SPONSORED CONTENT

Laying a Secure and Trusted Foundation by Design for Cloud Migration

Accelerating cloud migration is central to the IT modernization road map — yet securing a hybrid, multicloud IT estate is a heavy lift for most organizations. The move can slow transformation and prompt many to seek out partners and services that can help mitigate the risks.

The hybrid, multicloud landscape introduces a variety of security challenges, with applications running across multiple clouds and a need to integrate data securely across the entire IT estate. With organizations ripe for modernization that enables them to respond quickly to changing business needs, there's ample desire to simplify and integrate the IT landscape so applications can be built once and securely deployed and managed anywhere.

As companies migrate more of their critical applications to the cloud, the attack surface is expanding. Ensuring the proper safeguards now requires a strategy that embeds security in every layer of the environment, with data at the center. Many organizations, already slow to embrace robust security protocols, are inadequately prepared to implement the new paradigm, because they lack experience in cloud security practices or the capacity to get it done.

Cloud providers such as Amazon Web Services (AWS) deliver a robust portfolio of cloud-native security controls, but sometimes they aren't configured beyond default settings and tailored to a customer's environment. As a result, organizations may need resources and expertise to effectively integrate those controls into a broader solution that delivers security and visibility across the hybrid cloud.

Another key requirement is centralized visibility across the hybrid cloud infrastructure. There is a need to simplify the IT landscape, defining an architecture that establishes a single, secure hybrid cloud platform along with the ability to manage costs and deployment as a unified portfolio.

One of the challenges in securing hybrid cloud infrastructure is understanding the shared-security model — and the role of the customer. Providers such as AWS are responsible for the security "of" the cloud, including elements such as the virtualization layer and all the physical infrastructure and data center facilities.

"A key challenge for customers is understanding the shared-responsibility model and not just between the hyperscaler and the consumer but, within the consumer organization, the shared responsibility between IT, security, and lines of business," says Abhijit Chakravorty, global executive for the Cloud Security Services Center of Competency at IBM. "There's the question of who is actually responsible for hardening the cloud services per the compliance and regulatory needs of an organization."

There's also the very real issue of a continuously changing pipeline of cloud-native security skills, making it difficult to stay current. Most organizations don't have the depth of talent to stay abreast of the evolving landscape or the budgets to staff experts fluent in all the different cloud platforms and enterprise security tools.

Security Concerns Impede Cloud Migration

The scale and complexity of the security mandate have become a barrier to cloud migration. Continued security skills shortages and lack of business confidence in migration without a formal security road map are hampering modernization and transformation efforts. A Forrester study[1] on cloud security found that 60% of security leaders still don't have a holistic, well-documented cloud security strategy, which is undermining any ability to get business on board with comprehensive migration plans. Another study, conducted by the Ponemon Institute, confirmed

[1] Forrester, Cloud Security Spotlight Study, 2021

the concerns, citing specific challenges including network monitoring/visibility (48%), in-house expertise (45%), increased attack vectors (38%), and siloed security solutions (36%) as the most significant barriers.

Compliance and regulatory obligations are also among the roadblocks to the cloud migration and modernization timeline. Even though cloud providers have comprehensive security and compliance controls as well as certifications and accreditations, it doesn't mean that an application running in one of their clouds is implicitly compliant with those standards. "Given the security of the cloud, sometimes assumptions are made that if an application or data requires compliance standards like PCI, HIPAA, or SOX, then migrating to the cloud will automatically make them compliant — it won't," explains Gilson Wilson, Global Security Principal, security, GSI partner development, for AWS.

The cloud remains an epicenter of cybersecurity incidents, illustrating the pervasiveness of the problem. [IBM's "Cost of a Data Breach 2022"] report confirmed that 45% of all breaches are cloud-based and that 83% of organizations are grappling with more than one data breach. Gartner[2] found that 99% of cloud security incidents through 2025 will be deemed the customer's fault.

A weak security posture is bad for business. The average cost of a data breach was $4.35 million in 2022, reaching an all-time high, 12.7% higher than the $3.86 million in 2020. The IBM report estimated that incidents occurring in a hybrid cloud environment resulted in, on average, $3.8 million in costs, compared to $4.24 million for private cloud breaches. Public cloud attacks were even more costly, associated with a $5.02 million price tag. There is additional fallout beyond costs. IBM research found that 60% of organizations' data breaches had led to price increases that were passed on to customers.

Redefining Security as an Enabler for Cloud Migration

Whereas the efforts needed to properly address the security challenges described here can seem to be obstacles to business modernization, the opposite is the case. Positioning security properly at the front of business modernization initiatives can become an accelerator to the business.

Whether customers are moving to AWS Cloud or already operating AWS Cloud, IBM Security offers a comprehensive combination of solutions and expert services to help develop, implement, and scale a security strategy, eliminating roadblocks and accelerating cloud migration.

With cyberattacks becoming an organized crime, the key to capitalizing on security as an enabler is to embed the security fabric in all phases of the AWS Cloud journey. This starts with the planning and identification of applications moving to AWS Cloud

[2] Gartner, "Is the Cloud Secure?" October 2019

and then applying a secure-by-design approach for the migrating stack, including all domains of cybersecurity: DevSecOps, container, infrastructures, identity access management (IAM), data, and incident response.

IBM's Secure AWS Foundation (SAF), a cornerstone of the cloud platform, embeds a secure-by-design cloud strategy early in the migration plan, helping keep the business confident in cloud migration while establishing security as a cloud enabler, not an inhibitor. SAF defines and deploys an optimal security architecture, using industry-focused, prebuilt patterns and templates that meet compliance needs and establish secure landing zones. The solution automates security enforcement, ensuring that when new workloads spin up, they adhere to enterprise security policies. SAF delivers many benefits, including accelerating deployment from months to weeks, enabling a 75% reduction in security deployment costs and speeding cloud migration by 40%.

The SAF Service offering enables a foundational security architecture and aligns with a management and governance model for core cloud-native controls in addition to providing security maturity, threat detection, and response readiness. IBM and AWS can be engaged for periodic assessments of security posture to ensure continuous improvement as the threat landscape and security climate evolve. In addition, the offering facilitates integration with other IBM/AWS services, including IBM Security QRadar SIEM (security information and event management), QRadar SOAR (security orchestration, automation, and response), IBM Security Guardium (data security), IBM Security ReaQta (endpoint detection and response [EDR]), and security for SAP transformation, in addition to other capabilities.

IBM Security will execute SAF capabilities through a managed security service (MSS) model, which can function as an extension of the IT organization, delivering advanced solutions and expert guidance to protect the AWS Cloud as part of a broader hybrid, multicloud environment. IBM Managed Security Services, working in tandem with SAF, has been endorsed by AWS as a Level 1 MSSP (managed security service provider) Competency Partner across 15 core specialization areas, including AWS Resource Visibility, AWS Security Best Practices Monitoring, AWS Compliance Monitoring, vulnerability management, threat detection and response, and edge security, among several other capabilities.

"Every client could do this, but they would have to hire the right skills, understand concepts such as the AWS Well-Architected Framework, and ensure they manage that talent adequately," says IBM's Chakravorty. "Alternatively, a service partner like IBM Security could do it for them in a shared-services model. We have built a platform with accelerators and reusable assets and have knowledge gleaned as a system integrator working across multiple clients across myriad industries."

Best Practices for Success

For turning security into an enabler of cloud migration and modernization, IBM Security and AWS experts make the following recommendations:

- **Adopt a secure-by-design mentality.** Focus on security before any migration planning starts or before mapping out requirements and system design, not as an afterthought. "Implementing security strategy and secure-by-design at a later stage of migration or halfway through an implementation or modernization journey will be a lot more expensive," says Ayyala Mahendra, lead for AWS's global solution architect practice.

- **Embrace cloud-native.** Native security controls are most effective when the applications are refactored to be cloud-native, with far more depth and defense than you would get from a lift-and-shift migration to cloud. Many organizations don't attempt a cloud-native approach, because their teams are structured with more traditional competencies. That's where a third-party services provider and systems integrator can help, because it has prebuilt patterns and templates in addition to a deep bench of cloud-native talent and extensive skill sets.

- **Exercise continuous improvement.** Once companies understand the line of demarcation for the shared-security model, they mistakenly believe that the work is done and that the proper safeguards are in place. Yet the model demands continuous improvement. "There needs to be some mechanism or governance model that constantly revisits security and makes changes as companies move ahead in their cloud adoption and migration journey," says AWS's Wilson.

Cloud holds the key to digital business success, yet mounting concerns about cybersecurity are holding up full-scale migration. The combination of managed services and solutions from partners IBM Security and AWS can bolster companies' cloud security posture, accelerating cloud adoption and paving the way to the modern enterprise.

IBM Security works with organizations as an extension of their team, offering expert guidance, consulting, prebuilt templates, and managed security services to help protect their AWS cloud environment. It enables you to embrace AWS-native controls while aligning them with your enterprise security programs to simplify and centralize visibility. IBM's modern security supports migration to cloud, so organizations can programmatically mature and transform enterprise security operations in addition to capitalizing on security as an accelerator for business modernization.

For a full view of our IBM Security offerings for AWS, please visit here.