February 2026
Infographic
Sponsored by Veeam

A Pragmatic Approach to Meeting Data Sovereignty and Microsoft 365 Resilience Mandates

The data sovereignty battleground is intensifying amid rising data sensitivity, geopolitical uncertainties, and the stickiness of SaaS in digital operations. Navigate through the art of the possible to deliver on sovereignty mandates.

Archana Venkatraman
Senior Research Director,
Cloud Data Management, IDC Europe

Data resilience and sovereignty become non-negotiable

Data sovereignty is no longer optional for compliance. Instead, it has become the core of digital trust and risk management.

Data sovereignty and potential cloud changes were cited as the greatest concerns for 2026.

The reasons for the heightened focus are:

- Rising data value and sensitivity
- Geopolitical uncertainties
- High reliance on third-party platforms for digital business operations

Source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 5*, June 2025

Sovereignty and resilience risks and exposure span across cloud environments, especially SaaS

SaaS applications dominate digital environments over IaaS and PaaS. As a result, their role as the primary repository for sensitive, critical business data can no longer be ignored.

For **47%** of organizations, SaaS environments are where business data is growing fastest or second fastest.

53% of IT support teams
42% of cybersecurity teams

admit that the Microsoft 365 environment is where they are most concerned about data loss, accidental deletion, lack of recovery, or audit failures.

Source: IDC's *EMEA Cloud Survey*, 2024; IDC's *2024 CloudOps Survey*

Breaking Free from Defacto Thinking: A Resilience-Centric Action is Essential to Make Data Controls Practical

Sovereignty is multi-faceted and complex requiring a pragmatic, resilience-centric approach and the first hurdle to overcome is defacto thinking.

6 in every 10 organizations still rely on native Microsoft 365 data protection mechanisms.

Percentage of respondents:

	EMEA	Total
Third-party software	18.7%	19.2%
SaaS vendor-provided protection	62.8%	61.7%
No data protection	5.6%	6.6%
Do not use	12.9%	12.5%

This introduces risks such as data loss due to default, inflexible, and limited data retention features, as well as rigid data recovery capabilities in the event of a crisis.

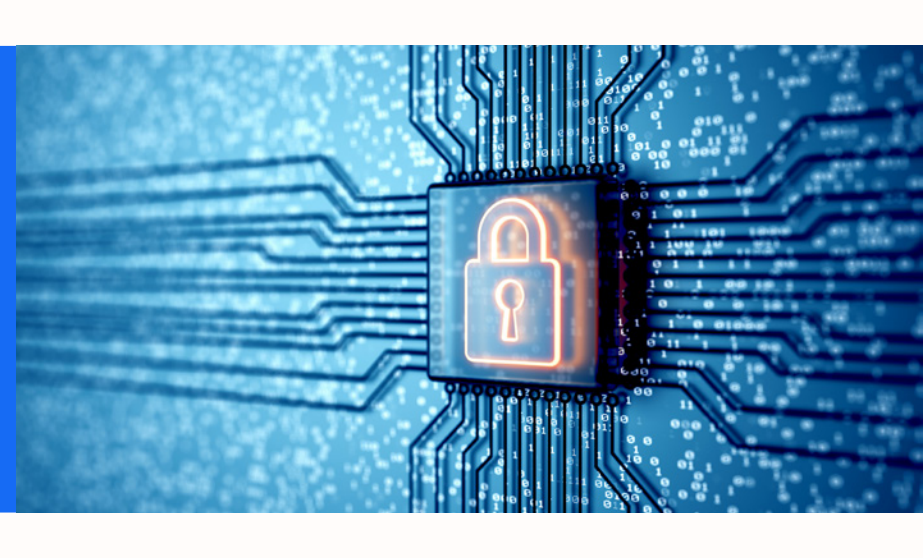
Heavy reliance on native features also means organizations lack flexible access to their data and, more importantly, lack full control over the information needed for continuity, sovereignty, and compliance.

Source: IDC's *Cloud Data Logistics and Protection Survey*, August, 2025

The value of data protection, security, and resilience technologies and the growing chasm between digital natives and followers

Rapid data growth in SaaS, such as Microsoft 365, underscores the importance of ensuring the control and strategic autonomy of data assets.

87% of digital natives (77% of all organizations) commit to investing more in SaaS data protection.
Organizations rate data classification and data protection as two areas that are "extremely important" to address in the near future.



However, 62% of organizations still rely on native or default Microsoft 365 data protection capabilities, significantly increasing risks.

Security, risk, and compliance remain tech domains that are not only immune to budget cuts, despite macroeconomic uncertainties, but will even see "significant budget increases" in 2025 and beyond.

Source: IDC's *2024 CloudOps Survey*; IDC's *Future of Enterprise Resiliency and Spending Survey*, December 2024

Data sovereignty and Microsoft 365 resilience design principles

A sovereign Microsoft 365 environment is a set of architectural choices and legal frameworks.

Organizations must establish a resilient data strategy that includes regulatory oversight. They should transform their processes, starting with data classification, roles and responsibility documentation, and their risk policies.

The technical controls strategy needs to cover three pillars of data sovereignty:

Legal jurisdiction:
Ensure clarity on backup data governance, access controls, and encryption.

Data residency:
Ensure choice and flexibility in where backup data is stored, and be in control of data movement and data audits. Ensure that metadata is treated with sensitivity.

Operational autonomy:
Verify the necessary control for cyber-resilience and regulatory compliance with features such as data immutability, traceable audit logs, and logical separation. Focusing on recovery more through mechanisms such as granular recovery, faster time to recovery, and complete Microsoft 365 estate coverage is essential for operational integrity and business continuity.

Source line: *IDC Research*, 2025

IDC Custom Solutions
February 2026 | #US54202726-SIG | Sponsored by Veeam
IDC Custom Solutions produced this publication. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

idc.com
@idc
@idc

Message from the sponsor