Techstrong Research PulseMeter

Sponsored by snyk

2022 Container Security Trends

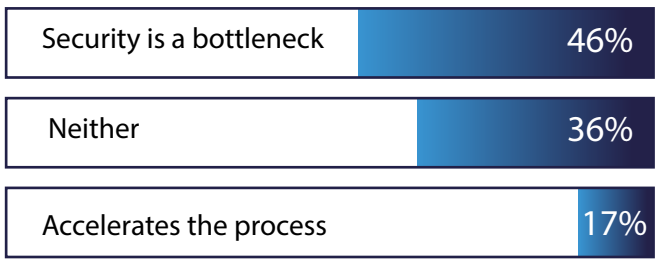
Cloud computing environments are increasingly defined and controlled by infrastructure-as-code (i.e. Terraform), containers and Kubernetes. With this shift, we are seeing an emerging trend that is familiar to those who have followed DevOps. Increasingly DevOps teams have placed a high priority on identifying and remediating security issues as early as possible in the development cycle. Similarly, cloud teams are pushing to identify potential security problems earlier in the process – as containers and cloud resources are being designed, not after they are deployed. However, one of the major challenges is that most developers are security-aware but are not experts. Therefore, there is an increasing need for developer-friendly approaches that help identify security issues in code (application and cloud configurations).

In March of 2022, Techstrong Research conducted several flash polls among the Techstrong Group member community. The goal of these polls was to understand our members' evolving priorities around creating secure cloud environments. Across all of the polls, we received more than 1,700 responses.

The impact of security on cloud deployments

Spotting cloud security issues and misconfigurations earlier in the design process is a growing trend because organizations want to increase the velocity of cloud deployments. Many view security as a bottleneck in their processes.

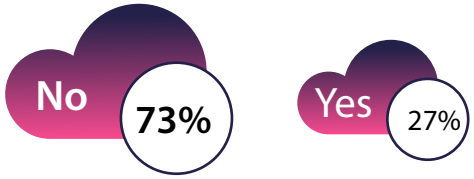
Does security slow down your cloud deployments?



Application teams aren't security experts

Developers wear many hats, and to be successful they must be security-aware. Automation can help them to create secure cloud environments.

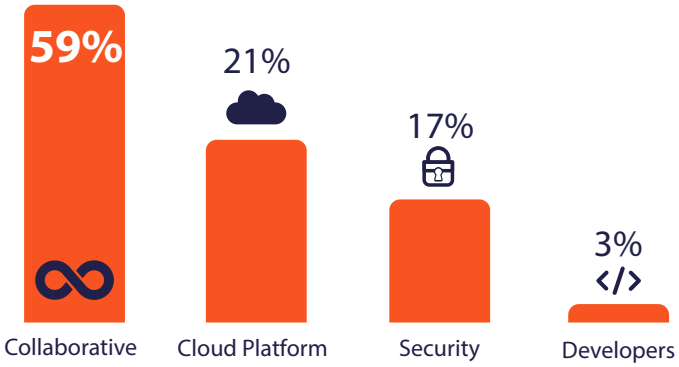
Do application teams have enough experience and context to identify cloud security vulnerabilities and cloud misconfigurations?



Securing your Cloud Environment

Securing a cloud environment requires input from security and infrastructure teams. The bottom line is that creating and securing your cloud environment is a team effort.

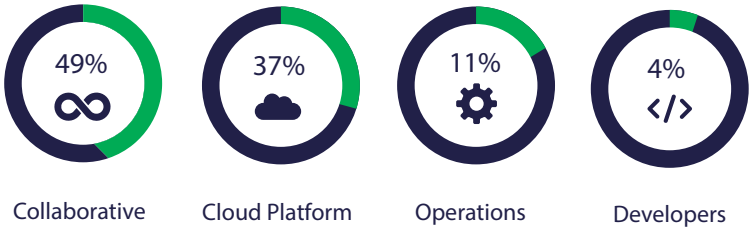
Who is primarily responsible for securing your cloud infrastructure environment?



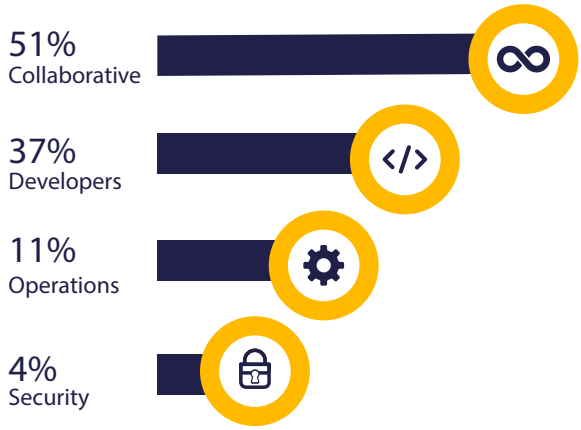
Securing your Cloud-Native / Container Environment

While the majority of respondents agree that creating a secure container environment requires collaboration, many developers take on this duty alone on top of their other responsibilities.

Who is responsible for creating cloud infrastructure configurations?



Who designs and configures containers within your organization?



Techstrong Research Analyst View

The trends towards shifting security left – meaning addressing security earlier in your planning process – means that developers must have tools that empower them to spot and fix security issues on their own. At the same time, it's still critically important that developers focus on creating the types of digital experiences that customers demand. If a web or mobile application fails to satisfy rising customer expectations, there is no shortage of competitor offerings.

Security is still too often identified as a bottleneck. However, by using tools that have automation and best practices built into the offering, security no longer needs to be thought of as a roadblock. As we talk to leaders within IT organizations, it's clear that there is a need to push security earlier in the cloud environment design process.