Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

# Trends in Workload and Container Security

**Doug Cahill,** VP and Group Director

NOVEMBER - 2020

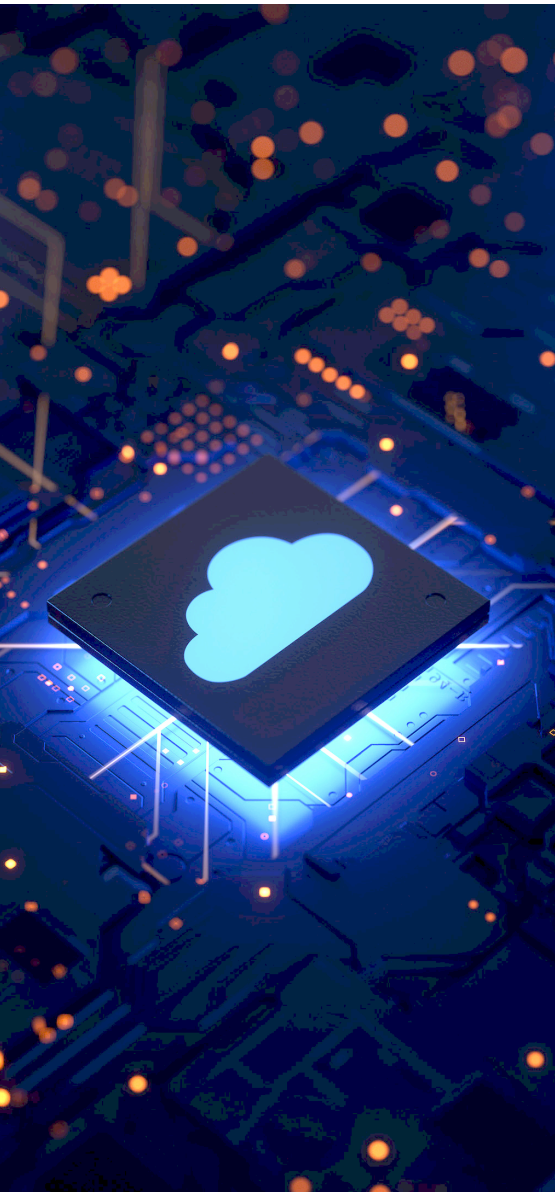
PREPARED BY ESG FOR

cisco SECURE

# CONTENTS









# Container Security Landscape

Fundamental changes to application architecture and the infrastructure platforms that host them is antiquating existing cybersecurity technologies and challenging traditional approaches to protecting business-critical applications. Indeed, the continuous integration and continuous delivery (CI/CD) processes of DevOps are as impactful a change to cybersecurity programs as the changes to the applications and infrastructure these methodologies manage.

Cloud security is now a discipline that transcends physical locations by focusing on securing cloud-native applications delivered from both public and private clouds. Microservices architectures comprising application containers will coexist with legacy technologies, contributing to a heterogenous application stack. While many recognize the growing importance of containers relative to these other vital application platforms, confidence levels in the ability to secure containerized workloads are lagging. Automating security via integration with the CI/CD toolchain (DevSecOps) is gaining interest, but specificity of use cases by stage is required to operationalize this new approach.

# Research Methodology

To gather data for this report, ESG conducted comprehensive online surveys[1] of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America (United States and Canada). To qualify for these surveys, respondents were required to be IT, cybersecurity, or application development professionals involved with securing application development tools and processes. All respondents were provided an incentive to complete surveys in the form of cash awards and/or cash equivalents.

[1]Sources: ESG Research: *Trends in Modern Application Environments, December 2019; Leveraging DevSecOps to Secure Cloud-native Applications, March 2020; Modern Application Development Security, August 2020.*



Back to Contents

# Key Research Findings

**The need for agility is driving the development of container-based applications.** No longer relegated to tertiary use cases, internally developed cloud-native applications deployed on IaaS/PaaS platforms serve as the backbone of front, middle, and back office operations. Application containers support the level of agility businesses require to develop and deliver business-critical cloud-native applications.

**As server workloads shift to public clouds, container-based applications are being deployed across hybrid, multi-clouds.** The portability of application containers affords deployment flexibility. As such, the tiers of cloud-native applications that utilize containers will be deployed across disparate environments based on a best fit approach.

**Concerns related to securing the application lifecycle include a focus on detecting misconfigured server and container workloads.** Cloud environments are actively under attack as evidenced by the three-quarters of respondents who reported a cloud-related cybersecurity incident or attack over the last 12 months. The prevalence of shadow IT, the improper use of sanctioned cloud applications, and sharing data with third parties create a visibility gap, resulting in many organizations being unsure of whether they have lost cloud-resident data.

**Top container security use cases start pre-deployment and follow into runtime.** Cloud-native applications that employ containers are on a rinse-and-repeat cycle of continuous integration and continuous delivery (CI/CD). This continuous loop requires that container security measures be applied from pre-deployment through runtime.

**Securing the continuous integration and continuous delivery (CI/CD) of containers requires integration into DevOps processes.** DevOps practices are broadly adopted by project teams developing cloud-native applications and delivering them into production. Securing these applications requires the integration of container security controls into DevOps processes to automate pre-deployment and runtime container security use cases.



Back to Contents

# Container Adoption

The need for agility is driving the development of container-based applications.

# Amid Time-to-market Pressures, Containers Are Providing Agility and Gaining Traction

The application economy creates pressure to write code faster and deploy to production faster. This has led to an increased adoption of microservices, with containers front and center. And they're delivering on the promise of enabling greater agility.

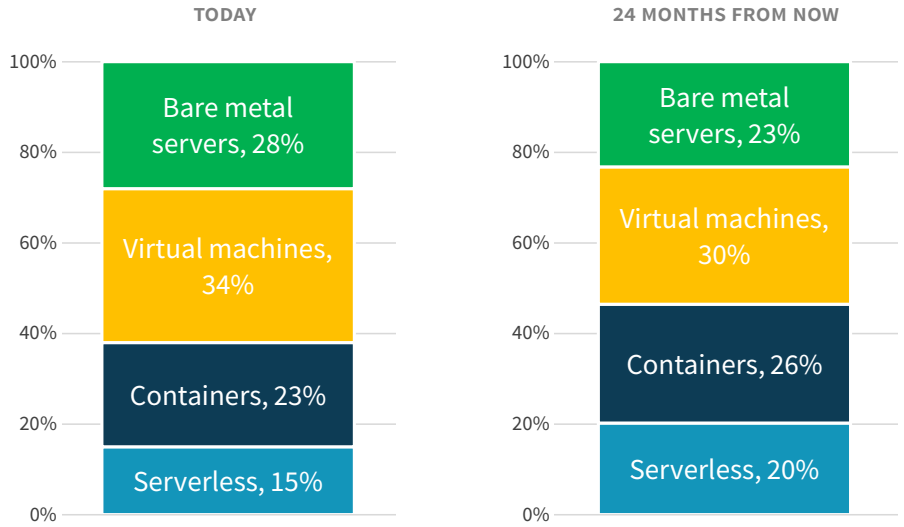
**86%**
report being under pressure to launch new apps and services.

**79%**
have run containers in production for over a year.

**37%**
Organizations running containers in production are 3x likelier to report being ahead of app deployment schedules (37% versus 14%).

Containers and serverless are marginally cannibalizing VMs and bare metal servers and thus will coexist with these server types as the underpinnings of both cloud-native apps and legacy apps.

» **Percentage breakdown of production apps running on each server type.**






Back to Contents

# Container Deployments

As server workloads shift to public clouds, container-based applications are being deployed across hybrid, multi-clouds.

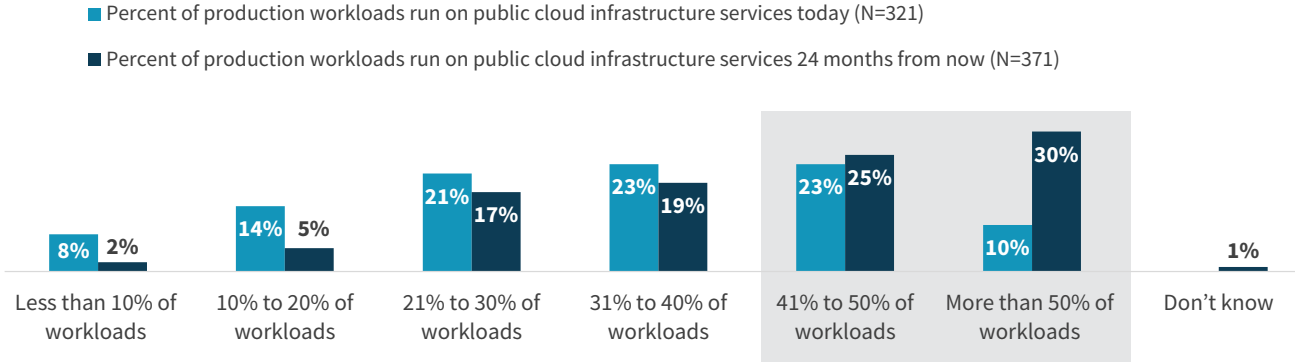
# Production Server Workloads Are Shifting to Public Cloud Platforms

Consistent with a general shift toward the consumption of public cloud computing services, production workloads have started to shift to public cloud platforms and will continue to do so.

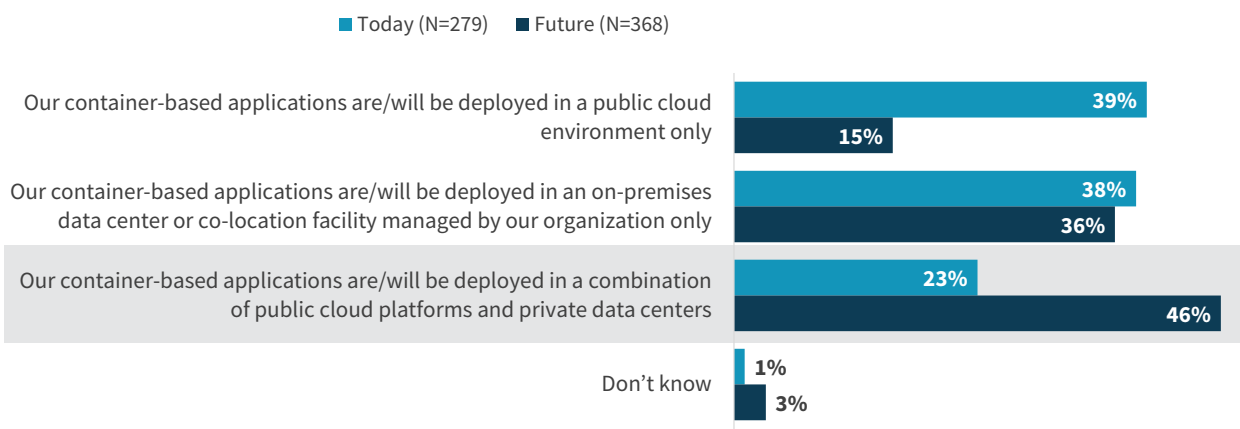
Organizations have yet to decide where cloud-native apps will be deployed, likely embracing portability as a means to such optionality. As such, and more generally, cloud-native apps will be deployed across hybrid clouds. The early stage of on-premises "data center-as-a-server IaaS stacks" (e.g., AWS Outposts, Google Anthos, and MSFT Azure Stack) muddy these waters as these implementations are evaluated.



## » Server workloads are shifting to public clouds




## » …but containers will be deployed across hybrid, multi-clouds.




Back to Contents

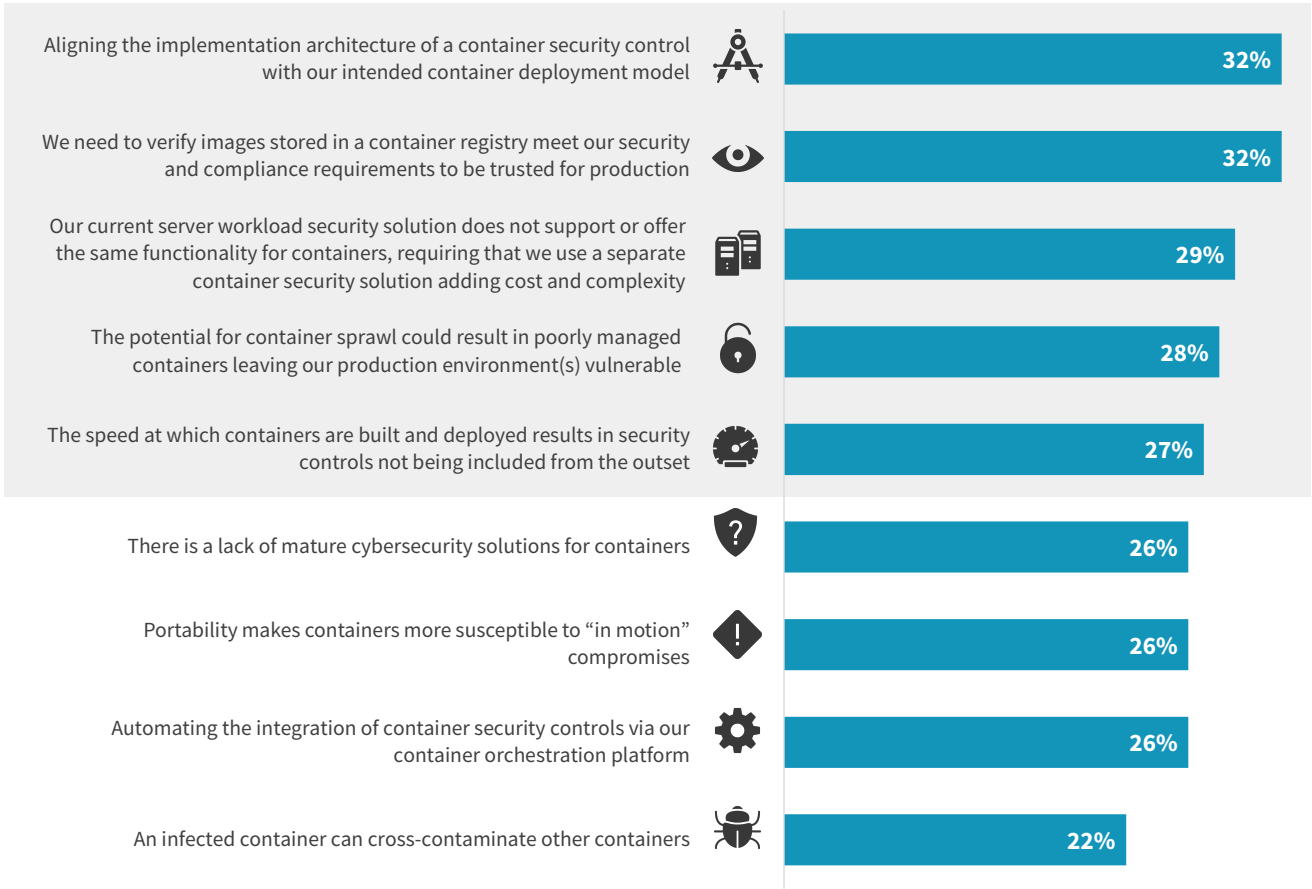
# Container Security Concerns

Concerns related to securing the application lifecycle include a focus on detecting misconfigured server and container workloads.

# Container Security Concerns Span CI/CD Stages of an Application's Lifecycle

In addition to a focus on issues associated with securing the container lifecycle, alignment of deployment model and implementation as well as tool maturity are of concern. Architectural implementations should support public cloud deployments.

» **Top security concerns for containers.**



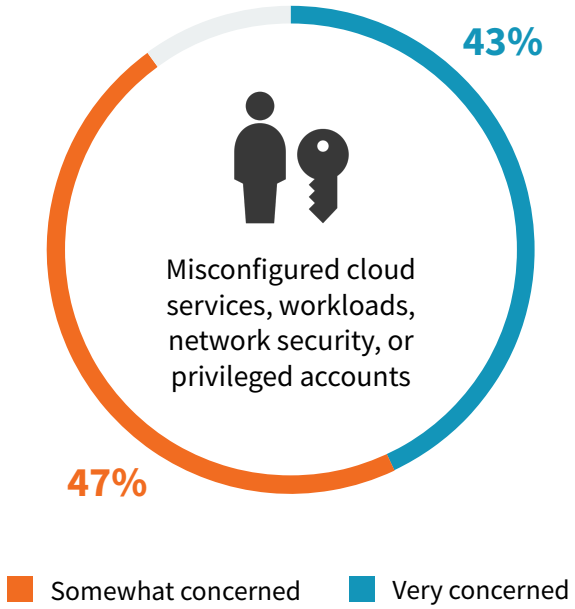


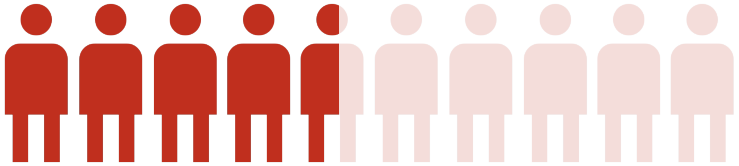

Back to Contents

# Workload Configurations Are the Top Public Cloud Visibility Priority

The lack of access to the network perimeter puts a focus on workload and container hardening and auditing. Why? Misconfigurations are often exploited as an attack vector, representing a need to gain greater visibility into workloads that have gone adrift from secure configurations such as those based on an industry regulation or industry benchmark.

» **Concern level over threats to cloud-native applications.**



***47% of organizations cite identifying workload configurations that are out of compliance*** *as one of their top priorities for improving public cloud security visibility.*



Back to Contents

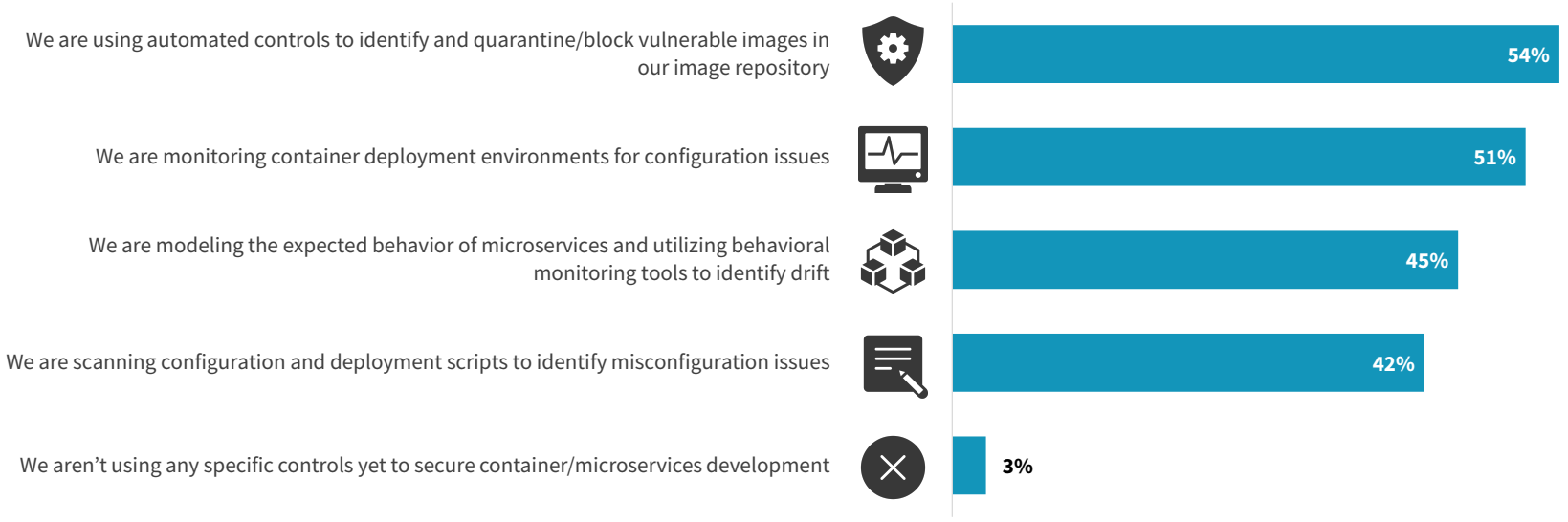
# Container Security Use Cases

Top container security use cases start pre-deployment and follow into runtime.

# Container Security Use Cases Span the Application Lifecyle

Container security often starts pre-deployment by scanning registry-resident container images for both software and configuration vulnerabilities to ensure that containers deployed into production are hardened. Once in production, in addition to the use of micro-segmentation to secure the east-west traffic between containers, monitoring runtime behavior serves to detect drift from a known-good configuration and for anomalous activity that could be indicative of an exploit.

» **Controls organizations have in place to secure container/microservices development.**



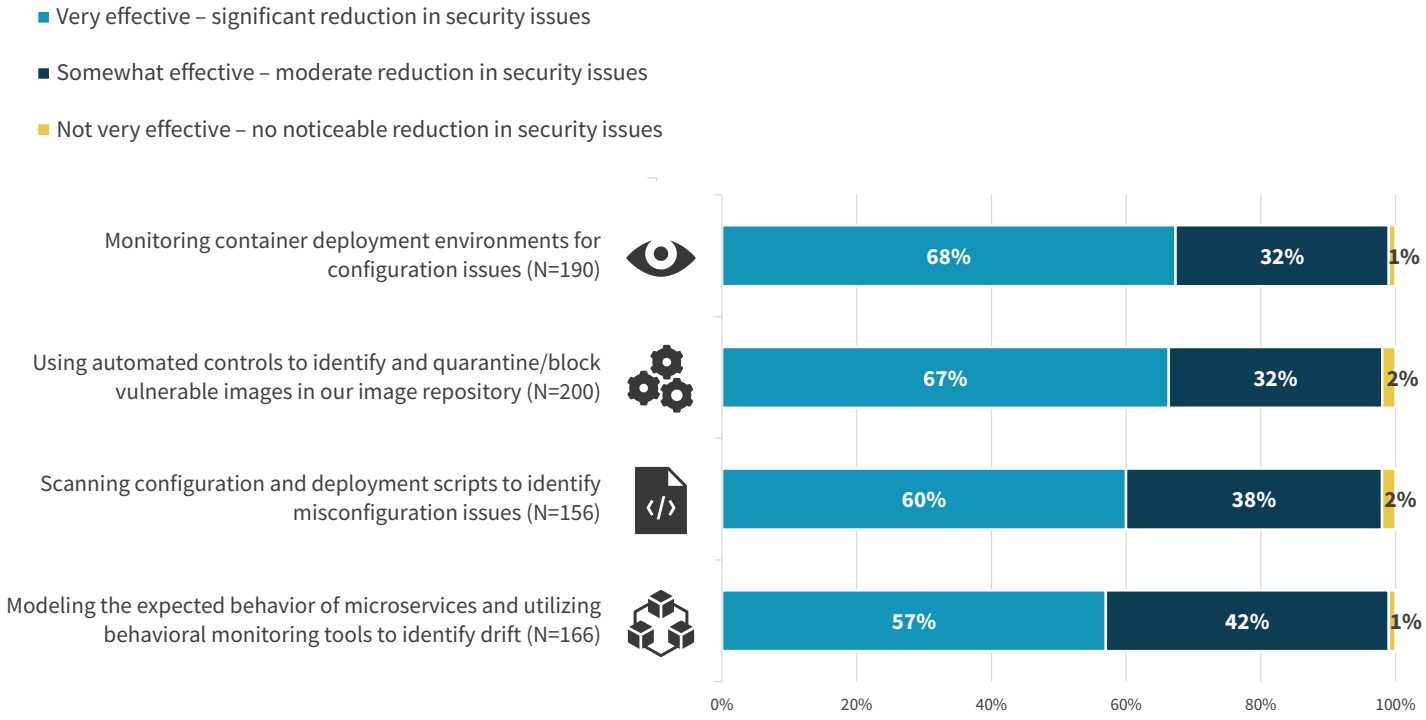



Back to Contents

# Most Feel Confident in the Efficacy of Container Security Tools

The controls employed to implement the top use cases are largely viewed as effective. This assessment of efficacy is rooted in metrics centered on a reduction of vulnerabilities in production environments.

» **Effectiveness of security controls in use for securing containers and microservices.**






Back to Contents

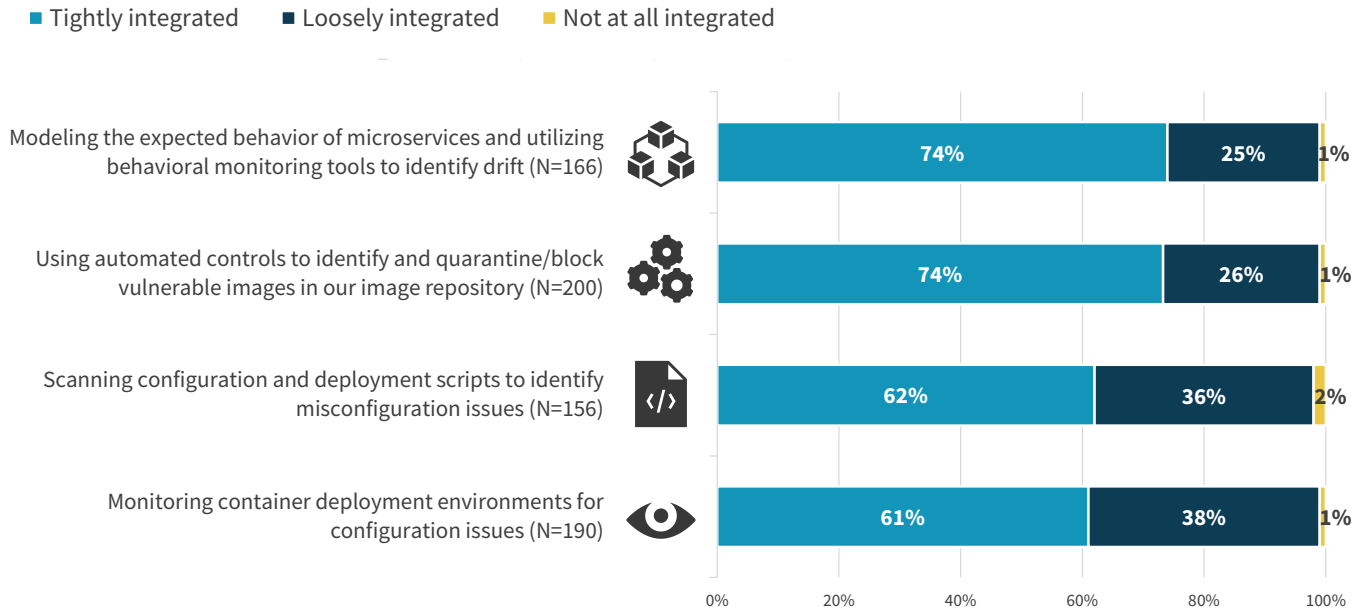
# The Role of DevSecOps

Securing the continuous integration and continuous delivery (CI/CD) of containers requires integration into DevOps processes.

# Most Have Tightly Integrated Security Controls into the DevOps Toolchain

The implementation of container security controls to enable the top container security use cases is predicated on tight integration with the continuous integration and continuous delivery (CI/CD) processes of DevOps. These DevSecOps use cases automate the introduction of these container security checks, thus assuring trusted images are deployed to runtime, and they are monitored for deviations once in production.

**» Level of integration between container security controls and DevOps processes.**



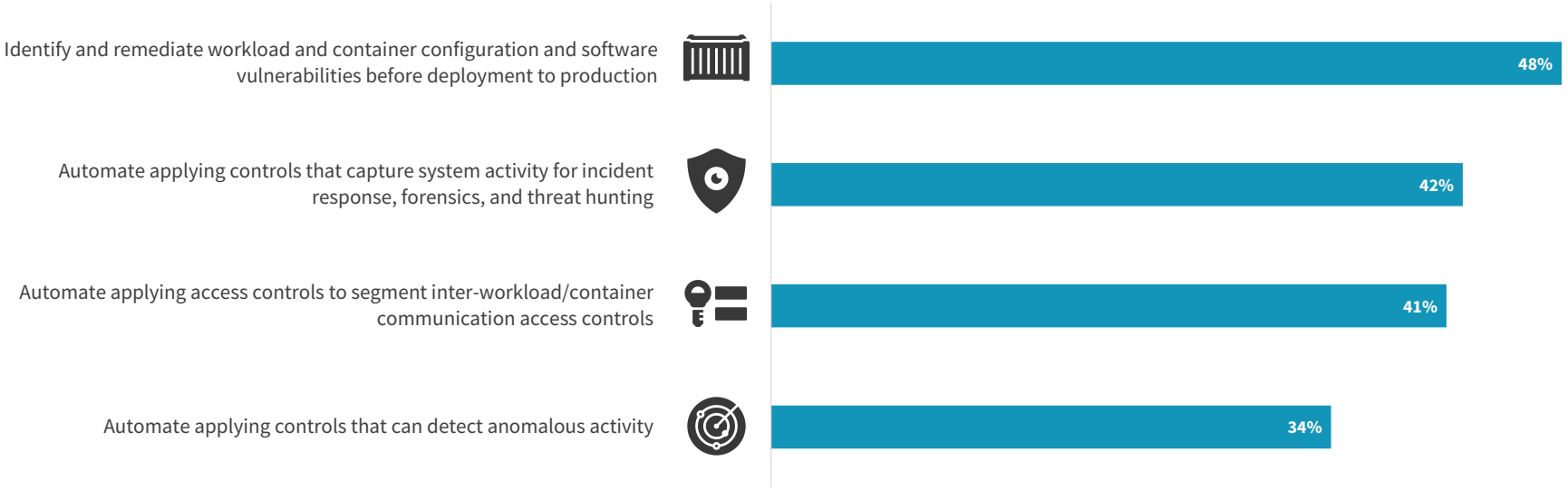



Back to Contents

# Automated Micro-segmentation is a Top DevSecOps Use Case

CI/CD integrations enable automation of shift-left hardening and shift-right runtime threat mitigation; either are a solid starting point. Of note is the foundational role micro-segmentation serves in protecting cloud-native applications by preventing the lateral movement of threats between containers.

**» How security practices are being automated via integration with DevOps processes.**






Back to Contents

## About ESG

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



Back to Contents