aqua

2017

Container Security in the Enterprise

SURVEY REPORT

Executive Overview

Containers continue to grow in popularity with developers and DevOps teams as customer-obsessed companies improve user experience and functionality with frequent, agile application releases. Containers enable micro-services with code portability and scalability, while increasing speed for development, testing and release cycles. Containers have the advantage of being portable, running on any modern Linux or Windows system, and supporting a hybrid environment of on-premises and cloud deployments, thus isolating developers from having to anticipate diverse configurations and platforms.

The main business driver behind a new era of container development is the need for agility. Web-scale companies such as Google, Facebook and Netflix have completely changed user expectations and how rapidly applications evolve to meet them. Now enterprises are following suit.

What does this mean for security? Containers bring many potential improvements to enterprise security, but introduce new processes and changes to infrastructure that require a significant shift in focus.

To learn the current state of container security in the enterprise, Aqua Security surveyed 512 individuals meeting the criteria of using containers in development or production today, or planning to use them in the near future.

We wanted to learn what focus areas their organizations consider key for secure use of containers, and understand the governance of securing container environments - who “owns” container security today, and who should ultimately own it going forward. We also examine how people’s views on these topics vary by experience, adoption, role and company size.

Key insights

- **50%** of respondents have one or more container applications in production
- **80%** see room for improvement or dedicated security measures for dealing with security in the container era
- **53%** overall rank vulnerabilities in images and code as a top focus, changing to managing ‘secrets’ for those running multiple apps in production or those who are developers. Those in security roles show an increased focus on network segmentation for containers.
- Larger, more experienced companies with multiple container apps in production place container security in DevOps today, and future ownership in the hands of DevSecOps or Security
- Mid-sized companies with intermediate experience and using containers mainly in development place container security both today and moving forward with Security teams
- Smaller companies showing similar overall adoption levels as mid-sized companies place container security in DevOps today but in the hands of DevSecOps going forward.

There is no one specific model for successfully securing container-based applications – if anything, this survey demonstrates that the market is in flux, with many variants of how organizations view and treat the issue of transforming their security while they adopt containers. However some additional themes surface from the survey. Developers and DevOps have the most experience with containers and are open to migrate future ownership to DevSecOps or Security.   While Security teams desire sole governance of the topic, they have to ‘shift left’ into DevOps and earlier into development processes for their security policies and measures to be effective. Wrapping security controls around container based applications as an afterthought to the DevOps process misses the opportunity.

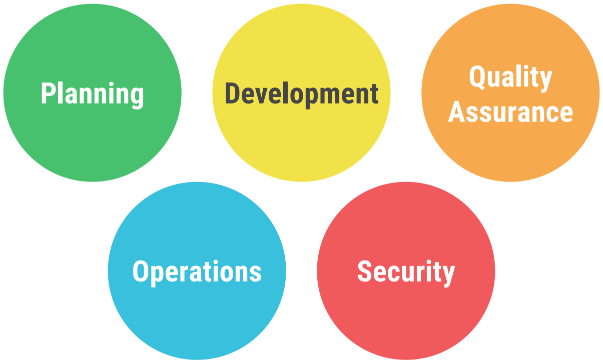
> “The significant change that containers introduce to application delivery and deployment requires a more collaborative approach by security and DevOps teams. Organizations would do well to embed security early into the process, rather than apply security controls after the fact.”
>
> - Doug Cahill, Senior Analyst, Cybersecurity at Enterprise Strategy Group

For the benefits of containers there are security focus areas including trusted images, vulnerabilities, secrets management, host isolation, access privileges, network segmentation and runtime visibility to consider. We invite you to review the complete survey report to learn more details from your peers using or planning to use containers.

DIGITAL BUSINESS AGILITY AT SCALE

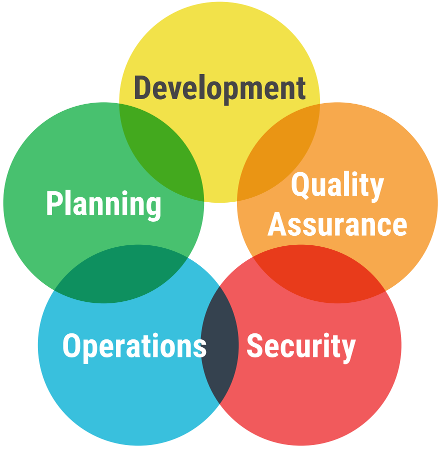
Old School

- Hand offs between each function with little communication in lifecycle
- Specialization within functional areas and expertise become competing factors
- DevOps has ownership while Security has accountability as silos
- Security after the fact to monitor with limited visibility and control
- Business unable to react to digital transformation and improve experience.



New School

- DevOps goal to speed up the lifecycle with efficiencies
- DevSecOps goal to validate the building blocks without slowing the lifecycle
- Ownership and accountability converge within teams, silos break down
- Security embedded from the start increasing compliance
- Business enabled with faster feedback cycles at customer speed.



Challenge – multiple cross-functional teams require people short in supply, especially security.

Solution – automates scanning, testing, deployment and monitoring for scale, aligned to DevSecOps processes, with real-time response capabilities.

Introduction

Container popularity with developers and DevOps teams continues to grow, alongside focus areas for security and the opportunity to evolve into DevSecOps cross-functional teams. Security starts at the beginning with containers, and this provides a ‘shift left’ security proposition into early stage processes for companies. The survey seeks to understand three primary items: focus areas for container security, ownership of the topic today and in the future, and how organizations are assessing their own posture vis-à-vis containers and security. More than technology is required. We need new processes, automation and cross-functional teams working closely with developers and line-of-business owners to integrate security into their container stack and enable a new era of agile and secure deployments.

Survey Methodology & Data Sources

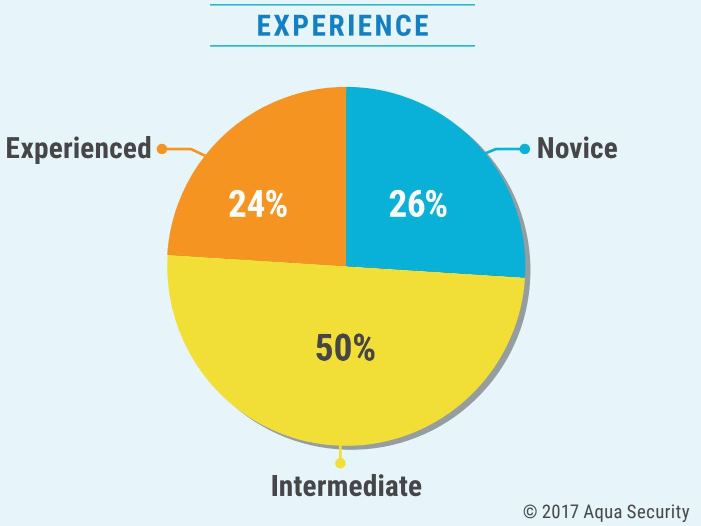
Screening questions were utilized to filter respondents in the online survey to those either using containers today or planning to use them in the near future. This provided 512 peers from various industries, roles, experience, adoption levels, company sizes and geographies. Full details on respondent demographics are provided in the last section of the survey report.

Survey questions include focus areas for container security with multiple choices per respondent, plus questions on current and future ownership, and how companies assess their own container security efforts. The goal is to assess the current state of container security filtered by experience, adoption, role and company size.

Data sources for the 512 respondents include 138 individuals from the 2017 DockerCon NA event held in Austin, Texas and 374 individuals surveyed online.

Experience with Containers

Given the screening questions to participate in the survey, 74% of respondents already have experience with containers and the remaining 26% plan to use containers in the near future. Respondents not using containers today or in the near future were disqualified from taking the survey.   The pie chart below shows respondent self-reported experience and familiarity with containers.



© 2017 Aqua Security

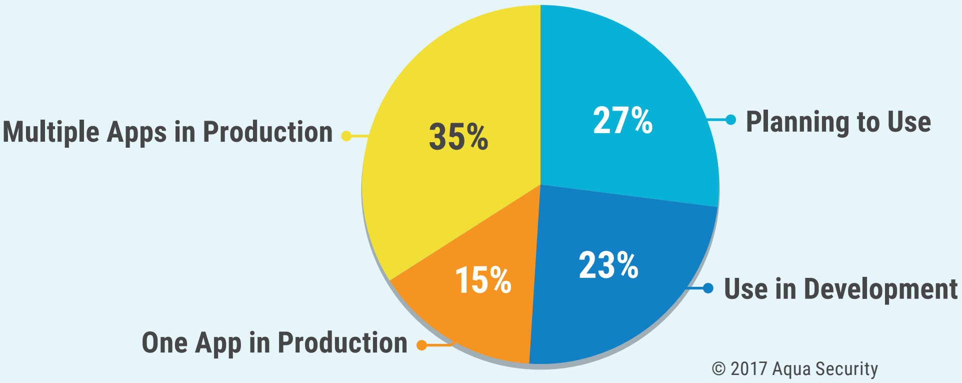
Leveraging experience with containers as a filter surfaces varying degrees of importance for focus areas and prioritization of who owns and should own container security. Details are provided below within each report section for these survey questions.

Note: *When experience level is filtered by company size, small companies have the highest percentage of novices at 36% and mid-sized companies the lowest percentage of experienced users at 15% for this respondent pool. Intermediate experience was the top percentage for each company size range varying from 39-63%. The most experienced level respondents at 34% was for companies with 501-1000 employees.*

Adoption Level of Containers

As noted in the executive summary, 50% of respondents have one or more container-based applications in production as the most advanced adoption levels in the survey. Below is a pie chart representing adoption levels for the 512 respondents.

ADOPTION LEVEL



© 2017 Aqua Security

The table below reflects adoption level by industry categories as a filter. Information Technology was the leading industry represented in the respondent pool followed by BFSI (Banking, Financial Services, Insurance) and the Internet/Telecom/Media category.

ADOPTION LEVEL BY INDUSTRY CATEGORY

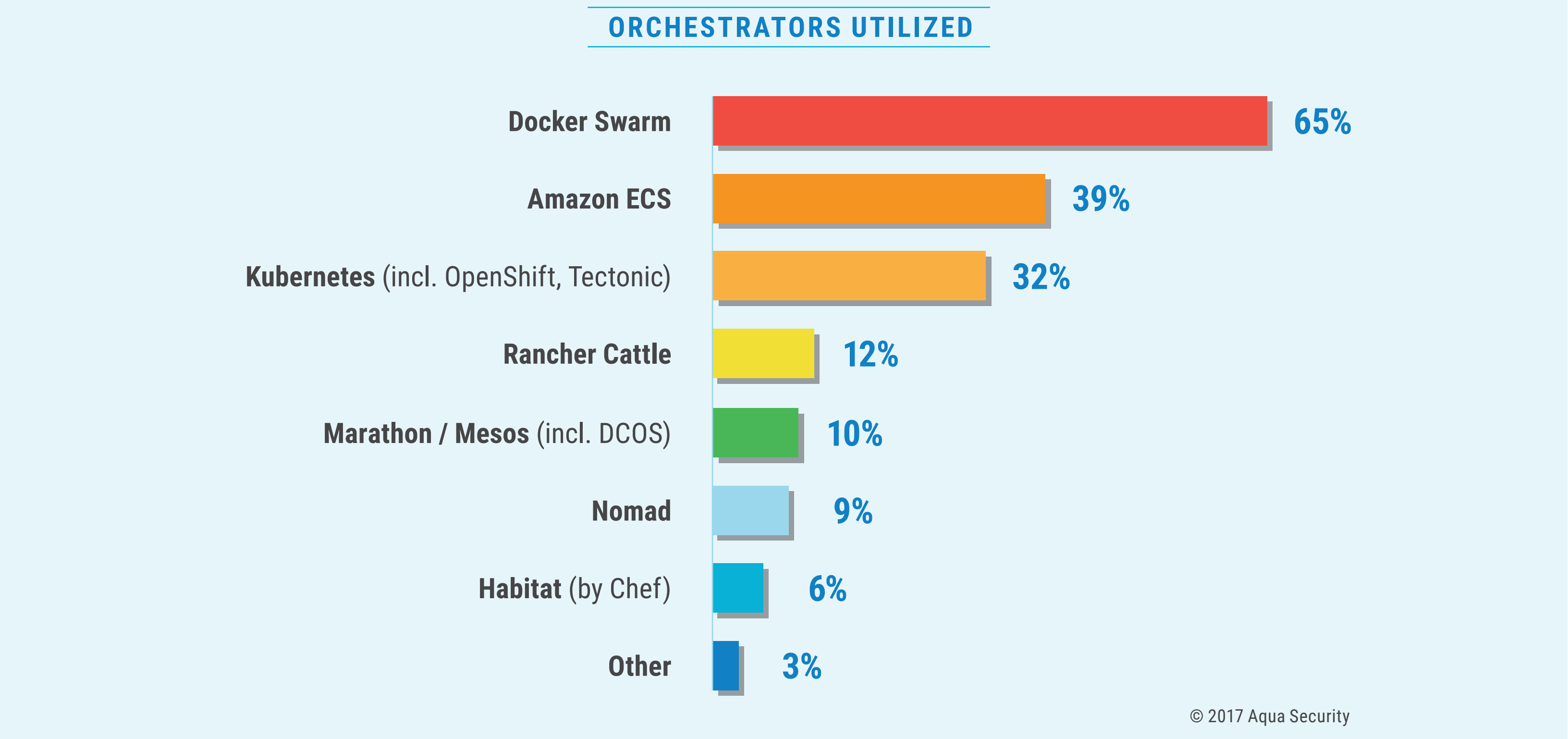
Industry	Plan to Use	Development	One App	Multiple Apps	Total	Percentage
Aerospace & Defense	1	1	2	2	6	1.2%
Agriculture & Mining	1	1	1	0	3	0.6%
BFSI	22	20	17	31	90	17.6%
Business Services	10	4	2	8	24	4.7%
Consumer Goods & Retail	7	8	5	9	29	5.7%
Education & Non-Profit	6	2	3	8	19	3.7%
Energy & Utilities	1	2	1	5	9	1.8%
Government	7	7	5	5	24	4.7%
Health/Pharmaceutical	5	4	5	11	25	4.9%
Information Technology	37	39	17	62	155	30.3%
Internet/Telecom/Media	19	15	9	24	67	13.1%
Manufacturing	15	14	7	11	47	9.2%
Travel	6	4	3	1	14	2.7%
Total	**137**	**77**	**121**	**177**	**512**	**100%**

When adoption level is filtered by experience, the highest experienced use at 57% is for companies with multiple apps in production was no surprise. And as expected, the highest percentage of novices at 47% falls into the ‘planning to use’ category. Adoption level as a filter does show varying degrees of importance for focus areas, plus who owns and should own container security. The details are provided in the sections below for these survey questions.

Container Orchestrators Utilized

Orchestrators schedule container startup and shutdown, often across clusters of servers, and are a key component of any container stack. Below is a table of orchestrators utilized by respondents with multiple choices available.

Note: *Since the DockerCon NA event was utilized as one of the collection methods for this survey, there is a possible bias towards Docker Swarm as an orchestrator.*

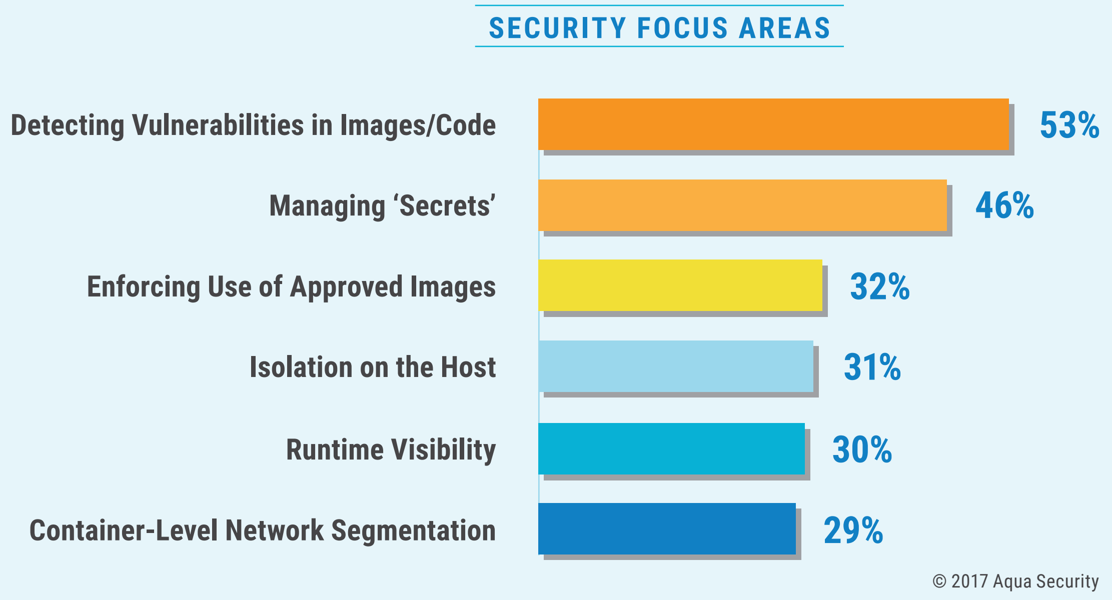


When filtering orchestrators by adoption level, those with ‘multiple apps in production’ using Kubernetes had a 43% representation, significantly higher than their 32% average for all adoption levels.

Security Focus Areas

A primary objective of the survey is security focus areas and filtering them by experience, adoption, role and company size. Learning through peers using containers at various stages, do variances exist for focus areas? Below is a bar chart for focus areas where respondents where open to multiple choices.

Note: *A free text field for "Other" was provided, but didn't yield any meaningful responses.*



When filtering by role, Security respondents rated network segmentation at 40%, a significant variance from Developers at 17% and DevOps at 23% for this focus area. Also when filtered by role, Developers ranked managing 'secrets' at 50% over vulnerabilities in images/code at 44% as an exception to all other roles ranking vulnerabilities first. When filtered by adoption level, those with multiple container apps in production also ranked managing 'secrets' at 58% over vulnerabilities at 54% as another exception. Filtering by company size and experience with containers had no distinct impact on focus area prioritization compared to all respondents in the bar chart above.

Details About Security Focus Areas

Vulnerabilities in Images/Code – purpose-built or open-source containers may contain known vulnerabilities, malicious backdoors, malware or newly discovered vulnerabilities after deployment, putting companies at risk. Old school security scans for vulnerabilities after deployment migrate to new school software delivery with quality gates to continuously scan for vulnerabilities, as containers are being developed, tested and deployed. This is a prime example of the 'shift left' concept for security.

Managing 'Secrets' – containers and micro-services need to talk to each other, such as processing code accessing a database and this requires confidential information such as access credentials, tokens, keys and passwords. These 'secrets' need to be communicated and stored securely as containers may be operating across clusters of servers and hybrid environments. Also, secrets should not be hard coded into container images, exposing them to those with approved or illegitimate access.

Enforcing Use of Approved Images – due to the ease with which images can be downloaded from public registries and used by developers, enterprises must enforce the use of trusted images, have them digitally signed and tracked throughout their lifecycle.

Isolation on the Host – containers run native on hosts, they are not VMs with their own OS environment and therefore require namespace isolation to limit interactions between containers and the shared kernel of the host OS. Containers should not have root access. The host itself should also be analyzed for vulnerabilities, patches and hardened. Additionally, identity access management (IAM) and privilege access management (PAM) tools should be utilized for user and administrator access leveraging two-factor authentication for privileged access.

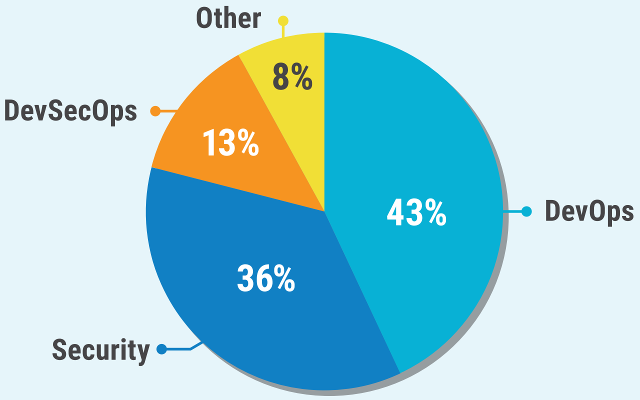
Runtime Visibility – beyond preventive measures to detect vulnerabilities and signing approved images, what happens during runtime with containers is vital to understand what is effective, working or broken. Visibility comes in many forms, one being deterministic for known policy issues and then another for behavior analysis for the unexpected. Traditional security monitoring tools lack visibility for containers; they are likely to only detect the container environment and runtime itself.

Container Network Segmentation – restricting the network connectivity of containers is crucial to limit the "blast radius" in case of an attack or a compromised container, but is challenging due to the ephemeral and portable nature of containers, which are not tied down to specific IPs or hosts. Basic network security is insuffienct, as it lacks container-level visibility and application context that would allow it to prevent suspicious connections while permitting legitimate ones.

Who Owns Container Security Today?

A secondary objective of the survey was to understand who owns container security today and to filter these results by experience, adoption, role, and company size. Containers provide an opportunity for security to be involved in DevOps for the security concerns reviewed in the section above, as noted earlier this involvement is called ‘shift left’ into early stage processes for security teams. So where container security exists today sets the stage for its future ownership in the next report section. Below is a pie chart on container security ownership today for all 512 respondents.

WHO OWNS CONTAINER SECURITY TODAY



© 2017 Aqua Security

Filtering by **experience level** surfaces the following for container security ownership today:

- **52%** of experienced responses note container security with DevOps
- Intermediate responses ranked Security at **42%** and DevOps and **39%**
- **44%** of novice responses note container security with DevOps.

Filtering by **adoption level** surfaces the following for current ownership:

- Planning to use respondents are almost evenly split with DevOps at **40%** and Security at **39%** for current ownership of container security
- **47%** of those with multiple apps in production note DevOps own container security today.

Filtering by **role** surfaces the following for current ownership:

- Architects are split **40%** for both DevOps or Security owning container security today, however they favor Security going forward as shown in the next report section
- **53%** of Developers note DevOps own container security
- **61%** of DevOps note they own container security
- **65%** of Security roles state they own container security, the highest percentage for this question when filtered by role.

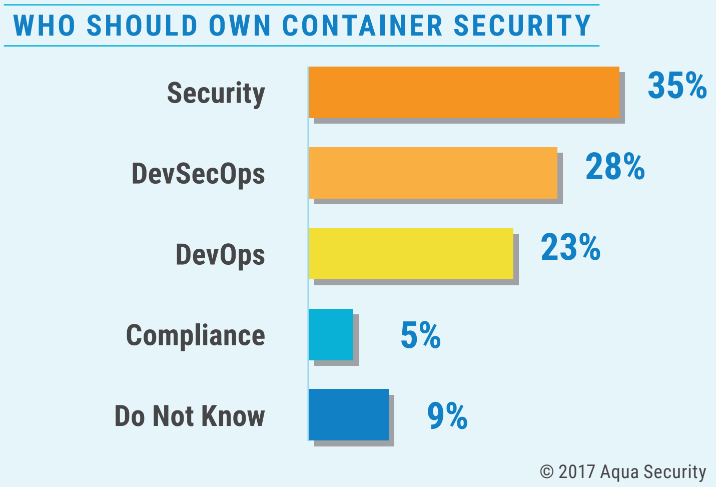
Filtering by **company size** surfaces the following for current ownership:

- **42%** of the largest organizations have container security in DevOps
- **56%** of the smallest organizations have container security DevOps
- **51%** of mid-sized firms place ownership today with Security

Overall the filters show larger, experienced companies with multiple apps in production have container security in DevOps today, while mid-sized companies with intermediate experience place ownership with Security. The security role filter shows that Security has the most polarity for ownership at 65% followed by DevOps at 61%. DevSecOps was not significant overall or using filters for current ownership.

Who Should Own Container Security?

A third objective of the survey is to understand the future ownership of container security and to filter results by experience, adoption, role and company size. In these results we see DevSecOps taking a role in container security and by nature of the acronym 'DevSecOps', Security 'shifts left' into DevOps processes to address security concerns in cross-functional teams with automation and quality check gates. On the following page is a bar chart of who should own container security for all 512 respondents where Security moves into the first position and DevOps ranks third after DevSecOps.



© 2017 Aqua Security

Filtering by **experience level** surfaces the following for future ownership of container security:

- Experienced respondents favor DevOps at **34%** and Security at **30%** for future ownership
- Intermediate experience favors Security at **40%** and DevSecOps at **28%** for future ownership
- Novice experience levels had the highest future ownership support for DevSecOps at **31%**.

Filtering by **role** surfaces the following for future ownership:

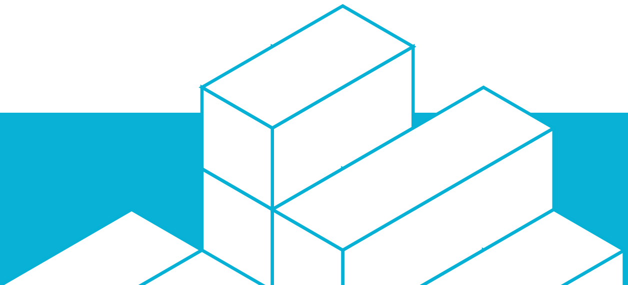
- While Architects are evenly split at **40%** between DevOps and Security for current ownership, they favor Security at **36%** and DevSecOps at **29%** going forward for ownership
- Developers favor DevOps at **30%** for future ownership
- DevOps favors DevSecOps at **37%** for future ownership
- Security favors itself at **55%** going forward for container security, a decline from their **65%** response for current ownership.

Filtering by **adoption level** surfaces the following for future ownership:

- Respondents with multiple container apps in production are evenly split at **33%** for DevSecOps or Security owning container security
- **39%** of respondents with a single app in production favor Security future ownership
- **33%** using containers in development favor Security future ownership along with **35%** planning to use containers.

Filtering by **company size surfaces** the following for future ownership:

- **34%** of the largest and **32%** of the smallest organizations migrate container security to DevSecOps for future ownership
- **46%** mid-sized organizations migrate container security to Security.



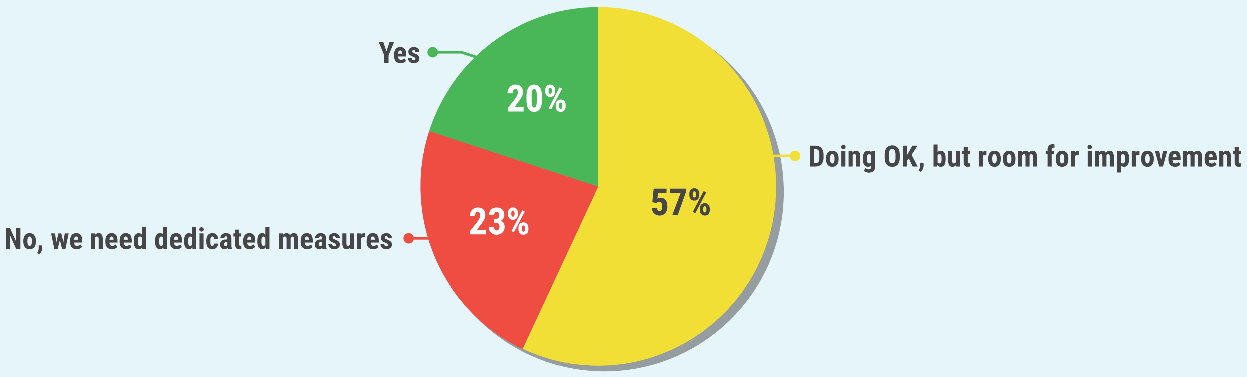
As noted in the executive summary, there is no one model for container security success. Security or DevSecOps have future roles in container security, and variances do exist from the filters. DevOps could be considered a transition state into DevSecOps, alongside maturing processes and automation to integrate security scans and check gates into the early stages of a new era of application development with containers. Security should partner with development and operations for success, as security is part of each container from the beginning.

Gartner "A complete strategy for container security must cover the entire life cycle of containers from creation into production and then back into development again for updates, patches and modifications – i.e., container life cycle protection."[1]

How is Your Organization Handling Security for Containers?

How companies manage change is key to their success and this question from the survey measures the current state of how well they are coping with securing their container environments.

COPING WITH CONTAINER SECURITY



© 2017 Aqua Security

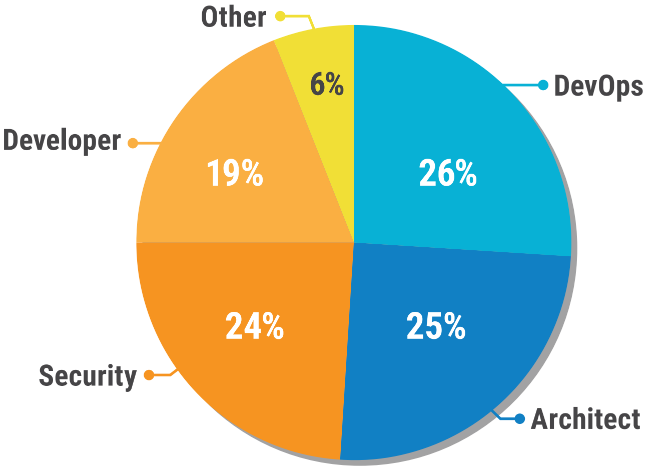
The net is that 80% see room for improvement or need dedicated measures to handle container security adequately. As expected, the companies with less experience or were planning to use containers, or respondents with Architect roles were more likely to respond 'no' this question. The confident 'yes' replies came from larger companies or with multiple container apps in production resulting in higher experience levels or led by Security roles.

[1] Gartner, Security Considerations and Best Practices for Securing Containers, Neil MacDonald, 10 November 2016

Respondent Demographics

The following bar chart shows the role for the 512 respondents in the survey.

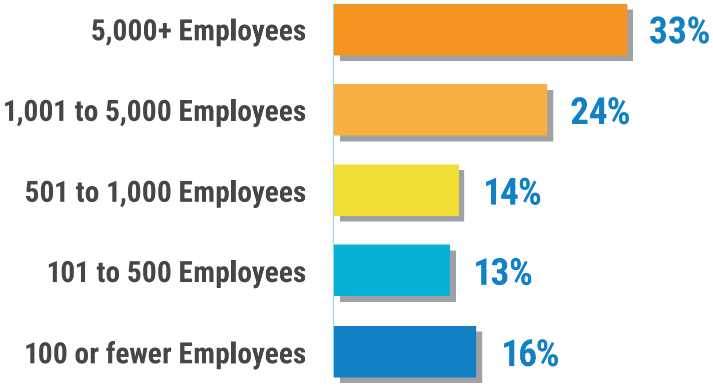
RESPONDENT ROLE



© 2017 Aqua Security

The following bar chart shows company size by the number of employees in sizing ranges.

COMPANY SIZE

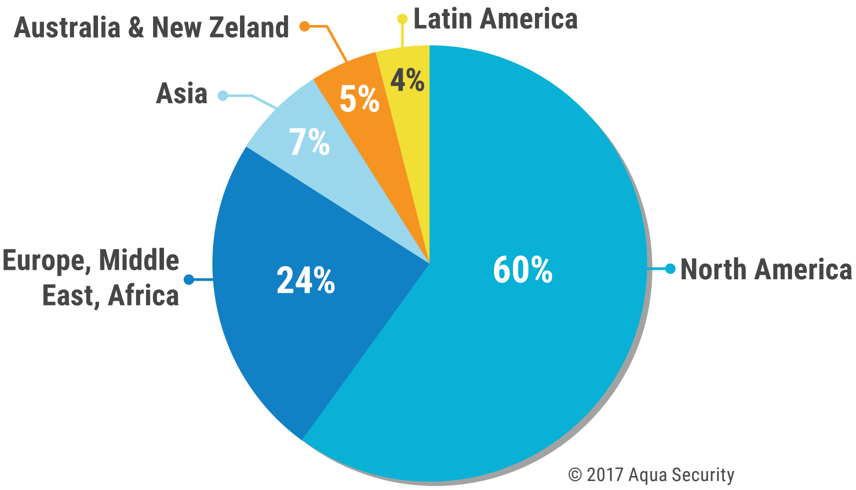


© 2017 Aqua Security

The following pie chart shows respondent geography.

Note: *One of the data sources was DockerCon NA held in Austin, Texas adding a bias for North America.*

RESPONDENT GEOGRAPHY



© 2017 Aqua Security

Survey Data Sources

There were two primary data sources for this survey as follows:

- 2017 DockerCon NA Event held in Austin, Texas April 17-20th (**138 respondents**)
- Email Surveys from Aqua Security during from May to August of 2017 (**374 respondents**)

Respondents were screened to identify those using containers today or planning to use them in the near future.

About Aqua Security

Aqua Security enables enterprises to secure their container-based applications from development to production, accelerating container adoption and bridging the gap between DevOps and IT security. Aqua's Container Security Platform provides full visibility into container activity, allowing organizations to detect and prevent suspicious activity and attacks in real time. Aqua was founded in 2015 and is backed by Lightspeed Venture Partners, Microsoft Ventures, TLV Partners and IT security leaders, and is based in Israel and San Francisco, CA. For more information, visit www.aquasec.com or follow us on twitter.com/AquaSecTeam.

Gartner Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.