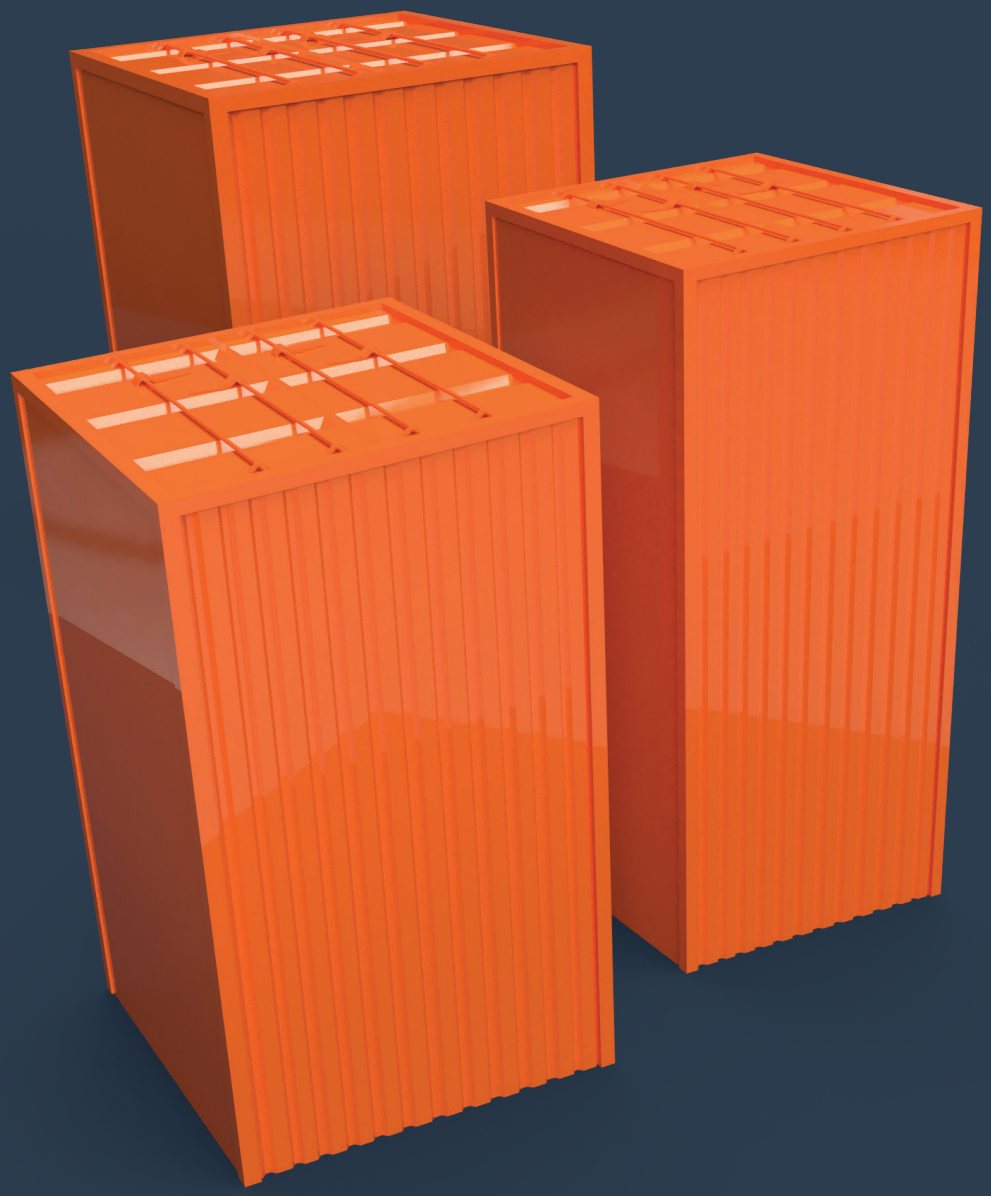
2019 Container Adoption Survey

Presented by Portworx and Aqua Security



portworx

aqua

Executive Summary

It has been nearly 5 years since Kubernetes was launched in June 2014. Docker may have kicked off the container revolution but it was the launch of Kubernetes that accelerated containerization into the enterprise. Portworx has conducted an annual Container Adoption Survey for the last three years (2016, 2017, 2018) in order to understand the direction of the container market seen through the eye of businesses and users. This year, Portworx and Aqua Security joined forces to understand container adoption with a special focus on container security.

This year's survey tells a story of unabated growth in containerization with over 87% of respondents stating that they are running container technologies up from only 55% in 2017. Of those running applications in containers, nearly 90% are running them in production, up from 84% last year and 67% in 2017.

The shift towards production workloads has been accompanied by an increased financial investment on the part of companies. 24% of respondents reported investing over half a million dollars a year on container technology. 17% of respondents spent over one million dollars a year, up from less than 10% in 2017. This speaks to an ecosystem full of innovation worth investing in.

The nature of data challenges with containers has also shifted over the years since this survey began as businesses move from development stages to production. Notably, while persistent storage was the top challenge to container adoption in 2017, it is no longer in the top 3. Data management (40%), however, and multi-cloud/cross datacenter support (36%) were often cited as challenges by respondants.

When asked to name their top three storage challenges, respondents most frequently cited data security (56%), concerns about data loss (46%), and planning for DR and business continuity (40%).

The decrease in customers reporting problems with persistent storage is not surprising given the amount of work the Kubernetes ecosystem has invested in storage fundamentals like CSI (Container Storage Interface). However, as customers move to production, they need more than just persistence to run mission-critical applications. Data security, disaster recovery, and multi-cloud operations are all critical components indicated by users.

This year's survey asked more questions about container security and the responses are also indicative of an increase in complexity of applications deployed in containers compared to previous years, as well as a continuing lack of clarity around organizational security responsibility.

Methodology

The 2019 survey was distributed in May 2019 by independent market research firm Market Cube and includes insights from 501 IT pros who were asked questions about the state of container usage, tooling, environments and barriers to adoption to get a snapshot of container adoption today. In order to achieve the most relevant responses, survey participants were asked a number of screener questions to ensure that they were part of the IT department, were familiar with both their company's IT strategies and financial investments, and worked for a company with at least 500 employees. The 2019 survey asked many of the same questions included in previous Portworx Container Adoption survey to create a multi-year dataset that we can use to draw conclusions on how container adoption has changed over time.

First, data security tops the list of security challenges with a super majority of respondents (61%) listing this as their top security challenges. This is not surprising given how much of a target data is for a variety of bad actors and its overall importance to modern enterprises. Companies, however, were also concerned with vulnerability management (43%) and runtime protection (34%).

When it comes to data security specific concerns, data protection and backup (46%) topped the list, with data encryption (21%), and detecting and preventing data exfiltration (19%) rounding out the top three.

To deal with these security concerns, enterprises are employing a host of strategies. Data encryption is the overwhelmingly top security strategy (64%), however, respondents also use runtime monitoring (49%), vulnerability scanning in registries (49%), vulnerability scanning in CI/CD pipelines (49%), and blocking of anomalies through runtime protection (48%).

When asked which team bears the main responsibility for container security, most (31%) named the organization's security team, with a joint responsibility or DevSecOps in second place (24%). However, respondent roles influenced the responses, with 47% of DevOps respondents naming DevSecOps as the main owner, while 54% of Security respondents named Security as the main owner. This split manifests the confusion and lack of clear security governance for containers, with each team attributing more responsibility to itself than the others - which is better than the opposing alternative of evading responsibility.

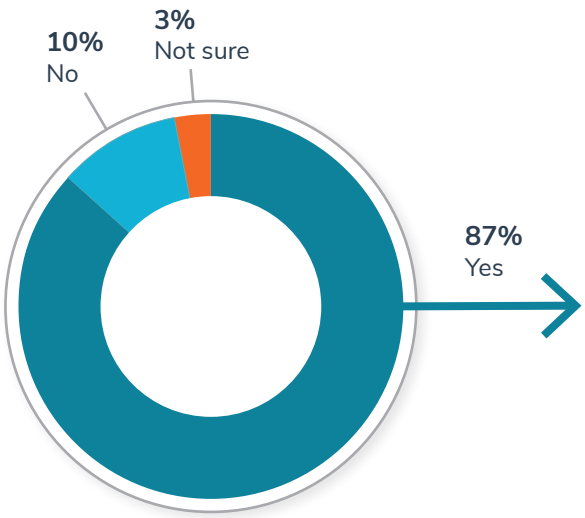
We hope this years survey provides you with insights into how the industry in general and your peers in particular are adopting containers. Until next year.

Container adoption continues to grow year over year

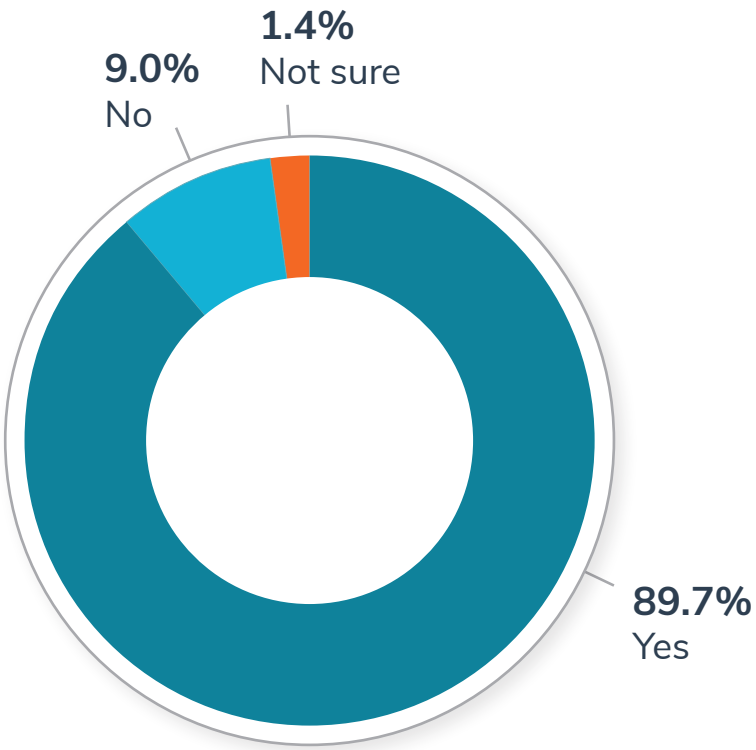
This year, over 87% of respondents said that they were running container technologies—a remarkable increase from two years ago year, when just over half (55%) said they were running container technologies. This percentage is also up from 80% in 2018. Of those running applications in containers, nearly 90% are running them in production, up from 84% last year.

Not only are more companies running containerized applications, they are running a greater percentage of their applications in containers with 71% of respondents reporting that they are running at least 40% of their application portfolio in containers. This is up from 65% in 2018 and 40% in 2017.

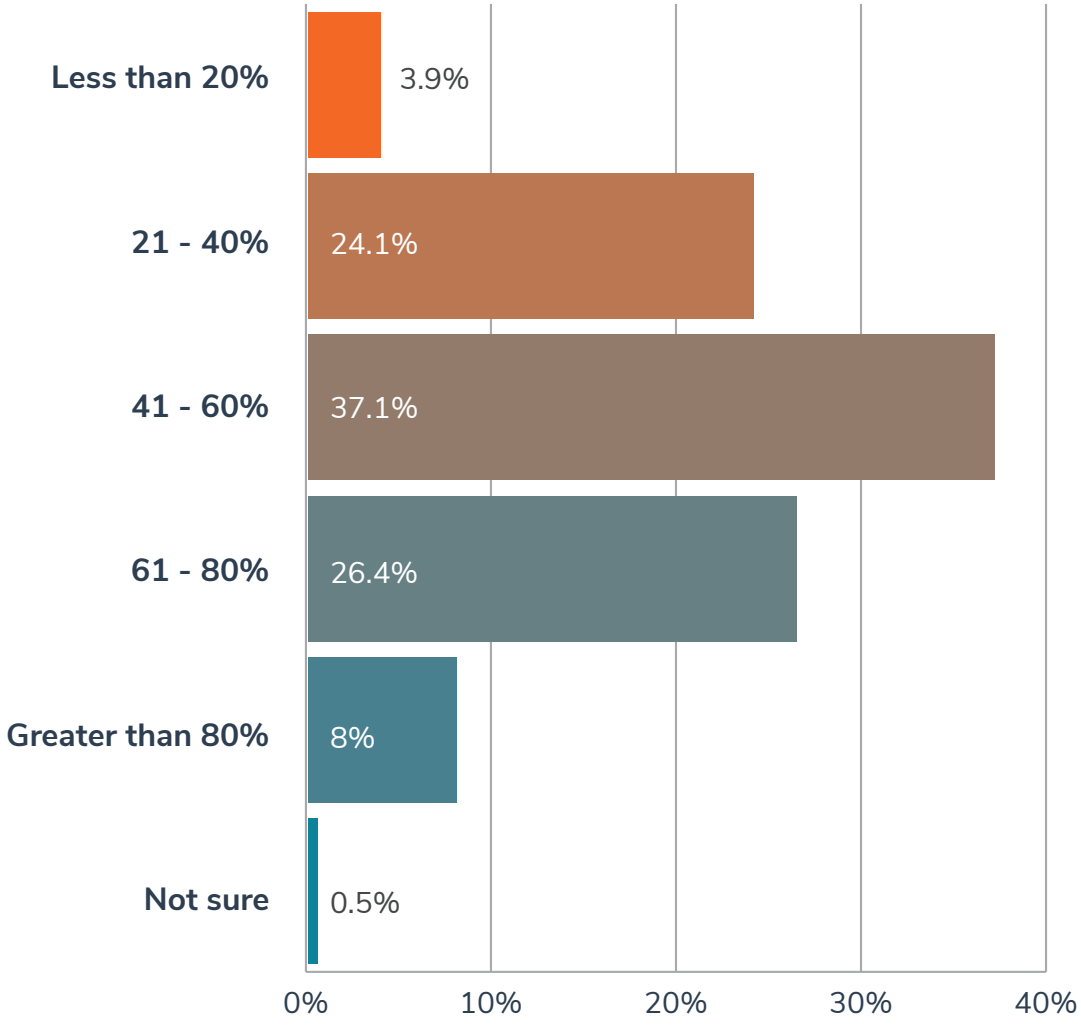
Does your organization run container technologies?



Does your organization run container technologies **in production**?



What percentage of your apps are running in containers?



Container Adoption is about driving developer efficiency

For the third year in a row, increasing developer speed and efficiency is the primary driver of container adoption with 37% of respondents listing it as the top benefit. 20% listed increased agility and 19% listed improvements in the ability to run on multiple clouds and avoid vendor lock-in.

What is the primary reason why your organization is running container technologies?

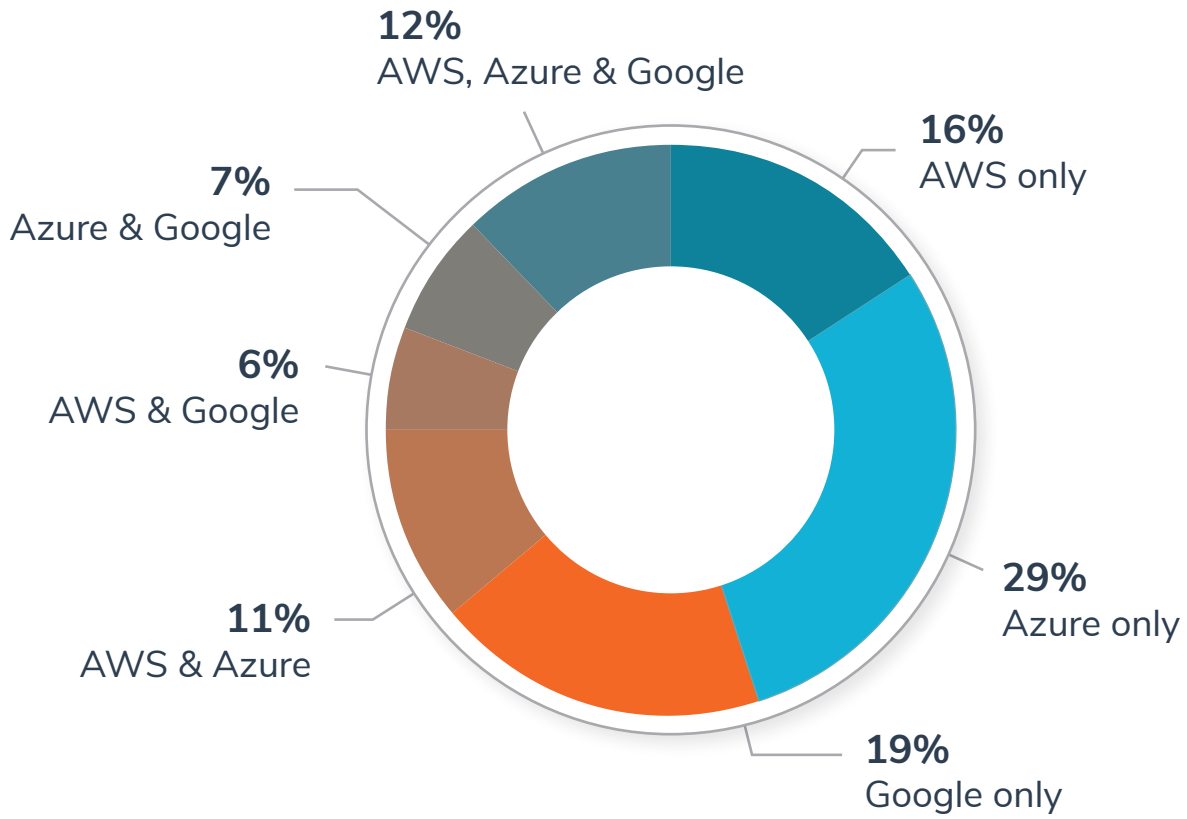
- **37%** Increase developer speed and efficiency
- **20%** Increase agility
- **19%** Enable users to run on multiple cloud platforms (avoid lock-in)
- **14%** Save on infrastructure costs
- **10%** Support microservices architectures
- **0%** Other

Multi-cloud is real and present today

One out of three respondents (36%) reported running on at least 2 of the 3 major public clouds, with 12% of the sample running on all three: AWS, Google and Azure. As the major cloud providers compete to offer hybrid cloud offerings based on Kubernetes, we expect the number of companies running in multiple clouds to grow.

Additionally, there seems to be a preference for multi-cloud operations in larger companies. Of those respondents saying that they ran only in a single cloud, 47% worked at companies with greater than 2,500 employees. However, of those saying they run in multiple clouds, 55% work in companies with greater than 2,500 employees.

Which of the following cloud providers do you currently use to run containers?

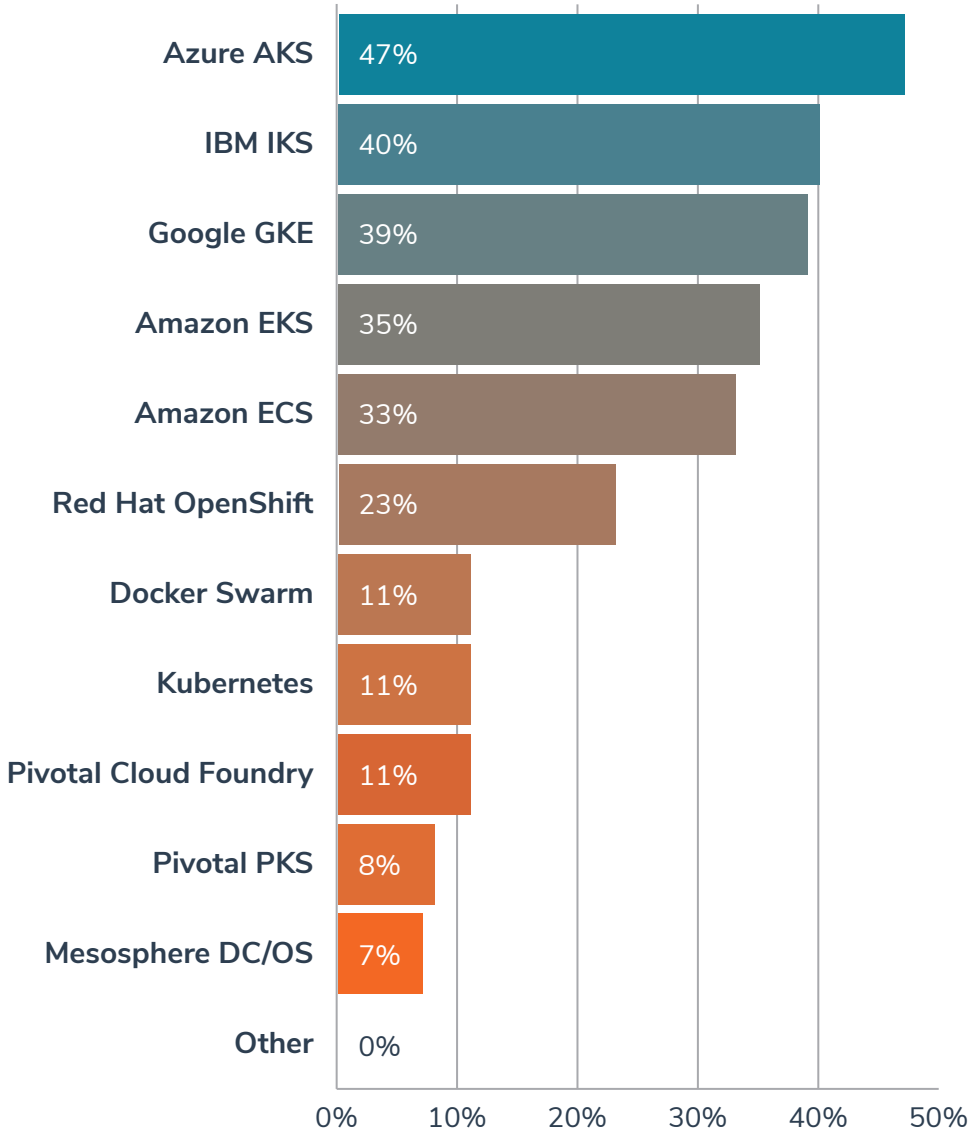


Kubernetes rules orchestration but companies need help to run it

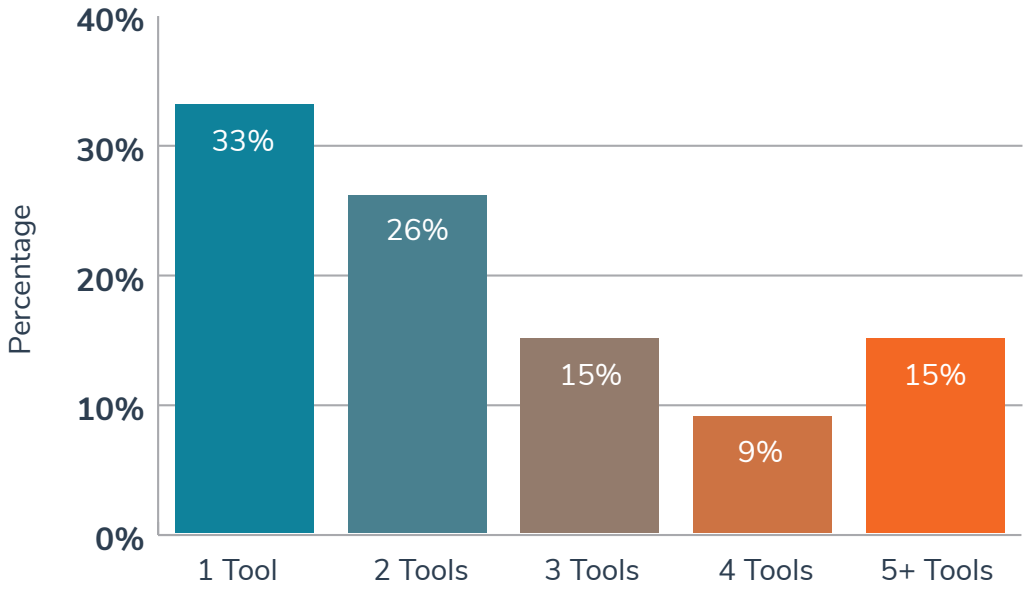
It is no surprise that Kubernetes continues to be the leading container orchestration solution on the market. Given an opportunity to name the container schedulers that they use, respondents most frequently named flavors of Kubernetes, whether that be pure open-source Kubernetes, or a vendor-specific Kubernetes offering like Azure AKS, Google GKE, IBM IKS, or Red Hat OpenShift.

The most popular single option for running Kubernetes was Microsoft AKS (47%), followed by IBM IKS (40%), Google GKE (39%) and Amazon EKS (35%). However, most customers cited using multiple tools, with 65% of the sample using at least two orchestration tools and 15% of the sample reporting the use of five or more tools. Together with the data on multi-cloud adoption, these results indicate that container users are not only adopting a single platform or cloud as they seek to avoid vendor lock-in while simultaneously increasing developer efficiency and agility.

Which container orchestration tools do your organization use?



Number of Orchestration Tools Used

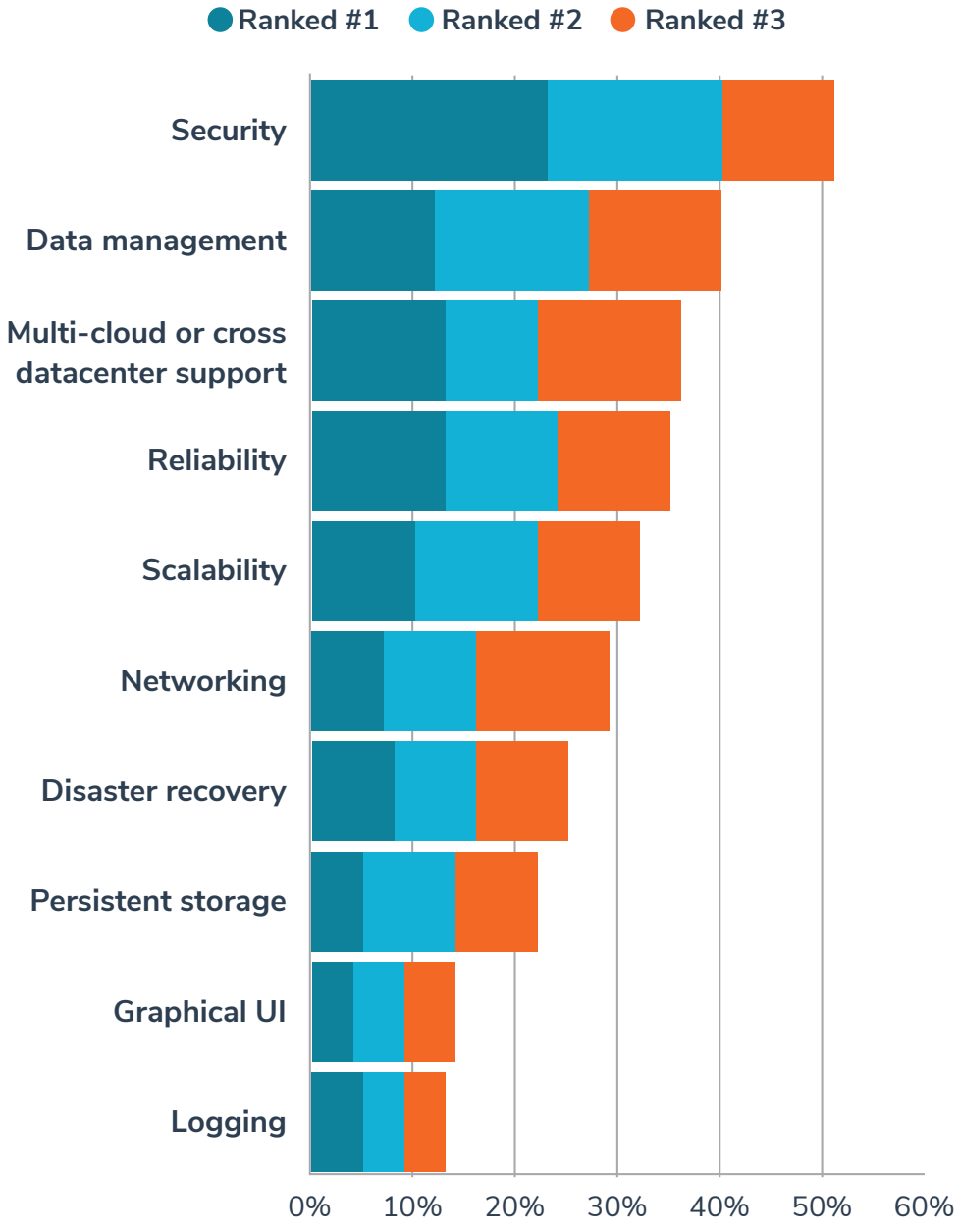


Security and data management top container challenges

When asked about their top challenges to deploy containers, security was listed as the most frequently reported challenge, at 51% of respondents top three challenges. This is down slightly from last year when security was listed by 56% of the sample as the top challenge.

Persistent storage, the top challenge of respondents in 2017, fell to number eight this year, however data management comes in at number two. This indicates that as the cloud native storage and container markets progress, higher level challenges (data management) replace lower level challenges (persistent storage). Multi-cloud or cross-data center support round out the top three most common challenges.

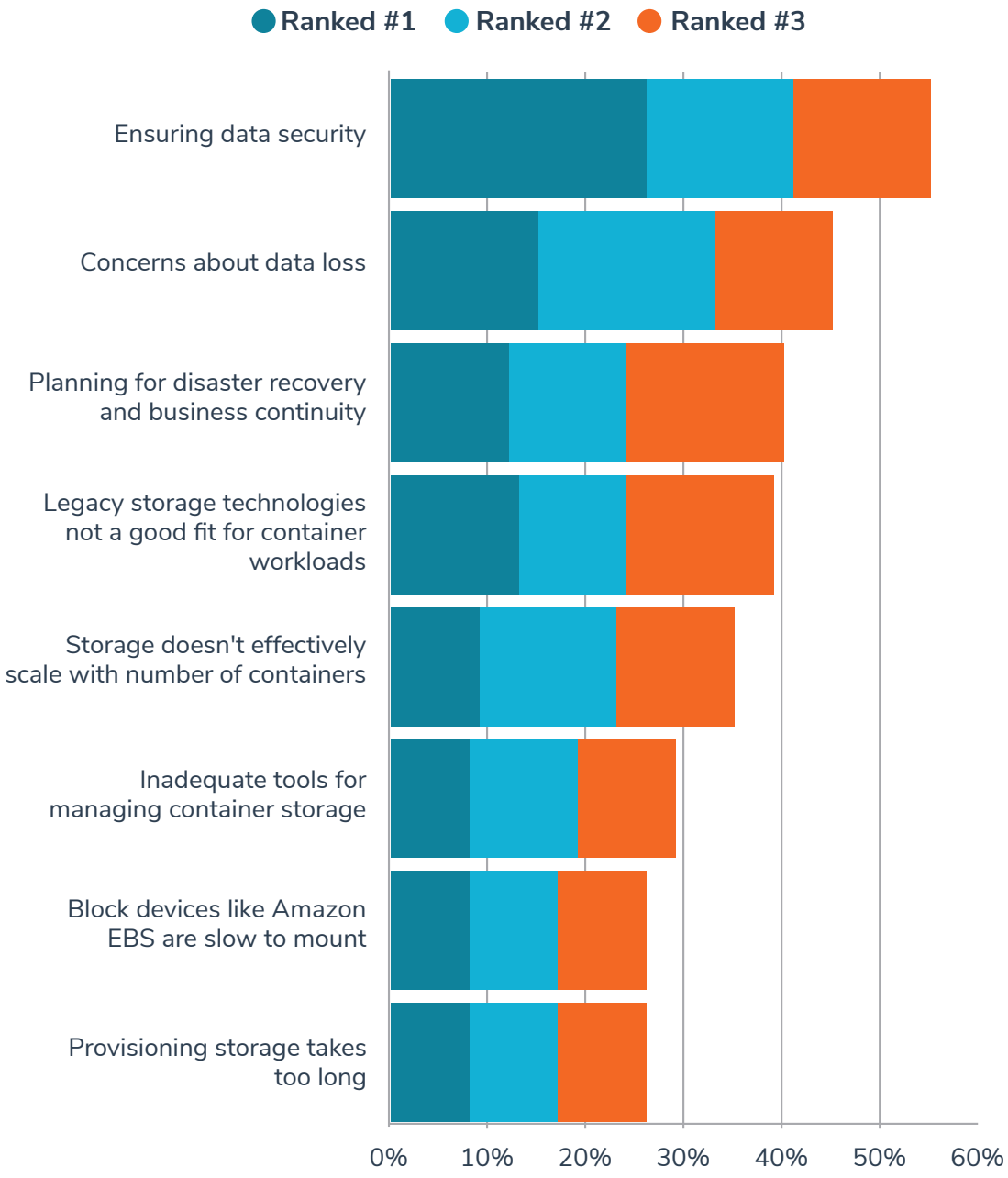
In order to deploy containers, which challenge has been the most difficult to overcome? Rank up to 3.



Data security, data loss, and DR top list of storage related challenges

When asked to name their top three storage challenges, respondents most frequently cited data security (56%), concerns about data loss (46%), and planning for DR and business continuity (40%). These responses provide further evidence to support the conclusion that as the container ecosystem matures, lower level challenges around persistent storage are replaced by higher order challenges.

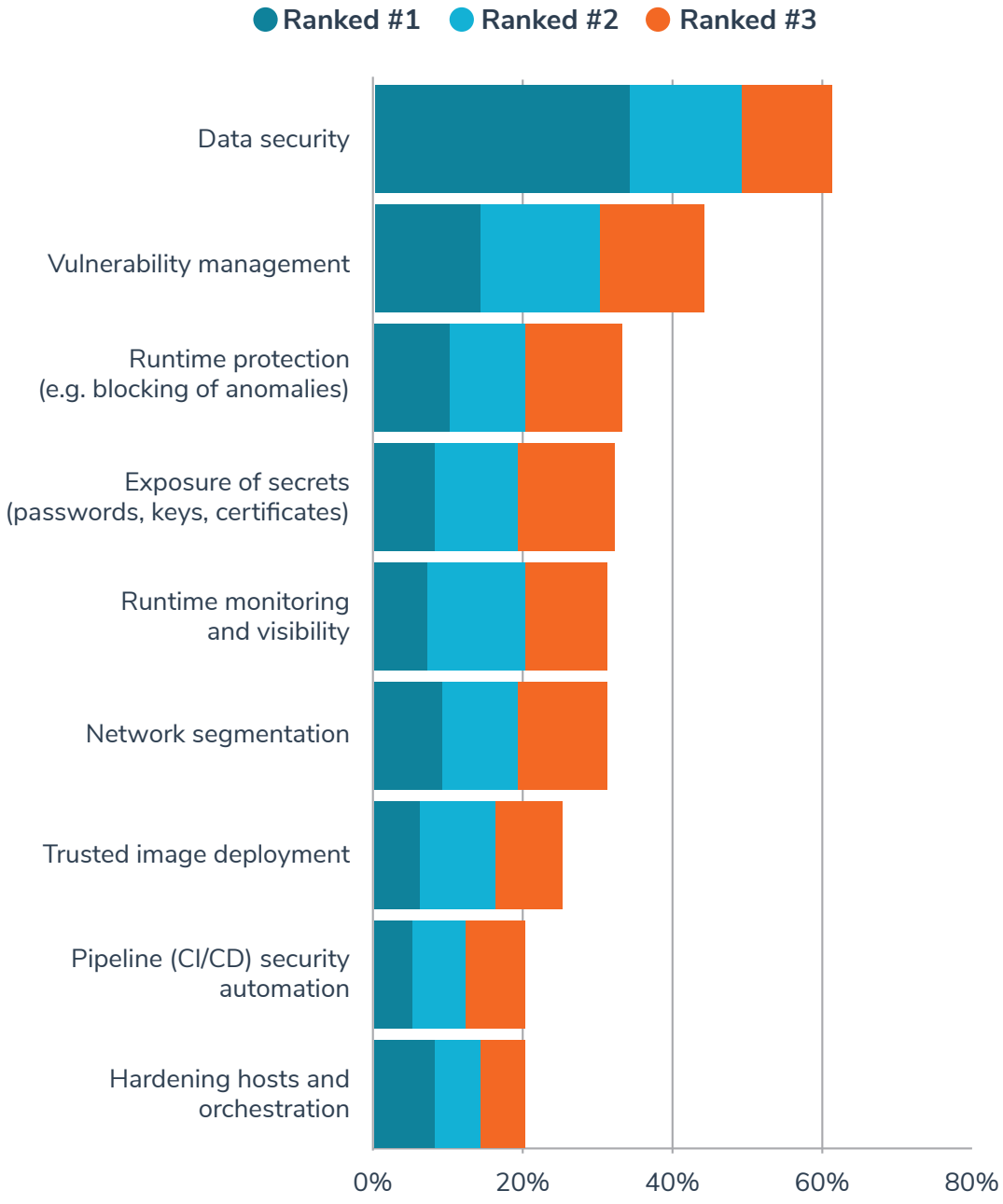
What are your top 3 storage challenges with containers? Rank up to 3.



Data security tops security challenges

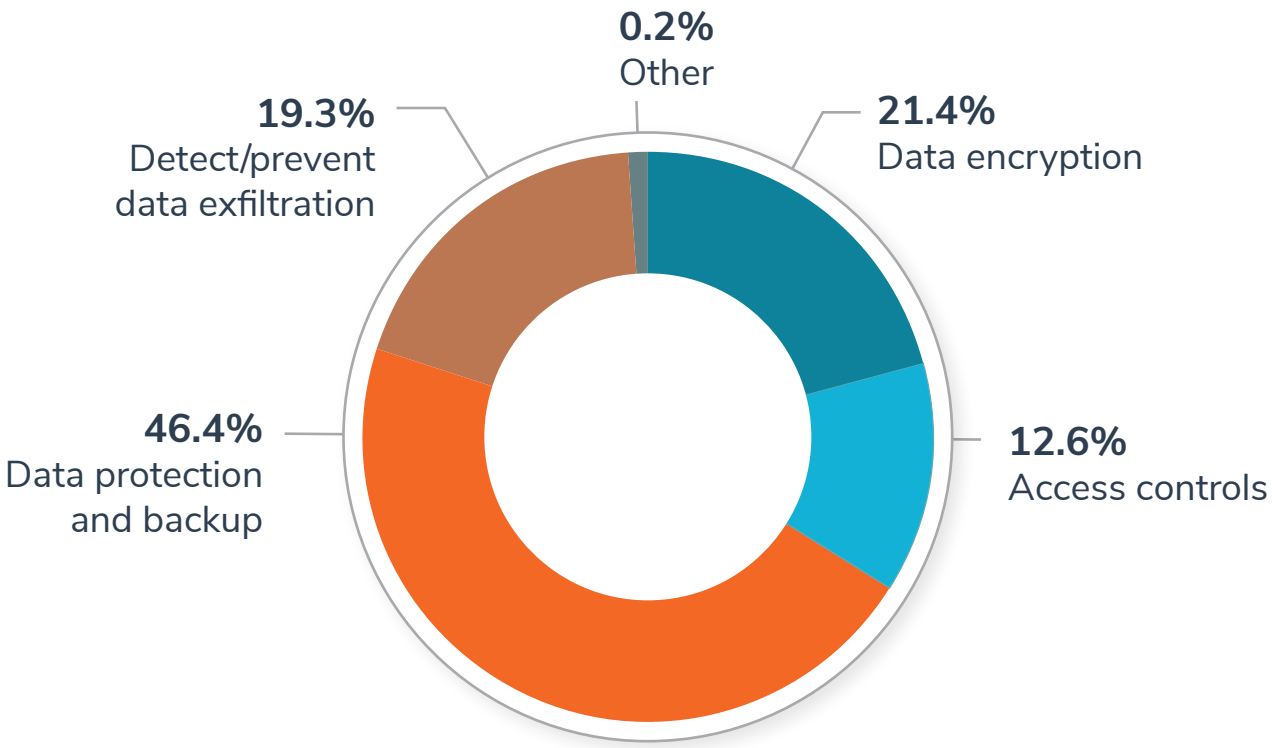
Respondents were also asked to name their top security challenges. Data security topped the list with 61% of the sample listing data security as a top challenges. 43% of the sample listed vulnerability management as the top challenge with runtime protection (e.g. blocking of anomalies) rounding out the top three with 34%.

What are your top 3 security challenges with containers? Rank up to 3.



Digging into top data security concerns, nearly a majority of respondents pointed to data protection and backup (46%) as the top concern, with data encryption (21%), and detecting and preventing data exfiltration (19%) rounding our the top three.

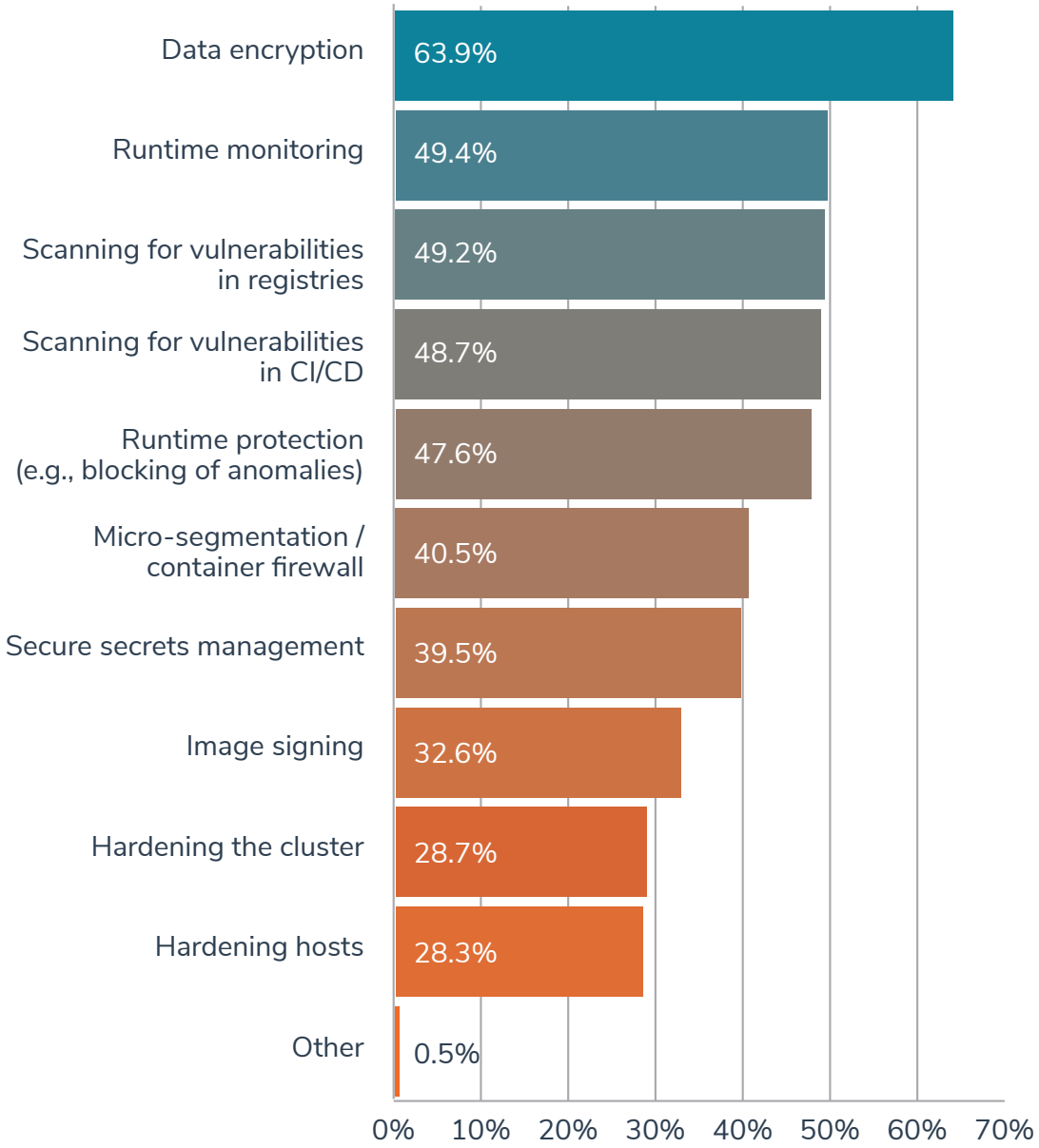
What is your top data security concern when it comes to running stateful services in containers?



Data encryption, host of other strategies employed to protect containerized workloads

When asked how they are protecting containerized applications today, a large majority pointed to data encryption (64%). This is consistent with the declared importance of data security noted by respondents. Businesses are using a host of other strategies, however, to protect their containerized applications, including run time monitoring (49%), vulnerability scanning in registry (49%), vulnerability scanning in CI/CD pipelines (49%), and blocking of anomalies through runtime protection (48%).

What steps are you taking today to secure containerized applications?



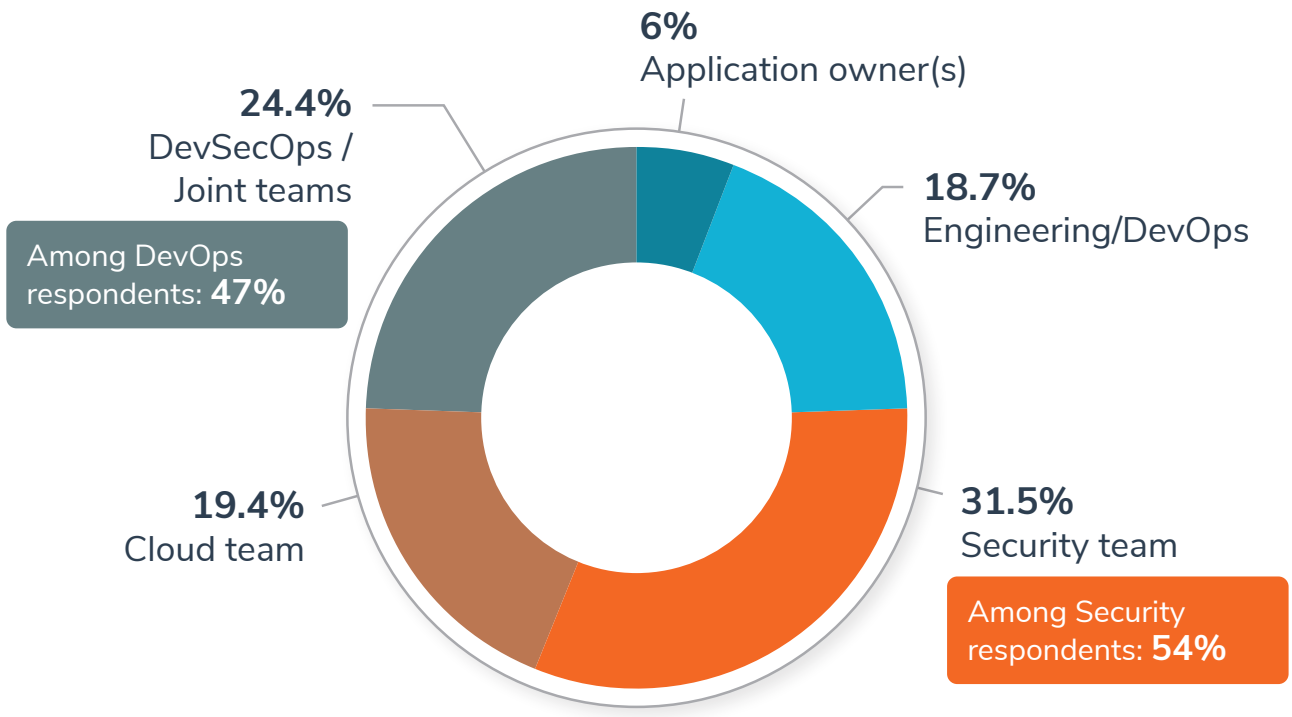
Who has responsibility for container security? It depends who you ask

There was a wide spread of responses to this question, with Security named as the main team responsible for container security at 31%, followed by a joint team or DevSecOps at 24%.

When analyzing the responses by the role of the respondents, however, it becomes clear that most teams assign more of the responsibility to themselves than others do. 54% of security professionals named their own team primarily responsible (compared with 31% among all respondents), while 47% of DevOps professionals pointed to a joint DevSecOps team as bearing the responsibility (compared with 24% of all respondents).

This demonstrates how the rapid adoption of containers has left organizations lacking clarity on who should own what when it comes to securing containerized applications. The good news is that teams seem to be taking on more, rather than less responsibility. While it might result in inefficiencies and duplication of effort, it is better than the alternative of each team assuming that the other team will handle it.

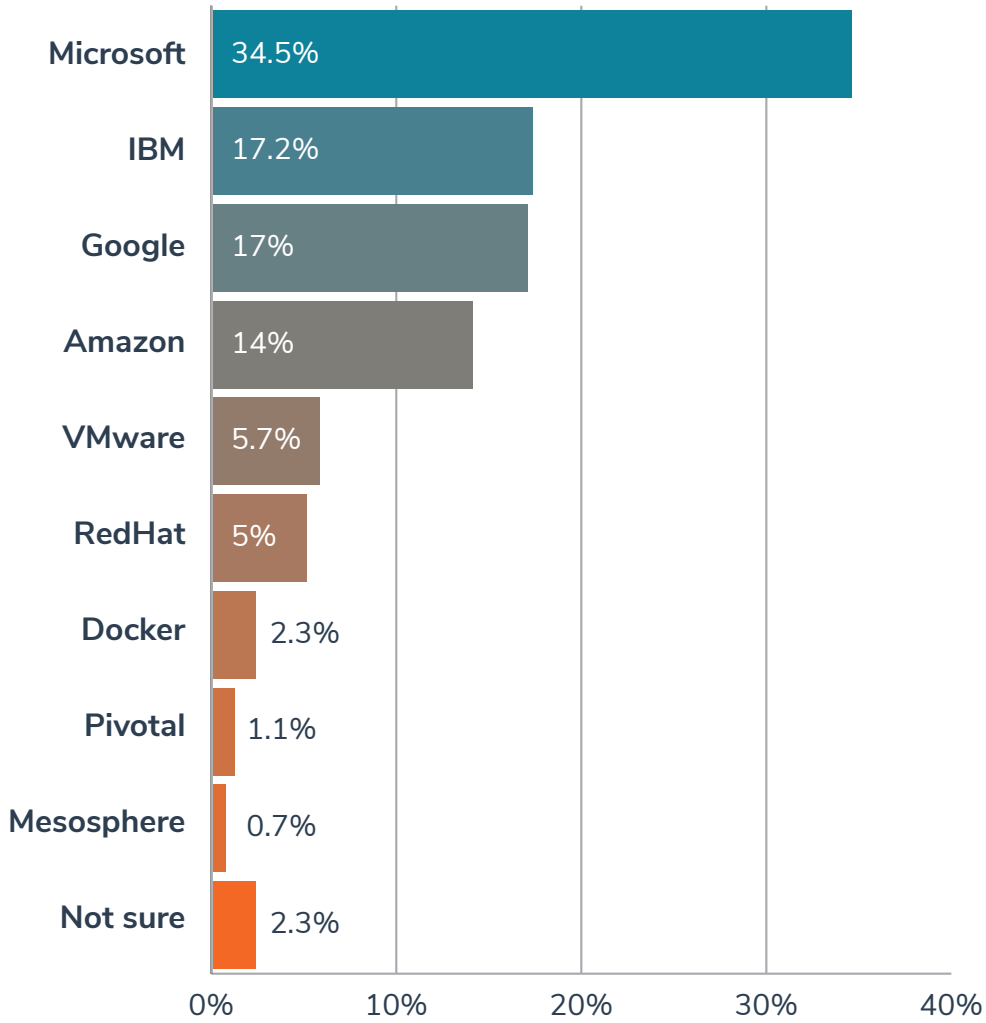
Who is the most responsible in your organization for securing containerized applications?



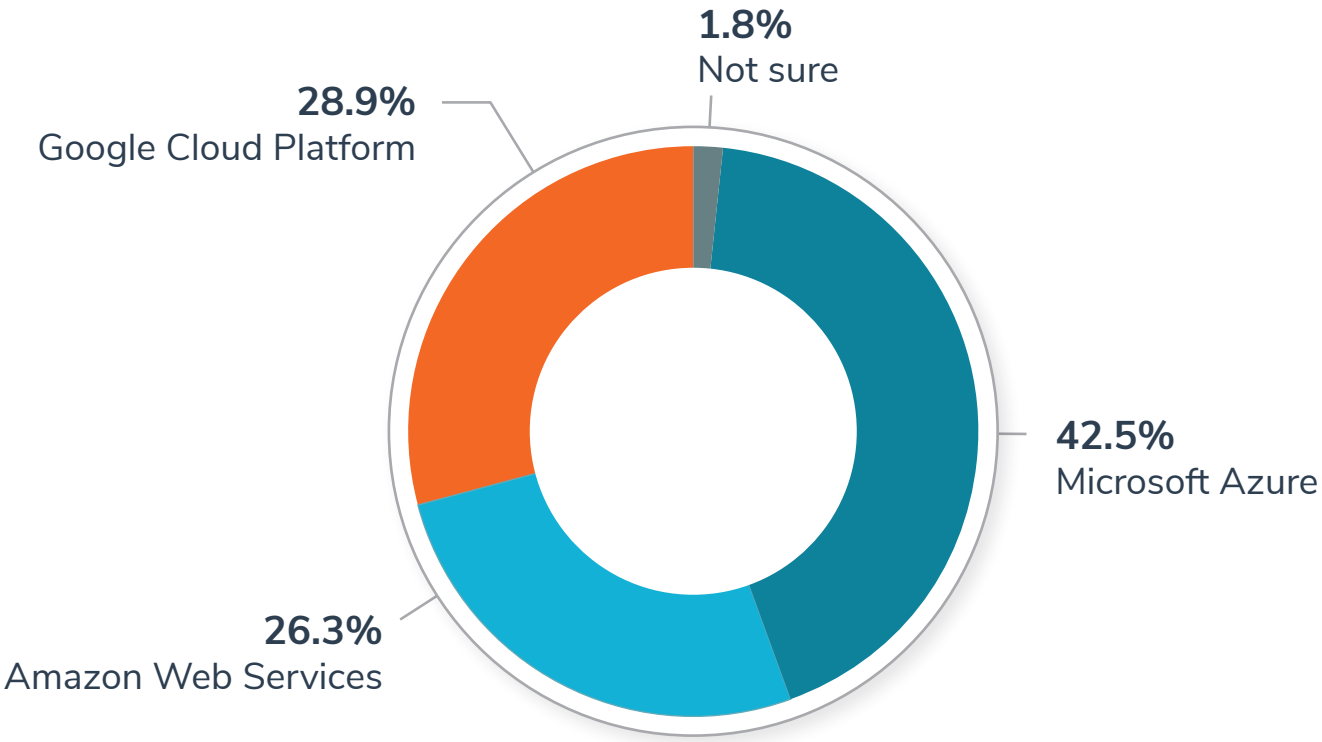
The clouds compete for container mindshare and usage.

With such rapid growth in containerization and the clear standardization around Kubernetes, an obvious question companies will ask themselves is who can help them to run Kubernetes successfully. The answer largely mirrors the adoption of cloud-specific Kubernetes services. Microsoft Azure, provider of the most popular Kubernetes service according to our survey, AKS, is the most trusted at 35%. IBM, with IKS, is the second most trusted at 17%. Google (17%), Amazon (14%) and VMware (6%) round out the top five.

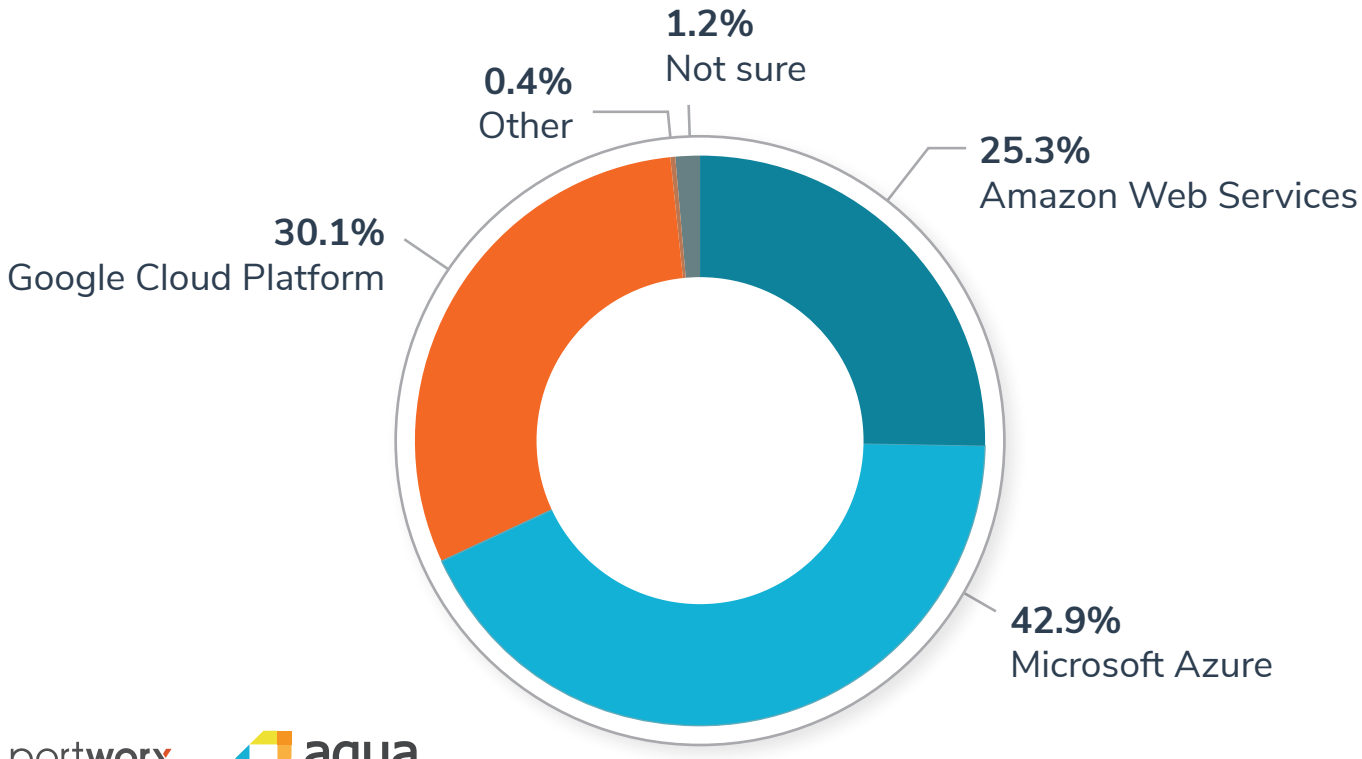
Which company do you most trust will help you succeed running Kubernetes?



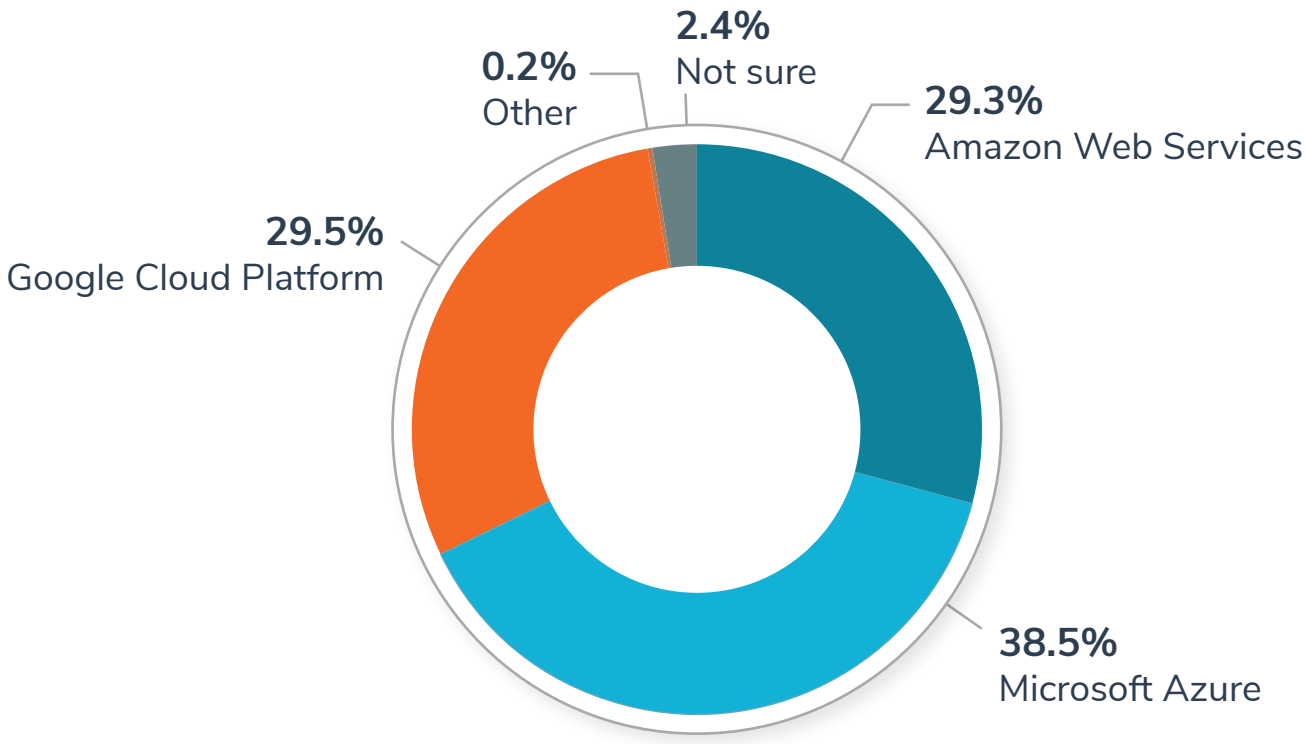
Which public cloud provider has the most developer-friendly environment for running containers?



Which public cloud provider do you consider to be most supportive of hybrid and multi-cloud deployments?



Which public cloud provider do you view as the best value for money?



Appendix - Full survey questions

Which public cloud provider do you trust the most to keep your data and applications secure? A rank of 1 means most trusted and a 5 is least trusted. Select up to 5.

	Amazon Web Services (A)	Microsoft Azure (B)	Google Cloud Platform (C)	IBM Cloud (D)	Oracle Cloud (E)
Total	N=475	N=480	N=481	N=471	N=451
Ranked #1	23%	38%	23%	11%	5%
Ranked #2	19%	22%	23%	23%	10%
Ranked #3	18%	18%	21%	18%	20%
Ranked #4	14%	10%	18%	23%	23%
Ranked #5	20%	8%	10%	19%	31%

What department do you currently work in?

	Total	Total
Total	N=501	501
IT	100%	501
Marketing	0%	0
Sales	0%	0
Finance	0%	0
Customer service	0%	0
Human resources	0%	0
Business development	0%	0
Other	0%	0

How knowledgeable are you about what types of IT technologies your company uses?

	Total	Total
Total	N=501	501
Very knowledgeable	86%	429
Knowledgeable	12%	60

Somewhat knowledgeable	2%	12
Not very knowledgeable	0%	0
Not knowledgeable at all	0%	0

How knowledgeable are you about how much money is invested in IT technologies your company uses?

	Total	Total
Total	N=501	501
Very knowledgeable	72%	362
Knowledgeable	20%	101
Somewhat knowledgeable	8%	38
Not very knowledgeable	0%	0
Not knowledgeable at all	0%	0

How many employees are in your organization?

	Total	Total
Total	N=501	501
1 - 99	0%	0
100 - 499	0%	0
500 - 999	19%	94
1,000 - 2,499	31%	157
2,500 - 4,999	18%	92
5,000 - 9,999	15%	73
10,000+	17%	85

Which of the following best describes your primary role?

	Total	Total
Total	N=501	501
DevOps	21%	103
Development	23%	115

Operations	33%	167
Security	17%	86
QA	3%	15
Other	3%	15

In what industry is your organization?

	Total	Total
Total	N=501	501
Aerospace and Defense	1%	5
Banking	5%	26
Biotech	1%	6
Chemicals	0%	1
Computer Hardware	3%	15
Construction & Design	2%	11
Education	4%	18
Finance	4%	20
Government	2%	11
Health Care	11%	55
Insurance	2%	12
Legal	0%	0
Manufacturing	9%	47
Real estate/Development	0%	2
Recruiting	0%	1
Retail/Wholesale	7%	37
Professional Services	4%	21
Software	7%	34
Telecommunication	3%	14
Technology	28%	138
Transportation	2%	11
Utilities	2%	9
Other	1%	7

Does your organization run container technologies?

	Total	Total
Total	N=501	501
Yes	87%	435
No	10%	51
Not sure	3%	15

What percentage of your apps are running in containers?

	Total	Total
Total	N=435	435
Less than 20%	4%	17
21 - 40%	24%	105
41 - 60%	37%	161
61 - 80%	26%	115
Greater than 80%	8%	35
Not sure	0%	2

In which of these non-production environments is your organization running containers?

	Total	Total
Total	N=435	435
Development	78%	338
Lab	42%	184
QA	49%	212
Testing	68%	296
POC	27%	117
Other	0%	1
Count	2.64	2.64

Is your organization running container technologies in production?

	Total	Total
Total	N=435	435
Yes	90%	390
No	9%	39
Not sure	1%	6

What is the primary reason why your organization is running container technologies?

	Total	Total
Total	N=435	435
Increase developer speed and efficiency	37%	161
Support microservices architectures	10%	45
Enable users to run on multiple cloud platforms (avoid lock-in)	19%	82
Save on infrastructure costs	14%	59
Increase agility	20%	86
Other	0%	2

Which container orchestration tools do your organization use?

	Total	Total
Total	N=435	435
Azure AKS	47%	204
IBM IKS	40%	176
Google GKE	39%	171
Amazon EKS	35%	153
Amazon ECS	33%	145
Red Hat OpenShift	23%	102
Docker Swarm	11%	48
Kubernetes	11%	47
Pivotal Cloud Foundry	11%	47
Pivotal PKS	8%	33

Mesosphere DC/OS	7%	32
Other	0%	1
Not sure	0%	1
Count	2.67	2.67

Which company do you most trust will help you succeed running Kubernetes?

	Total	Total
Total	N=435	435
Amazon	14%	61
Microsoft	34%	150
Google	17%	74
IBM	17%	75
Pivotal	1%	5
RedHat	5%	22
Mesosphere	1%	3
VMware	6%	25
Docker	2%	10
Other	0%	0
Not sure	2%	10

In order to deploy containers, which challenge has been the most difficult to overcome? Rank up to 3.

	Total	Ranked #1	Ranked #2	Ranked #3
Data management (A)	N=173	12%	15%	13%
Disaster recovery (B)	N=109	8%	8%	9%
Graphical UI (C)	N=62	4%	5%	5%
Logging (D)	N=56	5%	4%	4%
Multi-cloud or cross datacenter support (E)	N=156	13%	9%	14%
Networking (F)	N=124	7%	9%	13%
Persistent storage (G)	N=94	5%	9%	8%

Reliability (H)	N=152	13%	11%	11%
Scalability (I)	N=141	10%	12%	10%

What are your top 3 storage challenges with containers? Rank up to 3.

	Total	Ranked #1	Ranked #2	Ranked #3
Provisioning storage takes too long (A)	N=116	8%	9%	9%
Storage does not effectively scale with number of containers (B)	N=148	9%	14%	12%
Inadequate tools for managing container storage (C)	N=127	8%	11%	10%
Concerns about data loss (D)	N=198	15%	18%	12%
Legacy storage technologies not a good fit for container workloads (E)	N=172	13%	11%	15%
Block devices like Amazon EBS are slow to mount (F)	N=115	8%	9%	9%
Ensuring data security (G)	N=242	26%	15%	14%
Planning for disaster recovery and business continuity (H)	N=173	12%	12%	16%

What are your top 3 security challenges with containers? Rank up to 3.

	Total	Ranked #1	Ranked #2	Ranked #3
Vulnerability management (A)	N=188	14%	16%	14%
Pipeline (CI/CD) security automation (B)	N=86	5%	7%	8%
Trusted image deployment (C)	N=105	6%	10%	9%
Runtime monitoring and visibility (D)	N=137	7%	13%	11%
Runtime protection (e.g. blocking of anomalies) (E)	N=146	10%	10%	13%
Hardening hosts and orchestration (F)	N=87	8%	6%	6%
Network segmentation (G)	N=138	9%	10%	12%
Exposure of secrets (passwords, keys, certificates) (H)	N=140	8%	11%	13%
Data security (I)	N=265	34%	15%	12%

What steps are you taking today to secure containerized applications?

	Total	Total
Total	N=435	435
Scanning for vulnerabilities in CI/CD	49%	212
Scanning for vulnerabilities in registries	49%	214
Image signing	33%	142
Hardening hosts	28%	123
Hardening the cluster	29%	125
Micro-segmentation / container firewall	40%	176
Runtime monitoring	49%	215
Runtime protection (e.g., blocking of anomalies)	48%	207
Secure secrets management	40%	172
Data encryption	64%	278
Other	0%	2
Not taking any steps to secure containerize applications	0%	1
Count	4.29	4.29

Who is the most responsible in your organization for securing containerized applications?

	Total	Total
Total	N=435	435
Application owner(s)	6%	26
Engineering/DevOps	19%	81
Security team	31%	137
Cloud team	19%	84
DevSecOps / joint teams	24%	106
Other	0%	0
Unclear who's responsible / Not sure	0%	1

What is your top data security concern when it comes to running stateful services in containers?

	Total	Total
Total	N=435	435
Data encryption	21%	93
Access controls	13%	55
Data protection and backup	46%	202
Detect/prevent data exfiltration	19%	84
Other	0%	1

How much of a financial investment has your company made in containers in the last 12 months, including technology licenses, hardware and usage fees, and personnel expenses?

	Total	Total
Total	N=435	435
$0 - $9,999	2%	8
$10,000 - $99,999	12%	52
$100,000 - $499,999	45%	197
$500,000 - $999,999	24%	103
$1,000,000 or more	17%	75

What is the primary reason why your organization isn't using container technologies today?

	Total	Total
Total	N=51	51
Containers aren't useful for our applications	35%	18
I don't believe the hype around containers	10%	5
No compelling customer case studies around how containers provide benefits or ROI	22%	11
Not enough is known about container technologies to invest any resources in them	20%	10

Ecosystem of products and tools is too immature	8%	4
Other	0%	0
Not sure	6%	3

Which public cloud provider has the most developer-friendly environment for running containers?

	Total	Total
Total	N=501	501
Amazon Web Services	26%	132
Microsoft Azure	43%	213
Google Cloud Platform	29%	145
Other	0%	2
Not sure	2%	9

Which public cloud provider do you consider to be most supportive of hybrid and multi-cloud deployments?

	Total	Total
Total	N=501	501
Amazon Web Services	25%	127
Microsoft Azure	43%	215
Google Cloud Platform	30%	151
Other	0%	2
Not sure	1%	6

Which public cloud provider do you view as the best value for money?

	Total	Total
Total	N=501	501
Amazon Web Services	29%	147
Microsoft Azure	39%	193

Google Cloud Platform	30%	148
Other	0%	1
Not sure	2%	12

Which public cloud provider do you view as most reliable for running containers?

	Total	Total
Total	N=501	501
Amazon Web Services	27%	137
Microsoft Azure	43%	215
Google Cloud Platform	28%	139
Other	0%	1
Not sure	2%	9

Which public cloud provider do you trust the most to keep your data and applications secure? A rank of 1 means most trusted and a 5 is least trusted. Select up to 5.

	Amazon Web Services (A)	Microsoft Azure (B)	Google Cloud Platform (C)	IBM Cloud (D)	Oracle Cloud (E)
Total	N=475	N=480	N=481	N=471	N=451
Ranked #1	23%	38%	23%	11%	5%
Ranked #2	19%	22%	23%	23%	10%
Ranked #3	18%	18%	21%	18%	20%
Ranked #4	14%	10%	18%	23%	23%
Ranked #5	20%	8%	10%	19%	31%

Which public cloud provider do you trust the most to ensure the privacy of your customer's data? A rank of 1 means most trusted and a 5 is least trusted. Select up to 5.

	Amazon Web Services (A)	Microsoft Azure (B)	Google Cloud Platform (C)	IBM Cloud (D)	Oracle Cloud (E)
Total	N=483	N=486	N=479	N=477	N=469
Ranked #1	21%	37%	25%	14%	5%

Ranked #2	20%	22%	21%	23%	13%
Ranked #3	18%	19%	19%	18%	23%
Ranked #4	17%	11%	18%	24%	21%
Ranked #5	21%	9%	14%	17%	31%

Which of the following public cloud providers do you currently use to run containers?

	Total	Total
Total	N=501	501
Amazon Web Services	43%	216
Microsoft Azure	57%	285
Google Cloud Platform	43%	217
Other	1%	6
Not sure	3%	13
Count	1.47	1.47

Portworx, Inc.

4940 El Camino Real, Suite 200
Los Altos, CA 94022

Tel: 650-241-3222 | info@portworx.com

www.portworx.com

Aqua Security Software Inc.

800 District Avenue, Suite 310
Burlington, MA 01803

Tel: 781-362-4787 | contact@aquasec.com

www.aquasec.com