ESG Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Securing the Journey to the Cloud with IBM X-Force Cloud Security Services

Date: April 2020 **Author:** John Grady, Analyst

ABSTRACT: For many organizations, the adoption of cloud services has outpaced the security organization's ability to secure them. The breadth, complexity, and, in many cases, nascent nature of the security tools and processes required for a holistic cloud security strategy can be difficult for organizations to navigate. Engaging security service providers such as IBM X-Force Cloud Security Services for the development of a holistic cloud security strategy and assessment for future state roadmap, guidance across the spectrum of cloud security tools and processes, and the augmentation of in-house resources and IT resiliency through managed security services can help organizations accelerate their secure journey to the cloud.

The Rapid Pace of Cloud Adoption Has Introduced a Security Readiness Gap

It is no longer a question of whether, but rather, *how* companies are using cloud platforms. ESG research has found that 94% of organizations currently use public cloud to some extent, with as much as three-quarters of applications and workloads currently on-premises, on average, potentially moving to the public cloud over the next five years.[1] This adoption is often discussed broadly, but infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offer very different types of migration paths. Whether organizations choose to lift and shift existing applications to the cloud, re-platform to take advantage of cloud-native functionality, entirely refactor to fully embrace a microservices architecture, or replace with a third-party application can lead to very different security goals and challenges.

Cloud adoption is incredibly complex and nuanced, leading to a myriad of new and different security considerations for which many organizations are unprepared and unable to address.

Beyond the location of cloud infrastructure, the nature of the microservices in question further complicates matters. The adoption of containers and even serverless functions are accelerating quickly, with 35% of organizations currently running production applications or workloads in public cloud environments already using serverless functions extensively. In fact, the combined usage of serverless and container-based workloads will comprise 46% of production applications within the next 24 months.[2]

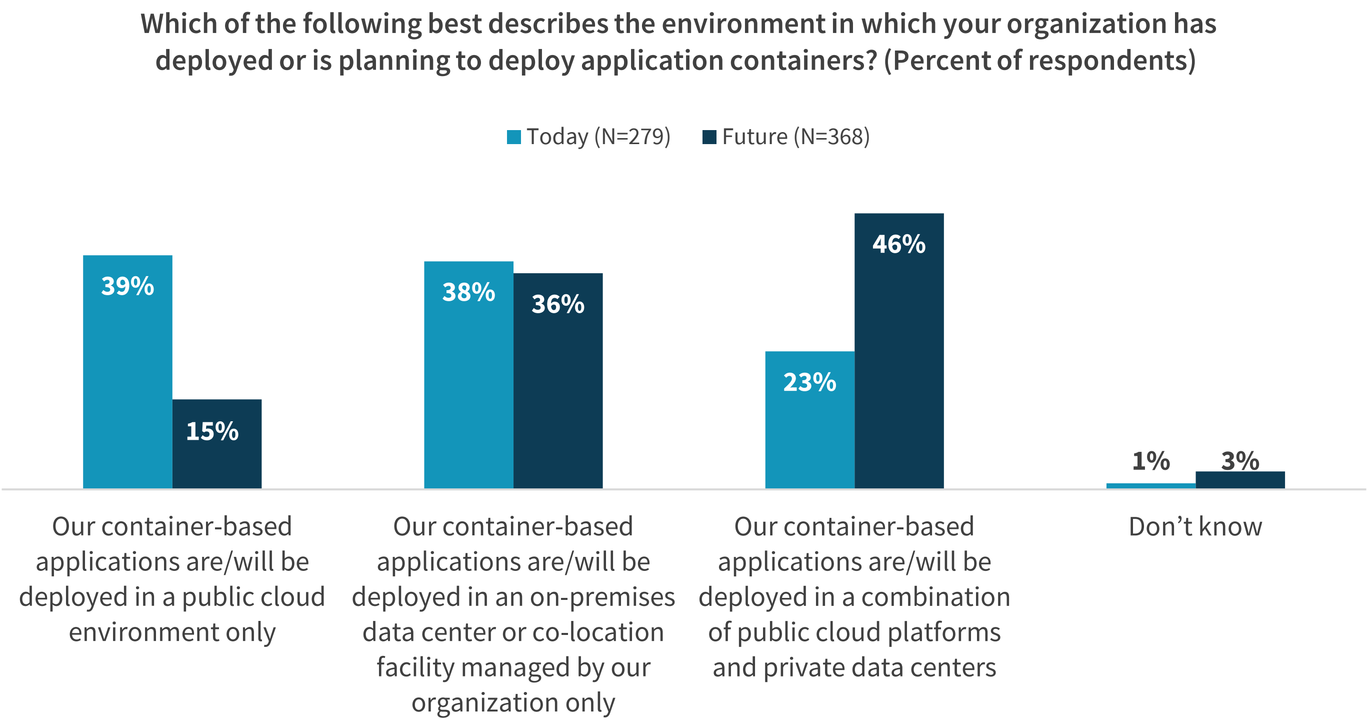
In part due to the adoption of containers and ultimately serverless functions, cloud repatriation will accelerate in some instances, increasing the prevalence of multi-location, hybrid infrastructures not just for organizations, but applications themselves. As microservices approaches are adopted, hybrid methodologies will be favored, with 82% of organizations reporting that their container-based applications will be deployed in a combination of public cloud platforms and private

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey,* January 2020.

[2] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.

data centers in the future.[3] Products such as AWS Outposts, Azure Stack, and Google Anthos were released specifically to address these use cases. In short, cloud adoption is incredibly complex and nuanced, leading to a myriad of new and different security considerations for which many organizations are unprepared and unable to address.

Figure 1. The Prevalence of Hybrid Cloud Is Exemplified by Container Adoption



Source: Enterprise Strategy Group

Security Processes and Culture Change with the Adoption of Cloud

In addition to the issues around tools, the security processes and culture are fundamentally different in a cloud model. The decentralization of IT is one of the biggest changes to which organizations must adjust. In an agile-focused, DevOps environment, speed is of the utmost importance in order to drive rapid innovation. Cloud resources can be procured and provisioned without the oversight of IT.

In this model, security (which is often perceived as slowing things down even in traditional IT processes) is frequently left to the side. The challenge is to allow DevOps to move at the speed of cloud, but to do so in a secure fashion. Creating buy-in from application teams to give security a seat at the table and pushing security teams to adapt tools and practices that integrate into established DevOps processes can be an uphill battle for even the most advanced organization.

The challenge is to allow DevOps to move at the speed of cloud, but to do so in a secure fashion.

Another issue which organizations continue to struggle with relative to cloud is the shared security model. In an on-premises environment, the security team has responsibility for everything from the infrastructure layer up to and including the data. However different types of cloud services come with different types of security responsibilities. In an IaaS environment, the customer is responsible for securing everything above the guest operating system, above runtime for PaaS and the data layer in SaaS. Beyond just the tools involved, CSPs must be integrated into security processes as well.

[3] ibid.

Taking incident response as an example, security teams must identify the correct personnel to work with when problems do arise to ensure a seamless reaction. Managing these different levels of responsibility across different types of cloud services and CSPs, especially when the security team may not even have visibility into all usage, can be difficult for even the most mature security organization.

Both Legacy and Cloud-native Security Tools Can Pose Challenges

The fundamental differences in the architecture of cloud-native applications often require new tools with different capabilities. Managing a mix of cloud-native tools from different cloud service providers (which typically only address a specific cloud environment), as well as third-party tools, introduces increased complexity and management overhead for security organizations. This is exacerbated when spread across multiple disciplines of cybersecurity, including:

- Threat – The threat model changes as the perimeter becomes nebulous. Firewalls and other perimeter-based tools made more sense when it was easier to delineate what was inside the network as good and what was outside as bad. The increasing impact of insider threats, both relative to malicious and curious insiders as well as entities which appear to be insiders due to credential theft have forced a rethinking of this model. Additionally, with workloads spanning on-premises and cloud, centralizing visibility and maintaining a deep, contextual understanding of the relationships between workloads within an application, between applications and other applications, and between users and applications becomes more difficult, but more important than ever. As the workloads of an application become dispersed, and even portions of the workloads containerized and further distributed, it becomes impossible to maintain this visibility with legacy tools.

- Data – Sensitive data is quickly being moved to the public cloud and typically across more than one provider. Many times, the IT organization may not even be aware of all of the cloud applications being used to house sensitive data. Even in a cloud model, enterprises remain responsible for discovering, classifying, and protecting their data, as well as maintaining encryption and key management programs. These concepts are difficult on-premises and can become more complex in the cloud. In fact, 50% of organizations report having lost cloud-resident data, while an additional 22% suspect they may have.[4]

- Identity – Credential theft remains among the most common methods for attackers to gain access to corporate data. The number of different resources and platforms organizations now use makes it difficult to maintain visibility and control over who has access to what and inconvenient for users to manage multiple credentials. As workloads become dispersed, authenticating one microservice to another and managing those identities becomes infinitely harder as well.

Where Security Services Can Help

Cloud security requires a different approach to many fundamental aspects of cybersecurity and many organizations lack the resources to have expertise in all facets. Further, because of the speed at which cloud adoption itself moves and the rapid innovation it enables, without an overarching strategy to guide a cloud security program, security teams will constantly be forced to play catch up to try to implement security after the fact. Engaging service providers for assessment and planning, assistance with the implementation of new processes and technologies, and managed security services can help accelerate the adoption of a holistic approach to cloud security.

- Assessment and Strategy – Service providers have deep industry security and compliance experience to help organizations benchmark against best practice standards and regulations, as well as assessing against specific

[4] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

business requirements such as cost management, risk tolerance, or geographic reach. This experience helps organizations prioritize remediation tasks and understand where on the roadmap specific improvements should fall—in essence, developing a strategy for both short- and long-term improvements to the company's cloud security posture. Finally, aligning the cloud security strategy to the organization's cloud strategy is an important component and imperative to successfully executing on the overall business strategy.

- Consulting and Integration – Common entry points for attacks on cloud services include misconfigurations, unpatched systems, and stolen credentials. Service providers offering planning and implementation capabilities can help close these gaps across many cybersecurity disciplines. Integrating cloud workload protection, cloud security posture management, and micro-segmentation tools across hybrid multi-cloud environments can be challenging but can significantly reduce the attack surface if done correctly. Employing proper identity and access management design and implementation to ensure multi-factor authentication and utilizing a least privileged model can prevent credentials from being misused. Employing a holistic approach to cloud data security, including encryption, classification, and discovery, can limit the blast radius in the event a breach does occur. Building end-to-end cloud risk and compliance, as well as intelligence and operations programs, can ensure that the organization's risk profile as it relates to cloud is fully understood, that relevant regulations are followed, and that processes are put in place to efficiently respond to issues when they arise. Finally, service providers can provide guidance and best practices for DevSecOps implementations, both from a culture perspective and relative to fitting all recommended security tools and processes into existing DevOps methodologies to improve automation.
- Managed Security Services – It is often necessary to outsource certain aspects of a cloud security program to reach the required scale across hybrid and multi-cloud environments, or to close gaps based on resource constraints. Specific examples can include visibility and management of cloud resources for threat prevention and anomaly detection, compliance and posture management monitoring and reporting, vulnerability management and offensive testing, all the way up through security operations and incident response.

Enter IBM X-Force Cloud Security Services

IBM's X-Force Cloud Security Services seek to help organizations navigate a landscape in which cloud security is difficult because a comprehensive security program must address every layer of the cloud stack. As such, IBM's cloud security services parallel the company's overall cloud services across the four pillars of Advise, Move, Build, and Manage, with DevSecOps a prominent theme throughout.

Advise

The Advise portion of IBM's cloud security services helps organizations with strategy and roadmap development to ensure a secure hybrid multi-cloud environment that is aligned with business strategy. The program establishes a security baseline by establishing a macro-level architecture design for every layer, mapping to regulatory and privacy requirements, and providing customers an industry-specific maturity roadmap. IBM performs critical data and cyber resiliency assessments to locate and classify critical data and create a strategy to protect and manage it across the entire cloud environment. Determining whether to utilize cloud-native or third-party security controls is a key consideration when creating a cloud security program. IBM's assessment and recommendations in this area provide guidance on where and when to use each type of tool and the tradeoffs of each. Specific to DevSecOps transformation, IBM also provides advisory and consulting DevOps Workshops to assess the current state of agile programs and begin the introduction of DevSecOps best practices.

Move/Build

The Move/Build aspects of the IBM cloud security services portfolio help organizations leverage the speed of cloud by shifting left to securely build applications. These services help organizations implement security controls across data, identity, containers, infrastructure, and endpoints that provide automation and plug into existing DevOps processes and toolsets. Additional services include recurring offensive penetration testing, disaster/incident recovery planning, cloud risk and compliance program development and implementation, and security intelligence and operations capabilities.

Further, DevSecOps-focused programs assist organizations in rolling out secure-by-design application development leveraging automation. Specific services include:

- DevSecOps Framework – provides the assessment and design of DevSecOps implementation across people, process, and tools.
- DevSecOps Culture Transformation – engages with an organization's DevOps team to assess and influence the culture to move toward a DevSecOps approach.
- DevSecOps Implementation – fully implements recommended DevSecOps tools and processes.

Manage

Finally, IBM X-Force Cloud Security Services offer managed services across many of the capabilities covered under the Advise and Move/Build portions of the portfolio. While foundational managed services of infrastructure and endpoint tools (such as firewall, IDS/IPS, CWPP, and others) as well as cloud data protection services (such as cloud access security brokers and Guardium) are available, IBM also provides more advanced managed services. Managed vulnerability scanning as well as continuous compliance and reporting offload the difficulty of maintaining visibility across multiple cloud environments from internal teams. Integrated threat management, incident response, and resiliency management services free up internal SOC personnel to focus on other priorities. Centralized visibility and policy management as well as automated runbooks via orchestration tools improve efficiency and reduce redundant processes. Finally, IBM offers a managed DevSecOps solution through its Custom Application Security Managed Services program, which includes both the management and oversight of the client's application security program and individual services within it.

The Bigger Truth

Organizations increasingly turn to the cloud to improve efficiency, lower costs, enhance performance and scale, and, perhaps most importantly, rapidly deliver innovative solutions to their customers. Yet in the rush to take advantage of these benefits, security is too often overlooked, potentially leaving critical gaps in an organization's defenses. The cybersecurity skills shortage is well documented and is particularly acute relative to cloud. As IT teams work to close the cloud security readiness gap and build out end-to-end security programs addressing today's hybrid multi-cloud environments, engaging service providers is an effective way to augment in-house resources. Providers offering strategy, deployment, integration, and management capabilities across the spectrum of security disciplines can not only help security teams put the right tools and processes in place, but also help with the cultural transformation required to secure agile environments. Leveraging its strong history of consultative business services, IBM X-Force Cloud Security Services has built a comprehensive portfolio to help organizations secure their journey to cloud.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188