CPL.thalesgroup.com #2020DataThreat

THALES

Executive Summary
2020 Thales Data Threat Report

European Edition

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE

Introduction

This IDC research shows digital transformation (DX) is well underway. European companies and organisations continue to increase their use of a wide variety of digital transformation technologies to improve customer experience, find new sources of revenue, and reduce costs. Thirty-seven percent of European organisations in our study say they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.

While DX can provide tremendous value, it also makes data security more complex. Companies are increasingly dependent on, and increasing, the amount of data stored in the cloud. As a result, security teams need to focus on aspects beyond traditional network perimeters. We have reached a point at which nearly half (46%) of all corporate data is stored in the cloud, and 43% of that data is sensitive. Additionally, most European organisations are multicloud. All of this adds up to today's data environments becoming increasingly complex, and this complexity is a top barrier to data security.

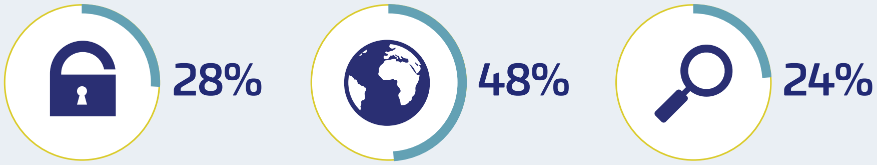
> "Nearly half (46%) of all corporate data is stored in the cloud, and 43% of that data is sensitive."

However, European companies are cognitively dissonant to data security. Nearly two-thirds believe they are not at all vulnerable, resulting in a continued freeze of their security budgets. Without additional funding, European companies will be challenged to implement processes and invest in technologies required to appropriately protect their data. Simultaneously, more than half of them have been breached or experienced failed security audits in the past year. And when it comes to securing data in the cloud, most European companies rely heavily on their cloud providers for security, instead of executing on the elements outside of the shared responsibility model by adding their own adequate controls.

When it comes to investments, data security still represents a small share of overall security budget. Thirty-eight percent of European organisations plan to increase data security spending in the next 12 months, significantly lower than the 49% of global respondents who expect spending to increase. And, European organisations still focus a disproportionate amount of spend on network security. One-third of European respondents' focus is on data security, yet data security averages just 14% of overall IT security budget. Lower budget allocation for data security in Europe compared to the rest of the world is counterintuitive, considering that trust and security are at the core of the European Union's Digital Single Market Strategy.

As organisations face expanding and more complex data security challenges, they need smarter, better ways to approach data security. European companies need to take a multilayered approach to data security by embracing cloud shared security responsibilities and adopting access management technologies that authenticate and validate users and devices accessing applications and networks, while also employing more robust data discovery, hardening, data loss prevention and encryption solutions. Importantly, data security should not undermine business efforts to pursue digital transformation by applying flexible frameworks leading to discretionary trust model implementation.

In the wake of the COVID-19 global pandemic, organisations must remain vigilant and be prepared for the post-COVID-19 data risk reality. This point is especially relevant today more than ever as the work from home migration has increasingly forced corporate data to be accessed remotely, sometimes on Bring Your Own Devices (BYOD). In addition, with the additional remote users, many organizations are adopting more cloud usage and removing requirements of using a VPN to access cloud data. The result is by passed perimeter security and loss of visibility of where data is stored and how it is accessed. This increases the requirements for encryption and access management to control data outside an organizations network perimeter.



of European respondents admitted to having been breached in the past year.

of European organisations have experienced a breach at some point in their history.

of European organisations report that they have failed a compliance audit in the past year.

Figure 1 – Data Threats Are Pervasive

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

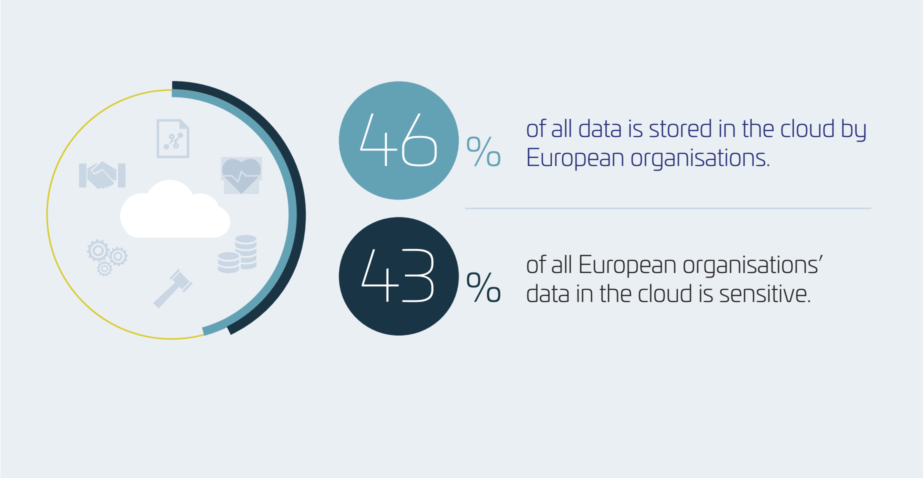
Data Threats are Pervasive

No organisation is immune from data security threats, with 48% of European respondents experiencing a breach ever and 28% having been breached in the past year. Another 24% of European organisations report that they have failed a compliance audit in the past year.

While organisations that digitally transform are realising new sources of competitive advantage, these companies face new data security challenges presented by DX. DX positively correlates to vulnerability: the more digitally transformed an organisation is, the more likely that it has experienced a data breach. Digitally determined organisations (those organisations making the strategic, organisational, technological, and financial decisions that will set them up to digitally transform in the next several years) may also have greater data threat exposure. Their greater level of sophistication may also mean they are more likely to be aware that they have been breached. Less sophisticated companies may have less exposure, or they just may have been breached without knowing it.

> *“28% of European respondents reported experiencing a breach in the past year. Overall, 48% of organisations have been*

The Amount of Sensitive Data in the Cloud is Growing



46% of all data is stored in the cloud by European organisations.

43% of all European organisations' data in the cloud is sensitive.

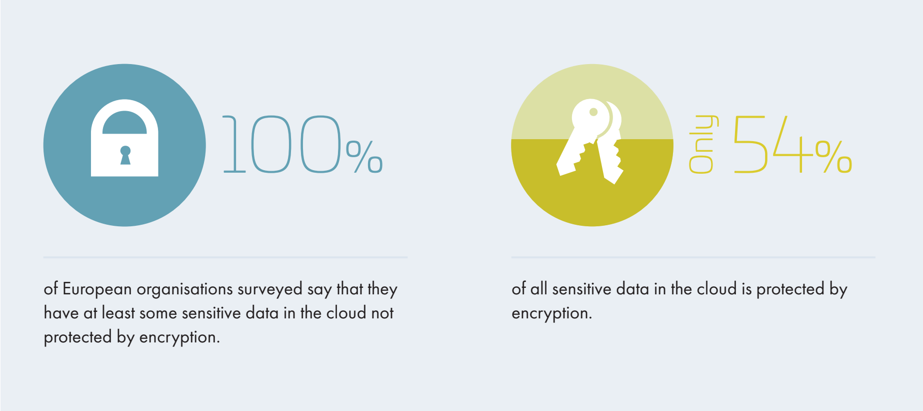
Figure 2 – Sensitive Data in the Cloud is Growing

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

All European organisations surveyed have some sensitive data in the cloud. Data stored in the cloud is nearing an inflection point with our study respondents who say that an estimated 46% of data is in the cloud, slightly lower than the global sample at 50%. More importantly, European respondents say that an estimated 43% of that data in the cloud is sensitive.

> *46% of corporate data is in the cloud, and 43% of that data is sensitive."*

Much Sensitive Data in the Cloud is at Risk



100% of European organisations surveyed say that they have at least some sensitive data in the cloud not protected by encryption.

Only 54% of all sensitive data in the cloud is protected by encryption.

Figure 3 – Is Enough Security in Place?

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> *Only 54% of sensitive data stored in cloud environments is protected by encryption."*

As more sensitive data is stored in cloud environments, data security risks increase. Yet, despite this significant sensitive data exposure, rates of data encryption and tokenisation are low. In fact, 100% of European respondents say at least some of their sensitive data in the cloud is not encrypted. Only 54% of sensitive data stored in cloud environments is protected by encryption and less than half – 44% – is protected by tokenisation.

Multicloud Environments Challenge Security

> 29% of European organisations have more than 50 SaaS applications to manage."

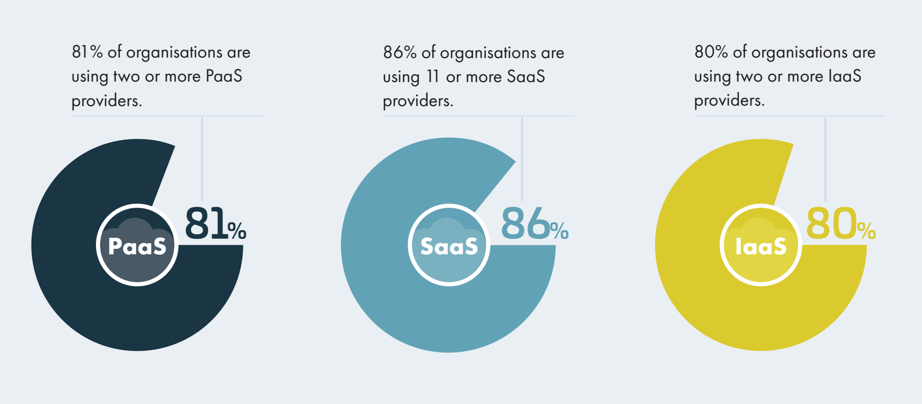


Figure 4 – Yes, It's a Multicloud World

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

As more data migrates to the cloud, security becomes more complex. But much of this complexity is self-inflicted, as multicloud has become increasingly common. European companies are using multiple IaaS and PaaS environments, as well as hundreds of SaaS applications. Eighty percent of European organisations are using more than one IaaS vendor, 81% have more than one PaaS vendor, and 29% have more than 50 SaaS applications to manage.

Quantum Computing on the Horizon

> 93% of respondents are concerned quantum computing will create exposures for sensitive data."

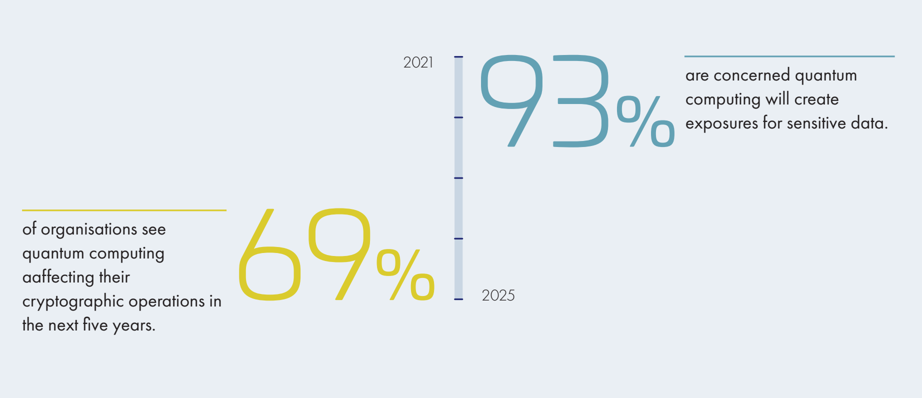


Figure 5 – Ready for Quantum Computing?

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Data security will only get harder with the advent of quantum computing. The impact of quantum computing is on the horizon as 69% of European organisations see it affecting their cryptographic operations in the next five years. Cryptography requirements highlight a critical security issue brought on by the power of quantum computing. Ninety-three percent of respondents are concerned quantum computing will create exposures for sensitive data, with 30% very/extremely concerned.

Modern Data Security for a Zero Trust World

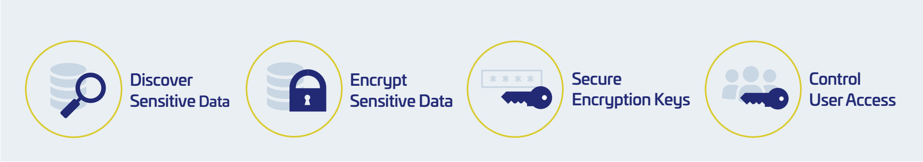


Figure 6 – Modern Data Security for a Zero Trust World

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

IDC Guidance

- **Invest in modern, hybrid and multicloud-based data security tools that make the shared responsibility model work. More sensitive data is stored in the cloud than ever.**
- **Consider a secure least privileged model that secures both data and the users accessing the data.**
- **Increase focus on data discovery solutions and centralisation of key management to strengthen data security.**
- **Augment discovery with robust classification for risk-based execution.**
- **Prepare for quantum computing's impact on cryptography.**
- **Focus on the right threat vectors.**
- **Data security solutions, especially rights management and encryption, are critical to remain vigilant against the post-COVID-19 data risk reality.**
- **Implement new security methods to protect our post-COVID-19 IT landscape.**

About the Report

This report concentrates on the findings from 509 European executives with responsibility for, or influence over, IT and data security from within a total global sample of 1,723. Survey, reporting and analysis were conducted by IDC and sponsored by Thales.

To download the full report,
visit cpl.thalesgroup.com/Euro-DTR/

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organisations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Thanks to our sponsors:

SENETAS

KEYFACTOR

PURESTORAGE® CSA cloud security alliance® EXCLUSIVE NETWORKS

OASIS Open standards. Open source. FIRST TECH INFINIGATE .... Adding Value to Distribution TiSafe

350 Longwater Avenue, Reading,
Berkshire RG2 6GF

0118 943 4500

>cpl.thalesgroup.com <

cpl.thalesgroup.com/Euro-DTR
#2020DataThreat