Breaches and audit issues are common in cloud environments. 40% have experienced a breach in their cloud environments, and 39% have had either a breach or an audit issue on their cloud environments in the past 12 months.

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

Thanks to our sponsors Visit cpl.thalesgroup.com/cloud-security-research to download the full report, including 451 Research recommendations.


- 73% are using 2+ PaaS providers
- 65% are using 26+ SaaS applications

Multicloud adoption is widespread, exacerbating complexity. 57% of global organizations are using 2+ IaaS providers.

Defining cloud security policies is squarely for security teams of organizations. 82% involve security teams in cloud security decisions, while 11% of organizations' cloud security is run independently by security teams and 16% is run collaboratively by security and cloud delivery teams.

Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Encryption, and DLP are leading technologies for securing cloud environments. 34% use CSPM, 32% use CWPP, 36% use CIEM, 39% use Encryption, and 39% use DLP.

Encryption is not widespread in the cloud. 83% use the cloud provider’s encryption, 35% use their own encryption, and 55% are encrypting less than half of sensitive data in multicloud environments.

For data encrypted in cloud:
- 45% use MFA to secure more than half of their cloud services
- 16% use MFA to secure more than half of their on-premises applications

Organizations still have a long way to go for MFA to be broadly adopted. 40% consider securing the combination of on-premises and cloud either “challenging” or “very challenging”.

Modern data security for a Zero Trust world

Thanks to our sponsors.