451 Research

Business Impact Brief

Security Management is a Critical Hybrid Cloud Challenge

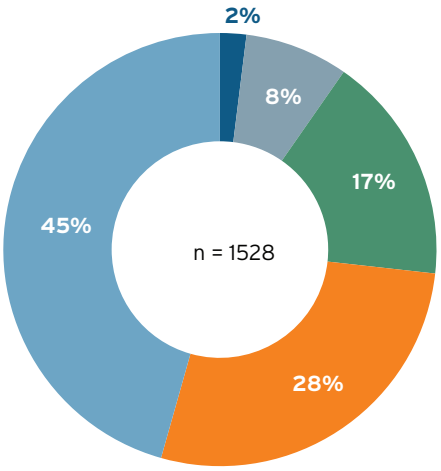
The 451 Take

As businesses transform their IT operations to take advantage of hybrid cloud resources, overcoming new security hurdles and managing existing security practices across interconnected environments will be among the most significant challenges they face. Security requirements will be an important consideration as businesses make choices related to hybrid cloud adoption.

According to research conducted by 451 Research and commissioned by NTT Communications in partnership with Dell EMC, a majority of businesses have plans to adopt hybrid cloud architectures, in which multiple cloud infrastructure environments interoperate to seamlessly deliver business functions. Security and compliance are the most important considerations in the hybrid cloud plans of nearly half of businesses surveyed, and are labeled at least an 'important' consideration by 90%.

Security and Compliance Are Critical to Hybrid Cloud Plans

How important are security and compliance considerations to your hybrid cloud plans?



- Not important, this design is not vulnerable or does not present a significant risk
- Meaningful but not an impediment to adoption
- Important
- Very important: necessary but flexible
- Critically important, first consideration, hard requirements

Understandably, this issue is important to some degree for 90% of all enterprises

Source: 451 Research

Businesses believe the hybrid cloud model has the potential to impact the security of their IT operations both positively, because of the availability of redundant environments and the opportunity to isolate specific environments, and negatively, because of the increased complexity and data portability requirements of hybrid cloud:

- For instance, 53% of businesses believe operational security will be positively impacted, and 33% expect a positive impact on disaster-recovery capabilities.
- 33% of businesses believe security management and monitoring capabilities will be negatively impacted, and 36% expect a negative impact on encryption practices.

Data sovereignty requirements are a similarly important hybrid cloud consideration. The capability to isolate sensitive data in single-tenant environments or in specific geographies, for both security and regulatory reasons, is a major motivator for many businesses taking a hybrid approach to cloud rather than going all-in on a particular environment. For this reason, datacenter footprint is a significant factor in vendor selection when implementing hybrid cloud.

Business Impact Brief

The 451 Take (continued)

Business Impact

For many businesses, overcoming the security management challenges associated with hybrid cloud adoption will require partnerships with external service providers that have security expertise associated with specific regulatory requirements or cloud platforms, as well as capabilities to execute and manage security across multiple cloud environments.

Businesses surveyed indicate that many of the services they are most likely to buy from an external managed security service provider (MSSP) have to do with operating, automating and managing the tasks related to cloud security. The services cited as most likely to be purchased in support of hybrid cloud include security orchestration and automation services (by 36% of businesses), risk and compliance management (35%), disaster-recovery services (33%), and identity and access management (33%).

PRIVACY REGULATIONS ARE A KEY CONTRIBUTOR TO SECURITY REQUIREMENTS. In the EU, legislation such as European Free Trade Area (EFTA) regulations, the General Data Protection Regulation (GDPR) and the European Union's ePrivacy Legal Frameworks all impact a significant majority of businesses surveyed, introducing further compliance and security concerns (beyond facilities-focused or industry-specific regulations) into the hybrid cloud picture.

SECURITY CONSIDERATIONS WILL BE A MAJOR FACTOR IN EVERY HYBRID CLOUD DECISION. As businesses make choices on the path toward hybrid cloud implementation, the organizational policies that result from security concerns will be a primary influence – on vendor/platform selection, management tools, and processes guiding consumption and procurement. Designing, applying and maintaining security and policy frameworks around decision-making will be a major ongoing aspect of hybrid cloud use, and a measure of the success of hybrid efforts.

DEVELOPING AND MAINTAINING CLOUD SECURITY EXPERTISE IS A CRITICAL CHALLENGE. The complexity of hybrid cloud environments brings new security challenges. Keeping up with those challenges becomes more important – and more difficult – as the environments become more intricate and the threats themselves evolve. Effective security requires a strategic, coordinated effort, and an ongoing investment in processes, tools and personnel. .

Looking Ahead

Businesses already regard security as a primary concern associated with the adoption of private cloud. However, as they progress toward implementing hybrid cloud, they will encounter additional practical security challenges and risks they may not have previously faced. Additional operating environments add new attack surfaces, security policies and practices must be extended to address multiple cloud environments, and data must be secured in transit as it moves between these environments. All of this must be managed and, where possible, automated.

Managed security services will prove essential to businesses at the hybrid cloud stage, not only in addressing the security challenges they have identified as most critical, but in helping to identify challenges they have not yet encountered, and to secure against those eventualities. External security service vendors have access to large numbers of clients, and therefore large volumes of threat and attack data across a variety of geographies and platforms, allowing them to better predict threats and protect their clients.

Specialization and scale also allow MSSPs to operate with a level of expertise and security operations capability not typically available to most businesses. Providers are frequently able to deliver these services with a degree of flexibility that allows the client organization to choose whether to augment internal functions or offload these functions altogether, while regarding MSSPs as trusted partners.

What do enterprises want from hybrid cloud? How are decisions being made about its suitability, and which issues are influencing the extent of its adoption across European businesses? To answer these questions and examine other criteria shaping the way enterprise executives are planning for hybrid cloud deployment – and what this means for the service provider community – read our commissioned report 'Going Hybrid: What Enterprises Want From Cloud Service Providers,' based on an independent study of over 1,500 IT decision-makers representative of Europe's largest businesses and key vertical sectors.