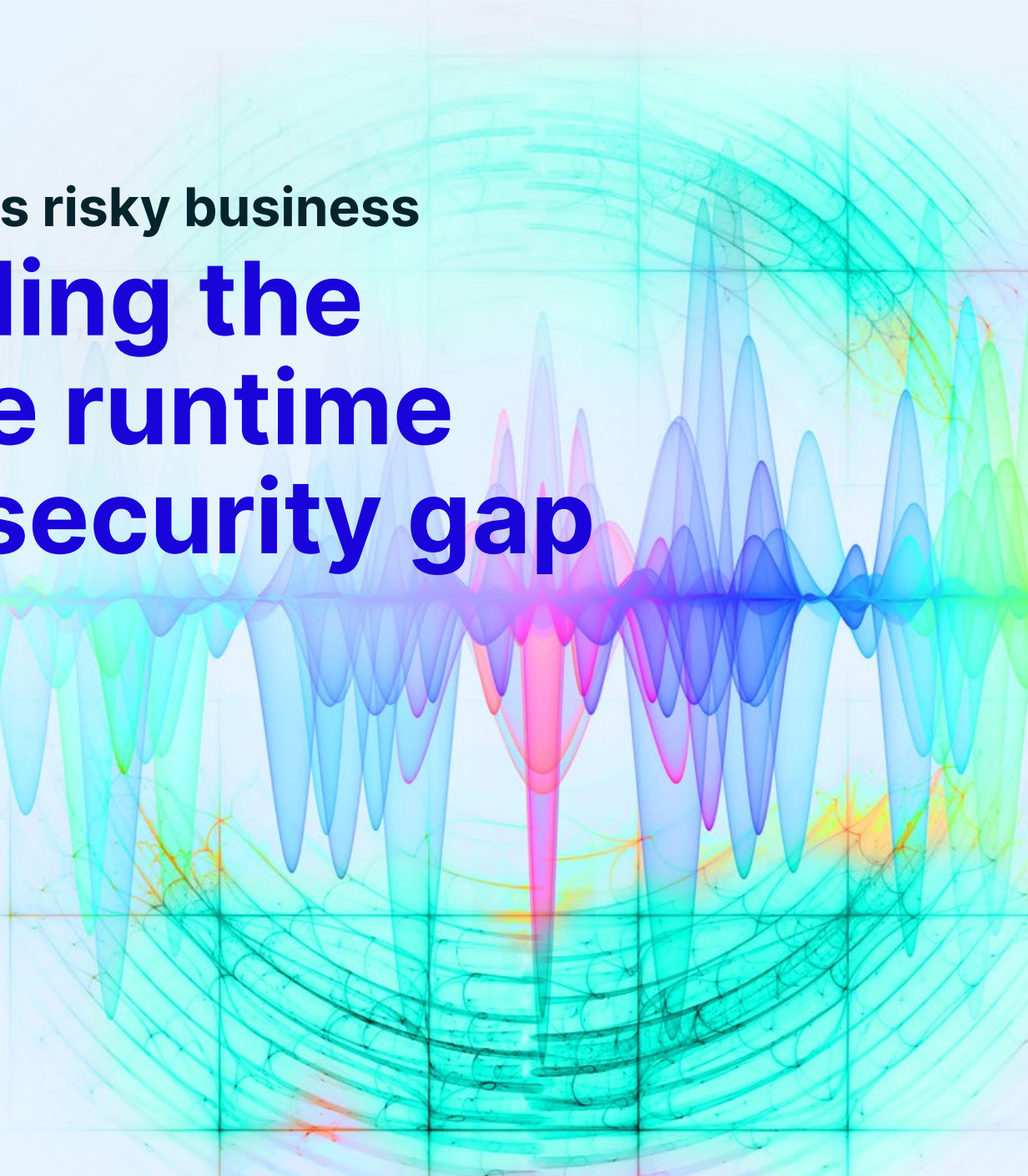
aqua

Winging it at runtime is risky business

Understanding the cloud native runtime protection security gap



A survey designed to help DevOps, Security and IT teams understand the real challenges they face when trying to secure cloud native applications

July 2021

Table of Contents

Introduction

Runtime protection, in cloud native security, can be defined as the ability to stop an attack in progress while a workload is running. Contrast this to protections applied in the build via “shift left,” where the goal is prevention.

Examples of runtime security include preventing drift, mitigating exploits, and stopping zero days that evade static scanning and make their way into production. While shift left, scanning, and hardening of cloud environments are critical elements of a full life cycle cloud native security strategy, all those efforts are moot without a way to protect in runtime against attackers who have evaded detection and have access to the production environment. Runtime security is also key to protect production environments from the well-intentioned efforts of administrators to make runtime changes that could open security gaps.

This survey was conducted to help DevOps and Security teams understand the real challenges they face when trying to achieve runtime protection. The goal of this survey is to use current perceptions to inform recommendations for practitioners to achieve practical, effective runtime security for their cloud native environments.

Key Findings

Knowledge gap

- Practitioners state more confidence in achieving runtime security than in achieving the necessary building blocks of runtime security, reflecting a knowledge gap
- A surprising number of respondents do not understand the real risks of cloud native environments. For example, only 3% agree that a container is not a security boundary

Consequences: Runtime security is not being prioritized

A large number of respondents reported a dangerously low level of prioritization of runtime security in future cloud native security initiatives.

Lower friction for ongoing management and purchasing

Runtime security appears to generally be both managed and purchased by the same team, which is not the case for other areas of cloud native security like vulnerability scanning or cloud security posture management (CSPM).

Runtime security aligns with the benefits of a unified platform

The top reason 79% of respondents prefer a unified platform for cloud native security is sharing context to prioritize security gaps. Runtime security is most effective with context sharing, making runtime capabilities an ideal addition in a unified platform.

The Biggest Education Gap in Cloud Native Security: Runtime

The results show that practitioners are less confident in their runtime security capabilities overall versus other cloud native security capabilities. Most importantly, practitioners think they are more protected than they are, since they report not taking the necessary steps to achieve runtime protection. This is true even for practitioners with five or more years of experience.

Confidence vs. reality

When asked which cloud native security capabilities they are confident they can achieve, only 32% of respondents were confident in their ability to stop attacks in progress. This is much lower than the confidence in achieving vulnerability scanning (59%) or protection against supply chain attacks (53%).

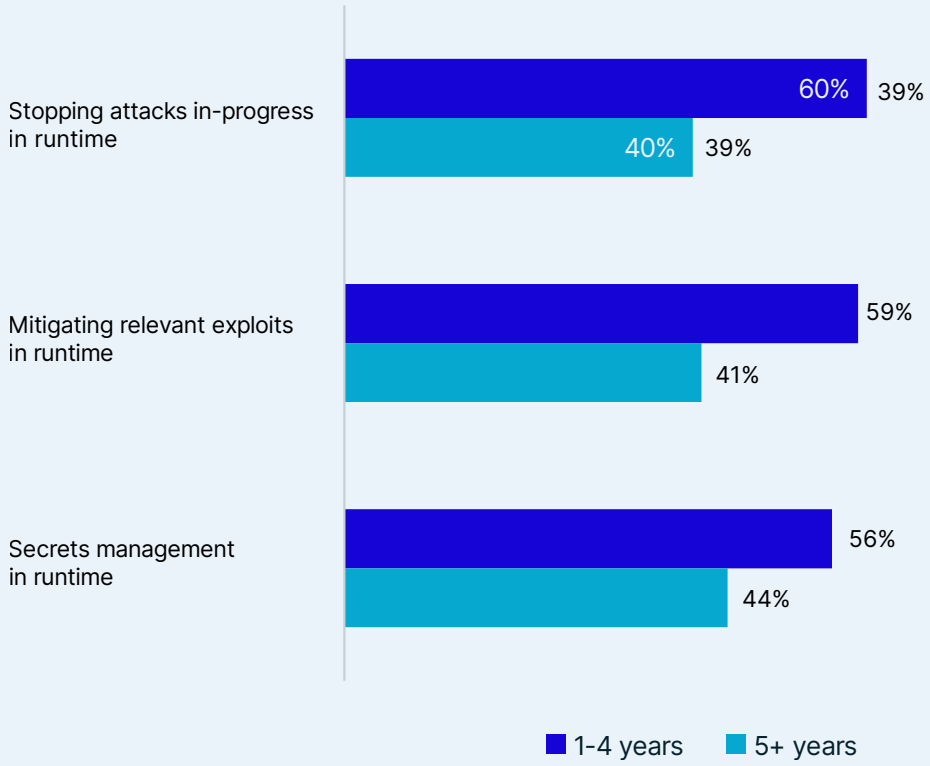
When respondents were asked to rate their confidence in achieving the building blocks of runtime security, their confidence was much lower:

- Only 14% were confident in enforcing image immutability in production
- Only 21% were confident in mitigating exploits in runtime
- Only 23% were confident in achieving secrets management in runtime

Effective runtime security requires these fundamental components. The difference between the confidence in runtime security overall and these building blocks of runtime security reveals a knowledge gap.

Those who have more years of experience were significantly less confident in their ability to stop attacks in progress, mitigate relevant exploits in runtime, and manage secrets in runtime, compared with those who have fewer years of experience.

Confidence in cloud native security capabilities by years of experience

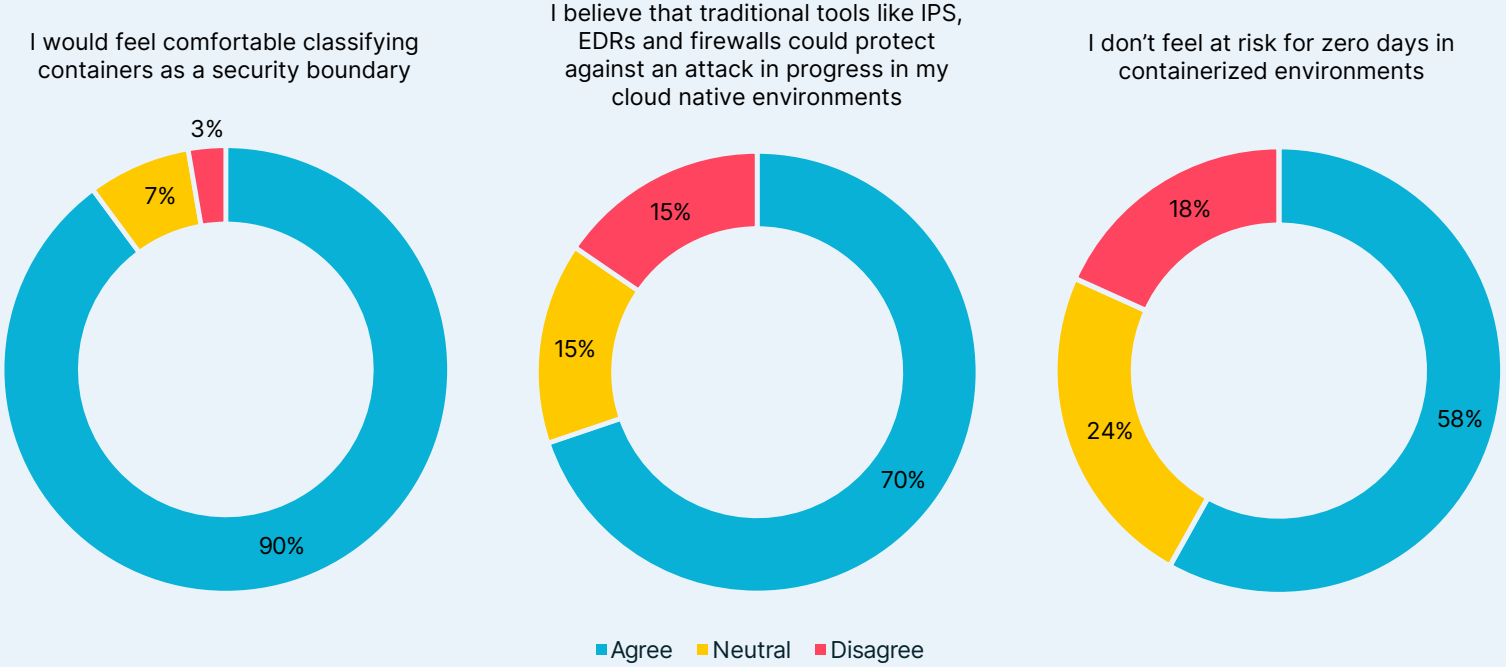


Understanding the real risks in cloud native environments

There also appears to be a large misunderstanding around key cloud native security concepts. Without an understanding of these concepts, it would be difficult to recognize the importance of runtime security.

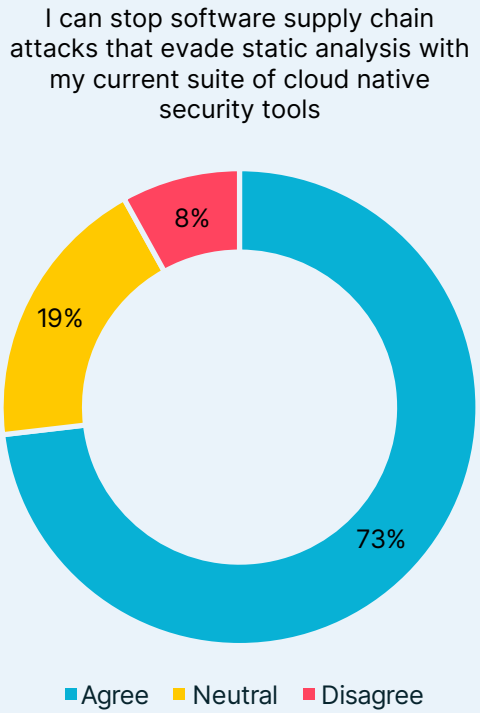
- Only 3% understand that a container is not a security boundary
- Only 15% understand that an IPS can't stop an attack in progress in a cloud native environment
- Only 18% feel at risk for zero days in containerized environments

Understanding of key cloud native security concepts



Despite the low levels of confidence in achieving runtime security overall, 73% believed they could stop software supply chain attacks evading static analysis. But stopping sophisticated supply chain attacks requires strong runtime protection. One potential explanation for the high confidence in stopping supply chain attacks is the fact that 85% of respondents felt their traditional tools could stop attacks in progress in cloud native environments.

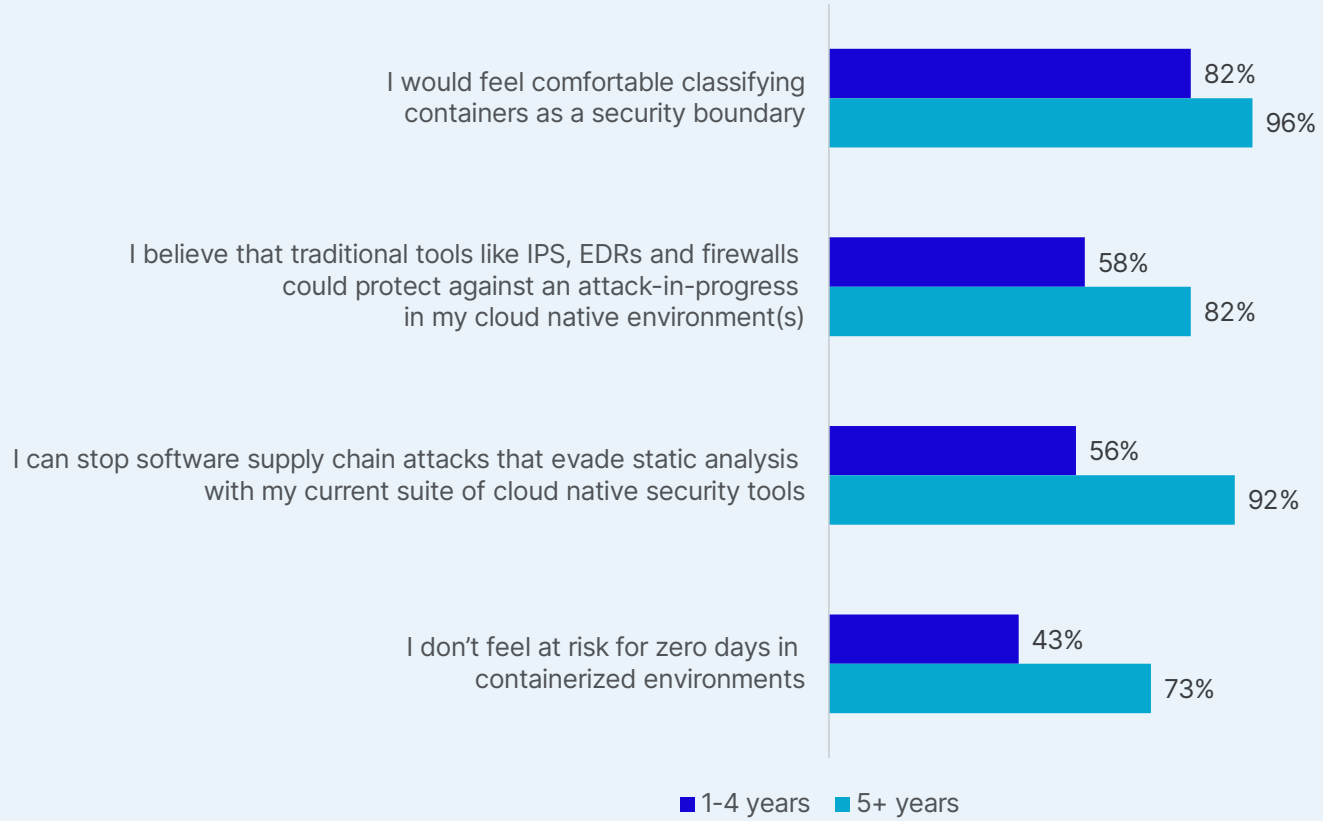
Understanding of cloud native security risk



Strangely, practitioners who have more experience were more comfortable classifying containers as security boundaries and more likely to believe that traditional security tools could work against attacks in progress in cloud native environments.

Those with more experience also felt less at risk for zero days in containerized environments and felt they could stop software supply chain attacks that evade static analysis.

Understanding of cloud native security concepts and risk by years of experience



Consequences: Runtime security is not being prioritized

More experienced practitioners did not show a greater likelihood to invest in this critical area. Instead, the more experienced practitioners were more likely to prioritize policies for controlling the build pipeline with future investment. But overall, the levels of intended investment were very low.

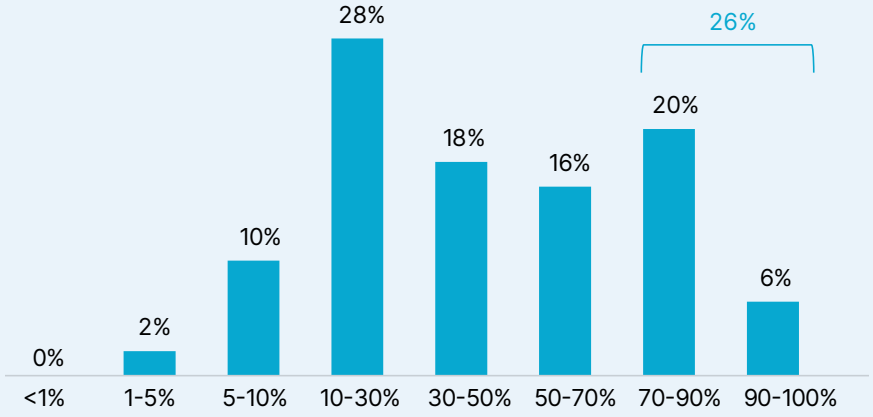
The less experienced practitioners were more likely to prioritize runtime capabilities such as supply chain attack protection, stopping attacks in progress, mitigating relevant exploits in runtime, enforcing image immutability in production, managing secrets in runtime, and forensics.

Overall, less experienced practitioners are both more confident in and more committed to prioritizing focus on runtime security than more experienced practitioners. Respondents were less likely to prioritize runtime security over other cloud native security capabilities.

Plans to prioritize in the next year by years of experience

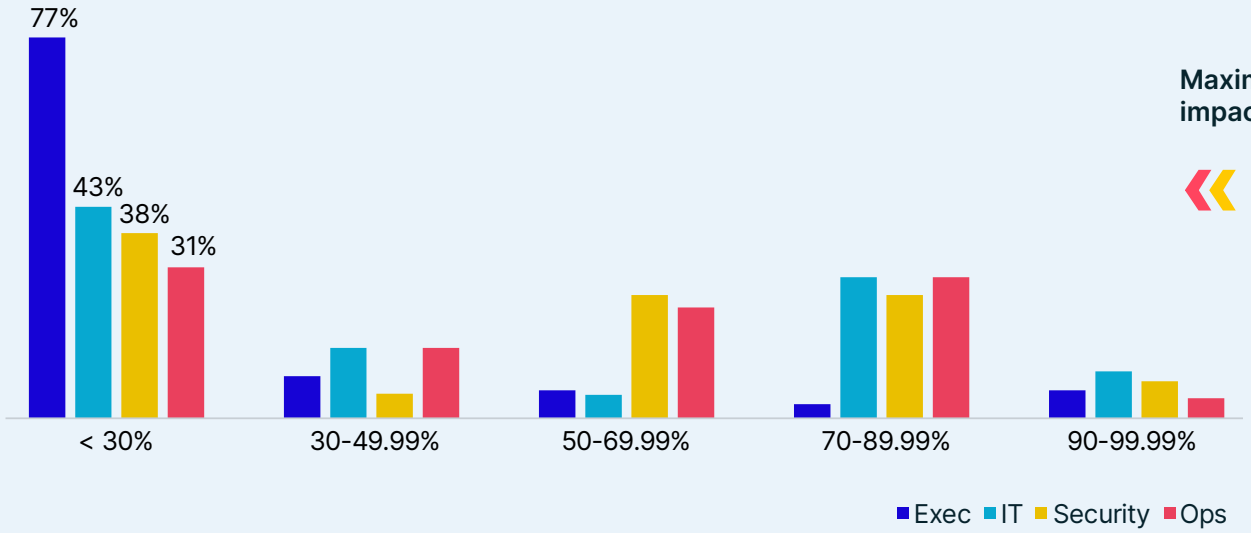
In their current stacks, only 26% of respondents said that 70% or more of their cloud native security solutions could stop an attack in progress in a running application. This signifies a general lack of coverage for runtime capabilities across the other 74% of respondents' toolkits.

Amount of current cloud native security stack that can stop an attack in progress



Interestingly, of all respondents, the executives (CIO, CISO, CTO) were the least likely to accept any performance impact for stopping attacks in progress. Seventy-seven percent of executives were only willing to accept a maximum performance impact to stop attacks in progress of 30% or less, indicating a much lower tolerance for security's impact to the speed of business at the executive level.

Maximum acceptable performance impact to stop attacks



Stopping the gap: The easiest route

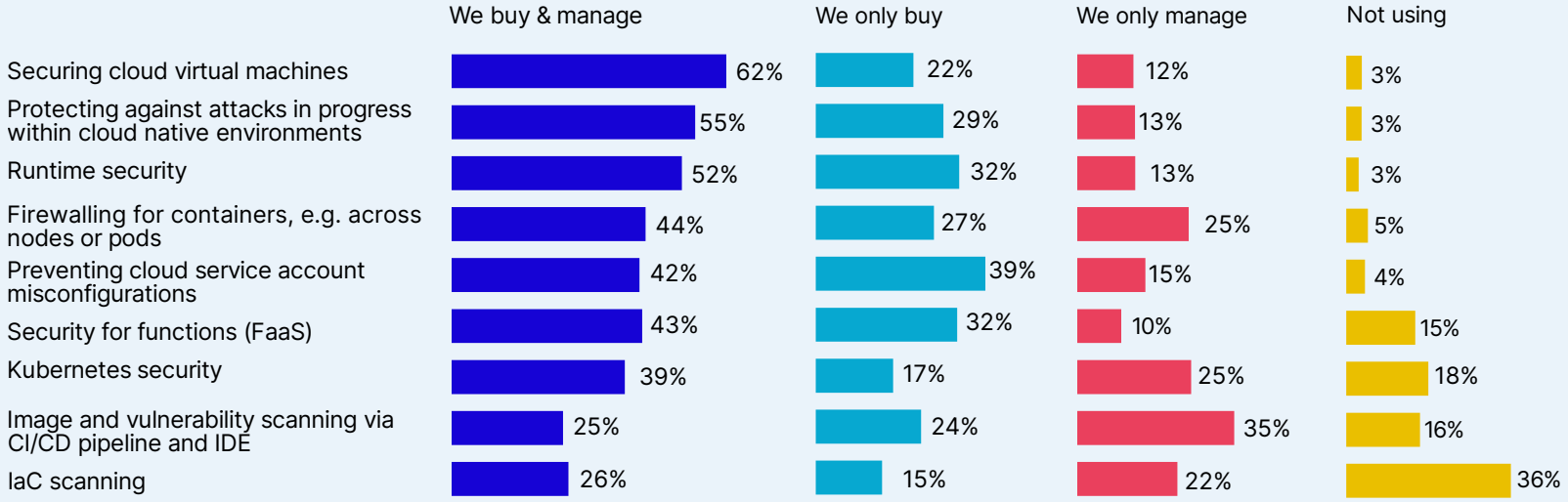
Low friction

Runtime security is the second-most-common cloud native security capability to be bought and managed by the same team or group. 52% of respondents said they both bought and managed runtime security, and 55% said they both bought and managed protection against attacks in progress in cloud native environments. Solutions to secure cloud VMs were the most likely to be both bought and managed, at 62%.

In contrast, the top cloud native security solutions that are only bought by the team are those to prevent cloud service account misconfigurations (38%). The top cloud native security solution that is only managed by the team is image and vulnerability scanning via CI/CD pipeline in IDE (35%).

So, despite the runtime security knowledge gap and the low levels of implementation, runtime security is possibly one of the areas with lowest friction in terms of managing internal dynamics for purchasing and ongoing management.

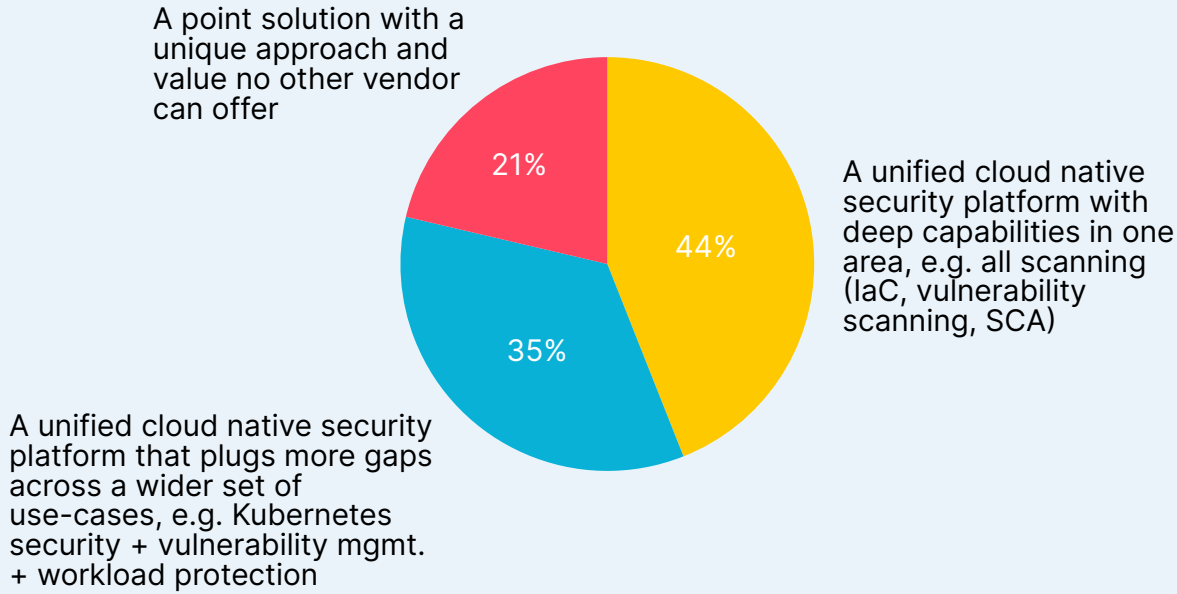
Cloud native security roles and responsibilities



Preferences for a unified platform

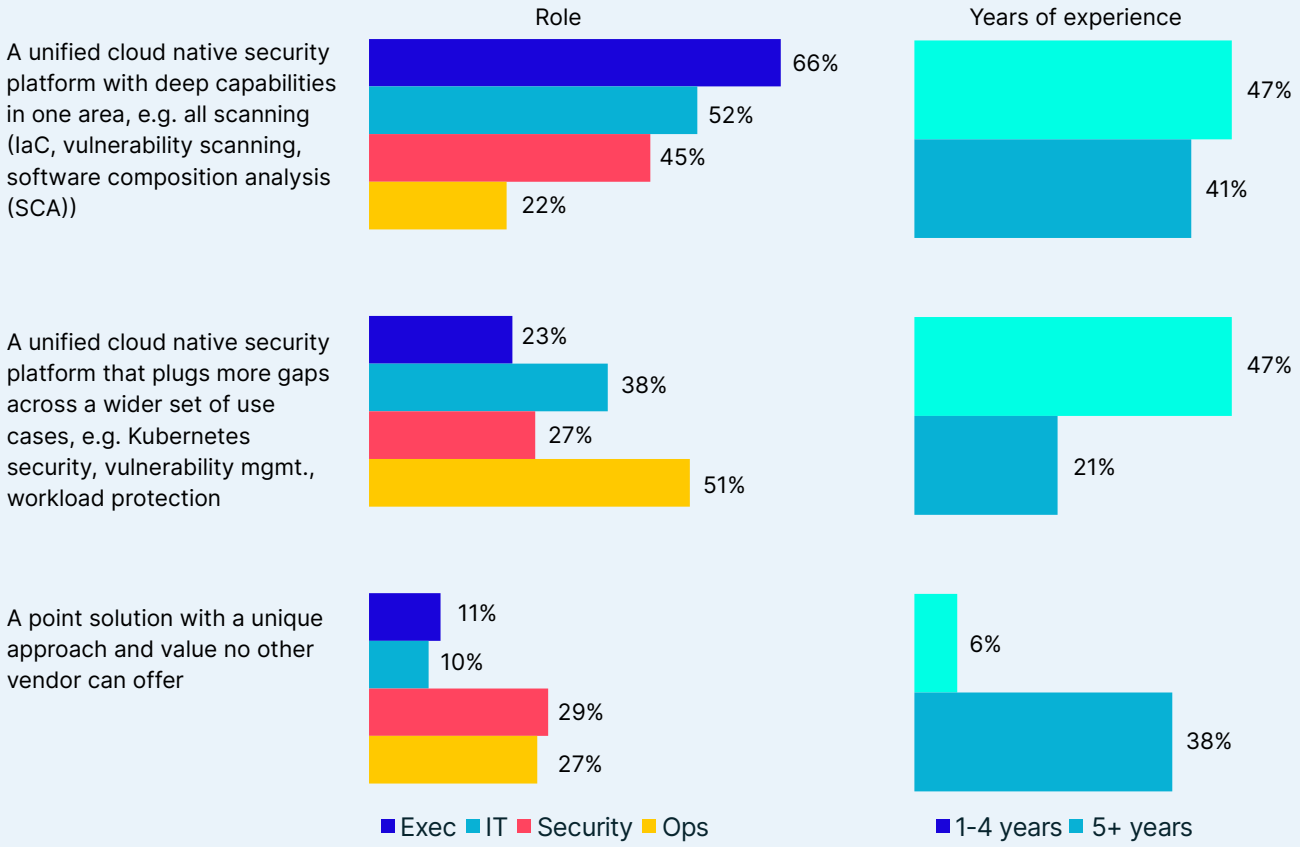
Implementing holistic cloud native security, which should be every practitioner's goal, is not just about runtime security or any other one focus area. It is about the entire application life cycle, from the build to the infrastructure and the workloads. Only 21% of respondents preferred a cloud native security point solution over a unified platform, regardless of whether that platform was deep in one area or covered a broad array of use cases.

Preference for unified platform or point solution



There was a stark difference in approach between practitioners with less than five years of experience and those with five years or more. Those with five or more years of experience were the only cohort that preferred a point solution. Of note, the more experienced practitioners who wanted point solutions were NOT executives, most of whom preferred a unified platform with deep capabilities in one area.

Preference for point solution versus unified platform



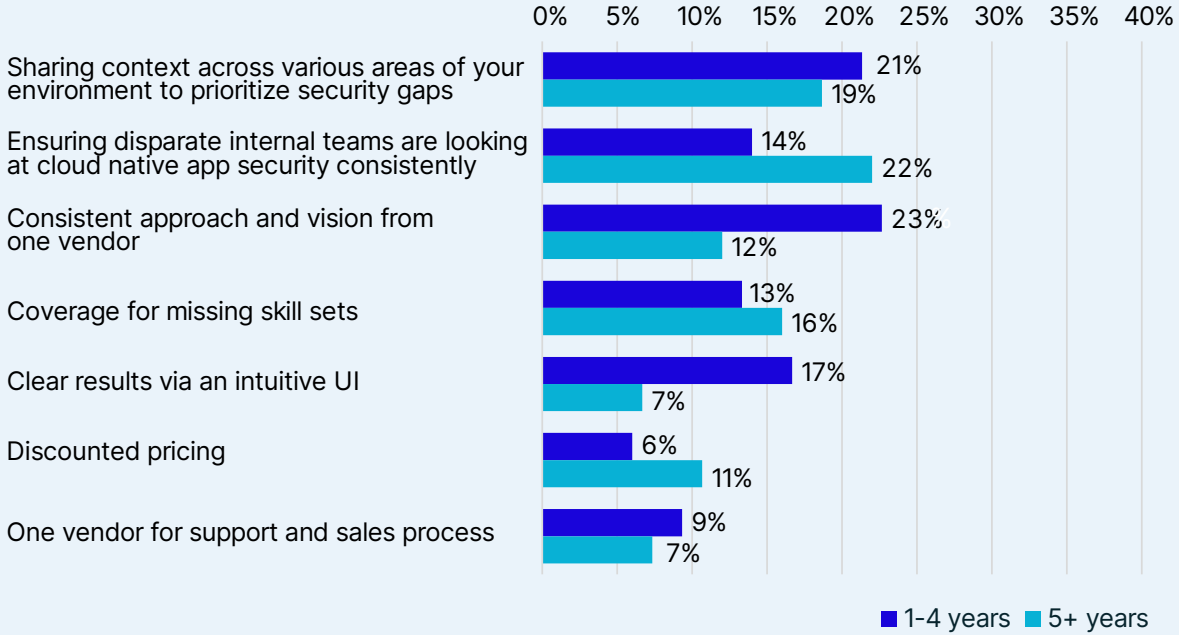
Expectations for a unified platform

Sharing context is critical in prioritizing runtime issues for effective remediation. The enforcement mechanism in production must also be as predictable and consistent as possible to minimize disruption. And achieving effective prioritization of issues along with minimal disruption requires separate internal teams to have a consistent view of cloud native application security.

Keeping this in mind, according to respondents, the top three benefits of a unified cloud native security platform are:

- Sharing context across various areas of the environment to prioritize security gaps (40%)
- Ensuring that separate internal teams are looking at cloud native app security consistently (36%)
- Achieving a consistent approach and vision from one vendor (35%)

Based on these responses, requirements for achieving minimal disruption and effective prioritization in runtime security are similar to those sought by respondents in a unified cloud native security platform.



Top benefits of a unified cloud native platform

Conclusion

The survey results surface key takeaways for teams wanting to achieve effective runtime protection in cloud native environments:

- Specific attention needs to be paid to the building blocks of runtime security; for example enforcing the immutability of containers
- Supply chain attack protection should be treated as both a runtime and shift-left capability
- Even though the production environment is sensitive, investing in runtime protection for cloud native environments might bring less friction between internal teams, in terms of managing and purchasing, than other cloud native security tools
- Internal experts in the complex security capabilities of containers, Kubernetes, and more, should invest time supporting their colleagues' projects and research initiatives to guide decisions about future investment in runtime security

The knowledge gap around workload protection has led to a striking number of misconceptions about how to implement it. The good news is that workload protection can probably be most conveniently and effectively implemented by virtue of a unified platform that also includes other critical cloud native security controls like Kubernetes security, image scanning, and cloud security posture management. In a unified platform, adding workload protection to your suite of cloud native security tools could be as easy as a simple subscription upgrade.

Report

Cloud Native Security Threat Report 2021

View the Report ›

Blog

Container Isolation: Is a Container a Security Boundary?

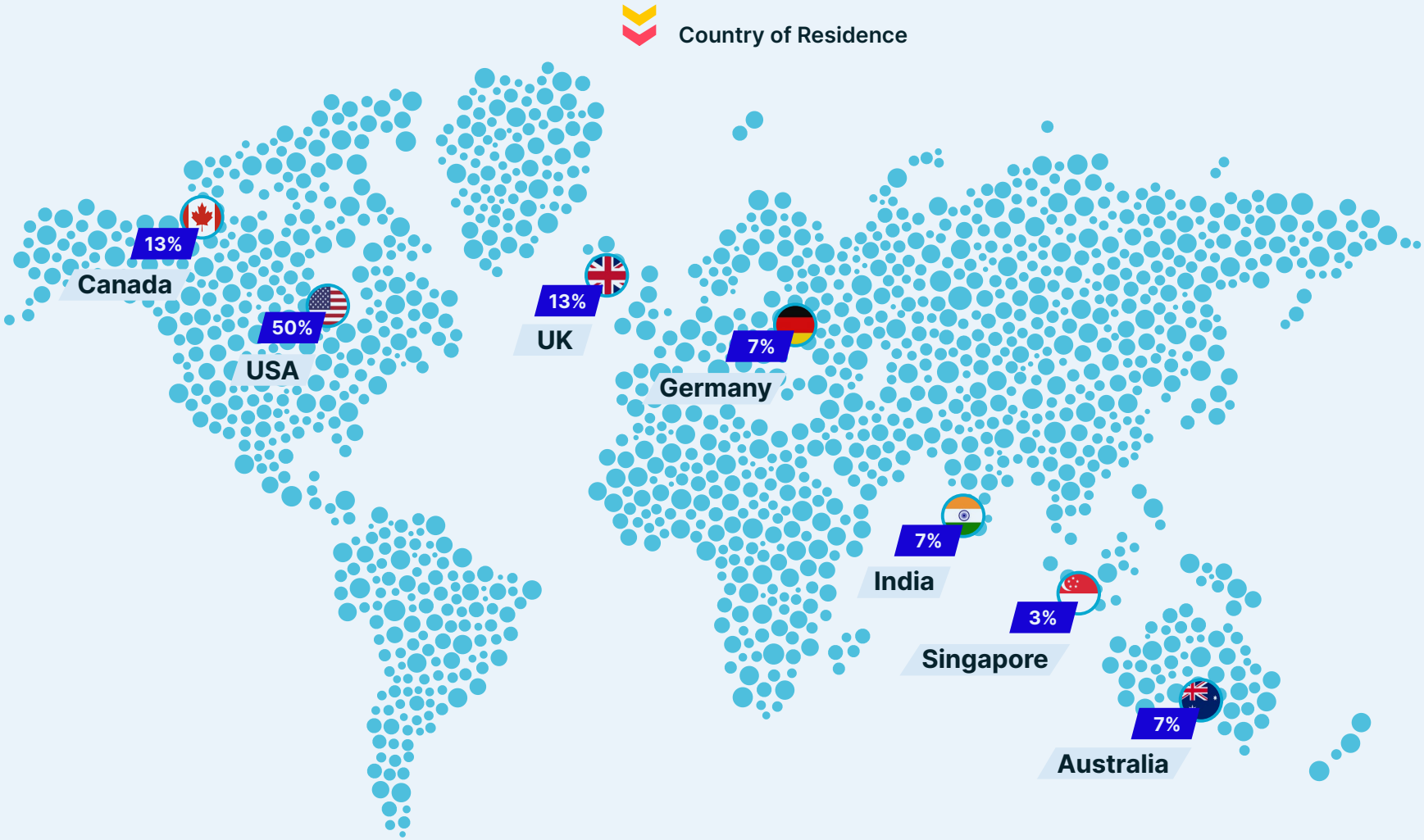
View the Blog ›

Video

Aqua Platform: Runtime Security Overview

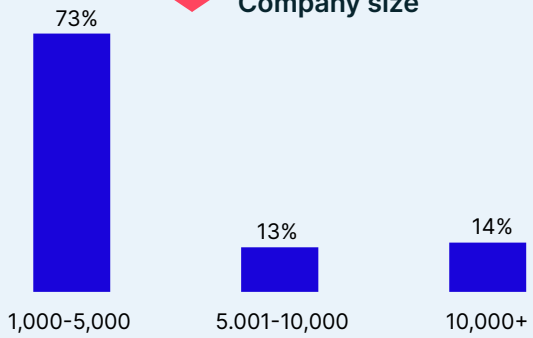
View the Video ›

Respondent Demographics

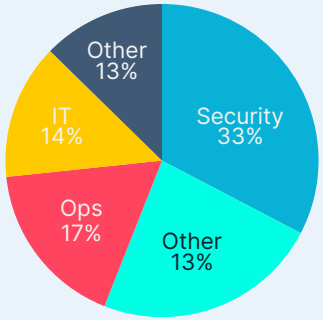


The study surveyed a global sample of 150 cloud native security practitioners across IT, Ops and Security functions, with varying years of experience. Mid-size and large companies were included across varying sectors such as financial services, technology, industrials, and more.

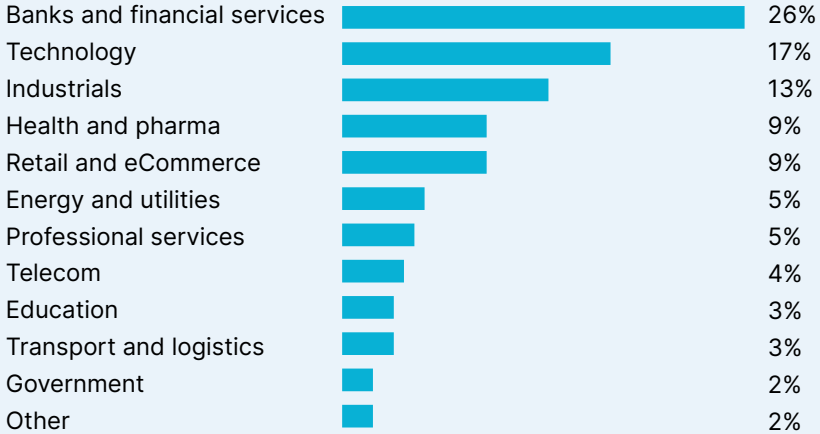
Company size



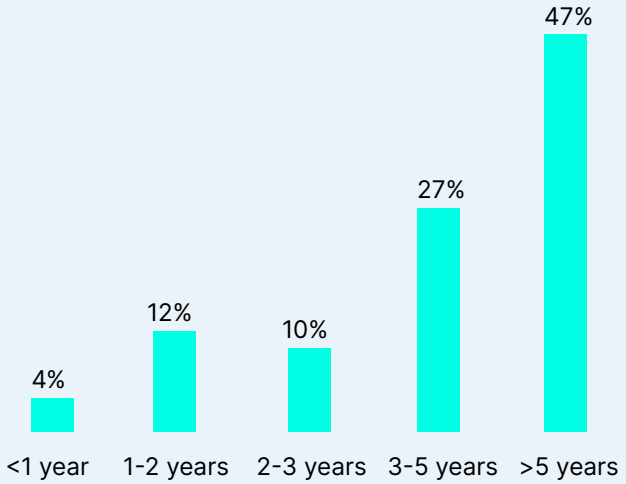
Job function



Industry



Years of cloud native security experience



Go Cloud Native with the experts!

Get a Demo ›

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they
are deployed.