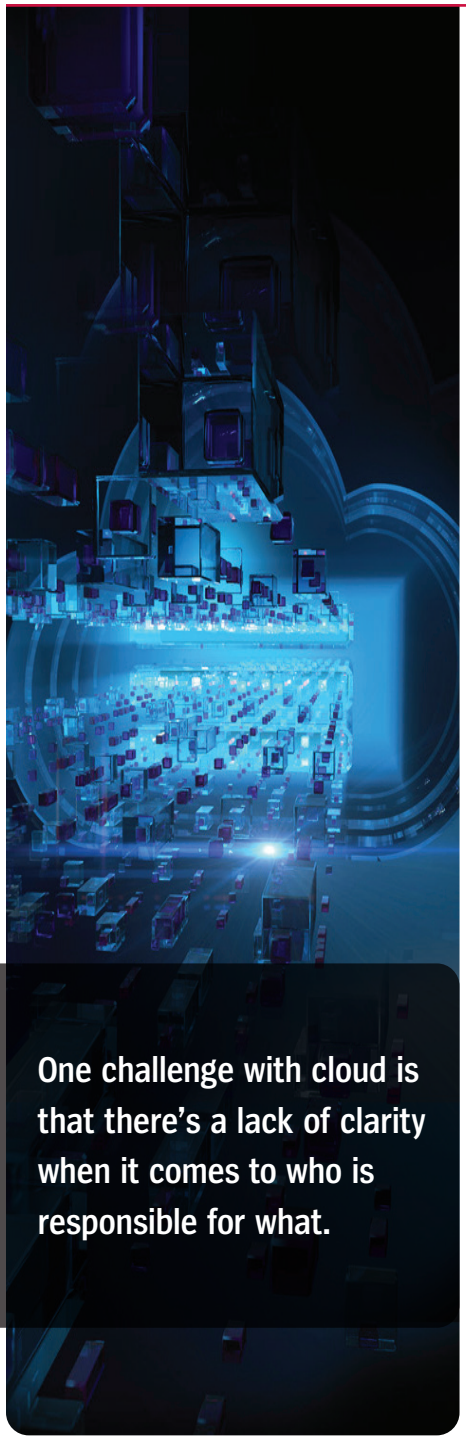
UNISYS | Securing Your Tomorrow®

Don't Take Cloud Security For Granted.

By Sudhir Mehta



One challenge with cloud is that there's a lack of clarity when it comes to who is responsible for what.

Organizations have widely embraced the cloud. The cloud is so firmly established that Gartner calls it "the new normal for enterprise IT."

The cloud is compelling because it is a lot more predictive in terms of an organization's IT spend. It drives innovation by enabling the quick and elastic provision of resources and by making a wide range of building blocks available from a single console. Organizations can be on the leading edge, be more agile and benefit from economies of scale.

Many organizations are already on cloud journeys today, but those journeys are still evolving. There is a lack of understanding of foundational paradigm shifts resulting from cloud usage. Compared to traditional data centers, the attack surface for cloud deployments is larger and more dynamic because of the use of ephemeral resources and more granular services. This is exacerbated by the sometimes-uncontrolled proliferation of cloud usage by teams within an organization.

A Lack of Clarity

One challenge with cloud is that there's a lack of clarity when it comes to who is responsible for what; this is true for organizations that use the cloud as well as between these organizations and public cloud providers. This includes DevSecOps operations such as continuous integration and deployment after initial cloud migration.

An Underestimation of Complexity

Organizations tend to underestimate the complexities of securing cloud environments. Applications running on-premises are within a well-understood and stable security perimeter under the organization's complete control. Moving to a cloud or hybrid environment changes this basic assumption. The increased flexibility and power of cloud services results in increased complexity of governance and operations, thereby increasing the possibility of vulnerabilities due to misconfigurations.

The unmatched flexibility and power of containerized microservices and Kubernetes also results in additional complexity by increasing the number of interfaces that may get exposed. The shorter deployment cycle for container images results in innovation and agility, but this also increases the possibility of compromised software within the security perimeter that is immune to boundary protections such as multifactor authentication.

Not understanding or investing in the tooling and expertise needed to manage this complexity has historically resulted in suboptimal configurations leading to exploits and data leaks. In a survey, nearly half of companies indicated that they have delayed moving an application into production due to container and Kubernetes security concerns.

Organizations need to address how their policies for data protection work when they don't have control of the infrastructure on which data resides.

An Unrealistic Expectation

Some organizations believe they can use on-premises security technologies in dynamic cloud environments. But traditional approaches don't work because the DNA has completely changed.

In the on-premises space, things follow a predicable progression. Step B follows Step A, and then Step C follows Step B. And it's typically based on an assisted framework where someone – usually an admin – is driving it.

However, in the cloud, Steps A, B and C could be operating at the same time. Now you need to have more of an automated process for cloud workload protection. You don't have the time or luxury of someone monitoring that on a day-to-day basis.

Inadequate Security Policies, Practices and Procedures

The cloud has consolidated a lot of infrastructure, systems and computing resources. Organizations need to address how their policies for data protection work when they don't have control of the infrastructure on which data resides.

Businesses that classify themselves as open-source companies typically provide microservices to other organizations. When organizations are using microservices in the development stage, they can play around with the code. But when those organizations move into production, there are different liability implications.

How to Handle Microservices

Microservices are gaining traction as a method for modularizing applications to leverage the benefits of Kubernetes. Software vendors offer containerized microservices that can be leveraged as components by applications. These come with a range of commercial and open-source licensing options with different levels of support or no support other than an online community. Some open-source licenses, such as GPL, can render software unsuitable for some production uses. The legal and cost implications of microservice licensing are an important aspect of this new application landscape. It is advisable to consider these during application development prior to the transition to production.

Why You Need Trusted Access

You also should employ trusted access. That means whoever has access to applications, communication routes or systems has the appropriate credentials.

Trust relationships and boundaries need to be managed in accordance with business objectives and legal constraints. In addition to robust authentication that uses credentials rotation and multifactor authentication, access privileges need to be defined in terms of roles based on least privilege. Least privilege implies that an HR role does not give access to sales – and an employee does not get access beyond the scope of their tasks.

Put the appropriate focus on cloud security, and not just on the cloud journey.

Sudhir Mehta
Sudhir is the Global Vice President for Product Management, Programs and Strategy wherein he leads and executes strategies across products and applications, partnering with Technology product owners, Enterprise Solutions and Public Sector to achieve defined business outcomes.

He can be reached at
Sudhir.Mehta@unisys.com

Limit and Secure Your Attack Surface

Efficacy in minimizing the attack surface implies limiting external and internal access (e.g., open ports) to what is absolutely necessary. It also implies disabling unnecessary software functions and infrastructure. This reduces the number of items that can be compromised.

Not only must the attack surface be limited, but it also needs to be guarded using an automated framework that intelligently detects anomalous traffic or software behavior. This should result in the appropriate policy-driven notification and quarantining actions, thus limiting the impact of breaches.

Approach Compliance With Care

Your overall framework should address all of the certification and compliance requirements your organization needs to meet. That should include all the criteria you met in your on-premises environment.

The cloud journey is exciting. Done right, it can bring many benefits to your company. If you don't do it right, however, the cloud can create significant nightmares. So, put the appropriate focus on cloud security, and not just on the cloud journey. Know that breaches will occur. And be ready to remediate and isolate breaches within seconds or minutes to limit the attack surface.

For more information,
visit www.unisys.com/closingthecloudgap

05/21 21-0263