

Halfway is No Way: Cloud Sovereignty Needs More Than Data Visibility



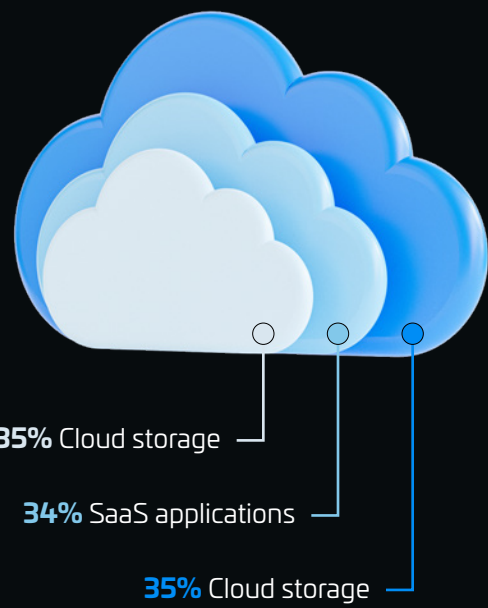
Cloud is Still the Top Target

The **2026 Thales DTR** found that cloud-based assets occupied all three of the top attack-target categories:

51% of cloud data is sensitive.

Only **47%** of sensitive cloud data is encrypted.

53% of organizations let their cloud provider hold the keys for most applications.



Why this matters

The average organization uses more than 2 cloud providers and 89 SaaS applications.

The business impact:

For organizations making commitments about where data is held, who controls it, and how it is protected, those gaps are important.

Cloud and DSPM Work Together

Cloud provides the scale, while DSPM provides the control.



CLOUD to DSPM

DSPM needs to scale with the cloud

As cloud environments expand, DSPM needs to scale with them. A SaaS-based approach provides the flexibility to keep pace.



DSPM to CLOUD

DSPM makes sovereignty easier to prove.

31% of organizations say they lack the tools needed to identify their highest-risk data sources, while more than half (54%) use four or more tools to manage data risks.

Because data sovereignty depends on knowing where sensitive data resides, who can access it, and how it moves across jurisdictions, DSPM helps close this visibility gap and provides the foundation for enforcing sovereignty requirements.

Control Matters as Much as Location

Organizations are already taking a broader view of sovereignty.

Geopolitical uncertainty and increasingly fragmented regulations are forcing them to consider not only where data resides, but which jurisdictions can access it and who ultimately controls it.

Data residency can determine where data should live. Encryption and external key management can determine who can access it. DSPM helps establish which data those requirements apply to and whether it has ended up somewhere it should not be.



45% cite portability as the primary driver of their sovereignty initiative.



34% cite full control over software and data.



49% say the location of cloud infrastructure matters for some or all workloads.



36% say strong encryption combined with external key management is sufficient, regardless of where the infrastructure is physically located.

Sovereignty Policies Have to Follow the Data

Organizations are already changing their cloud environments in response to sovereignty requirements.

40%

are actively reducing the amount of data held outside sovereign regions.

54%

are refactoring applications to segment or isolate data.

Neither is possible reliably without an accurate view of the data estate.

The larger and more distributed the cloud estate becomes, the harder it is to do manually.



Better Control Can Make Cloud Adoption Easier

Security and sovereignty requirements can put a brake on cloud projects when teams cannot quickly determine what data they have, where it resides, or what protections it requires.

Knowing the answers can remove some of that friction, helping teams decide what can move, where it can go, and which controls it needs.

Instead of treating all workloads the same way, organizations can identify their most sensitive data and apply the appropriate residency, encryption, and key management requirements.

For Executives, that means sovereignty requirements can be part of the cloud decision rather than something that must be resolved afterward.

Know Where To Focus Your Efforts

Protection-Centric Risk Prioritization

Take visibility to the next level by adding risk context and prioritizing the risks that matter most. Organizations can then apply the right protections to mitigate those risks before they affect the business.

[Find out more about CipherTrust DSPM](#)

