StackRox

The State of Container and Kubernetes Security

Spring 2019

With observations and analysis from AimPoint Group

AimPoint GROUP

In the fall of 2018, StackRox surveyed more than 230 IT professionals across a range of industries to understand the state of the container and Kubernetes deployments.

The key findings centered around security topping the list of container strategy concerns, the lack of security strategies in place, and the type of security risk and impacted life cycle phase that most worried respondents.

Given the fast-moving nature of the container and Kubernetes adoption, we decided to repeat the survey just six months later. This round, we were able to glean responses from 392 IT professionals, and this report includes analysis of the changes over the past six months as well as observations around Kubernetes and newer technologies such as service mesh and functions-as-a-service.

The data show fast maturation across a number of key areas, including defining a strategy for container security, moving more containerized workloads into production, and – no surprise – robust adoption of Kubernetes.

Organizations, however, are still struggling with security and a lack of detail as the prominent challenges they're facing in their container strategies. Despite having a greater percentage of containers in production, these organizations have only modestly reduced their security concerns. Worries about misconfigurations and runtime risks persist, and still too few organizations have a robust security plan in place.

We invite you to see the progress we as an industry have made in just the last six months and identify areas where your organization also needs to improve its security practices to protect your container and Kubernetes workloads.

We also share key take-aways from industry analyst Mark Bouchard of AimPoint Group, observations he makes from his more than 20-year career helping organizations with their security strategies and architectures.

– The StackRox Team

About Mark Bouchard, AimPoint Group

Mark Bouchard, CISSP, is a Co-Founder and the CEO at AimPoint Group, a research and consulting firm serving the needs of high-tech organizations worldwide. Mark's areas of specialization include information security, compliance management, application delivery, and infrastructure optimization. A former META Group analyst, Mark has analyzed business and technology trends across a wide range of information security and networking topics for more than 20 years. During this time, he has assisted hundreds of organizations worldwide with both strategic and tactical initiatives, from the development of multi-year strategies and high-level architectures to the justification, selection, and operation of security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about ensuring the success of his clients.

Concerns over container security have increased.

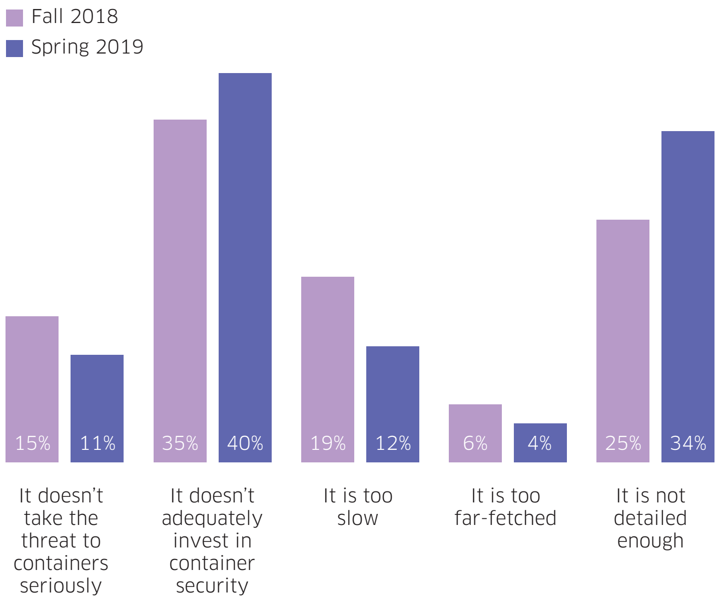
Despite maturity in container adoption, organizations are still struggling with their strategy for using and securing containers.

Concern has grown that organizations' container strategies are failing to invest sufficiently in security.

Inadequate investment in security dominates the list of concerns users have about their company's container strategy. The increase in both this worry and the concern that the strategies are not detailed enough provide clear signals that people are thinking more comprehensively about their use of containers.

These findings show maturation in how people are using containers and the importance of containerized apps in their business. That so few people see their plans as too slow or too far-fetched reinforces this conclusion.

Q. What is your biggest concern about your company's container strategy?

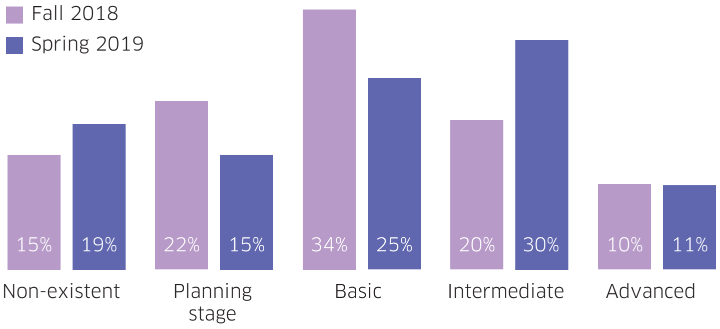


More than a third of respondents still lack any container security strategy.

Despite progress in the adoption rates of containers in production, 34% of respondents note they have no container security strategy or are just in the planning stages of formulating such a strategy. One possible explanation is that container adoption has outpaced investments in formulating a security strategy.

In positive news, respondents who consider their container security strategy to be either intermediate or advanced has increased from 30% to 41%. As organizations' container adoption matures, they realize they can't afford to treat security as an afterthought but instead must implement a security strategy across the entire container life cycle – from build to deploy to runtime.

Q: How would you describe the security strategy for your company's container and Kubernetes environments?



> "Organizations run a big risk by continuing to move forward with container adoption without making the needed investments in strategies and tooling to protect that critical application infrastructure."

Mark Bouchard
AimPoint Group

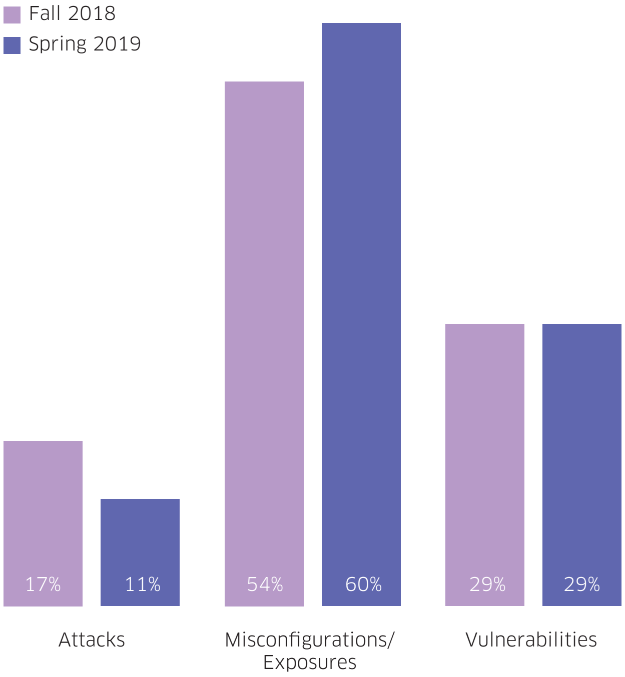
Despite repeated news of Kubernetes vulnerabilities, misconfigurations and runtime security remain the top sources of security concern.

Just as in cloud security, IT professionals expect misconfigurations to create the greatest security risk.

The year 2019 has been monumental for Kubernetes. As adoption has increased, news about challenges with implementation and security has increased. Despite recent discoveries of Kubernetes vulnerabilities, organizations continue to view user-driven misconfigurations and exposed Kubernetes dashboards or metadata as their biggest source of risk. The percent of respondents identifying misconfigurations and accidental exposures as their biggest security concern increased from 54% to 60% in a span of six months.

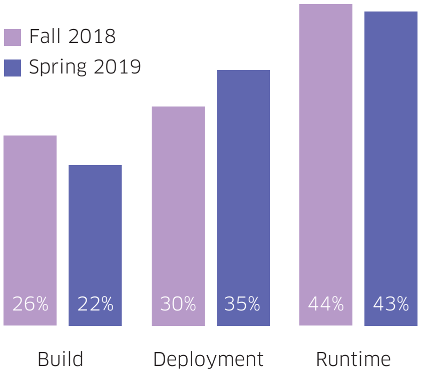
This finding is in keeping with what the industry sees as the biggest security threat to not only containers and Kubernetes but cloud deployments in general: preventable human error. The analyst firm Gartner contends that 95% of cloud security failures result from customer errors. Such has long been the case in security, where most incidents are caused by preventable user error.

Q: Of the following risks, which one are you most worried about?



Runtime remains the life cycle phase respondents worry about the most.

Q: Which life cycle phase are you most worried about?



Runtime continues to be the container life cycle phase that organizations are most worried about. This response shouldn't come as a surprise given the risk to the organization increases during runtime.

However, most organizations realize that runtime failures are a function of missed security best practices during the build and deploy phases. For that reason, more than half (57%) of respondents are more worried about what happens during the Build and Deploy phases. In other words, users realize they must "shift left" in their application of security best practices to "build it right" the first time.

Getting things right during the build phase drives two significant business advantages:

1. Research has shown it costs significantly less time and money to fix a security hole during the build or deploy phase than during the runtime phase.
2. The consequences of an overlooked Kubernetes setting, image vulnerability, network exposure, or other misconfiguration during build or deploy will be significantly higher if it's exploited during runtime.

Container and Kubernetes security approaches must span today's hybrid environments.

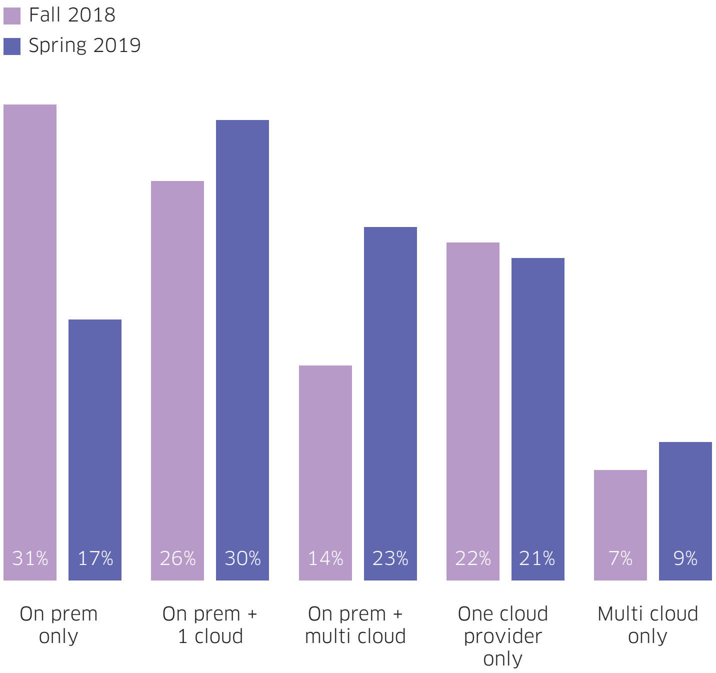
Containers are running everywhere: 70% of respondents are running containers on prem, but 75% of those running on prem are also running them in the cloud. Any workable security solution has to span both environments.

More than half of respondents (53%) are running in hybrid mode now compared to our last survey six months ago, in which 40% were running in hybrid mode.

Conversely, the percentage of organizations running containers only on prem has dropped nearly in half (from 31% to just 17%), while cloud-only deployments have remained steady.

These findings indicate that many of the on-prem-only organizations are transitioning to also using the cloud while they continue to run their own infrastructure. With the hybrid model poised to continue to grow as on-prem-only organizations divest from their data centers, a Kubernetes-native container security platform that delivers environment-agnostic controls will be essential.

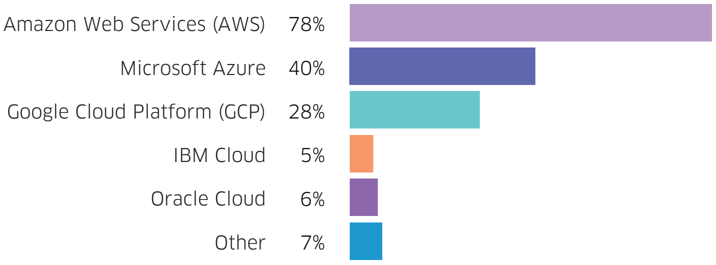
Q: Where do you have containers running?



AWS continues to dominate, but Azure and Google Cloud Platform are catching up.

Amazon continues its market dominance in container deployments, followed by Azure. Google comes in third, and it has gained considerable market share, growing from 18% six months ago to 28% today. We hear anecdotally from many of our customers who are cloud-native companies and SaaS providers that they view Google as a particularly attractive cloud partner given the company's deep expertise in containers and Kubernetes.

Q: If you're running containers in the public cloud, which provider(s) are you using? (pick as many as apply)



> "Google's announcement of Anthos is a clear indication that more and more customers want to adopt the hybrid model and will need a security solution that consistently applies a broad set of controls across different environments. This universal portability is crucial to realizing many of the benefits of containers."

Mark Bouchard
AimPoint Group

The growth in dominance of Kubernetes as the orchestrator of choice is dramatic.

In just six months, the percentage of respondents using Kubernetes has grown from 57% to 86%, a 50% increase.

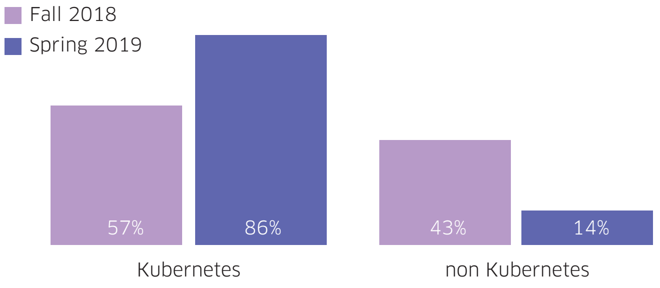
Industry watchers have loudly trumpeted the rapid adoption of Kubernetes – across various deployment modes, including self-managed clusters; managed services such as Amazon EKS, Azure AKS, and Google GKE; and Kubernetes distributions such as Red Hat OpenShift and Docker Enterprise Edition. Just six months ago, close to half of respondents (43%) were not using Kubernetes in any of its forms. In our survey today, only 14% are not using Kubernetes.

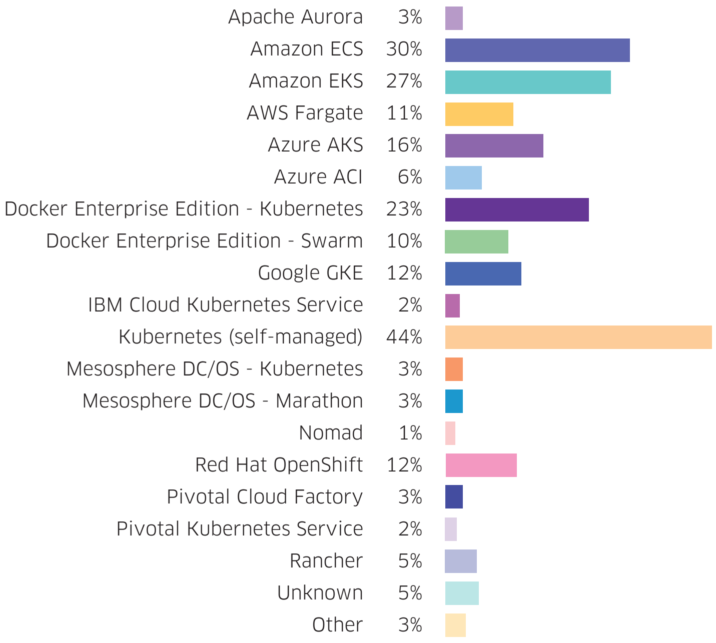
Isolating the responses within the "pick as many as apply" options reveals more detailed findings. More than half (51%) of the respondents who use Kubernetes said they self-manage at least some of their Kubernetes clusters, while 21% use nothing but self-managed Kubernetes.

Nearly a third (31%) of all respondents who use Kubernetes use nothing but a single managed service, while 17% of respondents running Kubernetes use it in a managed form across two or more managed services – and zero unmanaged.

The diverse way Kubernetes is deployed requires an equally portable security solution that spans cloud and on-prem environments as well as self-managed and managed service versions of Kubernetes.

Q: What do you use to orchestrate your containers? (pick as many as apply)

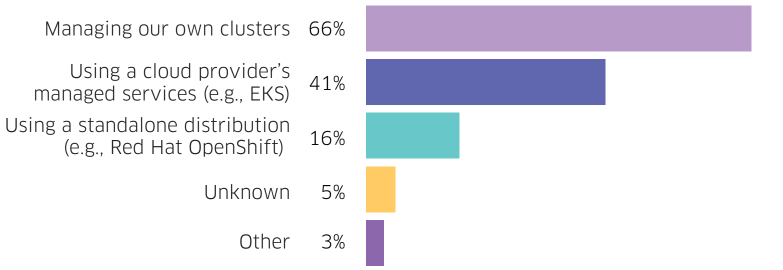




Two-thirds of respondents manage at least some of their own clusters in addition to using a managed cloud service or managed distribution. Digging further into the responses shows that more than 40% of respondents are managing all clusters themselves. Only 20% of all respondents manage their clusters using only a cloud provider's managed service, while only 6% of respondents use just a standalone distribution.

Anecdotal evidence from customer conversations shines a light on why self-managed Kubernetes remains so popular. The earlier findings around hybrid and multi-cloud deployments is related. Several customers have relayed their choice to run native Kubernetes rather than a cloud provider's managed instance so they can maintain consistency in managing all their Kubernetes clusters across multiple environments.

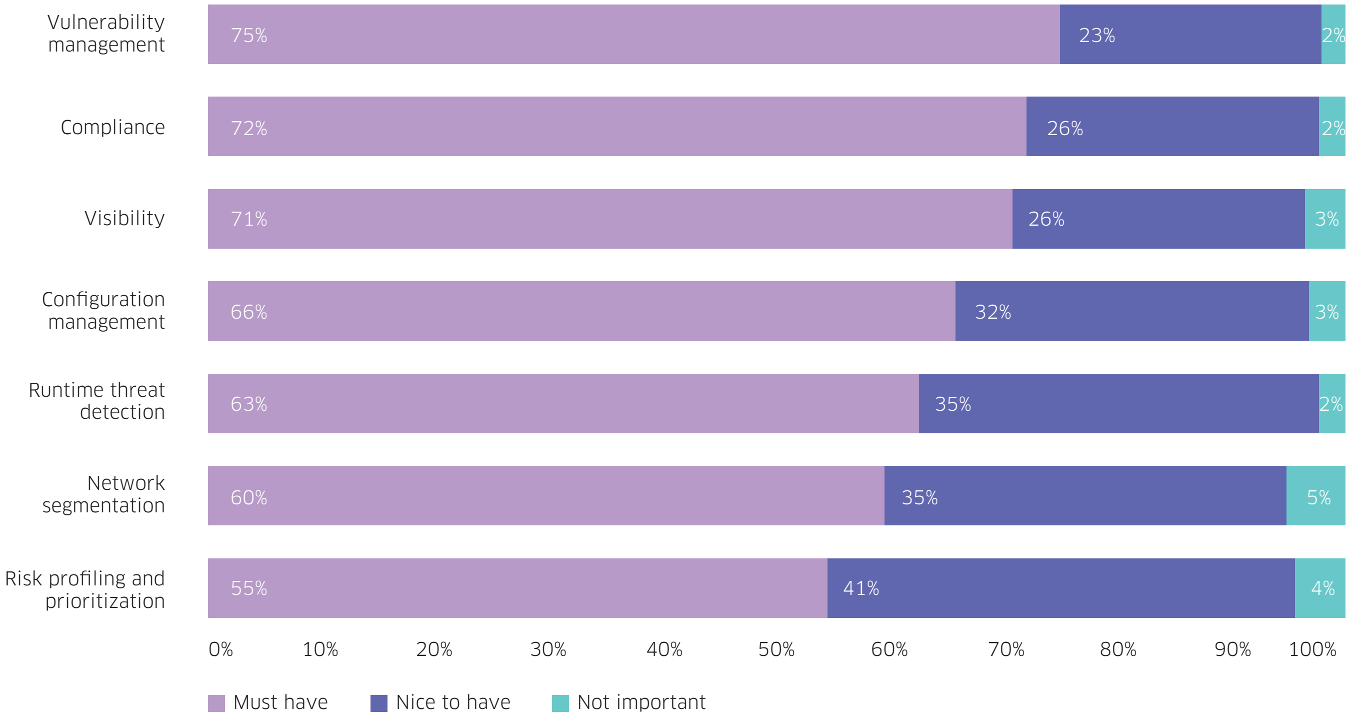
Q: How are you managing your clusters? (pick as many as apply)



Respondents expect very feature-rich container and Kubernetes security platforms.

Respondents put a high value on a broad array of container security use cases, with more than half citing each one as a "must have" capability. This demand for a rich feature set that spans DevOps and security activities shows that organizations expect both broad and deep functionality in their container and Kubernetes security platforms.

Q: How would you rate the importance of the following container security capabilities?



DevOps focus is evident

Vulnerability management beats out compliance and visibility as the top use case, with 75% of respondents citing it as a "must have" capability.

> "As container and Kubernetes deployments have surged, organizations are demanding comprehensive security controls across the full stack and the full software development life cycle. That users deem so many security capabilities as "must have" features demonstrates how critical they view this app dev stack."

Mark Bouchard
AimPoint Group

Top use case requirements map to DevOps and DevSecOps taking lead in managing container security.

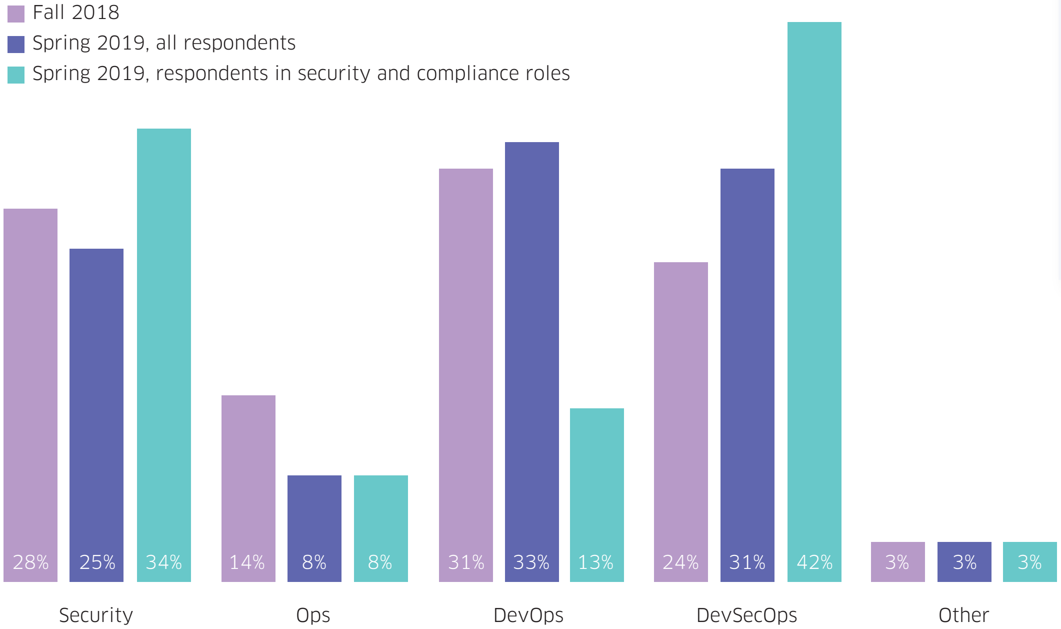
The DevSecOps role takes on increasing prominence in managing container security.

Across all operations roles, the allocation of management responsibility by role remains consistent, but the jump in those citing DevSecOps as the responsible operator for container security is significant. This increase came despite 38% of respondents identifying their role as product development/engineering.

We see an even larger jump in allocation of responsibility to DevSecOps when we isolate responses from those who are in a security or compliance role. Among those respondents, 42% view DevSecOps as the right organization to run container security platforms.

> “This survey shows IT Security professionals find value in designating the specific role of DevSecOps and its responsibility in running container security platforms.”
>
> Mark Bouchard
> AimPoint Group

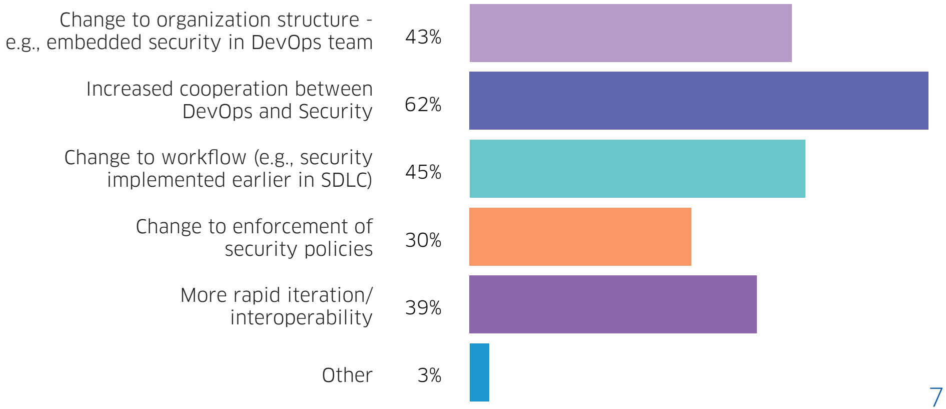
Q. Who will be responsible for operating a container security platform?



The cloud-native infrastructure invites – and demands – closer collaboration between DevOps and Security.

Team names aside, containers and Kubernetes have the power to unify what used to be very separate disciplines. The opportunity to create “security as code” is powerful with the cloud-native stack, but it requires workflows, processes, and security tooling that creates and enables that integration across groups.

Q: How are containers changing how DevOps and Security work together?



Implications for container and Kubernetes security.

The findings in this survey of 392 respondents make clear that organizations are putting at risk the operational benefits of agility and flexibility by not ensuring their cloud-native assets are built, deployed, and running securely. No longer can security be "bolted on" in this world – it must be built in, from the start, and the adoption rates for containers and Kubernetes captured in this survey demonstrate we're well past "the start."

1. Leverage Kubernetes-native architectures and controls.

The rapid adoption of Kubernetes has surprised the entire industry, and tying into the rich data and native controls inherent in the orchestrator provides the basis for stronger security. The context Kubernetes can provide about how your assets are configured and running will enrich your understanding of risk in your environment. Leveraging Kubernetes for admission control, network segmentation, scaling anomalous services to zero, and killing infiltrated pods will enable far better enforcement than layering in separate proxies or shims. Further, that approach will ensure that DevOps and Security share a common source of truth.

2. Implement full life cycle security, from build/deploy to runtime.

Security has long been an afterthought – the last gate before deploying a new application. With containers and Kubernetes, we have the opportunity and responsibility to help developers build good security into their assets right from the start. Look for a container security platform that incorporates DevOps best practices and internal controls as part of its configuration checks, and that it also assesses the configuration of Kubernetes itself so developers can focus on coding.

3. Require portability across the hybrid cloud.

With most organizations deploying containers in both on-prem and public cloud environments, you need security to apply consistently wherever your assets are running. The common element in any deployment is likely to be Kubernetes, so, as Point 1 highlights, making Kubernetes your source of truth, your point of enforcement, and your universal visibility layer is essential to enabling consistent security. Managed Kubernetes services are growing in popularity – ensure you have a strategy for consistent monitoring and control regardless of where your workloads run.

4. Enable a bridge between DevOps and Security.

Given most organizations expect DevOps or DevSecOps teams to run container security platforms, your security tooling must help bridge these disciplines. To be effective, the platform must provide developers with prioritized assessments of which assets need remediation – handing over a list of 48 vulnerabilities will ensure none of them gets fixed, but if your tooling can highlight the five most critical assets to remediate, with a rationale and clear steps to fix it, your security posture will vastly increase.

> "Three findings from this survey really stand out to me. One, organizations are adopting containers and Kubernetes without having mapped out how they'll secure the infrastructure. Two, whatever security approach they adopt must effectively protect that infrastructure in hybrid deployments. Three, effective security approaches must deliver rich capabilities across a broad array of features. Organizations should feel a tremendous sense of urgency to test and deploy container security solutions that will effectively protect their cloud-native apps."

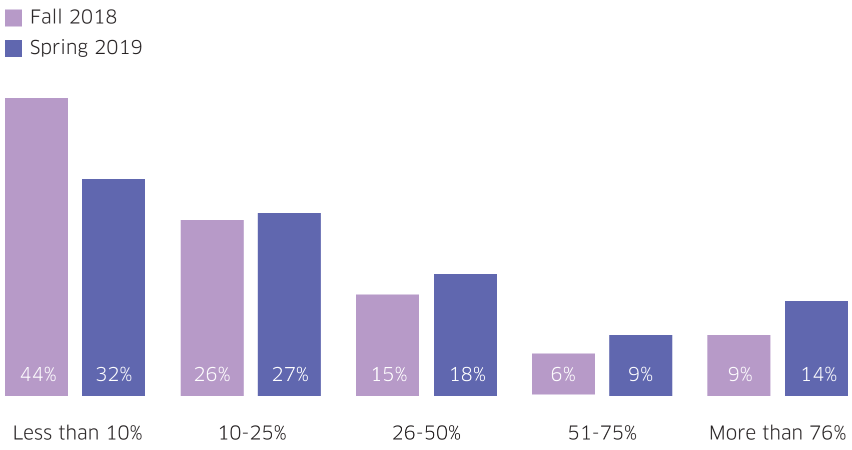
Mark Bouchard
AimPoint Group

About our respondents - containerization rates

In the past six months, organizations have increased the percentage of applications they're containerizing.

In the past six months, the percentage of organizations that containerized more than 50% of their applications has risen from 15% to 23%, a growth rate of 53%. At the same time, the number of organizations that have containerized less than 10% of their apps fell from 44% to 32%.

Q: What percentage of your apps are currently containerized?



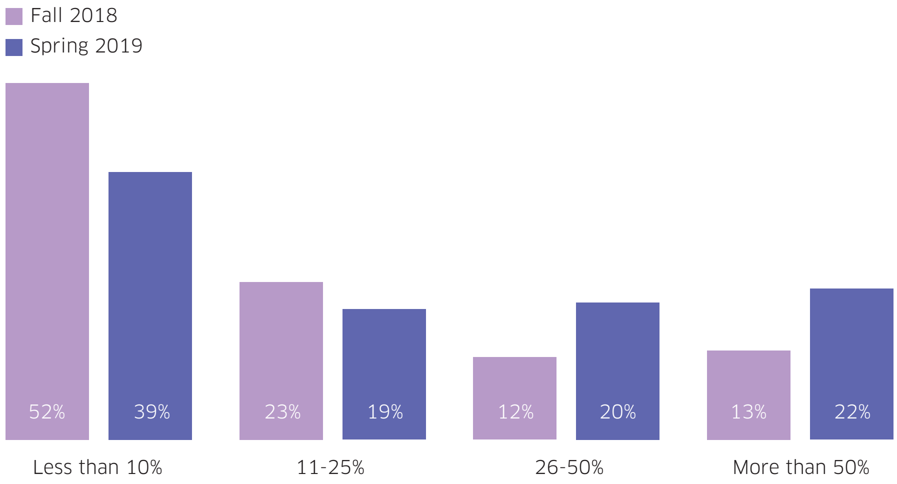
> "Companies need to move past their out-of-date perspective that security matters only once containers are in production. In a DevOps world, security applies even in dev/test, since it's all about building the assets securely."

Mark Bouchard
AimPoint Group

Organizations have far more containers running in production than just six months ago.

The percentage of organizations with more than 50% of their containers running in production has increased from 13% to 22%, a growth rate of 70%. In the same six months, those running less than 10% of their containers in production has fallen from 52% to 39%.

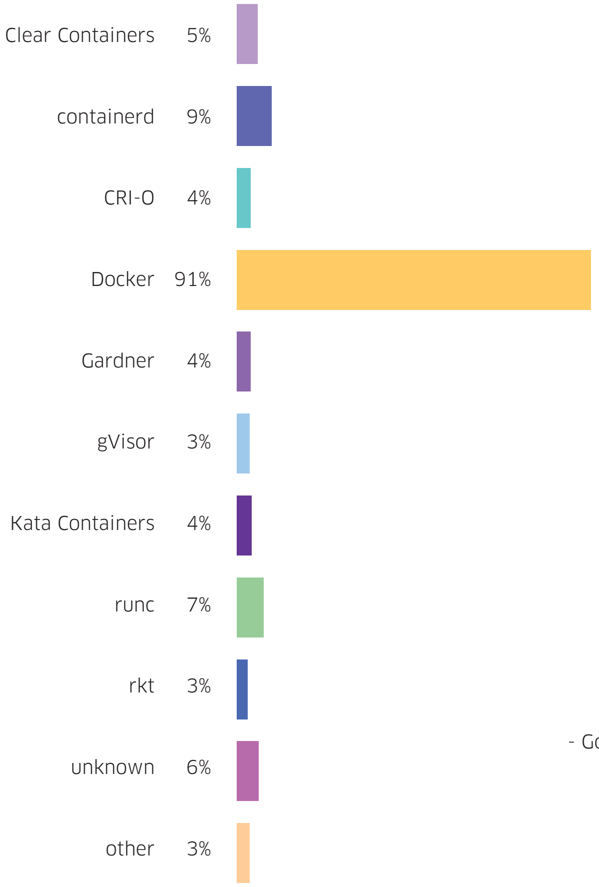
Q: What percentage of your containers are running in production?



About our respondents - technologies being adopted

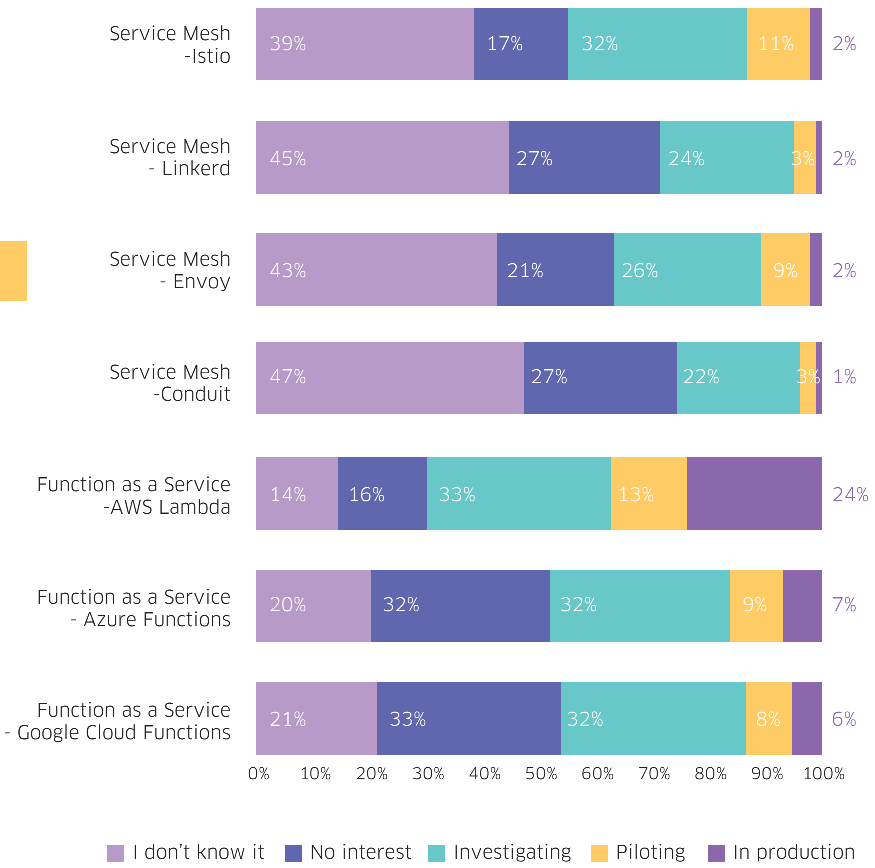
The prominence of the Docker runtime engine has never been more prevalent. Only containerd managed to show more than 5% penetration.

Q. What container runtime(s) do you use? (pick as many as apply)



Emerging cloud-native technologies aren't finding a strong foothold yet. Only AWS Lambda has achieved significant use in production.

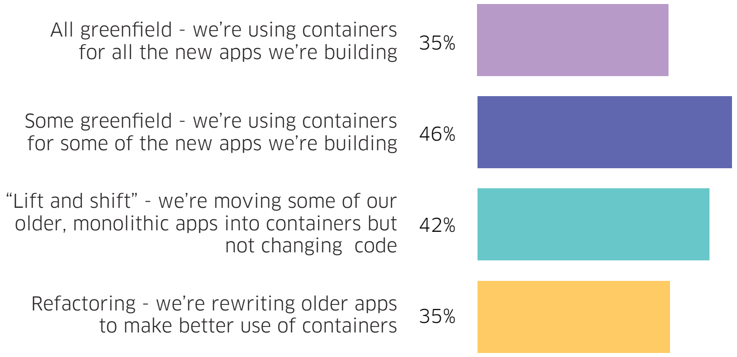
Q: What newer cloud-native technologies are you considering or using?



Organizations are containerizing old and new apps at fairly even rates, which highlights the fact that containers are just as applicable to legacy applications as new ones.

When you think of containerized applications, you might think of next-gen, microservices-based apps. However, much like six months ago, we continue seeing organizations containerize legacy applications. In a move reminiscent of the old "lift and shift" days in the cloud, these organizations are simply taking existing code and putting it into containers. More than a third of respondents are containerizing older apps – with and without code changes.

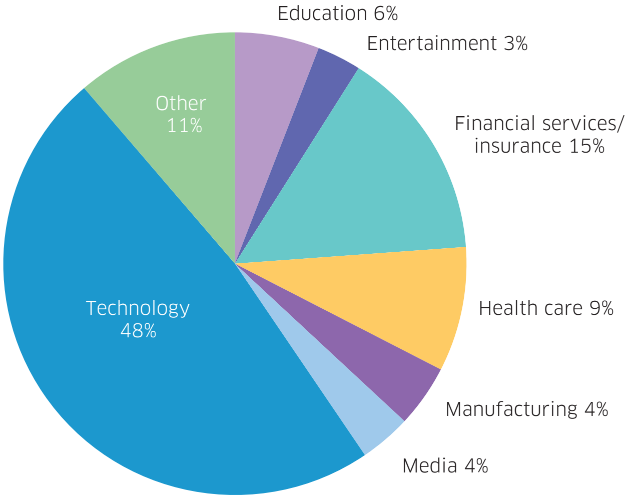
Q: What apps are you containerizing?



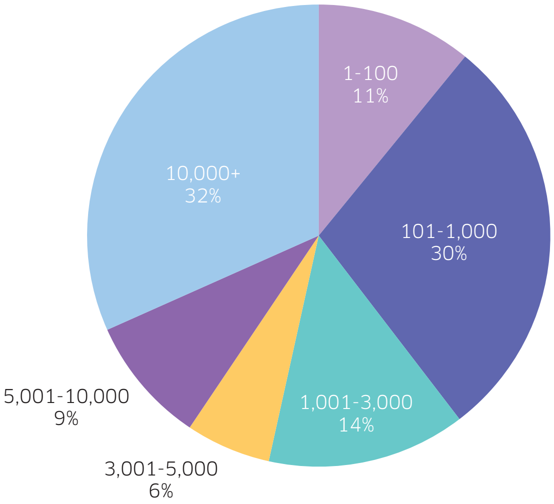
About our respondents - core demographics

More than 390 IT decision makers shared their perspectives for the second edition of this industry-first survey on the State of Container and Kubernetes Security. A quarter of them identify security as their primary IT role, and nearly half work in large companies of more than 5,000 employees. Many pundits associate containers with cloud-native companies – the interesting observation is how many G2K organizations have adopted containers to maintain their competitive edge. It's no surprise that high-tech and financial services companies dominate our survey responders – high-tech companies typically adopt the tech they create, and financial services companies are either next-gen fin-tech companies themselves or needing to innovate fast to keep pace with them.

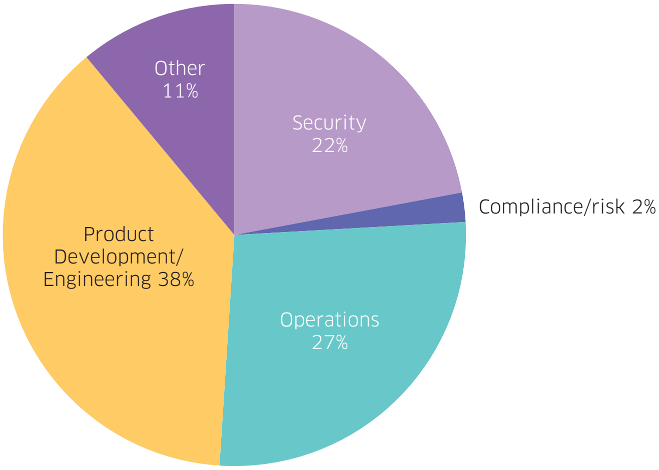
Industry



Company Size



Functional Role



> "The high representation of very large companies in this survey, tied with high adoption rates of containers and Kubernetes, demonstrates the power of this cloud-native stack in enabling business innovation. If the adage has been 'software is eating the world,' the new adage should be 'Kubernetes is eating the software world.' "

Mark Bouchard
AimPoint Group

Eight reasons why Kubernetes-native container security delivers a better outcome

The rapid adoption of Kubernetes as the de facto orchestrator and the growing use of containers in production environments means DevOps and Security teams need a comprehensive security solution that's portable, protects the full container life cycle, leverages Kubernetes' rich context for smarter and scalable policy enforcement, and builds a bridge between DevOps and Security. These teams need a next-gen security solution that's container-native AND Kubernetes-native.

	First Generation	**Next Generation**
	Container-native	Container- and Kubernetes-native
VISIBILITY	Containers, images, and vulnerabilities	Containers, images, and vulnerabilities as well as deployments, clusters, and Kubernetes data
VULNERABILITY MANAGEMENT	Image vulnerabilities	Image vulnerabilities, Kubernetes vulnerabilities
COMPLIANCE	CIS Benchmarks for containers and Kubernetes	CIS Benchmarks for containers and Kubernetes, NIST, PCI-DSS, HIPAA
NETWORK SEGMENTATION	Via third-party proxy	Via Kubernetes network policies
RISK PROFILING	List of vulnerabilities	Prioritized list of risks by deployment
CONFIGURATION MANAGEMENT	Of containers	Of containers and Kubernetes (deployments, network, RBAC, etc.)
THREAT DETECTION	Insights into container activity	Insights into container activity and Kubernetes context
INCIDENT RESPONSE	Isolated actions on containers	Integrated Kubernetes controls

StackRox

StackRox helps enterprises secure their containers and Kubernetes environments at scale. The StackRox Kubernetes Security Platform is the industry's first and only Kubernetes-native container security platform. Its Kubernetes-native architecture enables security and DevOps teams to enforce their security and compliance policies across the entire container life cycle, from build to deploy to runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security. StackRox customers span cloud-native startups, Global 2000 enterprises, and government agencies.

LET'S GET STARTED

Request a demo today!
info@stackrox.com
+1 (650) 489-6769
www.stackrox.com