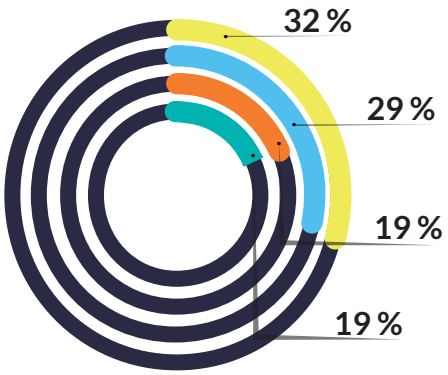
Techstrong Research

PulseMeter Sponsored by nirmata

Security Concerns are NOT Slowing the Kubernetes Express



One-third are holding back on K8s due to security concerns. That means the other two-thirds are pressing forward; 20% without a plan to address those concerns.

Have security concerns or prevented your use of Kubernetes?

- 32 % Yes, security concerns are preventing us from deploying Kubernetes
- 29 % Yes, but we are moving forward and working to improve Kubernetes security
- 19 % No, we know how to secure Kubernetes
- 19 % No, but we still have security concerns

Kubernetes (K8s) is taking the cloud-native world by storm, growing at 60%+ year-over-year with 5.6 million developers actively using K8s. The flexibility, scalability and open nature of K8s has proven extremely attractive to organizations of all sizes evolving to cloud-native infrastructure.

The excitement around Kubernetes' growth often overshadows concerns regarding the environment's security. Like other technologies, the main security concerns involve addressing misconfigurations, detecting runtime threats and security policy management. And Kubernetes faces the same lack of skills, time and resources to provide adequate security that plague most open source, cloud-native software solutions. Yet these concerns are not slowing the adoption of Kubernetes, as our research shows that 81% of respondents have not slowed their use of Kubernetes due to security concerns. These organizations resort to a "deploy now, figure out security later" approach.

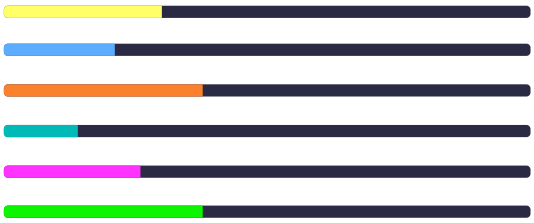
In 2022, Techstrong Research polled our community of DevOps, cloud-native, cybersecurity and digital transformation readers and viewers to take their pulse on Kubernetes security. Even though Kubernetes adoption is accelerating, respondents are concerned about the lack of skills (27%), lack of understanding of policy best practices (23%) and lack of time and resources (22%). To address these concerns, slightly more than one-third (36%) of respondents either have a funded project or believe Kubernetes security is a priority for 2023, while 35% plan to continue addressing issues tactically on a project-by-project basis.

Copyright © 2022 Techstrong Group

Misconfigurations, Runtime Threats and Pod Security are the Top Security Concerns

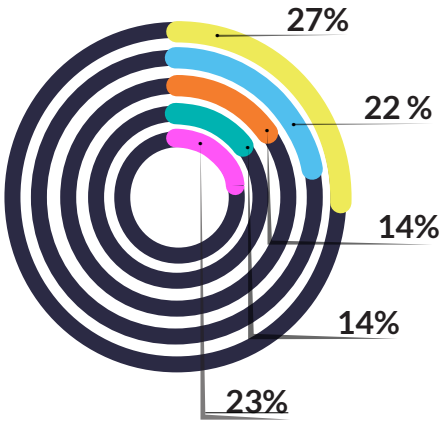
These concerns can be addressed with security best practices: Implementing strong policies and monitoring for attacks.

What are you top Kubernetes security concerns?



19 %	Pod security policy management
12 %	Image supply chain integrity
23 %	Configuration errors
7 %	Over provisioning of permissions
16 %	Writing and enforcing security policies
23 %	Runtime thret/incident detection

Skills, Time and Resources to Address K8s Security in Short Supply



It's not point solutions or vendor functionality gaps creating challenges; it's the people's side of the equation.

What are your greatest challenges securing Kubernetes?

27 %	Lack of the necessary K8s security skills
22 %	Time and resources to address K8s security
14 %	Point K8s security solutions don't fit into our DevOps workflows
14 %	Current vendors we use do not adequately address K8s security
23 %	Lack the understanding of K8s security policy best practices

Despite K8s Security Issues, Only a Third are Taking Proactive Action.

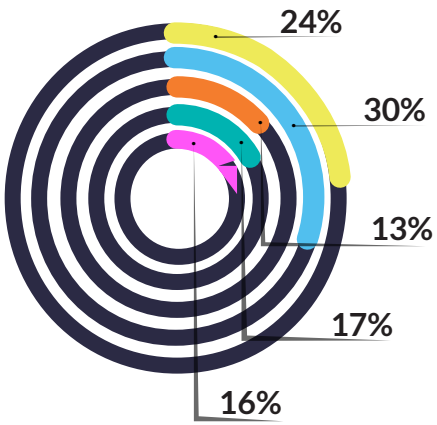
Security is widely perceived as a problem, but two-thirds have not yet made it a priority and plan to handle security tactically.

Is Kubernetes pod security a priority for your organization?

15 %	Yes, we have an funded, active project
21 %	Yes, it is a priority for 2023
35 %	Somewhat, we address on a project-by-project basis
18 %	No, but we know we need to do more with Kubernetes security
11 %	No, not currently a significant issue

Copyright © 2022 Techstrong Group

Policy Management Addressed by a Combo of OSS and Native Pod Security Policies



About one-third use commercial or cloud provider offerings, with 15% doing nothing.

What are your sources for Kubernetes policy managment?

- 24 % Open source software
- 30 % Kubernetes native Pod Security Policies
- 13% Commercial security product offering
- 17 % Cloud service provider security offerings
- 16 % Do not have a solution at this time

K8s Security Responsibility Falls Predominately to DevOps/DevSecOps

K8s is treated as separate infrastructure, as only 18% of security teams are responsible for securing K8s.

What role is responsible for Kubernetes security in your organization?

- 9 % Development
- 24 % DevOps
- 37 % DevSecOps
- 18 % Security
- 12 % Platform Engineering

Techstrong Research Analyst View

Security concerns have not slowed Kubernetes adoption or its use in corporate environments, with 29% moving forward and trying to improve security and another 19% pushing ahead despite the security issues. Based on the results of the PulseMeter, the security concerns are underappreciated by the respondents, given that 35% address security issues on a project-by-project (tactical) basis and another 18% know they need to do more. Surprisingly, 11% currently don't see any security issues.

Even if these organizations wanted to address the problem, they face a lack of K8s security skills (27%) and don't have the time or resources to address the issues (22%). Almost one-quarter (23%) of respondents don't know how to implement security best practices, even if they have the resources. The respondents' knowledge of K8s security solutions also seems limited, with only 13% using commercial offerings and another 17% relying on cloud provider solutions.

The bottom line is that Kubernetes security issues will continue growing as adoption accelerates. DevOps and DevSecOps teams must grapple with the complexity of Kubernetes environments and increasingly sophisticated security threats. We believe implementing security policies before Kubernetes is in production is the best first line of defense against top security concerns such as misconfigurations, pod security and software supply chain security incidents. Ignoring policy management in these early phases will lead to more challenges down the road.

The business and technology leaders' responses to the PulseMeter make it clear that there is a strong need to bridge the skills and resources gap for K8s security solutions. It's also vital that those solutions meet the needs of both the developer and the operations teams. Emerging Kubernetes security policy management solutions should be evaluated by all teams planning to deploy Kubernetes in production.

Copyright © 2022 Techstrong Group