Simplifying Multicloud Security With Managed Services

A managed security service provider can help CIOs and CISOs simplify their multicloud security environment, and help create a robust, sustainable and scalable security position for the enterprise

By Nitin Mishra

Enterprise IT has evolved dramatically over the last few years. Customer engagement and inter-connectivity are at the centre of every business application today, and cloud based applications have become the new normal. With more and more organizations now adopting multi cloud environments, security challenges have become even more complicated. While multi clouds offer unmatched flexibility in deployment and workload performance, they often lead to integration complexity, new security challenges and added vulnerabilities.

Managed security services can be a good way to tackle the challenges. A managed security service provider can be help CIOs and CISOs simplify their multicloud security environment, and help create a robust, sustainable and scalable security position for the enterprise. Here are three reasons why you need to partner with an established and state-of-the-art MSSP for multi-cloud security.

Handling Coverage and Complexity

With multicloud environments, security perimeters of IT organizations have widened far beyond their traditional scope of coverage. While allowing different business units operate on different cloud environments may bring home several cost and availability benefits, managing your IT security position in this dynamic environment is something that IT teams are not used to (or have been trained for).

For example, in a banking scenario, mobile apps today not just allow access to customer data but also provide the ability to perform a wide range of operations – such as banking transactions, mutual fund portfolio management, insurance purchases, loan applications, etc. Often, these workloads are placed in different clouds, and even different organizations. Across this environment, we can expect continuous changes to applications, data architectures and security protocols. The cloud vendors in use also keep adding new features and extending their platform capabilities, which further complicates the environment.

The MSSP Advantage: In such scenarios, managed security services can help organizations simplify and consolidate their security environment using a single layer (that includes security management, dashboards, people and standard processes). This has two important benefits: (a) scalability using a SaaS based model and (b) readiness to adapt and evolve the security environment to stay aligned to a continuously changing IT environment.

Addressing New Risks

Creating a loosely coupled cloud ecosystem also creates new risks. For example, there may be cases where teams make ad hoc or unannounced additions of shadow applications, or introduce new cloud platforms. In such scenarios, CIOs and CISOs need to rethink their IT security approaches and account for the added complexity that multicloud brings. Not to mention the added pressures of increasingly stringent regulations and security norms to protect data.

User demographics and motivations are also changing. More and more enterprise applications and data are being exposed to consumers, regulatory bodies, partners and other stakeholders. In the wake of a rapidly evolving user landscape, it is hard for security officers to overlook the ocean of possible threats such as uncharacteristic activities, untrusted modifications and unauthorized access.

The MSSP Advantage: The pace at which such threats occur give organizations very little time to react address each and every change across all IT assets across the organization. Since the rate of obsolescence in the world of IT security is high, building this level of security preparedness would be extremely cost and resource intensive for individual organizations. MSSPs have the necessary scale to make continuous investments in skills and technology tools to monitor, detect and react to changing security needs.

> With the definition of enterprise IT environment continuing to change, the complexity of handling a multicloud scenario will keep on increasing

Aligning Multiple Cloud Platforms

Although all major cloud vendors offer adequate security controls for the data and assets specific to their environments, they differ from each other in approaches to data back-up, access controls, compliance and other security features. As a result, data security officers are poorly positioned to develop a well-coordinated, unified response to any breach or attack. The problem amplifies when you have data being shared across different cloud providers, often making it difficult to meet overall compliance norms.

The MSSP Advantage: Finding a common ground to build a centralized orchestration across all your cloud platforms environments, and address the above challenges, becomes a key imperative. Without partnering with a proven MSSP, organizations may end up with a sub-optimal security position, and expose themselves to new, less understood risks.

With the definition of enterprise IT environment continuing to change, the complexity of handling a multicloud scenario will keep on increasing. Without a robust multicloud security approach, organizations risk growing overheads, skill shortages and new vulnerabilities. Therefore, irrespective of where they are in their multicloud journey, IT decision makers need to think well in advance about their security challenges and take proactive steps to mitigate risks in this new and fast changing environment. ■

The author is Senior Vice President & Chief Product Officer, Netmagic (An NTT Communications Company)