of potential data exposure, but they also create management complexity in the handling of their key material because they have to coordinate their activities across different environments for the on- and off-premises key management systems.”

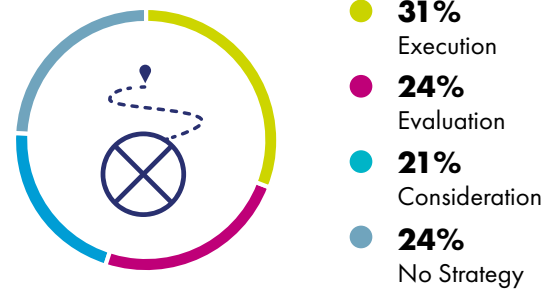
The Zero Trust Journey

One of the trends that the survey identified was the shift to greater use of Zero Trust operating principles. Organisations are looking to improve their security posture by limiting access and applying more granular, policy-based controls that the Zero Trust operating mindset offers. It's a focus that can be particularly effective in securing the distributed model that cloud offers. Respondents reported that they are at the beginning of their journey to Zero Trust, with less than a third saying that they are executing on a Zero Trust plan.

The good news is that the survey results found that a strong majority (76%) believe that Zero Trust principles shape their cloud security strategy. That's an indication that they see the importance of being able to apply more granular controls. It also reiterates the need for investment in the technologies required to achieve Zero Trust capabilities. Zero Trust requires a solid security foundation that includes effectively managed data protection and access management. The survey results show that organisations need to invest in modern authentication, like MFA, and key management systems to deliver the full protection of data encryption.

FIGURE 3 Zero Trust Journey

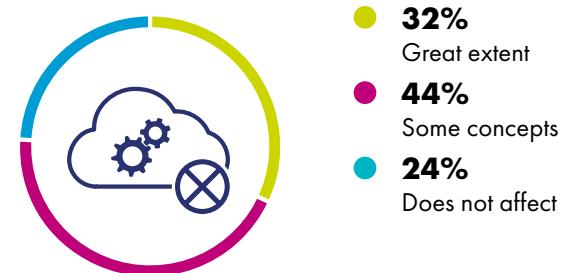
Where are you on your Zero Trust journey?



Source: 451 Research's 2021 Cloud Security custom survey

FIGURE 4 Zero Trust in Cloud Strategy

To what extent does Zero Trust security shape your cloud security strategy?



Source: 451 Research's 2021 Cloud Security custom survey



“ Organisations are looking to improve their security posture by limiting access and applying more granular, policy-based controls that the Zero Trust operating mindset offers.”

43%

of European respondents indicated their organisation has had to deal with a breach in their cloud environment

“ More senior decision-makers may be insulated from the realities of their environments and may not understand the urgency with which investments need to be made.”

Breaches and Audit Issues

The ultimate proof of security effectiveness is the number of successful attacks that organisations experience. The survey looked at breaches, and 43% of European respondents indicated their organisation has had to deal with a breach in their cloud environments. This is higher than the global average of 40%. The Netherlands was higher at 52% respondents indicating a breach. Swedish respondents reported the second highest European breach level at 49%. The survey compared these numbers with recent activity, and 46% of European respondents indicated they had either a breach or an audit issue in their cloud environments in the past 12 months (52% in the UK and 49% in Sweden).

The survey looked at differences in breach perception across organisational roles. Reported levels of breach declined with increasing levels of management. In other words, fewer senior executives reported that their organisation has had to deal with a breach than senior managers, and their numbers were lower than direct staff. This implies that more senior decision-makers may be insulated from the realities of their environments and may not understand the urgency with which investments need to be made. Such a situation is likely to hamper the necessary improvements that could strengthen their security posture.

Moving Ahead

Organisations are working hard to address the forced changes brought on by the pandemic while moving ahead with technology investments that will keep them competitive. Mastering security and operations for cloud-based infrastructure is a necessary part of this journey. The survey results showed that there is considerable use of hybrid and multicloud patterns as businesses expand to get closer to their customers and partners and support a more distributed workforce. The results also found that there is much more work to be done to secure these new infrastructure elements effectively and operate them efficiently. The greater use of hybrid and distributed resources adds operational complexity, and organisations need to invest in capabilities that will allow them to scale up without placing a crippling burden on their security teams.



Contact us

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

cpl.thalesgroup.com/cloud-security-research

