451 Research

S&P Global
Market Intelligence

Business Impact Brief

The Urgency of Addressing Cloud Security

The 451 Take

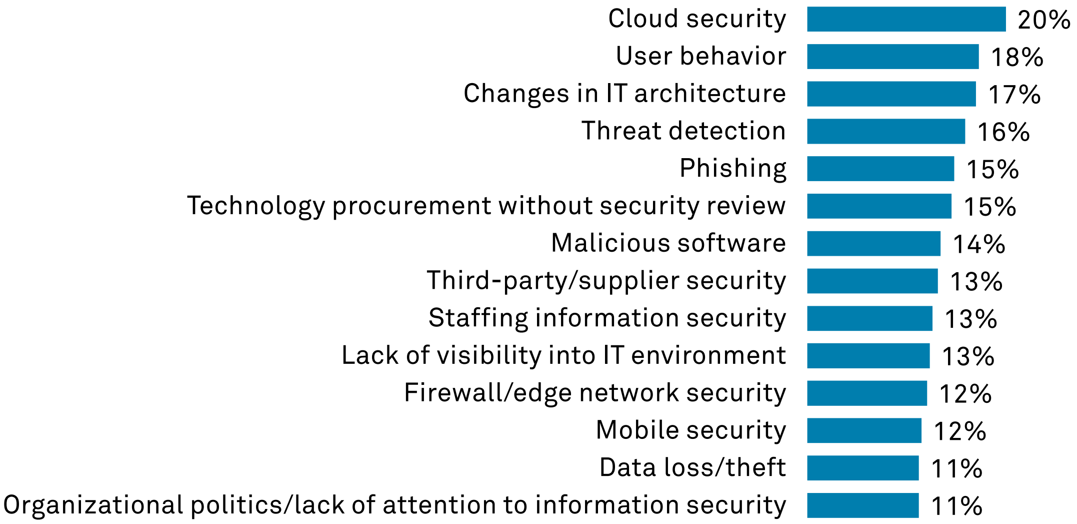
The shift toward widespread use of cloud services was well underway even as the pandemic hit. The key business drivers behind cloud adoption – cost optimization, faster time to market for new initiatives and others – merely accelerated as organizations shifted to increased reliance on digital channels. Cloud-based services and infrastructure now underpin many of the value chains for most organizations.

The adoption of cloud technology imposes significant changes to an organization's technology estate, and that has significant impacts across the dimensions of people, IT processes and underlying technologies. With IaaS or PaaS deployments, it often means using the concepts and APIs offered by the cloud providers, which is something many organizations still report as a key knowledge and skills gap across IT in general, but also specifically within their security teams.

Security teams have recognized that cloud security is an important issue to address; data from some of 451 Research's surveys indicate that cloud technologies are a key area where organizations need to make progress around security skills and capabilities. But considering the deluge of requests and requirements hitting most security teams – security awareness needs, endpoint updates, network security needs, enterprise risk management considerations – how high does cloud security really rank in terms of priorities? As it turns out, very high indeed.

451 Research regularly reaches out to key IT stakeholders to research, among other things, different quantitative and qualitative aspects of their security programs. The data below comes from 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2021 survey, where security practitioners were asked how they felt about broad topics related to their overall security initiatives, including prioritizing their concerns.

Top Information Security Pain Points



Q. What are your organization's top three information security pain points? Please select up to 3.

Base: All respondents (n=358)

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2021

While figures do fluctuate quarter to quarter, the past few editions of the survey were significant in terms of respondents selecting cloud security as a top overall area of concern, even when compared with other important security topics such as data privacy, endpoint security and phishing.

Business Impact

Cloud security requires *immediate* attention. Even if security teams are facing multiple additional demands – ranging from addressing ransomware concerns and better aligning security to enterprise risk management to supporting new work patterns due to the pandemic – supporting cloud security initiatives is a top-level priority. It's not as if other teams within IT, or even within the lines of business, are waiting to incorporate cloud environments or applications in their efforts.

Cloud security requires efficient collaboration with engineering/DevOps/cloud teams. A key factor in cloud adoption is the incredibly distributed nature of work across the organization: many teams are being empowered to use cloud capabilities, and they are doing so at a rapid pace. This requires security professionals to actively seek collaboration with those teams so that proper governance can be instilled in their initiatives even as security personnel themselves are not directly involved. The proper relationship between security and engineering creates a 'force multiplier' effect for delivering secure outcomes.

Cloud security requires a rethink of the threat models organizations are using. Delivering cloud security outcomes is not just about introducing existing controls or technologies in cloud environments. Rather, proper cloud security requires rethinking what threat actors, capabilities and exposure the organization is concerned with, and then responding accordingly. The inherent capabilities of cloud environments – high degrees of API-driven automation, scalable resources and more – require teams to reconsider how a cloud-based incident may play out very differently than one on-premises, be it because of duration, severity or response.

Other security pain points have a cloud dimension as well. Organizations should also be aware that the broader use of cloud technology by partners, suppliers and others means that the footprint for cloud security likely extends beyond one's own initiatives with cloud-based applications. In many cases, it is important to understand how cloud technologies are being used to support activities such as data exchange with a partner, or onboarding new clients. Having a proper contextual understanding of what cloud technologies are in play becomes critical.

Looking Ahead

The expectation is that cloud adoption will increase and evolve, with cloud environments rising in popularity, although on-premises workloads are expected to remain in specific use cases. Technology shifts are likely to include more variety in compute formats (from virtual machines to serverless) and execution environments (from edge to cloud), which will continue to drive the need for meaningful security capabilities.

We expect that cloud security will remain a key area of focus for both general IT deploying to clouds (as a key requirement) and also security teams, which start to incorporate cloud security guidance as part of their enterprise security program. How cloud security functionality will be delivered will vary, but it should trend toward support for better automation and workflows. As mentioned above, overall security team priorities may fluctuate from quarter-to-quarter, but cloud security should remain a top concern as organizations shift to more cloud-based operations.

As customers specialize in terms of how they achieve their business and technological cloud objectives, the expectation is that they will look to cloud providers themselves for security functionality, and will also seek help from trusted partners, particularly in the case of multicloud support. Furthermore, we expect that future attack and defense dynamics, when added to the inherent technical complexity of cloud environments spanning multiple use cases and providers, will dictate that organizations have proper and efficient contextual understanding of their cloud presence.