

Building Customer Trust in a Multicloud World



Dave McCarthy
Research Vice President
Cloud and Edge Infrastructure Services, IDC



Jennifer Glenn
Research Director, IDC

ABOUT THIS INFOGRAPHIC

As cloud deployments expand to include hybrid and multicloud architectures, a holistic security strategy is required.

IDC Predictions

The need for more control over cloud environments is driving demand for enhanced security through automation.

BY THE END OF 2024

65% of major enterprises will mandate data sovereignty controls from their cloud service providers to adhere to data protection and privacy regulatory requirements.

BY 2026

30% of large enterprise organizations will migrate to autonomous security operations centers accessed by distributed teams for faster remediation, incident management, and response.

Source: IDC FutureScape: Top 10 Predictions for the Future of Trust

Reduce the Threat Landscape

68% of organizations expect their data volume to increase over the next three years. Of those, nearly 40% expect volume to increase by 25% or more.

How to protect data:

Minimize potential business disruptions by **shrinking the attack surface** and reducing risk exposure.

Design a well-protected environment that includes **centralized log monitoring and anomaly detection**.

Implement continuous **multi-layer control monitoring and proactive scanning**.

Segment cloud infrastructure by **creating virtual private clouds** that act as regulated enclaves.

Source: IDC's Data Privacy Survey, December 2022

Automate, Simplify, and Standardize

39% of organizations state that IT security professionals are in the highest demand for tech initiatives globally.

Ways to make security staff more productive:

Create templates that simplify rapid deployment of security processes and reduce human error.

Standardize on key control mechanisms to assess risk.

Quicken threat detection and self healing by implementing **security as code**.

Build security at scale with an automated approach, that reduces burden on staff and ensures consistency in the cloud

Source: IDC FERS Survey, July 2022

Build Confidence with Regulators and Customers

68% of organizations ranked security and 66% ranked compliance as the most important areas for being perceived as trustworthy. 32% of organizations expect cybersecurity threats/regulations will have the greatest impact on their business.

Keys to strengthening compliance and security:



1 Demonstrate commitment to compliance with policies and procedures that align with government, industry, and corporate governance requirements.

2 Adapt hyperscalers' ready-made compliance code to enable automation.

3 Be transparent about security efforts with public-facing and NDA-level self-service mechanisms like Trust Centers.

Source: IDC's Future Enterprise Resiliency and Spending Survey, July 2021; IDC's CEO Survey, January 2022

Essential Guidance

Security in a multicloud environment requires a multi-faceted approach:

Reduce the risk profile of the organization by improving efficiency in the security and compliance process.

Empower security teams through strategic distribution of security resources and increase productivity with automation.

Maximize customer satisfaction and brand preference with transparency and reliability.

Work with suppliers that have demonstrated expertise in meeting multicloud security challenges.

Message from the Sponsor

NetApp

Learn what experienced teams do to secure an expanded hybrid multicloud IT landscape and how to improve your processes to achieve business outcomes that go beyond risk management to include team empowerment, customer satisfaction and brand preference.

[Click here to learn more](#)