IBM India/South Asia Blog

Securing your Journey to Hybrid Multicloud

Feb 25, 2021

Sudeep Das, Security Software Technical Sales Leader, IBM Technology Sales, India/South Asia

In 2020, businesses shifted swiftly to the cloud to adapt to new remote work needs –and cybercriminals followed suit. In fact, today, 98% of organizations that have already embraced the cloud, use not just one, but multiple cloud environments to support their business needs.

While enterprises will continue with their digital transformation journey, we still see 80% of mission-critical workloads have not yet migrated to the cloud. The latest X-Force Threat Intelligence Index 2021 highlighted that cloud-based attacks have been on a rise globally. This continues to be a key deterrent for organizations to move mission-critical workloads to the cloud.

Several enterprises are still stuck in the 'planning phase' when it comes to an integrated security strategy, even as they continue to invest in point products for securing the cloud.

Point products lead to too many tools and vendors, creating silos within an organization

There are many cloud-focused security tools and native controls available in a hybrid multicloud environment. Such deployments run the risk of becoming silos, something you do not want to happen, as silos make it difficult to detect threats, investigate and remediate in an agile manner.

With mission-critical workloads and data moving from one cloud environment to another, determined by business needs – as a cybersecurity leader, you are expected to be an enabler of trust while ensuring a smooth and secure user experience across this journey. Securing enterprise hybrid cloud, hence, requires a comprehensive security program, integrating security into every phase of your journey.

Along this journey, key questions you must ask – and answer – include:

·How do we get started and what’s our goal?

·How can I integrate or extend my existing security tools to gain insight across my environment?

·How do I adapt to threats and respond to attacks that are now possible due to the increased footprint of my IT infrastructure?

·How do I protect my critical data across the sprawl?

·How do I build, deploy, and manage workloads securely in the cloud?

Reimagining security in a multicloud environment

Traditional security can’t keep pace. You need to reimagine security to help your organization move confidently to hybrid multicloud:

·A modern, open, and unified approach to security to detect, investigate, and respond to threats faster.

·A zero-trust security framework to help protect your data and resources by making them accessible only after the right level of verification.

How can IBM help?

IBM Security, with the experience of monitoring 70+ billion security events every day, is helping organizations align security strategies to their business; protect digital users, assets, and data; manage defences against growing threats; and modernize their security program with an open, multi-cloud platform.

With IBM Cloud Pak for Security, the foundation of IBM's open security strategy, you get a single platform that connects security across disparate tools and clouds. It leverages IBM's investment in Red Hat, including OpenShift, to advance security across hybrid cloud environments. Learn more here.

Zero Trust requires a broad portfolio of security capabilities and experience, and IBM Security offers tools and services to help lead you through every stage of your zero trust journey. Learn more here.

Use Confidential Computing to protect your sensitive data in the cloud Confidential Computing provides for a higher level of isolation for secure enclaves of data. Similarly, newer quantum-safe encryption technologies like homomorphic encryption allow computation on data without decrypting. Learn more here

Blog Categories

Secure