RESEARCH HIGHLIGHTS

Leveraging DevSecOps to Secure Cloud-native Applications

Doug Cahill,
Senior Analyst and Group Practice Director, Cybersecurity
CONTENTS

Research Objectives 3

Key Research Findings 4

Cloud-native applications are—and will continue to be—composed of heterogenous microservices deployed across hybrid clouds. 5

Cloud-native applications further complicate the ability to secure hybrid and multi-cloud environments. 8

Automating security via CI/CD integration—i.e., DevSecOps—is becoming the standard approach for securing cloud-native applications and is now a top product requirement. 11

Businesses are shifting from product and organizational silos to an integrated and unified approach, with increased involvement of the cybersecurity team resulting in multiple influencers and buyers. 14

To enable a unified approach, buyers require solutions that secure the build-ship-run lifecycle and the entire technology stack, independent of deployment locality. 17

Research Methodology 20

Respondent Demographics 20
Research Objectives

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

In order to get more insight into these trends, ESG surveyed 371 IT and cybersecurity professionals at organizations in North America (U.S. and Canada) responsible for evaluating, purchasing, and managing cloud security technology products and services. These organizations are mature cloud users in terms of public cloud services and/or containers. This study sought to:

- Examine the current and future composition of cloud-native applications.
- Gain insight into the challenges associated with securing cloud-native applications.
- Understand the people and processes involved in and employed to secure cloud-native applications.
- Gauge the functional requirements, priorities, and spending intentions for securing cloud-native applications.

Survey participants represented a wide range of industries including manufacturing, financial services, health care, communications and media, retail, government, and business services. For more details, please see the Research Methodology and Respondent Demographics sections of this report.
Key Research Findings

1. **Cloud-native applications are composed of heterogeneous microservices deployed across hybrid clouds.** Consistent with a general shift toward the consumption of technology as a service (XaaS), production workloads will continue to shift to public cloud platforms. While the mix of server types for the typical organization is skewed toward VMs and bare metal today, this is expected to shift noticeably in the next 24 months, with containers and serverless platforms supporting, on average, 46% of production applications. However, when it comes to supporting cloud-native applications specifically, there is no clear predominant technology platform preference at this point.

2. **Cloud-native applications further complicate the ability to secure hybrid and multi-cloud environments.** The heterogenous mix of server workload types, as well as the composition of cloud-native applications and increasing use of multiple public cloud platforms, is leading to a more complex environment, making maintaining consistency across hybrid clouds problematic. Due to a perception that existing security controls do not support cloud-native applications, many organizations have turned to a series of point tools managed by separate teams, which only exacerbates the aforementioned complexity problem.

3. **Automating security via CI/CD integration is becoming the standard approach for securing cloud-native applications and is now a top product requirement.** More than two-thirds of respondents expect that, within two years, their organization will secure more than half of its production cloud-native applications via DevSecOps practices, up from 42% today. The focus on DevSecOps automation influences product decisions, with DevOps integration being the top business driver influencing product selection.

4. **Businesses are shifting from product and organizational silos to an integrated and unified approach, with increased involvement of the cybersecurity team resulting in multiple influencers and buyers.** While a majority of organizations involve their cybersecurity team in the process of securing cloud-native applications before they push to production, too many wait to prioritize cybersecurity. Additionally, as cybersecurity teams develop cloud security skills, and the criticality of cloud-native applications increases, more cloud-native projects will involve a member of the cybersecurity team.

5. **To enable a unified approach, buyers require solutions that secure the build-ship-run lifecycle and the entire technology stack, independent of deployment locality.** Half of respondents expect their organization will consolidate controls by leveraging suites and platforms procured from a smaller set of vendors or even a single vendor. The most important attributes of products used to secure cloud-native apps include a rich set of pre-deployment capabilities, runtime capabilities, and support across a mix of server workload types, with flexible deployment options.
Cloud-native applications are and will continue to be composed of heterogeneous microservices deployed across hybrid clouds.
Production workloads are shifting to public cloud platforms, and organizations are quickly adopting serverless functions.

Consistent with a general shift toward the consumption of as a service (XaaS), production workloads will continue to shift to public cloud platforms. Indeed, the percentage of organizations reporting that more than 40% of their production applications run on public cloud infrastructure services is expected to increase from 33% today to 55% in 24 months.

Given this affinity for and commitment to public cloud infrastructure, it follows that there is already an appreciable use of serverless functions, especially in the enterprise, with many evaluating or planning to use serverless functions. Specifically, more than half of respondents indicate that their organization's software developers are already using serverless functions to some extent, with another 44% either evaluating or planning to start using serverless within the next two years. Those who are planning or evaluating will need to understand the associated threat model and means of mitigating risks.
Production server workloads including cloud-native applications are, and will be, a heterogenous mix.

Containers and serverless are marginally cannibalizing VMs and bare metal servers and are expected to coexist with these server types as the underpinnings of both cloud-native and legacy applications. However, while the server type mix for the typical organization is skewed toward VMs and bare metal today, this is expected to shift noticeably in the next 24 months, with containers and serverless platforms supporting, on average, 46% of production applications.

When it comes to supporting cloud-native applications specifically, there is no clear predominant technologies preference at this point. While the expected de facto structural composition of cloud-native applications is split between microservices and VMs, the plurality (35%) of respondents anticipate using a mix of these platforms.
Cloud-native applications further complicate the ability to secure hybrid and multi-cloud environments.
Consistency across hybrid clouds is the top cloud-native security challenge, which is exacerbated by specialized tools.

This heterogenous mix of server workload types, as well as the composition of cloud-native applications and increasing use of multiple public cloud platforms, is leading to a more complex environment, making maintaining consistency across hybrid clouds problematic. When it comes to challenges specific to securing cloud-native applications, the perceived need for specialized controls by the environment creates concerns around consistency (43%), as well as cost and complexity. This introduction of new technologies including serverless functions also creates a need for organizations to update their understanding of the threat model.

Due to a perception that existing security controls do not support cloud-native applications, many organizations have turned to a series of point tools managed by separate teams. However, this just exacerbates the complexity problem as 73% of respondents believe that their organization uses too many specialized products to properly secure cloud-native applications. 43% of respondents believe that maintaining security consistency across their own data center and public cloud environments where their cloud-native applications are deployed.

35% of respondents believe that the use of multiple cybersecurity controls increases cost and complexity.

35% of respondents believe that the lack of understanding of the threat types, and attack vectors and methods specific to their cloud-native applications.

73% of respondents believe that their organization uses too many specialized products to properly secure cloud-native applications.
Container security concerns span stages and deployment plans, while API vulnerabilities and hygiene top serverless security anxieties.

What specific concerns do organizations have when it comes to securing containers? In addition to a focus on issues associated with securing the container lifecycle, the alignment of deployment model and implementation, and tool maturity are common concerns. Architectural implementations of container security controls should support XaaS deployments.

- Aligning the implementation architecture of a container security control with our intended container deployment model (32%)
- We need to verify images stored in a container registry meet our security and compliance requirements to be trusted for production (32%)
- Our current server workload security solution does not support or offer the same functionality for containers, requiring that we use a separate container security solution adding cost and complexity (29%)
- The potential for container sprawl could result in poorly managed containers leaving our production environment(s) vulnerable (28%)
- The speed at which containers are built and deployed results in security controls not being included from the outset (27%)
- There is a lack of mature cybersecurity solutions for containers (26%)

When it comes to the use of serverless functions, nearly two-thirds (63%) cite API-related security concerns. In order to understand the serverless threat model, cybersecurity, developer, and DevOps teams would be well-served by better familiarizing themselves with different types of API vulnerabilities to identify and remediate them pre-deployment and during runtime.

- Use of unapproved APIs, 9%
- API vulnerabilities, 32%
- Exposure of secrets, 26%
- Escalated privileges, 11%
- API calls that result in the unencrypted transfer of data, 22%
Automating security via CI/CD integration—i.e., DevSecOps—is becoming the standard approach for securing cloud-native applications and is now a top product requirement.
DevSecOps is emerging as the predominant methodology for securing cloud-native applications.

Agile software development and DevOps are in lock step with security emerging as a common use case (i.e., DevSecOps), making DevOps integration a product requirement. Indeed, of the current DevOps practitioners, 84% have already incorporated security into these processes to some extent.

As DevOps teams establish repeatable and scalable DevSecOps integrations, more applications will be secured via such use cases. Specifically, 68% expect that within two years, their organization will secure more than half of their production cloud-native applications via DevSecOps practices, up from 42% today.

- Percent of production cloud-native applications secured via DevSecOps today (N=200)
- Percent of production cloud-native applications secured via DevSecOps 24 months from now (N=352)
DevSecOps use cases span pre-deployment and runtime stages, with aspirations of automation.

The focus on DevSecOps automation influences product decisions, with DevOps integration being the top business driver influencing product selection. CI/CD integrations enable automation of shif-left hardening and stay-right runtime/anti-threat mitigation; either is a starting point.

**Pre-deployment:**
- **48%** Identify and remediate workload and container configuration and software vulnerability before deployment to production
- **47%** Identify and remediate malware before deployment to production
- **46%** Inspection of the security posture of how APIs are being used
- **38%** Discover and inventory APIs in source code

**Runtime:**
- **42%** Automate applying controls to capture system activity for incident response, forensics, and threat hunting
- **41%** Automate applying access controls to segment inter-workload/container communication access controls
- **38%** Automate applying preventative runtime controls
- **34%** Automate applying controls which can detect anomalous activity

What is driving investments in third-party cloud-native application security controls? These use cases indicate a strong requirement for integration with build-time, orchestration, and workflow DevOps tools to enable both pre-deployment and runtime DevSecOps automation. Other key reasons for pursuing a third-party strategy include an increasing volume of cloud-resident assets, the domain-specific knowledge of these organizations, and the assurance of regulatory compliance requirements.

- **39%** Allows for automation of security controls via integration with existing DevOps tools
- **37%** Fears about security incidents you organization may experience in the future
- **36%** The sheer number of assets which are cloud-resident
- **32%** Domain-specific knowledge and depth of capabilities provided by third-party security vendor
- **32%** Assuring regulatory compliance/passing external audits
Businesses are shifting from product and organizational silos to an integrated and unified approach, with increased involvement of the cybersecurity team resulting in multiple influencers and buyers.
Too many wait to involve their cybersecurity team in their cloud-native application projects, but expect earlier collaboration going forward.

While a majority (52%) of organizations involve their cybersecurity team in the process of securing cloud-native applications before they push to production, too many organizations do so reactively—either after an incident, for funding, or due to concerns around cloud-resident sensitive data. For many, a lack of cloud skills or insufficient personnel on the cybersecurity team is likely a contributing factor.

As cybersecurity teams develop cloud security skills, and the criticality of cloud-native applications increases, more cloud-native projects will involve a member of the cybersecurity team. While only 39% of respondents report that members of their cybersecurity team are involved with more than half of cloud-native application projects today, that number is expected to jump to 78% in the next two years.

Too many wait to involve their cybersecurity team in their cloud-native application projects, but expect earlier collaboration going forward.
Most companies have or plan to merge the security teams to enable a unified approach.

Less than one in five organizations has a unified approach to securing cloud-native applications. However, consistent with how new technologies are typically embraced, 50% have started with the development of technical competencies associated with securing cloud-native applications across different groups and intend to merge these groups into a centralized team over time.
To enable a unified approach, buyers require solutions that secure the build-ship-run lifecycle and the entire technology stack, independent of deployment locality.
Organizations are split when it comes to the stage at which they introduce security controls to protect cloud-native applications. While more than one in five view the importance of pre-deployment and runtime security equally, 40% prioritize runtime controls, with the remaining 37% prioritizing a pre-deployment approach.

We view the importance of pre-deployment and runtime cloud-native application security controls equally, 22%

We prioritize runtime controls to assure our cloud-native applications are protected from threats in production, 40%

We prioritize pre-deployment controls to assure our cloud-native applications are hardened before deployment to production, 37%

Each CI/CD stage is important, and the most important security controls span stages.

However, when asked about the most important cloud-native application security controls, malware detection and prevention (32%) and vulnerability scanning (30%)—both of which are performed post deployment—are the two most commonly identified. As far as pre-deployment tools, more than one-quarter point to software vulnerability scanning of registry-resident container images.

**Pre-deployment:**
- 26% Software vulnerability scanning of registry-resident container images
- 25% API vulnerability management (in both)
- 23% Software vulnerability scanning in the build pipeline
- 20% Discovery, inventory, and auditing of APIs in mobile and cloud native apps (in both since discovery and runtime is pre and auditing is runtime)

**Runtime:**
- 32% Malware detection and prevention
- 30% Software vulnerability scanning of production containers and server workloads
- 26% System activity recording for incident response
- 26% Network segmentation and monitoring of inter-container and workload communication
- 25% API vulnerability management (in both)
- 23% Exploit detection and prevention
- 20% Discovery, inventory, and auditing of APIs in mobile and cloud native apps
- 20% Access controls and auditing of management actions

We prioritize runtime controls to assure our cloud-native applications are protected from threats in production, 40%
Consolidation of vendors and products is on the horizon, with deployment flexibility and coverage as most attractive attributes.

In terms of likely forward-looking cloud-native application security control selection strategies, half of respondents expect their organization will consolidate controls by leveraging suites and platforms procured from a smaller set of vendors or even a single vendor. As businesses look to leverage suites to reduce complexity and realize a unified cybersecurity posture across hybrid clouds, there is a preference for established product categories including CWPP and CSPM.

The most important attributes of products used to secure cloud-native apps include a rich set of pre-deployment capabilities, runtime capabilities, and support across a mix of server workload types, with flexible deployment options (SaaS and on-premises). Prevention, visibility, and integrations are all important, but buyers require that functionality across server types and want deployment options.
Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between May 22, 2019 and June 3, 2019. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally responsible for evaluating, purchasing, and managing cloud security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 371 IT and cybersecurity professionals.

Respondent Demographics

Respondents by Number of Employees

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,500 to 4,999</td>
<td>18%</td>
</tr>
<tr>
<td>5,000 to 9,999</td>
<td>18%</td>
</tr>
<tr>
<td>10,000 to 19,999</td>
<td>15%</td>
</tr>
<tr>
<td>20,000 or more</td>
<td>12%</td>
</tr>
</tbody>
</table>

Respondents by Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>18%</td>
</tr>
<tr>
<td>Technology</td>
<td>15%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>15%</td>
</tr>
<tr>
<td>Retail/Wholesale</td>
<td>7%</td>
</tr>
<tr>
<td>Health Care</td>
<td>7%</td>
</tr>
<tr>
<td>Business Services</td>
<td>15%</td>
</tr>
<tr>
<td>Government</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>17%</td>
</tr>
</tbody>
</table>

Respondents by Age of Organization

<table>
<thead>
<tr>
<th>Age of Organization</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 50 years</td>
<td>5%</td>
</tr>
<tr>
<td>21 to 50 years</td>
<td>24%</td>
</tr>
<tr>
<td>11 to 20 years</td>
<td>31%</td>
</tr>
<tr>
<td>6 to 10 years</td>
<td>15%</td>
</tr>
<tr>
<td>1 to 5 years</td>
<td>5%</td>
</tr>
</tbody>
</table>
Prisma Cloud protects cloud-native workloads and applications, spanning hosts, containers, serverless, and PaaS resources across cloud platforms. It dynamically discovers resources as they are deployed and correlates cloud service provided data (resource configurations, flow logs, etc.) with threat intelligence to identify insecure configurations. It uses machine learning to profile user and app behaviors to prevent anything abnormal.

Prisma Cloud integrates with any CI/CD process and environment to provide full lifecycle vulnerability management, runtime defense, and cloud native firewalling. It vastly simplifies the task of maintaining compliance with the industry’s most complete library of compliance frameworks.

Prisma Cloud provides this through deep context sharing that spans infrastructure, PaaS services, users, development platforms, data, and application workloads. Seamless integration with security orchestration tools ensure rapid remediation of vulnerabilities.

Get Ready to Move Fast!