451 Research | Business Impact Brief

Managing Encryption Keys and Identities Tops Priorities for Cloud Security

The 451 Take

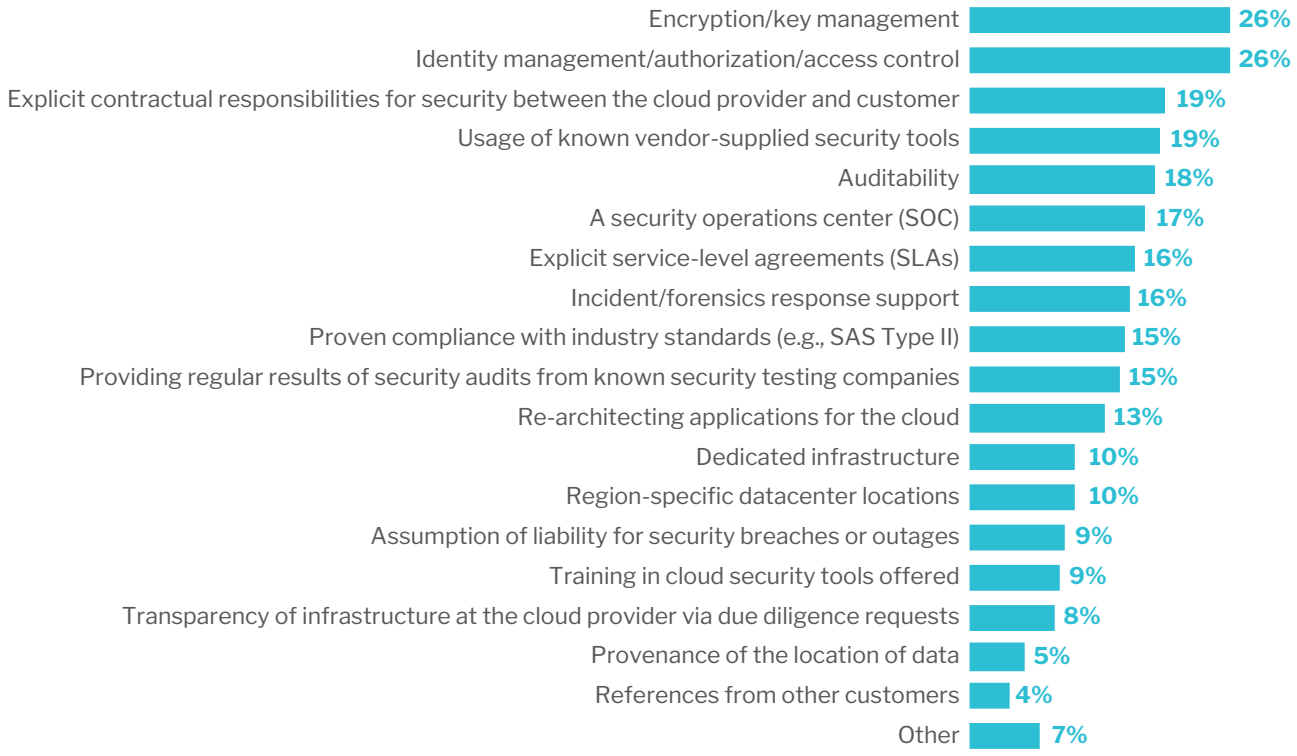
As organizations enthusiastically embrace modern application architectures, whether as part of a refresh or just business as usual for a cloud-native organization, there are three key forces acting in unison: first, there is a clear demand for increased velocity and agility in delivering value – people expect results in days or weeks, not months; then, there is tremendous autonomy being given to individual project teams and/or business units to pursue their own paths when it comes to technology choices, often looking to tie things together via newer concepts such as microservices; finally, all this is being done in a new reality where organizations have a much deeper relationship with an external provider, to the extent that many topics are now out of the hands of the contracting organization.

These trends have a profound effect on security. Now, seemingly suddenly, organizations are scrambling to support – hopefully in a consistent manner – typical security objectives such as confidentiality, integrity and availability across multiple environments, multiple technologies, multiple providers, working with multiple internal teams, at a much faster pace. This has led security teams to rethink how they address these concerns. While typical security controls will still play a part, the chart below shows how organizations are focusing on different aspects of this new reality.

Addressing Security Concerns with Hosted Cloud Solutions

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

Q: Of the following, what are the top ways your organization is addressing security concerns with hosted cloud solutions?



451 Research | Business Impact Brief

The 451 Take

These data points clearly highlight how organizations are selecting a combination of both contractual and technical controls. Interestingly, the two key technical controls are related to how the organization is managing data security – encryption and key management, which also includes secrets management – and identity management – access control, authorization, etc. Looking in aggregate, this data points to a scenario in which the organization is willing to relinquish some security controls to external providers but retains tight control over how it manages essential aspects such as keys/secrets management and the identities used in multiple environments.

Business Impact

INCREASED IMPORTANCE OF KEYS, IDENTITIES (AND SECRETS). As the data shows, many organizations are choosing to look at how they perform management of keys, secrets, identities and access control as a key area to focus on as they embrace more modern cloud environments. This means there is broad recognition that there's an opportunity to consider improvements in these areas, particularly as many vendors bring offerings to address this demand.

DEPLOYMENT OF MORE SECURITY CONTROLS AS SAAS. This shift in focus on which controls to apply – contractual, organizational or technical – gives organizations an opportunity to reconsider how these controls are being deployed. If they can address the tremendous variety, scale and agility required by modern cloud environments, not to mention regulatory and security requirements, there is potential for organizations to rethink deploying some of these controls themselves versus consuming them as services.

CUSTOMERS MAINTAIN RESPONSIBILITIES. The broad application of multiple types of security controls also highlights the need for the organization to retain control of sensitive information – encryption keys, secrets, identities, among others – even as it uses external services. This is important not only to facilitate transitions between services as needed, but also as a key regulatory concern: in many cases, using external services does not free the organization of accountability over security concerns.

SECURITY SERVICES MUST BE EASY TO CONSUME. Finally, organizations must cope with the reality that in many cases, those consuming security services will be doing so in different scenarios: services may be consumed by humans or machines, by diverse cloud/project teams, sometimes at best assisted by security teams or experts. It's great that security teams are looking beyond traditional architectures to secure modern environments, but it is critical that the new controls or services being deployed be easily consumed by those implementing these modern environments.

Looking Ahead

The ongoing adoption of modern environments – whether hosted on clouds or not – and practices means a continuing pressure on IT organizations. This pressure consists of supporting diverse projects at scale, distributed across multiple environments, often in the context of shared responsibility models. This means there is a constant pressure for organizations to retain their key intellectual assets – data, intellectual property, etc. – while using external services and infrastructure.

For this to happen, organizations must have or build strong practices for managing sensitive data such as encryption keys, secrets, configuration parameters, identities and other artifacts. Ideally, the key/encryption/secrets/identities management is done in a way that meets several objectives: it must be easy to deploy and scale, it must preserve independence and security from the underlying cloud providers, it should support the scale and agility required by modern practices, and, importantly, it must still meet relevant regulatory requirements. Any approaches that don't meet the criteria above risk affecting the organization negatively – because they lack agility, operational overhead or, worse, run afoul of security obligations to customers or regulators.