Accelerate the AWS Cloud Journey *with Security Confidence*

Executive Summary

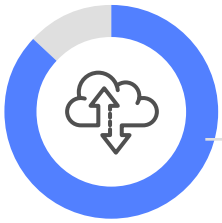
Companies are accelerating cloud migration as they look for every possible competitive advantage, from cost efficiencies to the ability to quickly scale and respond to shifting business needs.

The move to the cloud is also fueled by companies' push for digital transformation, a greater reliance on remote work models, and the drive to improve operational performance and agility. Among the ITDM respondents to a survey cited in LogicMonitor's "Cloud 2025" study, 87% expect the pace of cloud migration to pick up, and nearly three-quarters (74%) predicted that 95% of workloads will migrate to the cloud in the next five years.

Yet the pace of modernization is tempered by security challenges in the cloud, including new types of threats, lack of expertise, increasing alert volumes, and the mounting complexity of protecting workloads and applications across a hybrid landscape.

And while businesses aim to fast-track cloud migrations, security organizations often create bottlenecks as they navigate new cloud-native security paradigms; struggle with integration and visibility challenges; and try to hire or upskill their security staff with cloud-native security expertise, which is costly with talent in short supply.

The stakes are high: Misconfiguration of cloud environments led to more than one billion lost records in 2019.[1] In addition, customers' personally identifiable information (PII) has become the favored target of cybercriminals who have penetrated a cloud environment. Depending on the organization and the type of applications run in the cloud, a cyberbreach can lead to losses greater than $50,000 an hour, the report found.



87%

expect the pace of cloud migration to pick up, and nearly three-quarters (74%) predicted that 95% of workloads will migrate to the cloud in the next five years.

[1] IBM "Cloud Threat Landscape Report 2020"

Cloud Security Ushers in New Challenges

The number and type of security threats are growing, but the lack of visibility across the threat landscape and the siloed nature of cybersecurity tools can increase investigation and response times. A recent study by IDC reported that 79% of the participating companies have experienced at least one breach in the past 18 months, and among those impacted, 43% have encountered 10 or more cloud security incidents during that same timeframe. In that study of CISOs, 64% called out the lack of visibility into live cloud environments as the top threat to organizations.

Problems and challenges run the gamut:

An expanding footprint requires a unified security posture.
As the footprint expands across cloud and on-premises systems, having multiple security tools creates a disjointed security posture, making it difficult to establish a unified approach across all environments. This disjointed approach not only creates potential blind spots for attackers to exploit but also leads to longer-than-needed response times when threats are identified. There are also greater volumes of data running in the cloud, which increases the attractiveness of attack targets.

You can’t protect what you can’t see.
Meeting regulatory and compliance requirements is difficult without proper visibility across a hybrid landscape, and the process in the cloud is fundamentally different from that of an on-premises environment. In a private data center, the enterprise shoulders all the cost and responsibility associated with achieving and maintaining compliance.

In a cloud environment, on the other hand, compliance is a shared responsibility between the enterprise and the cloud provider and responsibilities are not always clearly delineated. Knowing exactly where sensitive data lies and who has access to it when there isn’t singular control over the environment is also problematic. Other complicating factors include the growth of shadow IT, which creates compliance challenges for cloud licenses that come into the enterprise under the radar screen of IT, as well as more complicated audit- and compliance-related reporting.

Cybersecurity and mitigation strategies need refining.
At the security-operations-center (SOC) level, many find it hard to detect cloud misconfigurations in a timely manner. Others spend too much time chasing down a high volume of low-value alerts versus channeling resources to real threats with greater impact. Organizations also struggle with the cost of maintaining staff to support cloud-native informed and specialized tasks in areas such as incident detection, penetration testing, correlation of global threat intelligence, and incident response. With cloud migration a top priority, organizations need to refine their cybersecurity and mitigation strategies to ensure timely response and recovery from potential disruptions to critical business functions.

“The penalty for getting security wrong is always very high,” notes Roy Stephan, AWS WW SI practice lead for security. “Many companies spend the time to train or hire people with the right skills, but working with an AWS Security Competency Partner such as IBM brings all of their knowledge on day one. This reduces the time for companies to migrate and launch AWS workloads by increasing security resources.”

The AWS Cloud Security Promise

AWS has a robust portfolio of native security capabilities designed to elevate security in the cloud. The platform integrates a wide range of global security and compliance controls that scale with workloads. These native tools provide visibility and automation not available in on-premises environments.

Integrated services such as Amazon GuardDuty, AWS CloudTrail, Amazon CloudWatch, and AWS Security Hub, among others, help organizations automate responses and remediation to react to attacks faster. Additional AWS services provide inline protection and guardrails that span the full life cycle of security. These native tools provide identity management, detective controls, infrastructure security, and data protection. AWS also incorporates numerous incident response solutions such as Amazon Detective and AWS Lambda while delivering access to the largest ecosystem of security partners and solutions.

The IBM Security Advantage—for AWS

IBM, an AWS Security Competency Partner, offers a unique combination of security technology and services as well as consulting and systems integration expertise. It can help organizations align security with the business; modernize security applied to cloud innovations and native security capabilities; protect users, assets, and data; and partner with customers as an operational security partner.

Customers can combine IBM Security integrated solutions to meet their needs, including IBM Security QRadar (Security Information and Event Management), IBM Security Guardium Data Protection, and IBM Security SOAR (Security Orchestration, Automation and Response) with IBM consulting, systems integration, and managed security services to support global delivery. IBM's services also provide full support for non-IBM technologies, providing critical flexibility to secure a hybrid cloud environment .

World-class security expertise and platforms

IBM's world-class security experts can augment the expertise of internal SOC analysts to help mitigate cost- and resource-related challenges of short-staffed security organizations. IBM tailors its advisory services to support AWS customers in different stages of cloud adoption. For example, the AWS Cloud Security Maturity Assessment provides a holistic review on strategy along with gap identification. The assessment can be extended to provide:

- **Holistic cloud security strategy and assessment**
- **Gap analysis**
- **Future state development**
- **Detailed road map to meet security objectives**
- **Best practice recommendations to improve cloud security implementations**

IBM consultants can also help build out infrastructure and endpoint security services, using secure-by-design best practices.

"There's a lot of pressure inside the business to modernize and innovate, and the AWS Cloud provides the capability to do that quickly," explains Mike Sanders, IBM Security program director for cloud security services. "Security must be an enabler for the move to the cloud. IBM helps organizations identify security gaps and quantify them in business terms, helping organizations understand areas they need to address and how. Examples include compliance and configuration monitoring, cloud workload protection, and enterprise threat management."

Intelligent threat management

In addition to consulting services, IBM Security X-Force Threat Management (XFTM), offers a comprehensive portfolio of services aligned with NIST standards that integrates asset insight, penetration testing, managed security services, incident response, recovery, AI, and orchestration into a single digital protection platform.

The Benefits of IBM Security Solutions on AWS

IBM's comprehensive security framework accelerates the modernization journey regardless of cloud maturity. IBM's portfolio of managed security solutions and consulting services aligns with AWS native security capabilities to secure applications and workloads across a hybrid environment. With an end-to-end approach, security becomes an enabler instead of a constraint for ramping up cloud migration and digital transformation.

In one example, IBM Security XFTM with QRadar can extend native AWS security and ensure that organizations meet their shared security responsibilities. Integrating the IBM and AWS security technologies and services provides holistic visibility, controls, and actionable insights across a hybrid environment, in turn simplifying security management, reducing alert volumes, and helping quickly identify and mitigate top threats.

Integration with AWS native security controls

Through native AWS integrations with services such as Amazon GuardDuty, AWS Security Hub, AWS CloudTrail, Amazon Detective, and others, QRadar ingests logs, flows, and events to ensure accurate and accelerated threat detection. The platform connects related events across a hybrid environment, so security teams receive only a single warning for a potential incident, which helps them optimize resources and avoid spending time handling redundant, low-level alerts.

Programmatic framework

IBM's programmatic framework, including AI-enabled threat investigation, automation, and orchestrated response capabilities, shortens the time to remediation for security misconfiguration and threats. The IBM Security "Cost of a Data Breach Report 2020," sponsored by the Ponemon Institute, found that misconfigured clouds were the leading cause of data breaches, cited by 19% of the respondents to the report's survey. Moreover, the report said companies fully deploying security automation saved an average of $3.58 million annually.

Companies are using IBM Security XFTM with QRadar to detect cloud misconfiguration, secure SaaS cloud applications, and perform real-time security analytics. Other advantages include leveraging the platform and services to meet regulatory compliance requirements and providing access to the X-Force Red team, a group that conducts extensive penetration testing on AWS environments and workloads and offers recommendations for mitigating security risks.

"Organizations may already have a security operations center, but as the business moves to the cloud for digital transformation, they don't get to build a second SOC," explains John Velisaris, program director, Strategy & Offering Management, Threat Management with IBM Security Services. "With XFTM services, IBM can help them operationalize cloud-native capabilities within the SOC they have today."

The Bottom Line

Cloud adoption is on the fast track as companies aim to improve efficiencies, lower costs, and scale innovations for competitive advantage. Yet, in the rush to take advantage of the benefits of the cloud, organizations may introduce new risks in their security posture.

By aligning with an AWS Security Competency Partner, such as IBM, that augments AWS native security with end-to-end capabilities and services, organizations can more efficiently close the cloud security readiness gap and navigate their cloud journey with confidence.

aws | IBM

Take the next step with IBM's Cloud Security Maturity Assessment for AWS to help identify gaps in your security posture.

Learn More