White Paper

Leveraging the Agility of DevOps Processes to Secure Hybrid Clouds

By Doug Cahill, ESG Senior Analyst

April 2018

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

Contents

Executive Summary

Fully leveraging technology to drive business has become paramount, with many organizations using an array of platform- and infrastructure-as-a-service (IaaS) cloud services to expedite building and delivering new applications, services, and entire lines of business. The broad adoption of cloud services and the new methodologies centered on automation punctuate the agility provided by modern technology. While fundamental changes in the computing landscape challenge established cybersecurity practices, they also represent notable opportunities for compelling improvements.

The perspective that code is infrastructure captures one of the foundational elements of how organizations now deliver, manage, and secure infrastructure. That is, the shift is beyond a technological one; agile software development and the continuous integration and continuous delivery (CI/CD) methodology of the DevOps movement embody the need for speed to gain competitive advantage. Today's IT business model, rooted in enabling business agility, demands that cybersecurity keep pace with the velocity of the cloud.

Today's IT business model, rooted in enabling business agility, demands that cybersecurity keep pace with the velocity of the cloud.

Securing cloud infrastructure requires not only understanding what is technically different about today's data center but also fully embracing and exploiting the benefits of DevOps as a means to codify cybersecurity practices and controls. In fact, according to a recent research study conducted by ESG, and discussed in this paper, 30% of research participants said that one of their highest priorities is to build a cloud security strategy that can be used across heterogeneous public and private clouds, making it the most-cited response.[1]

The Multiple Dimensions of Hybrid Clouds

Hybrid clouds are more than those comprised of an on-premises and public cloud footprint; they are a combination of disparate infrastructures with physical and amorphous perimeters. The use of services from multiple cloud service providers (CSPs) and a heterogeneous mix of server workload types has led to the multiple dimensionality of the modern data center.

Multi-clouds

The subscription to and consumption of services from multiple providers is consistent with how IT leaders and decision makers have historically procured offerings from a varied set of vendors in other areas of technology. While a market leader will emerge, other followers quickly enter the mix, creating not only more competition, but diversified IT environments. According to research conducted by ESG, 81% of organizations who consume infrastructure-as-a-service (IaaS) use such services from more than one cloud service provider (CSP). This research also reveals that the top drivers behind multi-cloud adoption include:

- The influence of large application vendors on cloud services and application selection.
- A best fit approach of aligning a cloud platform with the needs of a particular application.
- A desire to avoid vendor lock-in by not being dependent on a single CSP.
- Decentralized IT, in which different business groups will select different cloud platforms.[2]

[1] Source: ESG Research, *Trends in Hybrid Cloud Security: Minding the Gap*, November 2017. All ESG research references and charts in this white paper have been taken from this research survey, unless otherwise noted.
[2] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

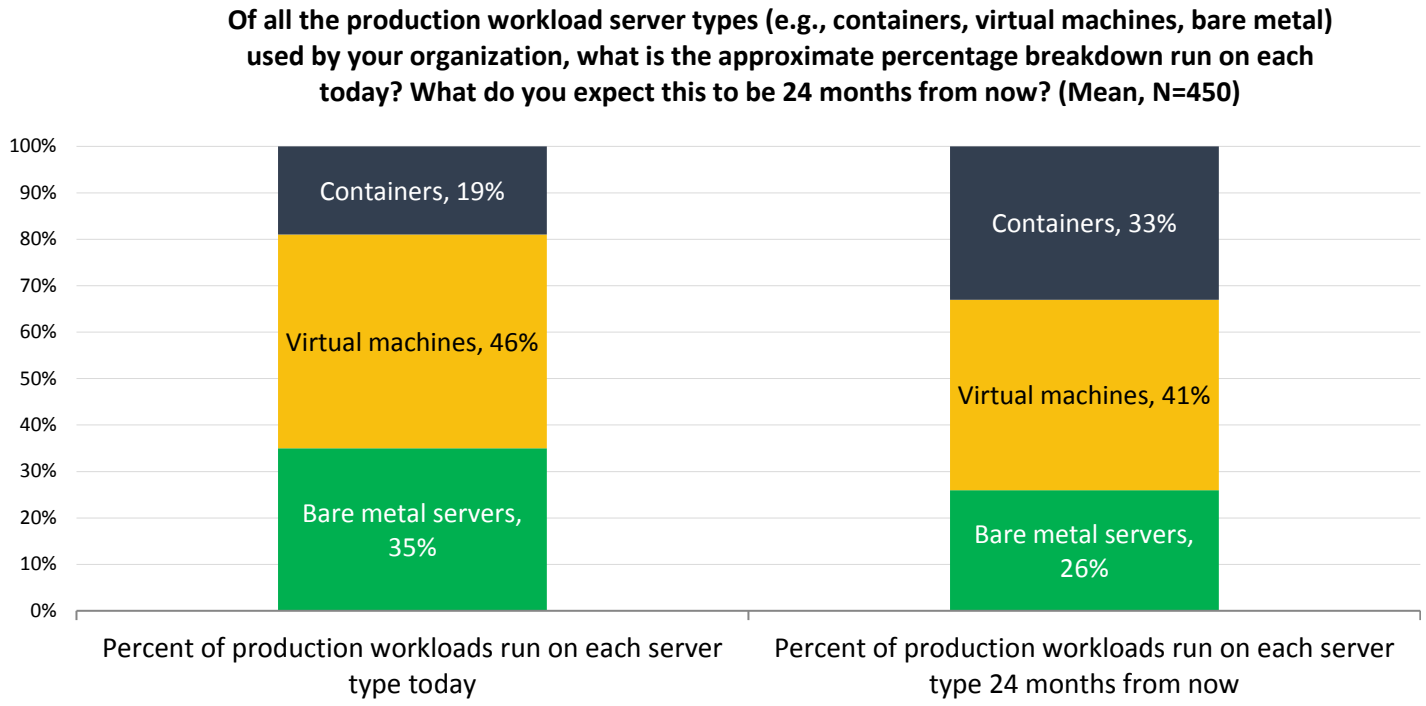
Heterogeneous Server Workload Types

The server form factors, locations, and operating systems employed across hybrid cloud environments are creating a highly heterogeneous mix of workloads. To leverage the agility of IaaS platforms, many organizations are shifting their server workloads to a public infrastructure, as highlighted by the 55% of participants in ESG research that indicated 31% or more of their production workloads will be cloud-resident in the next 24 months, up from 31% who have the same percentage of production workloads in a public cloud today.

At the same time, applications based on a micro-services architecture are leading to the deployment of containerized applications to production in customer-managed environments as well as on public cloud platforms. Containers are not delivery vehicles for new applications only; according to the ESG research, 73% of organizations are using or will use containers for "legacy" applications as they refactor such applications in distributed, micro-services implementations.

While this evolution to new architectures marginalizes old application stacks over time, virtual machine and client-server-based applications will remain meaningful elements of the heterogeneous mix of workload types (see Figure 1).

Figure 1. The Heterogeneous Mix of Server Workload Types



Source: Enterprise Strategy Group

Business Agility and Today's Speed of IT

This shift to multi-clouds and micro-services is driven by the business imperative to leverage modern technology to enable companies to pursue new opportunities. In fact, many established industries have been disrupted by new brands leveraging the agility of the cloud to offer new experiences to customers, creating an imperative to understand and embrace these dynamics.

The Decentralization of IT

The decentralization of IT introduced with the personal computer and accelerated by knowledge worker mobility is now manifested by the pervasiveness of shadow IT—the use of IT systems without explicit organizational approval—a clear

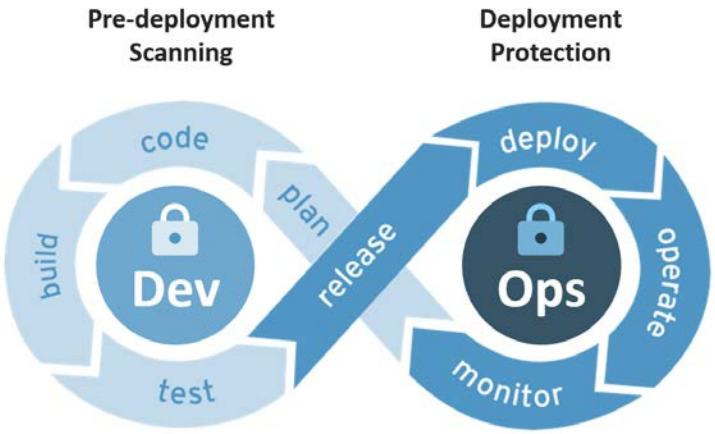
indicator that IT initiatives are being driven by lines of business. Autonomous business units leverage not only the self-service nature of SaaS applications, but increasingly have their own application development teams, a notable contrast to the traditional centralized IT model in which a business unit defined requirements for a new application and waited for the IT team to evaluate, procure, and provision the full application stack.

However, while cloud services have enabled shadow IT, decentralization has created cybersecurity concerns. Participants in the ESG research indicated that employees who sign up for cloud applications without approval and governance from IT, and business units that conduct application development and deployment on public cloud infrastructure outside of the purview of IT are two of their biggest hybrid cloud security challenges. The new reality of distributed IT means that cybersecurity runs the risk of being left behind by clinging to approaches not aligned with the technologies and methodologies of modern application development and delivery.

The Agile and DevOps Symbiosis

Sometimes left out of the conversation about DevOps is the central role that agile software development plays in today's IT methodologies and the symbiotic relationship between DevOps and agile. In a code-as-infrastructure context, agile user stories, sprints, and scrums are the planning constructs that map out not just features and functions but also how code is continuously integrated and continuously delivered (CI/CD) from dev and test environments into production (see Figure 2).

Figure 2. Embedding Security Into CI/CD Methodology of DevOps



Source: Trend Micro

It is worth noting that DevOps is often misunderstood and should be viewed first and foremost as a cultural shift to break down organizational boundaries between development and operations teams. The automated continuous integration and continuous delivery practices of DevOps in turn support the iterative nature of agile. These benefits are driving DevOps adoptions, with 36% of organizations, according to ESG research, now employing DevOps extensively or in a limited fashion, and another 54% either planning to employ DevOps in the next 12-24 months or interested in and investigating doing so.

Yet, herein lie opportunities to leverage DevOps to improve an organization's security posture.

Extending the DevOps cultural shift and applying CI/CD automation to include security is a work-in-progress. For some cybersecurity professionals up to the CISO level, the speed of DevOps can be disconcerting, with 20% of ESG respondents

indicating that keeping up with the rapid pace of change via DevOps automation makes it challenging to maintain security controls. Yet, herein lie opportunities to leverage DevOps to improve an organization's security posture.

One of the central concepts in the CI/CD delivery of code is that it is done across the pre-deployment environments of development and test, as well as in production runtime environments. As such, agile user stories should reflect the requirement to apply security measures and controls in pre-deployment environments to ready workloads for deployment to production.

Retooling Cybersecurity to Keep Pace with Hybrid Cloud Realities

These realities of decentralization and automation necessitate an evolved approach to securing hybrid clouds, one that re-orientates the IT business model while retooling skills, processes, and technologies.

Leveraging DevSecOps

Just as DevOps is a cultural shift, so too is DevSecOps, one that starts with championing the inclusion of cybersecurity team members, processes, and controls in the agile planning and project management process. Scrum teams should appreciate not only the value of delivering more secure applications to production but also the efficiency of addressing software and configuration vulnerabilities in dev and test environments rather than having to reactively update production. ESG research reflects this sentiment, with 29% of participants citing the ability to improve their security posture via tight integration with the CI/CD tool chain as the primary reason their organizations employ or plan to employ DevSecOps, and 40% noting that they are currently evaluating security use cases that leverage their DevOps processes.

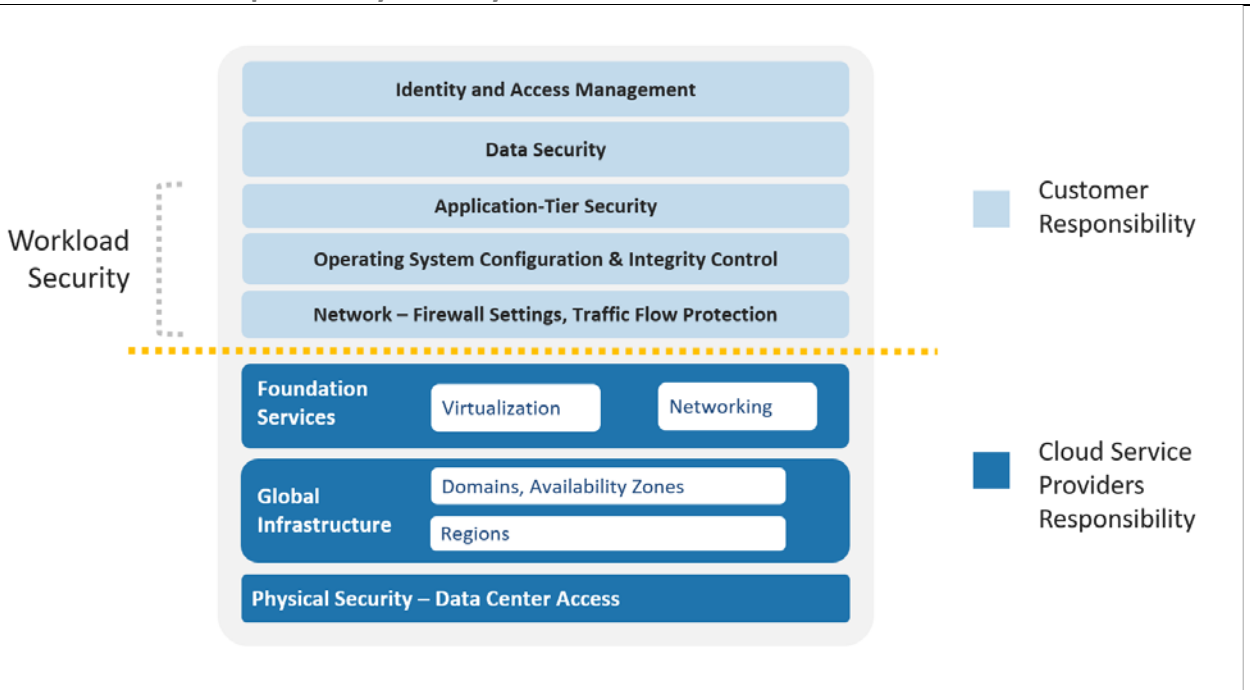
Because product owners author user stories and work collaboratively with development and operations leads to assign those stories for upcoming sprints, they are on point for prioritizing cybersecurity requirements. User stories should span dev, test, and production environments by defining the tasks required to automate secure software development, reducing the attack surface area via server hardening in test, and maintaining system integrity to prevent infections in production.

Understanding that security can also be automated via CI/CD should address any concerns that introducing security upstream will impede agility.

Employing a Workload-centric Model Across Hybrid Clouds

Physical network-based security controls such as firewalls, proxies, and intrusion detection and prevention appliances continue to play a critical role for securing the physical perimeter and customer-managed networks of hybrid cloud environments. However, because of the shared responsibility security model (see Figure 3), in which the CSP is responsible for physical network security, a hybrid cloud security plan needs to include a workload-centric strategy to secure an organization's public cloud footprint.

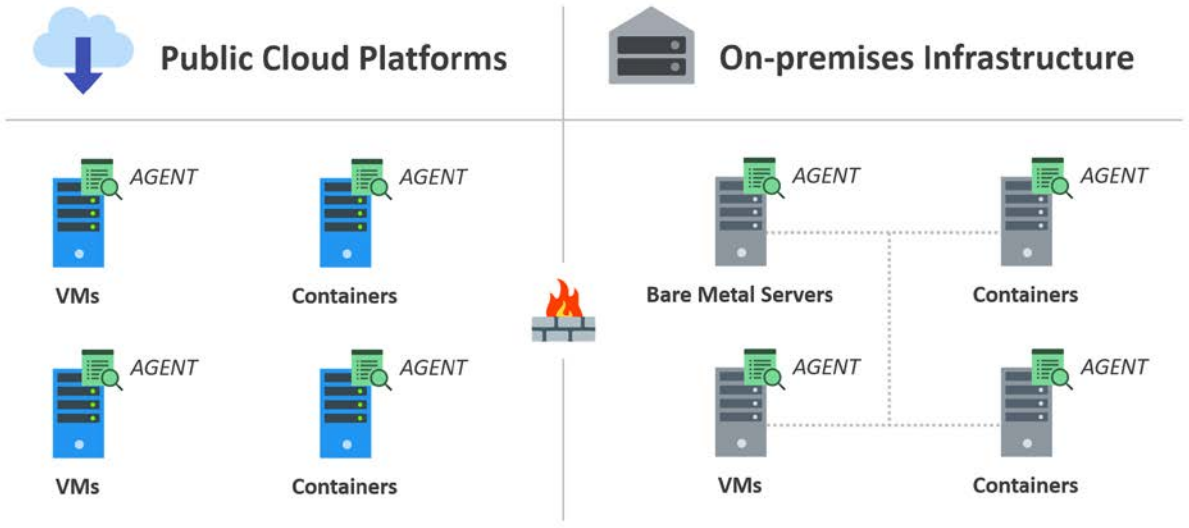
Figure 3. The Shared Responsibility Security Model for Infrastructure-as-a-service



Source: Enterprise Strategy Group

With the cloud service provider responsible for securing physical access to its data centers, its global infrastructure, and its virtualization and networking foundation services, customers are then responsible for securing the heterogeneous mix of server workloads across their hybrid cloud environment (see Figure 4).

Figure 4. The Workloads of Hybrid Clouds



Source: Enterprise Strategy Group

Examples of critical workload security controls that should be deployed in pre-deployment and production environments include:

- Vulnerability scanning and remediation to harden workloads before deployment to production.

- **Host-based firewalls** to limit communication via authorized ports and protocols.
- **Virtual patching** via host-based intrusion detection and prevention and web application firewalls to protect workloads against exploits.
- **System integrity controls** via application control and file integrity monitoring to assure only trusted software is allowed to execute and only authorized areas of file systems are accessed and changed.
- **Anti-malware** to detect and prevent known and unknown file and file-less malware by employing a comprehensive set of technologies including pre-execution predictive machine learning and runtime behavioral analysis.
- **Log inspection** of the audit trail of system activity including the record of who accessed sensitive data, a functional capability required to comply with industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS) designed to protect cardholder data.

The application of these controls and more can be automated via CI/CD tools such as Chef, Puppet, and Red Hat Ansible vis-à-vis support for workload tags, assuring that the right policy is applied based on workload role at the time of instantiation. IT and cybersecurity professionals should also be aware that server workload security solutions need to support the differences between on-premises environments as well as those between public cloud platforms. A workload-centric approach should also entail a policy lexicon and control plane to centrally manage assets deployed across disparate aspects of a hybrid cloud.

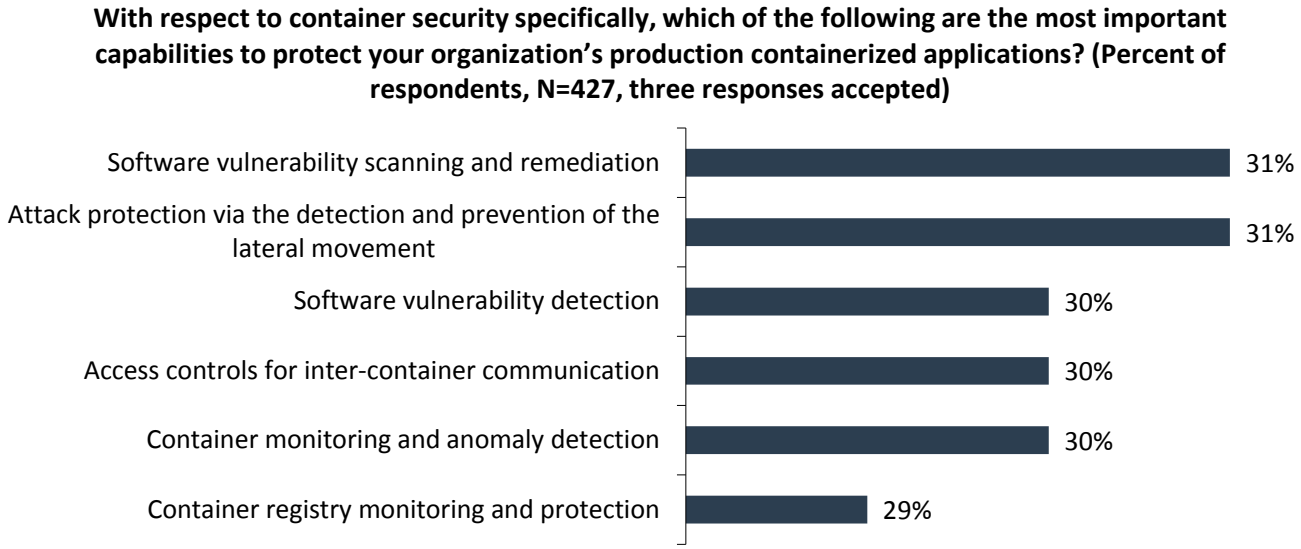
Spotlight: Application Containers

The rapid adoption of application containers requires extending a workload-centric security strategy to secure containers with the use of the aforementioned controls. However, a few notable differences in container environments require additional capabilities, including:

- **Image scanning** to assure registry-resident container images are trustworthy for deployment to production by virtue of being void of known vulnerabilities and of having hardened configurations. It is important to note that while many hosts of public registries perform image scanning, many organizations will deploy from a private registry, requiring them to also scan images for vulnerabilities.
- **Discovery** of containers, including those not based on a trusted image.

Just as DevSecOps should be employed to automate the application of security controls so too should DevSecOps automation be employed to secure containers across the build-ship-run continuum of the container image lifecycle. The capabilities deemed by ESG research participants to be most important to securing containers reflect an approach of securing containers in pre- and post-deployment environments (see Figure 4). For example, container registry monitoring and protection along with container hardening and software vulnerability scanning and remediation are best implemented pre-deployment while attack protection and access controls should be implemented in production environments.

Figure 5. Top Six Most Important Application Container Security Capabilities

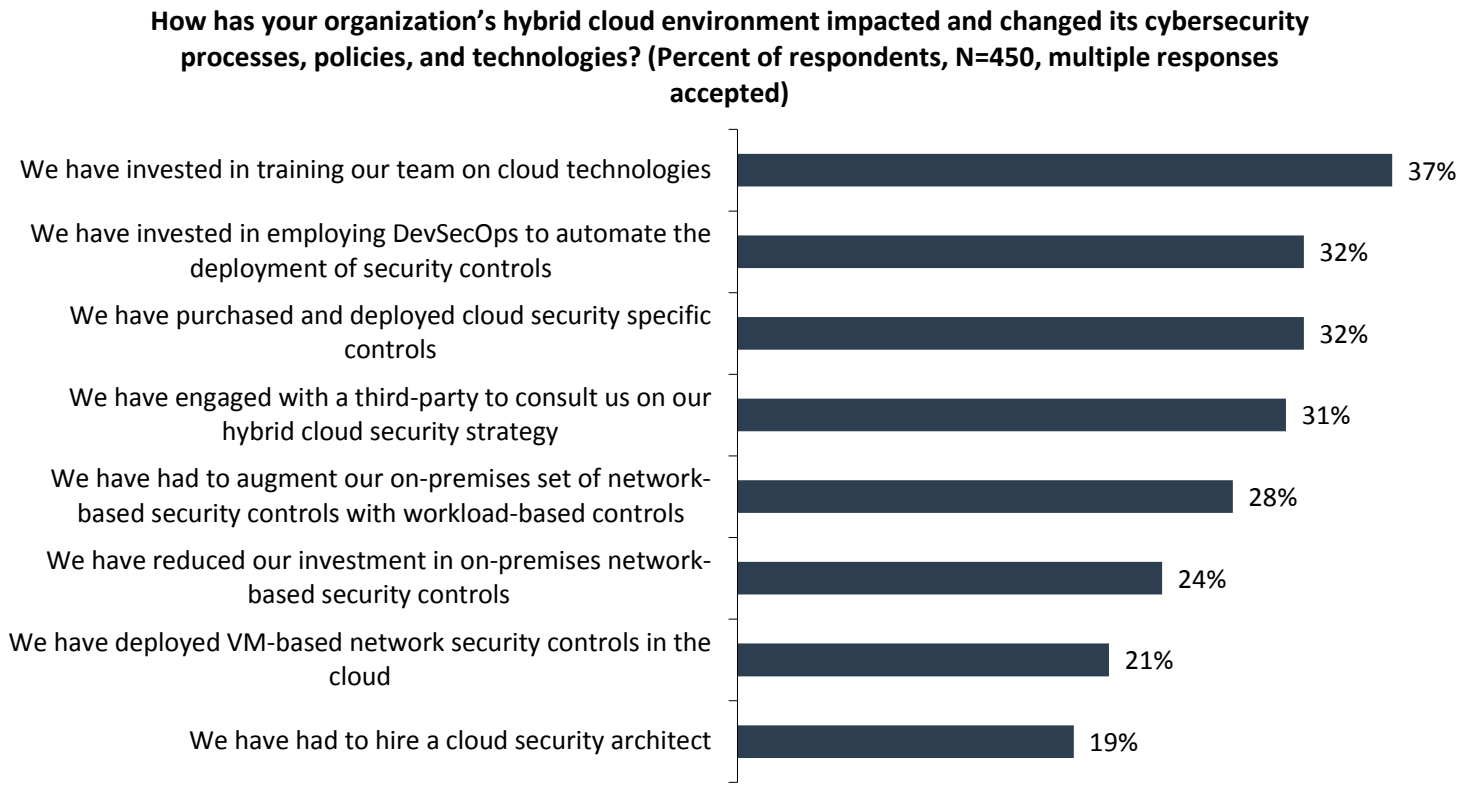


Source: Enterprise Strategy Group

The Requisite Investments in People, Processes, and Technologies

Amidst the ongoing problematic shortage of cybersecurity skills, many organizations understand the need to retool their skills and approaches. This level of self-awareness was conveyed in how ESG research participants stated their hybrid cloud environments have affected their cybersecurity processes, policies, and technologies (see Figure 6).

Figure 6. Impact of Hybrid Clouds on Cybersecurity Processes, Policies, and Technologies



Source: Enterprise Strategy Group

Spotlight: The Rise of the Cloud Security Architect

One of the cybersecurity roles that has risen in prominence to keep pace with the rate at which organizations are leveraging cloud services is that of the cloud security architect. These individuals are charged with filling the skills gap with respect to knowledge of both cloud technologies and CI/CD methodologies. As such, cloud security architects serve a critical role in defining and leading an organization's cloud security strategy and serving as a change agent by making the case for integrating security into DevOps CI/CD processes.

To bridge the gap that all too often exists between security and operations teams, cloud security architects are uniquely positioned to be an integral member of an organization's scrum team to define cybersecurity user stories for development, test, and production environments. By doing so, cloud security architects champion DevSecOps use cases that allow cybersecurity to move at the speed of DevOps. It's no wonder then that 68% of organizations surveyed by ESG indicate that they already have a cloud security architect or have recently created and filled this role.

> Cloud security architects champion DevSecOps use cases that allow cybersecurity to move at the speed of DevOps.

The Bigger Truth

The state of hybrid clouds reminds us that organizations do not immediately discard pre-existing infrastructure as they adopt and leverage new technologies, creating a hybrid perimeter comprised of physical demarcations and those that are fluid and temporal. Securing such environments requires a new approach that embraces the speed at which businesses move and cybersecurity solutions that allow for moving, over time, from a siloed approach to one of unification and consistency. Indeed, hybrid clouds bring changes to business models, methodologies, and technologies, the intersection of which represents an opportunity to efficiently improve an organization's cybersecurity posture while also enabling the speed of business.

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