451 Research | Business Impact Brief

Why data centres hold the key to multicloud encryption

The 451 Take

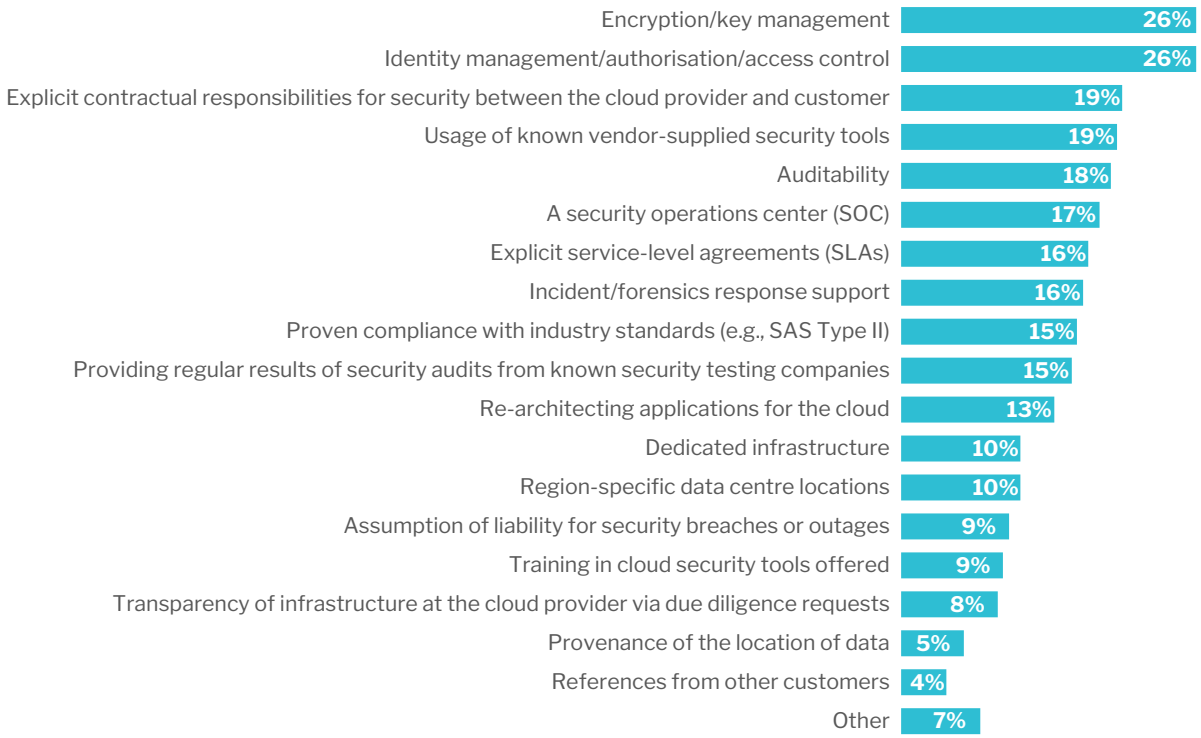
There are a number of compelling reasons why modern enterprises are embracing the cloud: the ability to quickly scale to meet spikes in demand; the ease of rolling out new features; and the potential to lower IT costs, both up front and over time. In fact, recent studies from 451 Research show that on average, 17% of workloads are currently running in public cloud (IaaS, PaaS and SaaS). However, 30% are expected to run in public cloud within the next two years, while use of hosted and on-premises private clouds is also expected to increase. Conversely, workloads running in 'traditional' on-premises IT infrastructure are expected to decline sharply, from 46% to 21%.

Yet despite all of the potential benefits of cloud, security concerns remain a primary obstacle – survey data from 451 Research shows that 42% of organisations still view security as the main impediment to moving more workloads to the cloud. Compliance is another big obstacle, particularly with new regulations such as GDPR and performance concerns. To address this, there are a number of security controls available from third-party security providers, as well as from cloud and service providers themselves. The top choice, however, for securing sensitive data in the cloud, is encryption and key management, at 26% (tied with access controls), according to survey data from 451 Research's *Voice of the Enterprise* service.

Addressing Security Concerns with Hosted Cloud Solutions

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2019

Q: Of the following, what are the top ways your organisation is addressing security concerns with hosted cloud solutions? (n=203)



451 Research® | Business Impact Brief

The 451 Take (continued)

There are multiple approaches to encrypting data in the cloud – many third-party security vendors offer encryption for cloud data while an increasing number of cloud and service providers offer encryption natively. However, two of the main issues to consider are how to span multiple clouds with a consistent security policy, and perhaps more important, how to manage the keys. In terms of technology requirements, encryption can typically be deployed via a proxy or an agent or embedded directly within an application, which has direct implications for network architecture and the types of workloads to be protected.

For key management, there are even more options – are the keys located on-premises or with a cloud or colocation provider? Are the keys stored in a traditional hardware security module (HSM) – either on-premises or in a colocation facility – or delivered as a service? And is the HSM as a service delivered via multi-tenanted HSM appliances that provide greater elasticity, or via single-tenant dedicated HSM appliances that offer greater control and performance? Most importantly, who controls the keys – the customer, the cloud provider or both?

Business Impact

BEST EXECUTION VENUE. Organisations tend to deploy applications and workloads in a location that makes the most sense for their specific requirements – on-premises or hosted, public or private cloud, or increasingly a combination of each, and across various geographies. The implications for security, performance, privacy and data sovereignty are non-trivial.

SO MUCH FOR CLOUD MAKING OUR LIVES EASIER. Save for those that have gone 'all in' on cloud, most businesses also have a substantial legacy estate to secure, with potentially dozens of legacy security tools used alongside a growing array of third-party and cloud-native security tools.

IN A MULTI-CLOUD WORLD, CLOUD-NATIVE SECURITY MAY NOT BE ENOUGH. Not all clouds are created equal – 451 Research survey data suggests that few enterprises (28%) are using just a single cloud provider, and many are using three or more. To avoid gaps in coverage, cloud security initiatives need to work across multiple cloud environments.

WHOEVER CONTROLS THE KEYS, CONTROLS THE DATA. With the passage of GDPR, the California Consumer Privacy Act, and other national and regional regulations, data sovereignty has become an increasingly hot issue. Encryption can serve as an important control for meeting compliance guidelines, although maintaining control over keys is critical.

STAFFING SHORTAGES REMAIN A PRIMARY HURDLE. Staffing concerns loom large in any decision to deploy new security tools, particularly those that can be complex and/or labour-intensive – such as encryption and key management. According to 451 Research survey data, information security trails only cloud platform management as the area with the greatest staffing challenges.

Looking Ahead

To avoid gaps in coverage, security policies need to be consistently applied across cloud environments – which can help explain why 48% of companies plan to utilise security services from a third-party service and just 35% will rely solely on services from their cloud provider. A centralised policy layer that works across various legacy and cloud assets can help avoid a 'hodgepodge' of security tools and policies. More specifically, encryption and key management offered as a single-tenant HSM as a service within an independent, globally distributed colocation service can allow customers to remain in complete control over who can see and access data and thus meet privacy requirements, while also helping to improve performance and limit latency.