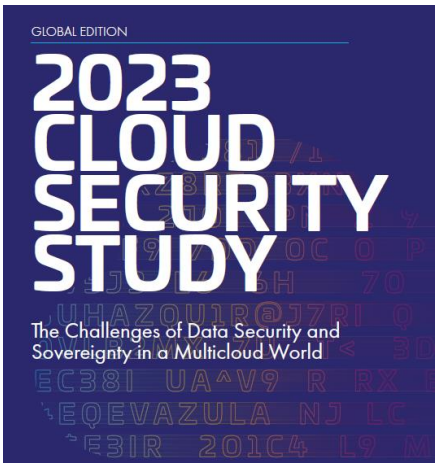
PRESS RELEASE
5 July 2023
Paris La Défense

Cloud assets the biggest targets for cyberattacks, as data breaches increase

- 39% of businesses experienced a data breach in their cloud environment last year, an increase of 4points from the previous year (35%)
- More sensitive data moving to the cloud with 75% of businesses saying more than 40% of data stored in the cloud is sensitive, up 26% from last year
- Despite dramatic increase in sensitive data stored in the cloud, on average only 45% of this sensitive data is encrypted



©Thales

Thales today announced the release of the 2023 Thales Cloud Security Study, its annual assessment on the latest cloud security threats, trends and emerging risks based on a survey of nearly 3,000 IT and security professionals across 18 countries.

This year's study found that more than a third (39%) of businesses have experienced a data breach in their cloud environment last year, an increase on the 35% reported in 2022. In addition, human error was reported as the leading cause of cloud data breaches by over half (55%) of those surveyed.

This comes as businesses reported a dramatic increase in the level of sensitive data stored in the cloud. Three quarters (75%) of businesses said that more than 40% of data stored in the cloud is classified as sensitive, compared to 49% of businesses this time last year.

More than a third (38%) ranked Software as a Service (SaaS) applications as the leading target for hackers, closely followed by cloud-based storage (36%).

Lack of Encryption and Key Control Causes Cloud Data Concerns

Despite the reported increase in sensitive data in the cloud, the study found low levels of encryption being used. Only a fifth (22%) of IT professionals reported that more than 60% of their sensitive data in the cloud is encrypted. According to the findings, on average, only 45% of cloud data is currently encrypted.

The study also found a lack of control over encryption keys by businesses, with only 14% of those surveyed stating that they controlled all of the keys to their encrypted data in their cloud environments. In addition, almost two thirds (62%) say they have five or more key management systems – creating increased complexity when securing sensitive data.

Multicloud Causing Operational Complexity

The adoption of multicloud continues to surge, with more than three quarters (79%) of organisations having more than one cloud provider.

Notably, it's not just infrastructure that is experiencing this growth. The use of SaaS apps is also on the rise significantly. In 2021, 16% of respondents reported their enterprises utilising 51-100 different SaaS applications, while in 2023 this percentage increased to 22%.

Despite the expansion of cloud usage, a significant challenge remains. More than half (55%) expressed that managing data in the cloud is more complex than in on-premises environments – up from 46% compared to the previous year. Digital sovereignty is also front of mind for respondents. Eighty three percent expressed concerns over data sovereignty, and 55% agreed that data privacy and compliance in the cloud has become more difficult.

Pathways to Better Cloud Security

Identity and access management (IAM) is a crucial measure in mitigating data breaches, emphasising the significance of strong security practices. Encouragingly, the adoption of robust multi-factor authentication (MFA) has risen to 65%, indicating progress in fortifying access controls.

Surprisingly, only 41% of organisations have implemented zero trust controls in their cloud infrastructure, and an even smaller percentage (38%) utilises such controls within their cloud networks. These statistics highlight the need for greater emphasis on adopting comprehensive security measures to effectively safeguard sensitive data and enhance overall cybersecurity resilience.

"The study shows that organisations are operating in a dynamic multicloud landscape, demanding seamless and efficient access to on-demand IT infrastructure and services," stated **Sebastien Cano, Senior Vice President for Cloud Protection and Licensing activities at Thales.**

"Treating cloud environments as an extension of existing infrastructure while maintaining exclusive control and security of data, especially sensitive data, is key to cloud security. Customer control of encryption keys is essential as it allows organisations to leverage the scalability, cost efficiency, and accessibility benefits of the cloud while ensuring the utmost integrity and confidentiality of their valuable information."

About the 2023 Thales Cloud Security Report

The 2023 Thales Cloud Security Report was based on a global S&P Global Market Intelligence survey commissioned by Thales of almost 3000 executives with responsibility for or influence over IT and data security. Respondents were from 18 countries: Australia, Brazil, Canada, France, Germany, Hong Kong, India, Italy, Japan, Mexico, Netherlands, New Zealand, Singapore, South Korea, Sweden, the United Arab Emirates, the United Kingdom, and the United States. Organisations represented a range of industries, with a primary emphasis on healthcare, financial services, retail, technology, and federal government. Job titles ranged from C-level executives including CEO, CFO, Chief Data Officer, CISO, Chief Data Scientist, and Chief Risk Officer, to SVP/VP, IT Administrator, Security Analyst, Security Engineer, and Systems Administrator. Respondents represented a broad range of organisational sizes, with the majority ranging from 500 to 10,000 employees. The survey was conducted in November and December 2022.

PRESS RELEASE
5 July 2023
Paris La Défense

About Thales

Thales (Euronext Paris: HO) is a global leader in advanced technologies within three domains: Defence & Security, Aeronautics & Space, and Digital Identity & Security. It develops products and solutions that help make the world safer, greener and more inclusive.

The Group invests close to €4 billion a year in Research & Development, particularly in key areas such as quantum technologies, Edge computing, 6G and cybersecurity.

Thales has 77,000 employees in 68 countries. In 2022, the Group generated sales of €17.6 billion.

PRESS CONTACT

Thales, Media Relations
Security & Cybersecurity
Marion Bonnet
+33 (0)6 60 38 48 92
marion.bonnet@thalesgroup.com

PLEASE VISIT

Thales Group

Cybersecurity Solutions | Thales Group