Techstrong Research
PulseMeter

Sponsored by **Orca security**

You can't secure, govern or audit what you can't see. This concept is becoming increasingly important as more and more applications and data are run and housed outside of your on-premises IT environment. Of course, the cloud has complicated security, but other emerging technologies like edge computing and serverless are also making it more important than ever to gain visibility over your IT infrastructure no matter where it resides.

Security, DevOps and business leaders are demanding visibility across infrastructure. Teams want to view disparate environments as if they were one integrated platform -- even though, of course, they are not.

During April of 2022, our team conducted several flash polls among the Techstrong Group member community. Techstrong Group members include readers, influencers and contributors to our various communities focused on DevOps, cloud-native, security and digital transformation. The goal of these polls was to understand our members' evolving priorities around cloud security and insight into cloud environments. Across all of the polls we received more than 435 responses.

## New Computing Environments Are Here to Stay

» You don't need research to tell you that the cloud is big and growing – however, the era of multi-cloud and serverless is here. Organizations not already investing in serverless have it on their strategic roadmap.

Are you using serverless technology on more than one cloud provider? (i.e. AWS, Google Cloud, Microsoft Azure, etc)
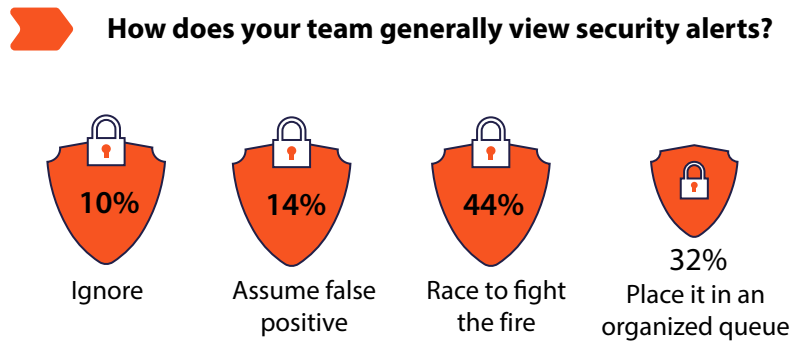
✓ **61%**
Yes - Multi-cloud approach

✕ 39%
No - One cloud approach

Are you using serverless technology?

86% →

48% **Yes**

5% **No** but within a year

33% **No** but on roadmap
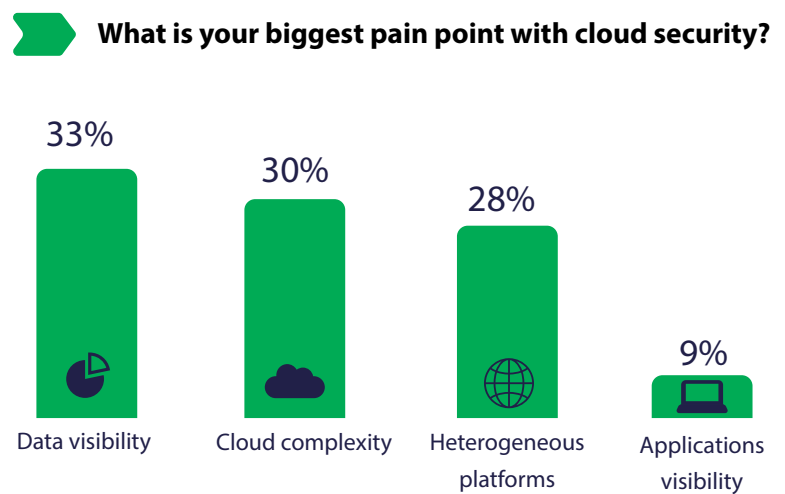
14% No serverless plans
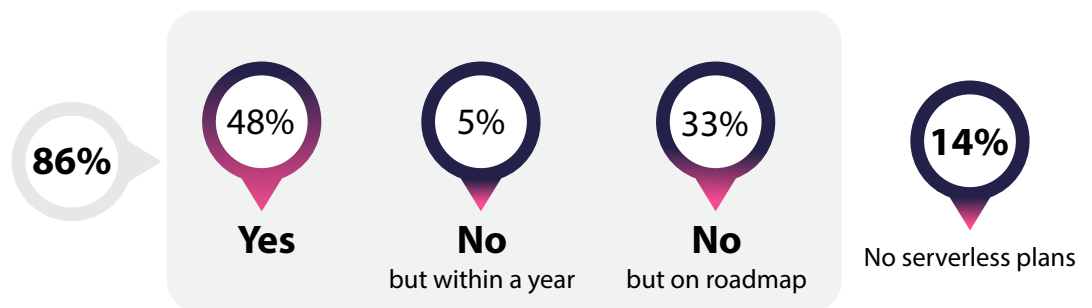
Alerts – Storms or an Organized Approach?

» Alerting has been built into IT security and operations platforms for decades; however, far too often systems are "too noisy," meaning they send too many alerts. The challenge with too many alerts is that prioritizing the alerts becomes complex and critical warnings can be missed.

How does your team generally view security alerts?

10% Ignore

14% Assume false positive

44% Race to fight the fire

32% Place it in an organized queue

The Challenge of Cloud Security

» It's clear that teams find visibility and complexity across multiple cloud environments a major challenge when trying to secure cloud workloads. There is clearly a need for simplified visibility offerings.

What is your biggest pain point with cloud security?

- **33%** Data visibility
- **30%** Cloud complexity
- **28%** Heterogeneous platforms
- **9%** Applications visibility

Techstrong Research Analyst View

It's clear that IT environments are becoming more complex as new deployment models are adopted. Your security, operations and entire DevSecOps organization must be able to support the technology platforms that can help your business support increasing customer expectations and business competition.

While individual cloud platforms offer native management capabilities, these systems are proprietary to a single cloud. In addition, although agent-based monitoring has been used for many years, there are clear drawbacks. The most serious security concern is that security gaps typically exist because an agent is often not deployed on every cloud instance.

Why does this security concern continually exist with agent-based approaches? It's simple: Agents are difficult to deploy and slow down the process of provisioning new cloud environments. This negates the advantage of being able to quickly and easily spin up new cloud instances. As we work with business and technology leaders, it's clear that there is a need in the market to abstract the challenges of multi-cloud security and provide visibility into applications and data across any infrastructure environment.

Sponsored by

Orca security