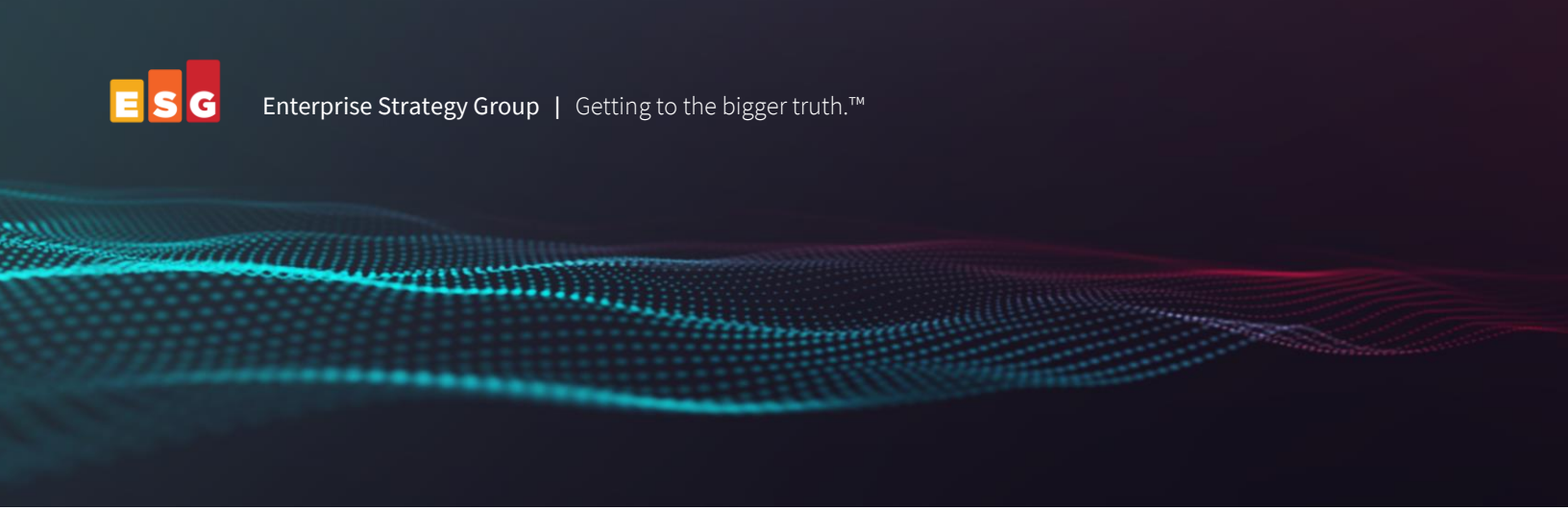



ESG WHITE PAPER

# Securing the Journey to Cloud

## Considerations for Overcoming the Cloud Security Readiness Gap

By John Grady, ESG Analyst

April 2020

This ESG White Paper was commissioned by IBM and is distributed under license from ESG.

## Contents

## Executive Summary

Cloud has fundamentally changed not only the tools and technologies business use on a daily basis, but the processes, organizational structure, and culture associated with IT as well. A clear example of this is DevOps, which has rapidly gained traction as application development teams seek to become more agile, efficient, and effective in creating value for customers.

Unfortunately, security considerations often continue to be overlooked. Securing cloud-native infrastructure, assets, and data introduces fundamentally new challenges to which cybersecurity teams are not accustomed. Due to the scale and complexity of updating cybersecurity programs to address cloud environments, engaging with third-party service providers can act as a powerful force multiplier to help organizations more efficiently close the cloud security readiness gap.

**Engaging with third-party service providers can act as a powerful force multiplier to help organizations more efficiently close the cloud security readiness gap.**

## The Impact of Cloud Adoption on Application Architectures and Development Methodologies

The benefits of migrating corporate resources to cloud-native platforms are well-established. Financial implications are often among the top reasons companies turn to the cloud. This can include limiting capital expenditures and shifting to an operating expense model, reducing infrastructure costs directly by paying only for those resources used, and lowering costs associated with data center management and operations. Organizations also turn to the cloud to efficiently and effectively expand their geographic reach. Performance and scalability are also key drivers, with cloud services providing organizations the ability not only to dynamically and reliably provision resources, but also to improve the velocity with which new applications can be built and deployed. Whatever the specific drivers for turning to cloud, organizations ultimately seek to shift away from infrastructure management and focus more of their resources on application development and innovation.

### The Migration to Cloud Is Complete, but Continues to Evolve

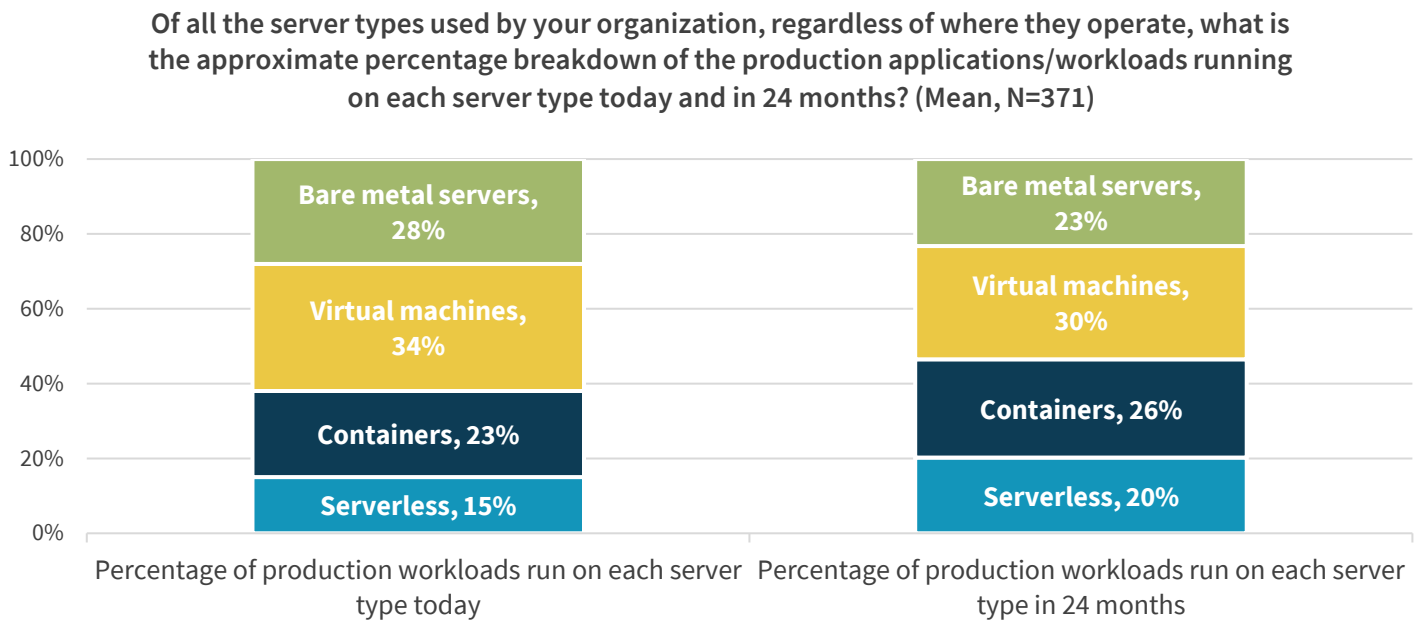
For these and other reasons, it is no longer a question of whether, but rather how companies are using cloud platforms. ESG research has found that 94% of organizations currently use public cloud services in some way; however, the nature of that usage has changed over time. Companies are no longer moving single applications or pre-production applications to the cloud. Rather, multiple mission-critical applications housing sensitive data are being shifted off-premises. Additionally, three-quarters of applications and workloads currently on-premises could move to the public cloud over the next five years. This migration can take many forms across infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), with most organizations choosing a mix of all three.[1]

Further complicating matters, the adoption of containers and serverless functions are moving quickly. ESG research has found that 35% of organizations running production applications or workloads in public cloud environments report using serverless functions extensively.[2]

Combined, serverless and container-based workloads will comprise 46% of these organizations' production applications within the next 24 months (see Figure 1).[3] Better application performance, improved software quality, better application portability, and the enablement of DevOps methodologies are all drivers for this ongoing shift.

[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.

**Figure 1. Container and Serverless Function Adoption Is Accelerating**




*Source: Enterprise Strategy Group*

In part due to the adoption of containers and serverless functions, cloud repatriation will accelerate in some instances. As these microservices-based approaches are more frequently adopted, the prevalence of multi-location, hybrid infrastructures not just for organizations but for applications themselves will increase. In fact, 70% of organizations expect their container-based applications to be deployed in a combination of public cloud platforms and private data centers.[4]

## Companies Are Still Adapting to the Changes in Process, Responsibility, and Organization Cloud Brings

While the migration to, and evolution of, cloud usage can be complicated from a technical standpoint, organizations must navigate additional factors. First, the rapid innovation enabled by cloud allows organizations to quickly adapt to changes in the market by developing and delivering new products to market faster. As part of this, the end-user experience (UX) becomes paramount and technologies or processes that may negatively impact UX may be ignored. Unfortunately, this can often include security when not updated to keep up with the new pace of adoption.

To enable this rapid innovation, many organizations have shifted from a waterfall to agile application development methodology. ESG research has found that 52% of organizations running production applications in the public cloud report using an agile software development framework.[5] Agile approaches, especially when coupled with cloud-native architectures, facilitate a more iterative development process through failing faster. The end-goal of this is to improve the incorporation of end-user feedback and ensure the quicker delivery of services. Yet as the development cycle becomes more fluid and less linear, traditional security testing and assessment processes become a bottleneck and are likely to be forgone.

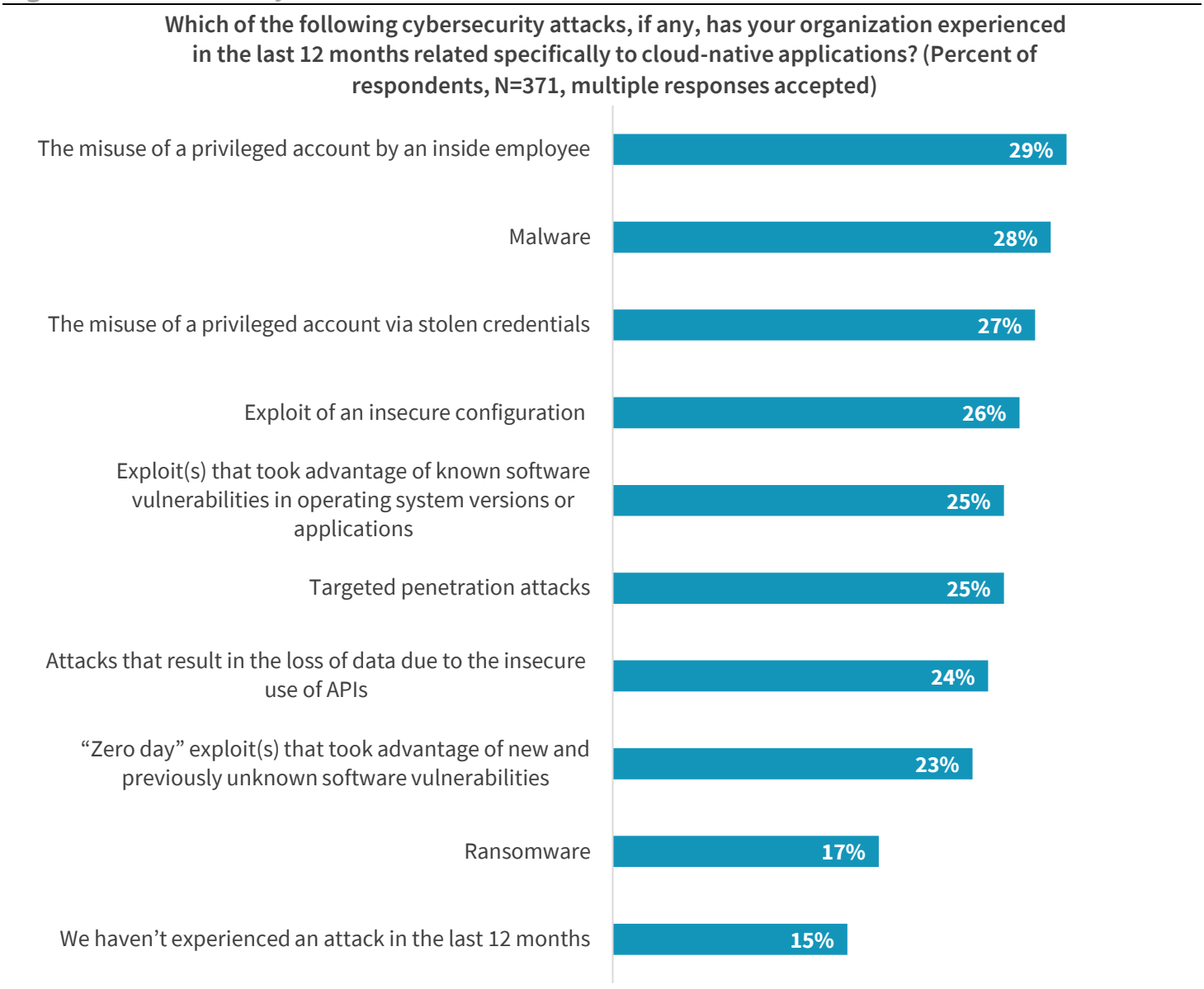
Finally, as traditional development models have evolved, the formerly centralized ownership of IT often becomes more distributed. Shadow IT can become a problem as lines of business utilize cloud applications without IT knowledge or approval. Developers become the de-facto decision makers, with IT tasked to support them and, at a minimum, not stand in their way. Security, too often seen as an inhibitor, is likely to become an afterthought in this model.

[3] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.
[4] Source: ESG Master Survey Results, *Trends in Modern Application Environments*, December 2019.
[5] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.

## DevOps Adoption Has Become Mainstream

In conjunction with and inspired by agile approaches, DevOps methodologies have begun to see broad adoption. Over half (57%) of organizations with production workloads in public cloud environments report employing DevOps methodologies.[6] DevOps formalizes a continuous integration and continuous delivery (CI/CD) model incorporating application development, integration, builds, testing, and delivery into production. DevOps improves communication and collaboration across different teams, delivers faster innovation, and when done correctly, leads to fewer defects and enables faster response to those defects that do occur. Despite all the benefits that DevOps offers, the lack of security as an inherent part of the methodology can lead to critical issues if not addressed.

**Figure 2. Cloud Security Threats**




*Source: Enterprise Strategy Group*

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

## Cloud Adoption Introduces a Security Readiness Gap

In addition to the organizational and process-centric changes companies must consider when adopting cloud services, a new set of security challenges are introduced. While malware and other "traditional" threats still exist in the cloud, exploits that target vulnerabilities in unpatched systems, the misuse of privileged accounts, or misconfigured workloads become more difficult to defend against in distributed cloud environments (see Figure 2).[7] Specifically, because the pace of cloud is accelerated with security considerations often an afterthought, a readiness gap exists between the use of cloud technologies and organizations' ability to secure them.

### Legacy Security Solutions Typically Do Not Address Cloud Use Cases

At a high level, the task of the security organization remains generally the same whether the focus is protecting resources located on-premises or in the cloud. Applications, devices, data, and identities must be protected. Attacks must be prevented wherever possible, detected quickly and effectively when not, and remediated efficiently. However, the specifics of how this is accomplished and differences in the architecture of cloud-native applications often requires new tools with different capabilities. Additionally, managing a mix of cloud-native tools from different CSPs as well as third-party tools introduces increased complexity and management overheard, which security organizations must overcome.

Data security is a good example of this dynamic. Sensitive data is quickly migrating to the public cloud, and typically is spread across more than one cloud provider. On-premises data security programs are fairly mature across people, process, and technology, and are centered on a baseline understanding of what the organization's sensitive data is, where it resides, and who should have access to it.

**50% of organizations report having lost cloud-resident data while an additional 22% suspect they may have lost cloud-resident data but are not able to confirm.**

Comparatively, cloud-focused DLP solutions are more nascent and do not always plug into an established data security program. As a result, policy violations, misconfigured access controls, and a lack of visibility into the movement of data between the network and cloud services can all lead to data loss. This scenario is not a hypothetical: 50% of organizations report having lost cloud-resident data while an additional 22% suspect they may have lost cloud-resident data but are not able to confirm.[8]

The threat model also changes significantly as the perimeter becomes more nebulous as a result of the adoption of cloud services. The old delineation of everything inside the perimeter being good and outside being bad was somewhat flawed to begin with in that it ignored the impact of malicious and curious insiders. However, with workloads now spanning on-premises and cloud, that legacy model cannot address today's dynamic environments. Centralizing visibility and maintaining a deep, contextual understanding of the relationships between workloads within an application, other applications, and users of applications has become more difficult yet more important than ever. As the workloads of an application become dispersed and portions of the workloads containerized, further distributed, and in many cases ephemeral, it becomes impossible to maintain this level of visibility with legacy tools.

[7] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.
[8] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

### Programmatic Elements of Cybersecurity Are Challenged by Cloud

In addition to the issues around tools and what is needed to secure a cloud-centric environment, programmatic challenges are introduced. The cloud shared security model can still be confusing for even the most mature security organizations to navigate.

Moving from an on-premises model where the organization has ownership over the entire security stack to a varying level of responsibility depending on whether the cloud platform is IaaS, PaaS, or SaaS is a fundamental change in approach. Some organizations continue to assume that cloud resources are secure by nature, and even those that do understand that they hold some level of security responsibility can have trouble maintaining consistency across different cloud platforms.

**Moving from an on-premises model where the organization has ownership over the entire security stack to a varying level of responsibility depending on whether the cloud platform is IaaS, PaaS, or SaaS is a fundamental change.**

As highlighted earlier, the decentralization effect cloud has on IT overall is arguably magnified relative to security. While there may be negative impacts to cost and productivity when IT does not have purview over technology use, the risks are far more significant when security is left out of the loop. Specifically, compliance issues can be introduced, vulnerabilities cannot be managed, and data loss becomes much more difficult to prevent.

Finally, relative to DevOps, there can be a clash of cultures when it comes security considerations. Application development teams may be hesitant to include security teams in their planning over concerns that it will introduce bottlenecks and slow down workstreams. Similarly, security teams can be hesitant to learn the additional skills required to plug into DevOps methodologies, and push back on adjusting their processes to meet another team's priorities.

## Best Practices in Cloud Security

Closing the cloud security readiness gap is not something that can be completed overnight or accomplished with a single tool. Instead, people, processes, and technology must all be accounted for, assessed, and integrated into a holistic cloud security strategy. Though not an exhaustive list, these best practices offer a starting point and some of the most important considerations when approaching cybersecurity as part of the journey to cloud.

### Cloud Security Assessment and Strategy

*Assess the Organization's Current Cloud Usage and Related Security Posture to Identify Critical Gaps*

The first step in closing the cloud security readiness gap is fully understanding the organization's current posture and where the greatest risks lie and prioritizing desired outcomes. Often cloud strategy and security strategy are developed independently, resulting in unaligned priorities. A cloud security strategy should first account for the business objectives of the organization's overall cloud goals.

**The first step in closing the cloud security readiness gap is fully understanding the organization's current posture and where the greatest risks lie and prioritizing desired outcomes.**

From there, the security imperatives can be addressed. Is the goal to meet regulatory requirements, improve visibility over cloud assets, tighten data security controls, or build security into the development cycle? While a complete cloud security program cannot be developed overnight, creating an overarching strategic roadmap upfront is important to build consistency and ensure alignment across the organization.

*Consider Adding the Role of Cloud Security Architect*

To centralize their cloud security strategy, many organizations are beginning to employ cloud security architects. These roles typically have technical, policy, and regulatory responsibilities around drafting the policies for how the use of cloud services are secured, defining the requirements for cloud security controls, vetting cloud service providers and their security capabilities, and creating technical evaluation criteria for cloud security controls. These roles are still being defined relative to not only responsibilities but also reporting structure. However, organizations that are prioritizing cloud security are quickly moving in this direction.

## Build a Cybersecurity-centric Culture and Standardize Security Processes Through DevSecOps

*Embed A Security-first Culture Across the Organization*

In today's world, the mantra for any organization serious about cybersecurity should be "every employee is in security." That culture must be driven from the top of the organization and lived every day. For the broader employee-base, this should include a digestible, engaging, and ongoing training and education program that drives employees to embrace a cybersecurity-centric culture.

Relative to the adoption of DevSecOps methodologies, DevOps must be an integral part of the planning and implementation process to ensure their voices are heard, their concerns addressed, and ultimately, their support won. Similarly, cybersecurity team members must be tightly aligned with DevOps teams to understand those processes and culture and ensure they are enabling rather than inhibiting the team. In action, this results in a continuous communication cycle where developers effectively relay the high-level goals, behaviors, and architecture of the applications being built and the security team efficiently provides the correct tests, controls and monitoring (ideally in an automated fashion) to address the application's specific needs.

*Utilize an Iterative Approach to DevSecOps That Expands Over Time*

While 55% of organizations report incorporating security processes and controls into their DevOps processes, it remains an iterative process that expands over time for many.[9] Initial use cases may lean toward workload and container segmentation, API inspection, and configuration and vulnerability assessment. Pre-deployment malware detection and visibility for incident response, forensics, and threat hunting may then be added over time. Finally, automating the detection of anomalous activity and applying preventative runtime controls could be incorporated at a later date.

*Both Pre-deployment and Runtime DevSecOps Use Cases Must Eventually Be Addressed*

There is no right answer on where to start with DevSecOps, and both pre-deployment and runtime use cases must ultimately be addressed in the methodology.

However, the idea of hardening workloads by ensuring known vulnerabilities have been identified and remediated prior to pushing to production is a core tenet of the methodology, a repeatable process, and generally as good a starting point as any.

**There is no right answer on where to start with DevSecOps, and both pre-deployment and runtime use cases must ultimately be addressed in the methodology.**

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

## Incorporate Controls Spanning Threat Prevention, Data Protection, and Identity

### *Deploy Cloud Workload Protection Platforms (CWPP) to Automate Defenses*

These workload-centric solutions are built to address public and hybrid cloud infrastructure and provide workload behavior monitoring, malware scanning, application control, and log management and monitoring among other capabilities. CWPPs typically offer integrations with DevOps orchestration tools to automate deployment and ensure consistency across multiple environments. Additionality, these tools are adding capabilities to address container and serverless environments. Through the deployment of controls as a privileged container within Kubernetes environments and runtime application self-protection (RASP) capabilities for serverless functions, CWPPs provide centralized protection across disparate environments.

### *Employ Cloud Security Posture Management (CSPM) to Ensure Consistency*

Many cloud security issues continue to arise due to misconfigurations. CSPM tools automate the assessment of an organization's cloud resources as compared to benchmarks. Additionally, they automate the assessment of an organization's cloud environment, inventorying resources (including instances of shadow IT), and detecting misconfigurations based on established security policy as well as compliance frameworks.

### *Apply Granular Segmentation to Limit the Blast Radius When Exploits Do Occur*

Segmentation and the cloud-centric practice of microsegmentation have been shown to reduce the attack surface but have historically been seen as a complex implementation. While CWPPs offer some microsegmentation capabilities, the functionality is not as advanced as purpose-built solutions. Infrastructure and hypervisor-based tools provide the ability to leverage existing infrastructure. However, host-based tools provide consistency across different cloud and on-premises environments, as well as detailed relationship mapping and security policy recommendations to streamline the segmentation process.

### *Ensure Visibility Over, and Protection of, All APIs*

Web APIs are ubiquitous, yet traditional application security tools often fall short in protecting them. Additionally, serverless computing relies heavily on APIs, resulting in API visibility and scanning becoming more important than ever for cloud threat prevention programs. While pre-deployment testing and validation and ongoing auditing built into the DevSecOps process can help, dedicated protection against both sophisticated bots and manual exploits is necessary to prevent fraudulent and malicious activity.

### *Use Multi-factor Authentication (MFA) and Single Sign-on (SSO)*

Multi-factor authentication has seen a surge as zero-trust networking concepts become more widely deployed and is just as applicable to cloud security. MFA should be employed for all users, but without question must be implemented for root and privileged accounts. As is the case with many tools, employing strong security can introduce user experience concerns. With this in mind, organizations utilizing multiple cloud platforms should consider single sign-on solutions to streamline the user experience and make MFA less intrusive.

### *Embrace a Least Privilege Model and Regularly Audit Those Privileges*

Following on the zero-trust concepts mentioned, the goal of any security organization should be to employ a least privilege model of access control. Users should only have the minimum level of access required to do their job. Further, the combination of employee turnover and managing identities across numerous cloud platforms creates the opportunity for attackers to exploit dormant accounts. As such, processes should be in place to regularly audit privileges and ensure they are revoked when no longer applicable.

*Implement Just-in-time (JIT) Privileged Access Management*

As shown in Figure 2, the misuse of privileged accounts is the most common type of cloud security attack. Just-in-time privileged access management reduces the risk of over-privileged accounts being exploited by hackers or insiders by granting elevated access only as needed, as opposed to maintaining that level of access consistently.

Rather than elevated privileges always being on, JIT solutions provide administrators a route to request additional temporary permissions on an as-needed basis.

**The misuse of privileged accounts is the most common type of cloud security attack.**

*Consider Service-to service Authentication Solutions*

Of increasing importance as applications become more likely to interact with other applications without human involvement is managing the identities and authentication mechanisms for those workloads and transactions. Solutions that address this use case are poised to become a central part of any cloud identity and access management strategy as hybrid and multi-cloud environments expand.

*Unify Data Security Policies Across On-premises and Cloud-resident Data*

With the lines between cloud and on-premises increasingly blurred, it has become imperative for organizations to create a set of data security policies that are location-agnostic. The difficulty in discovering and classifying sensitive data in cloud environments, made more difficult by the decentralization of IT discussed previously, has limited the maturity of cloud data security programs. However, this is beginning to change, and organizations should explore solutions that provide data security consistently across all environments.

*Ensure the Ability to Detect Data Loss in Real-time*

Organizations must detect suspected breaches and subsequent data loss in real time across the entire environment. Solutions that aggregate context around users, devices, and identity in conjunction with data content awareness across heterogeneous public and private cloud environments are table stakes for modern data security initiatives.

## Where Services Can Help

Because cloud security requires a different approach to many fundamental aspects of cybersecurity, most organizations lack the resources to have expertise across all facets.

**Engaging service providers for assessment and planning, assistance with the implementation of new processes and technologies, and outsourcing can help accelerate the adoption of a holistic approach to cloud security.**

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 and try to address security after the fact, which is never a successful approach. Engaging service providers for assessment and planning, assistance with the implementation of new processes and technologies, and outsourcing can help accelerate the adoption of a holistic approach to cloud security.

### Assessment and Strategy

As described earlier, the first step in building a comprehensive cloud security program is assessment. This includes inventorying the current state of cloud usage, assessing the security controls currently in place, determining where the

greatest risk lies and what should be prioritized, and finally developing a strategy for both short-term and long-term improvements to the organization's cloud security posture. Engaging service providers for this assessment can provide several benefits over an internal approach. First, service providers often have deep industry and compliance expertise and can help organizations benchmark against best practice standards and regulations in the context of the specific business needs of the customer (such as cost constraints, risk appetite, geographic considerations, etc.). Similarly, service providers with these capabilities are in a good position to prioritize remediation tasks and help organizations understand where on the roadmap specific improvements should fall. Additionally, because of the number of stakeholders involved across the organization, service providers offer not only a playbook for working across these different consistencies, but also a neutral voice during the process to build consensus.

### Consulting and Integration

After the assessment is complete and a strategic framework has been designed, implementing the resulting recommendations poses the next hurdle and another area where service providers can assist in bridging the gap. To start, a cloud assessment would likely include a recommendation to incorporate security into the DevOps process if it has not already occurred. However, this implementation can be difficult, and as discussed previously often includes a cultural shift as well. Leveraging a third party to provide guidance and best practices can ease the transition. The first step is translating how the new controls and processes recommended to fill the gaps identified in the assessment phase can be seamlessly integrated into a DevOps methodology without significantly changing existing workflows or development tools.

A key to linking the addition of new, cloud-native security tools with a DevSecOps process is automation. Choosing security solutions that plug into existing DevOps tools such as Chef or Puppet and automatically apply security controls without the developers having to modify their process can serve to ease the transition to a DevSecOps model by ensuring developers are still able to work at the speed to which they are accustomed.

### Outsourcing

Finally, it may be necessary to outsource certain aspects of a cloud security program to reach the required scale across hybrid environments, or close gaps based on resource constraints. The cybersecurity skills shortage is well documented and particularly acute relative to cloud. As new processes, tools, and frameworks are introduced to support cloud security, it can be more time- and cost-effective to shift to a managed security services model. The previously described assessment and strategy or consulting and integration services may be outsourced, as may core threat prevention, identity, and data security solutions. Further, service providers offering managed services across the following categories can significantly accelerate the improvement of an organization's cloud security posture:

- Visibility and management – Especially across hybrid environments, centralizing visibility across all facets of cloud and normalizing management processes across both third-party and cloud service provider security tools can be challenging. Service providers can serve as an aggregation point for these tasks.

- Compliance monitoring and reporting – In the same vein, managing compliance with the myriad of industry-specific and cross-domain regulations can become untenable as assets and data become distributed across multiple cloud platforms and providers. Though organizations will always have ultimate responsibility for their compliance, engaging service providers to develop a consistent reporting structure across different platforms and environments can help to ease the burden.

- Vulnerability assessment and offensive testing – Because cloud servicers are so dynamic, the threat and exploit landscape is constantly changing. This arguably makes vulnerability assessment and penetration testing even more

important for cloud environments. The differences in the shared security model across the different types of cloud platforms make this a much more complex process, addressing more stakeholders, with varying responsibilities. Centralizing and outsourcing these processes can improve the speed with which vulnerabilities are patched and the organization's security posture is improved.

- Security operations and incident response – Finally, incident response and security operations continue to be a key pain point for organizations across the board, in large part due to the cybersecurity skills shortage. Effectively integrating event monitoring and threat intelligence with forensics and incident response capabilities requires a significant investment in both tools and personnel. This says nothing of the complexity of translating these capabilities to cloud environments. Utilizing a service provider to augment existing SOC functionality, or fully outsource SOC responsibilities, while expensive, can provide cost savings in the long term, especially when compared to the potential costs of not adequately responding to a security breach.

## The Bigger Truth

There are many benefits associated with migrating to the cloud, including improved performance, scalability, velocity, and financial flexibility, all of which are vital for digital transformation strategies to be successful. Too often, cybersecurity is seen as an impediment to these initiatives and not integrated into the broader cloud strategy of the organization. The goal of all cybersecurity teams should be to enable the organization on its digital transformation journey through secure cloud adoption. However, accomplishing this requires the incorporation of new skills, tools and processes.

Designing, implementing, and managing an end-to-end cloud security program that addresses all the core cybersecurity tenets including infrastructure, identity, and data while also incorporating tools and processes that not only align with, but seamlessly integrate into DevOps methodologies is a complex task for even the most mature organization. As such, engaging service providers to develop an overarching cloud security strategy, assist with the implementation of new processes and tools, and in some cases outsource the management of day-to-day cloud security tasks should be considered by any organization seeking to close the cloud cybersecurity skills gap.

**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