TIGERA

The State of Cloud-Native Security

April 2022

INTRODUCTION

The State of Cloud-Native Security

April 2022

In our first **State of Cloud-Native Security** report, we look at security practices for containers, cloud-native applications, and supporting infrastructure. This report compiles survey results from more than 300 security and IT professionals from around the world, and sheds light on organizations' needs and challenges when it comes to containers and cloud-native applications, specifically in the areas of security, observability, and compliance.

We are pleased to see that many companies are focusing development on cloud-native applications; however, the report highlights that with cloud-native adoption comes a slew of new requirements and challenges that are driving delays. The survey results underscore the need for advanced security and observability capabilities to enable companies to mitigate risk and meet compliance requirements for their cloud-native workloads.

This report provides valuable information and insight into the state of the cloud-native security market. We hope you'll see an opportunity to take stock of your own organization's standing against the findings in this report to determine how to best move forward on your cloud-native journey.

This report is divided into 3 sections:

Cloud-Native Applications

- Which aspects of cloud-native applications do organizations find challenging?
- Which cloud-native application challenges result in slower deployments?
- What capabilities do organizations need for cloud-native application observability?

Containers

- What are the biggest barriers to successful container orchestration?
- What capabilities do organizations need for container security?
- What are organizations' network security needs for containerized applications?

Compliance

- What compliance requirements do organizations need to meet for cloud-native applications?
- What aspects of meeting container-level compliance requirements are challenging?
- Which audit reports are challenging to produce?

Key trends

Cloud-native applications gain momentum but present security, compliance, and observability issues

- 75% of companies are focusing development on cloud-native applications
- Security and compliance requirements slow cloud-native application development
- Container-level firewalls and workload access controls top security needs for cloud-native applications
- 97% of companies report observability challenges with cloud-native applications
- 76% need runtime visualization for cloud-native applications

Containers require security solutions for runtime, access, and networking

- 99% of companies indicate containers require access to other applications and services
- 98% need container security, with runtime security topping the list
- 99% of companies require network security for containerized applications

Cloud-native and container compliance requirements are driving delays and challenges

- 87% of companies state meeting compliance requirements is critical for their company
- 95% report they have compliance requirements for cloud-native applications
- 63% of companies must provide container-level information for compliance requirements
- 90% state audit reports are challenging to produce

CLOUD-NATIVE APPLICATIONS

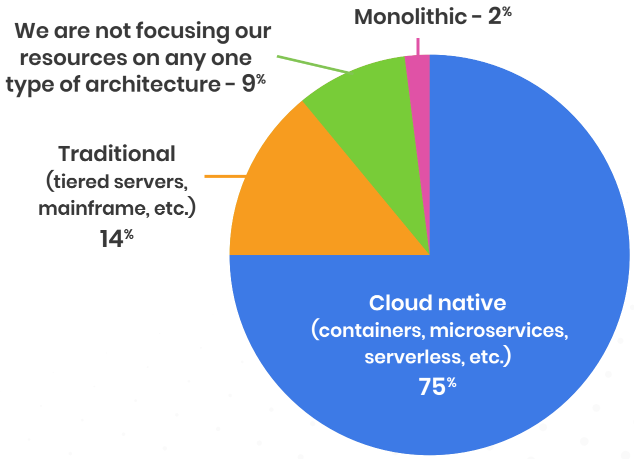
96% of companies found security, compliance, and observability to be the most challenging aspects of cloud-native applications

3 out of 4 companies are moving toward cloud-native applications

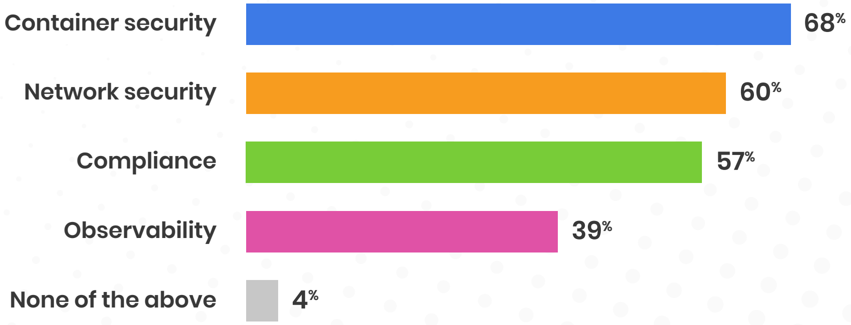
Security and compliance are two of the biggest inhibitors in realizing cloud-native goals

75% of respondents are focusing the majority of new development efforts on cloud-native applications. Given the dynamic, distributed, and ephemeral architecture of cloud-native applications, which in turn leads to a massive attack surface, it's not surprising that our survey shows 96% of respondents find one or more aspects of cloud-native application security to be challenging. Almost everyone surveyed (96%) said that security, compliance, and observability are the most challenging aspects of cloud-native applications.

Which type of architecture is your company focusing most of its new application development on?



Which of the following aspects of cloud-native applications are challenging for your company?

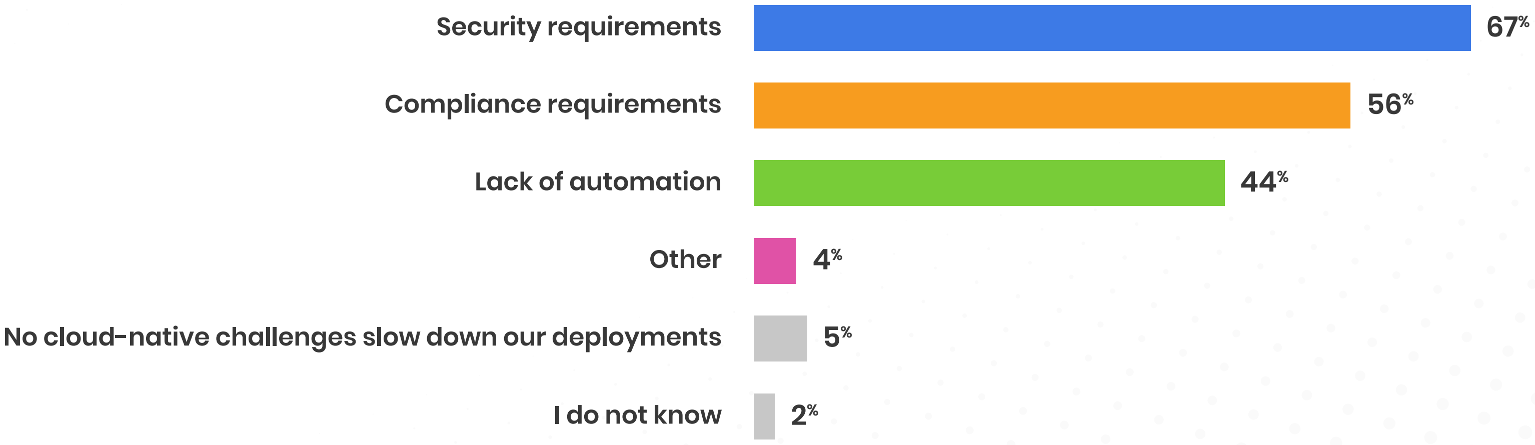


TIGERA PROJECT CALICO

The slowdown caused by issues related to security and compliance is the largest inhibitor to organizations achieving rapid development and deployment cycles

Our survey found that the cloud-native application challenges most (93%) companies experience lead to slow deployment cycles, with challenges related to security requirements (67%) being the leading cause. We weren't surprised to see that 56% of respondents said challenges related to compliance requirements cause delays, since traditional data collection and compliance reporting tools do not capture and correlate data at a granular service level. Lack of automation (44%) rounds out the top 3 inhibitors to rapid development and deployment cycles for cloud-native applications.

What cloud-native application challenges slow deployments for your company?



Container-level firewalls and workload access controls are the top two security needs companies have for cloud-native applications

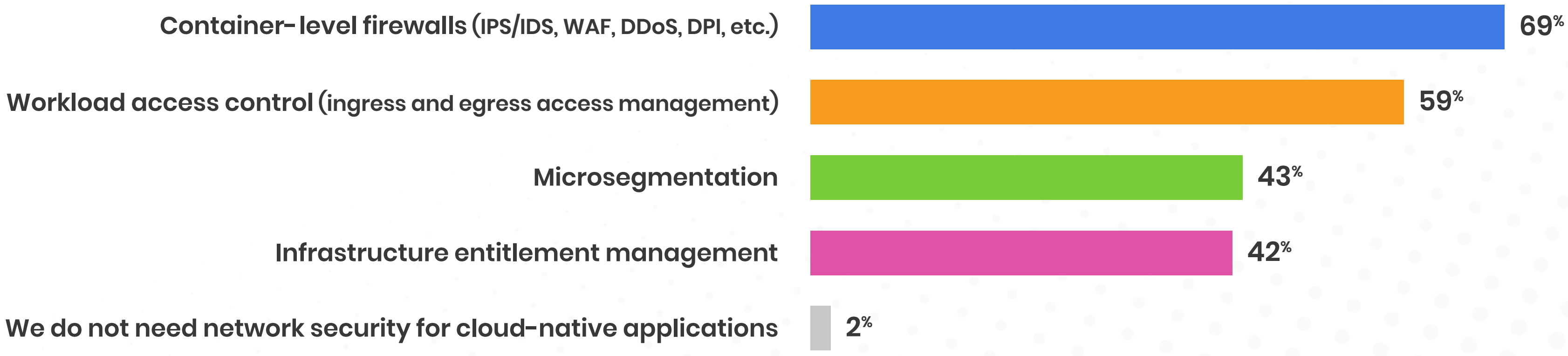
Learn why microsegmentation is critical in a modern, zero trust network environment, and best practices for rolling it out in your organization.

→ Learn More

In the past year, 98% of companies needed network security for cloud-native applications. Since the traditional network does not exist in the world of containers and Kubernetes, network security is effectively implemented at the workload level to secure workload-to-workload communication. It is therefore extremely important that the principles of zero trust are brought all the way to the workload level to protect access and communication between workloads.

Similar to what we hear in our conversations with customers, the survey results indicate that companies are looking to reduce application attack surface and quickly identify threats. In order to do that, they see workload-based IDS/IPS, DPI, DDoS protection, and WAF (69%), workload access controls (ingress and egress access management) (59%), and microsegmentation (43%) as the top network security capabilities they need.

What network security capabilities does your company need for cloud-native applications?



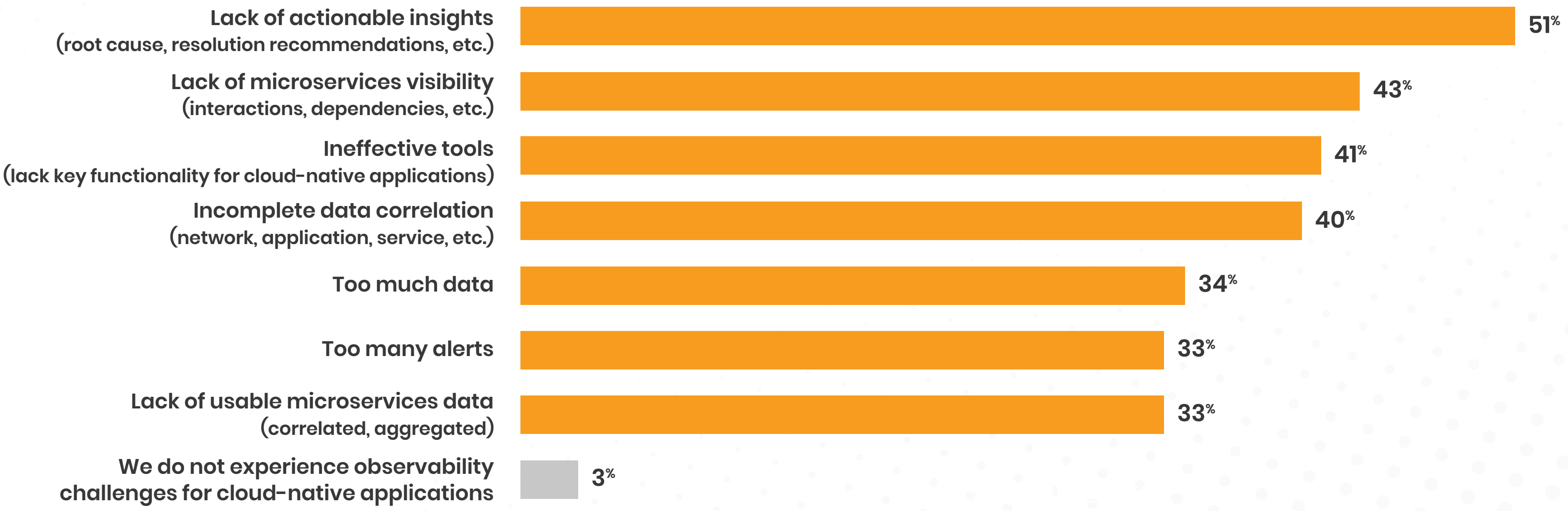
TIGERA PROJECT CALICO

97% of companies experience observability challenges with cloud-native applications

More than half cite a lack of actionable insights as the top challenge

Nearly all (97%) survey respondents stated they experience observability challenges when trying to secure their cloud-native applications, with more than half (51%) citing a lack of actionable insights, such as root cause and resolution recommendations, as the top challenge. 43% of respondents reported that a lack of microservices visibility (interactions, dependencies, etc.) is a challenge, while 41% said ineffective tools that lack key functionality for cloud-native applications is an issue.

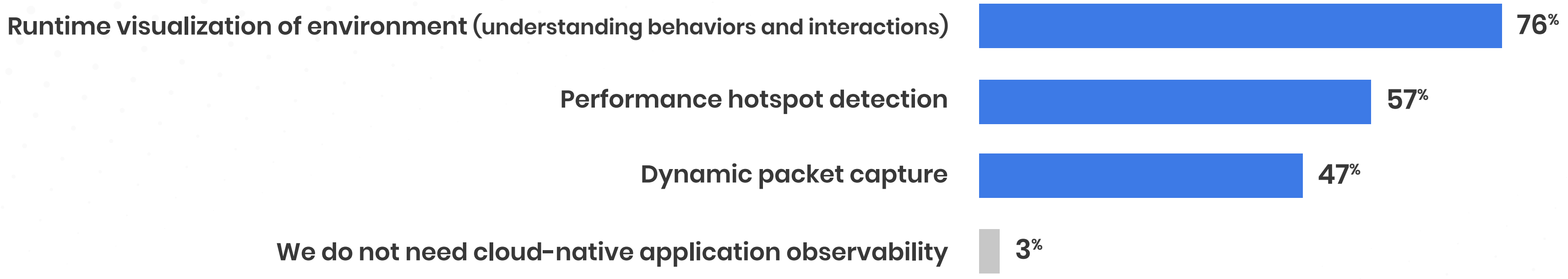
What observability challenges does your company experience with cloud-native applications?



The top capability needed to solve observability challenges is runtime visualization

To address these challenges, 3 out of 4 (76%) respondents indicated a need for runtime visualization to understand behaviors and interactions in their environment. More than half (57%) need performance hotspot detection, followed by dynamic packet capture (47%).

What capabilities does your company need for cloud-native application observability?



Curious about cloud-native security? Read our guide to discover five ways to improve security for your cloud-native applications. → Learn More

CONTAINERS

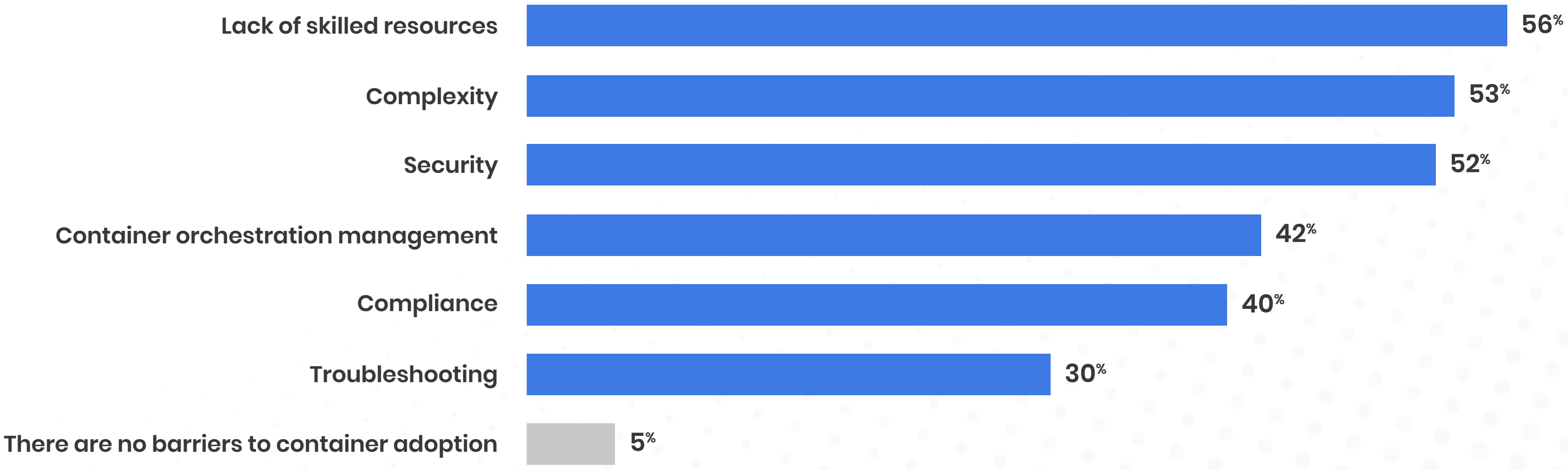
Security, complexity, and lack of skills are the top barriers to successful container adoption

Check out our container security guide to learn how to secure Docker, Kubernetes, and all major elements of the modern container stack.

→ Learn More

Since container adoption can be fraught with complexities (e.g. development, configuration, compliance, and security) across build and runtime stages, we wanted to understand which aspects of container adoption organizations were struggling with most. When asked about the biggest barriers to container adoption in their organization, respondents said the number one barrier was a lack of skilled resources (56%). Complexity came in second with 53% of respondents citing it as a barrier, followed closely by security (52%). Other barriers our respondents face include container orchestration management (42%), compliance (40%), and troubleshooting (30%).

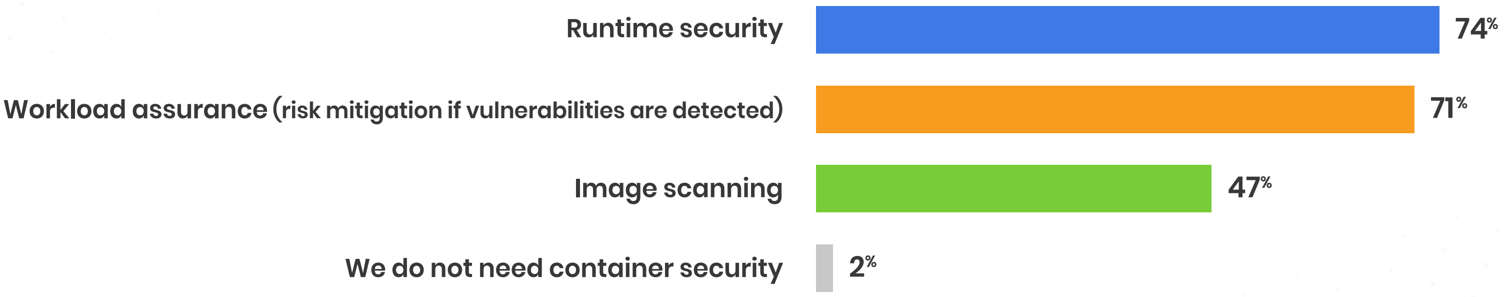
What are the biggest barriers for container adoption in your organization?



The #1 capability companies need for container security is runtime security

As one of the top three barriers to successful container adoption, it's not surprising that most companies (98%) expressed a need for container security. The top two capabilities companies need for container security are runtime security (74%) and workload assurance (risk mitigation if vulnerabilities are detected) (71%). Image scanning rounds out the top three, with 47% of companies saying they need this capability for container security.

What capabilities does your company need for container security?



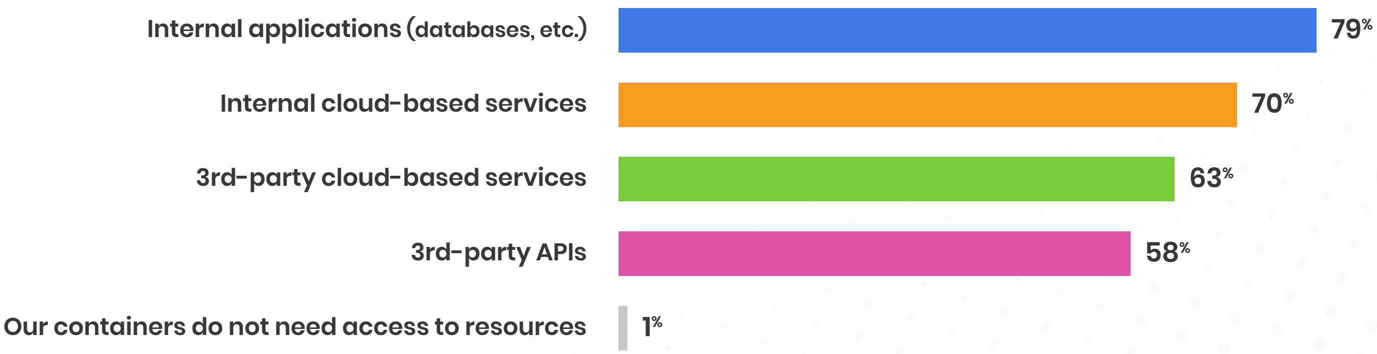
Understand the security risks of container images, technologies used for container security scanning, and best practices for effective container scanning. → Learn More

99% of production deployments have a need to communicate with workloads outside the cluster

Given the granular microservice architecture of cloud-native applications, combined with the widespread use of building blocks such as public cloud services, private services, 3rd-party APIs, and open-source components, it is common for individual services to access resources outside the cluster.

Unsurprisingly, almost all (99%) respondents indicate that containers require access to applications and services outside the cluster. Respondents reported that their containers mostly need to communicate with internal applications such as databases (79%) and internal cloud-based services (70%). Other notable resources containers need access to include 3rd-party cloud-based services (63%), and 3rd-party APIs (58%).

What types of resources do your company's containers need access to?

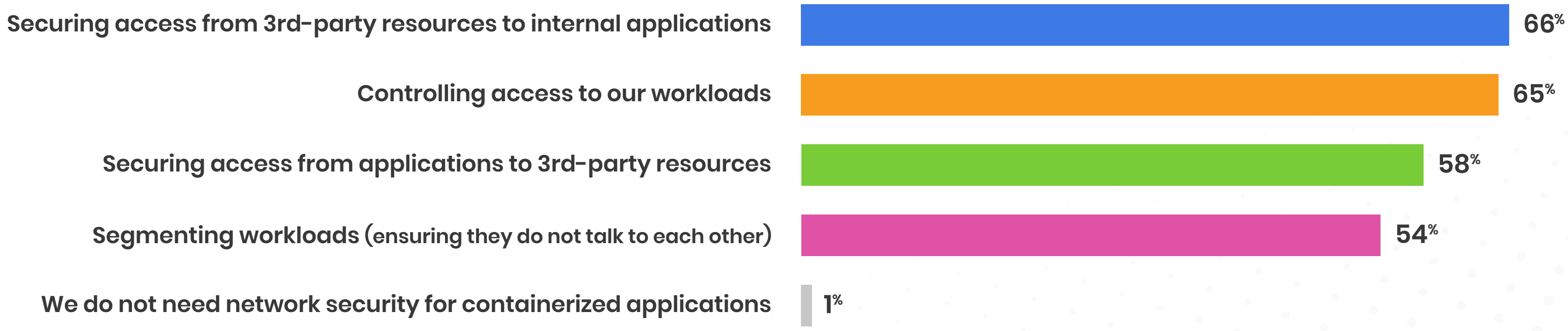


99% of companies need network security for containerized applications

The two most important network security needs are securing access from 3rd-party resources to internal applications, and controlling access to workloads

Our survey results underscore the need for network security for containerized applications, with a staggering 99% of respondents confirming this. Our survey indicates that securing access from 3rd-party resources to internal applications (66%) and controlling access to workloads (65%) are the two most important network security needs companies have for containerized applications. Companies also need to be able to secure access from applications to 3rd-party resources (58%) and segment workloads to ensure they don't communicate with one another (54%).

What are your company's network security needs for containerized applications?



Read our guide to understand container security challenges and learn about container security best practices, such as securing images, registries, and container runtime. → Learn More

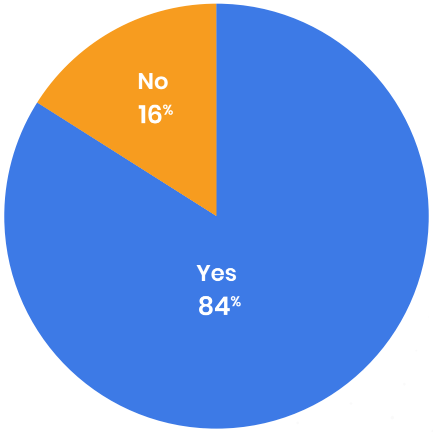
COMPLIANCE

95% of companies need to meet compliance requirements for cloud-native applications

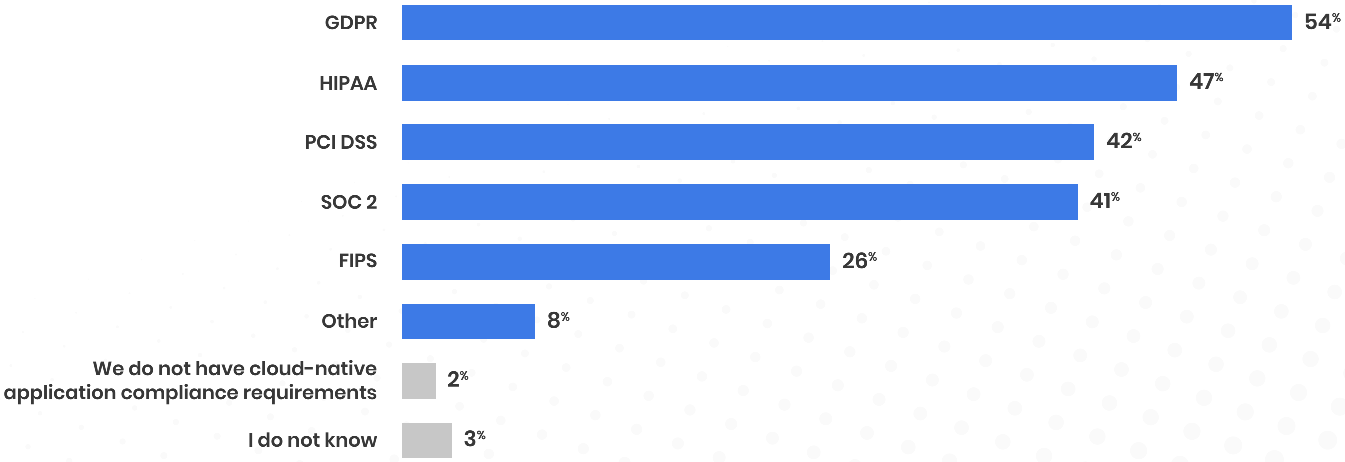
Compliance regulations are critical for cloud-native organizations and most (84%) are struggling with them.

Compliance plays a huge role in regulated industries and is extremely important. Nearly 9 out of 10 (87%) respondents indicated that meeting compliance requirements is critical for their company. 95% of them reported that they have specific compliance requirements for cloud-native applications, including GDPR (54%), HIPAA (47%), PCI DSS (42%), SOC 2 (41%), FIPS (26%), and more. Given the observability issues highlighted by our survey data, it is not surprising that 84% of respondents stated that meeting compliance requirements for cloud-native applications is challenging.

Is it challenging to comply with compliance regulations for cloud-native applications?



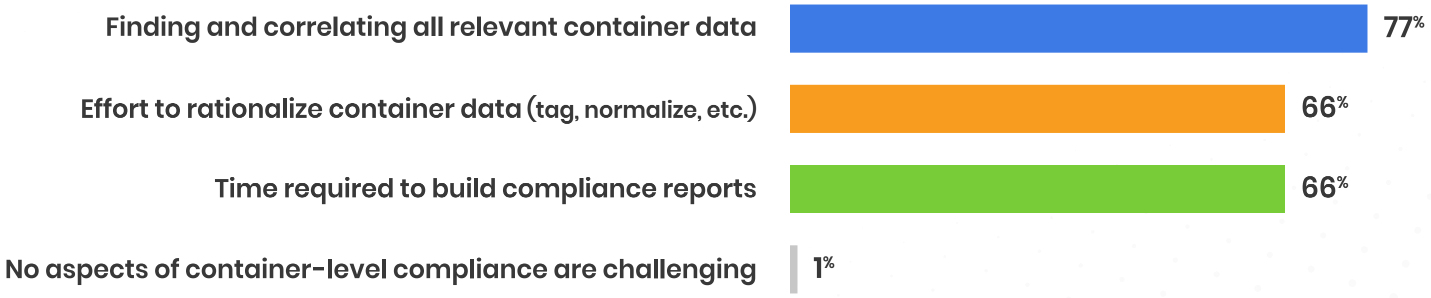
What compliance requirements does your company need to meet for cloud-native applications?



The top challenge to meeting container-level compliance requirements is finding and correlating all relevant container data

The reason companies find it hard to meet compliance requirements is that it is difficult to get internal container-level data. More than 6 out of 10 (63%) respondents indicated that they must provide container-level information for compliance needs, but that finding, correlating, and rationalizing container data is challenging. Finding and correlating all relevant container data (77%) leads the list of challenges respondents face when trying to meet container-level compliance requirements. Tied for second place at 66%, respondents find two other aspects of meeting compliance requirements challenging: the amount of effort needed to rationalize container data (tag, normalize, etc.), and the time required to build compliance reports.

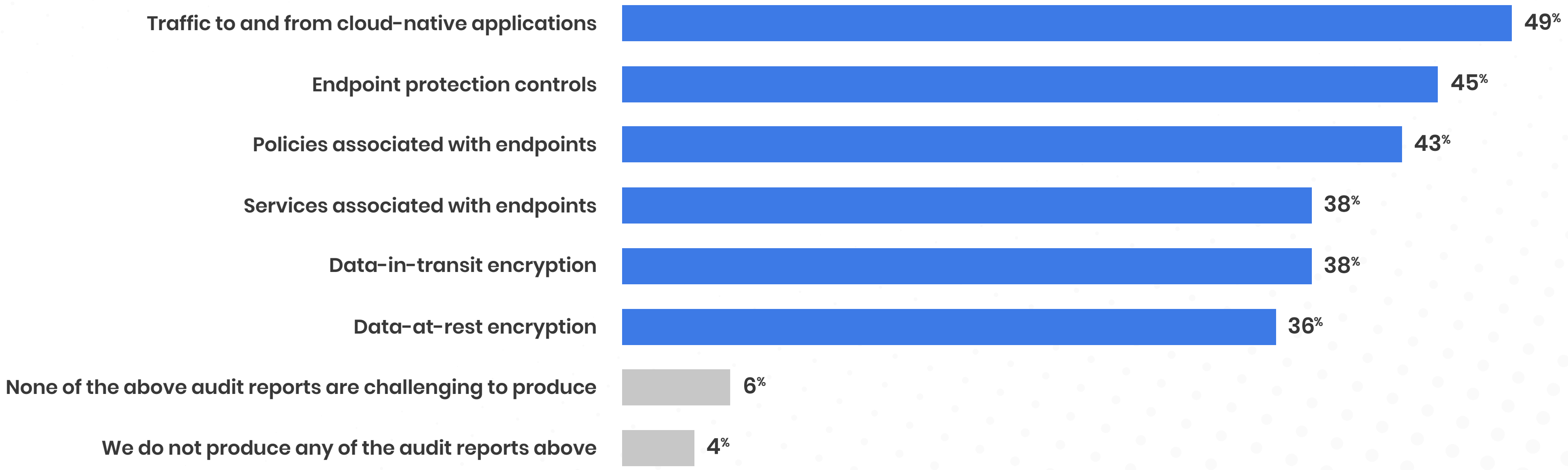
What aspects of meeting container-level compliance requirements are challenging?



90% of companies find it challenging to produce audit compliance reports

Given that so many companies are struggling to meet compliance requirements for their cloud-native applications, it should come as no surprise that 90% of respondents stated that application and container audit reports are difficult to produce. When asked which audit reports were challenging for their company to produce, respondents said it is most difficult to report on traffic to and from cloud-native applications (49%). Reports associated with endpoints, including endpoint protection controls (45%), policies (43%), and services (43%) are also difficult to produce. Encryption reports were also named as problematic, with both data-in-transit (38%) and data-at-rest (36%) encryption being cited as challenging.

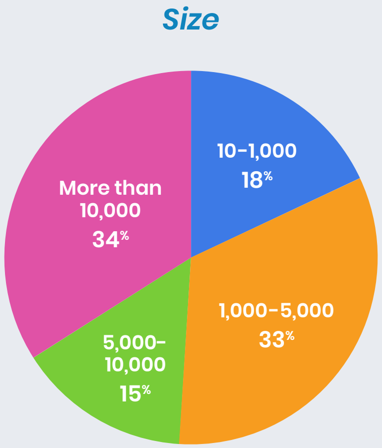
Which of the following audit (evidence) reports are challenging for your company to produce?

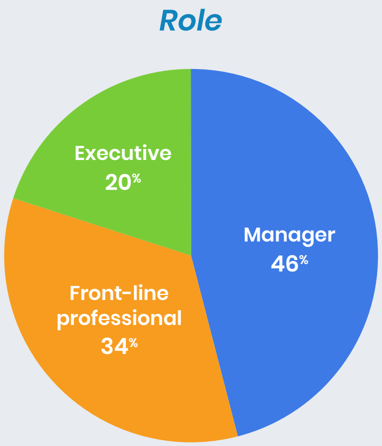


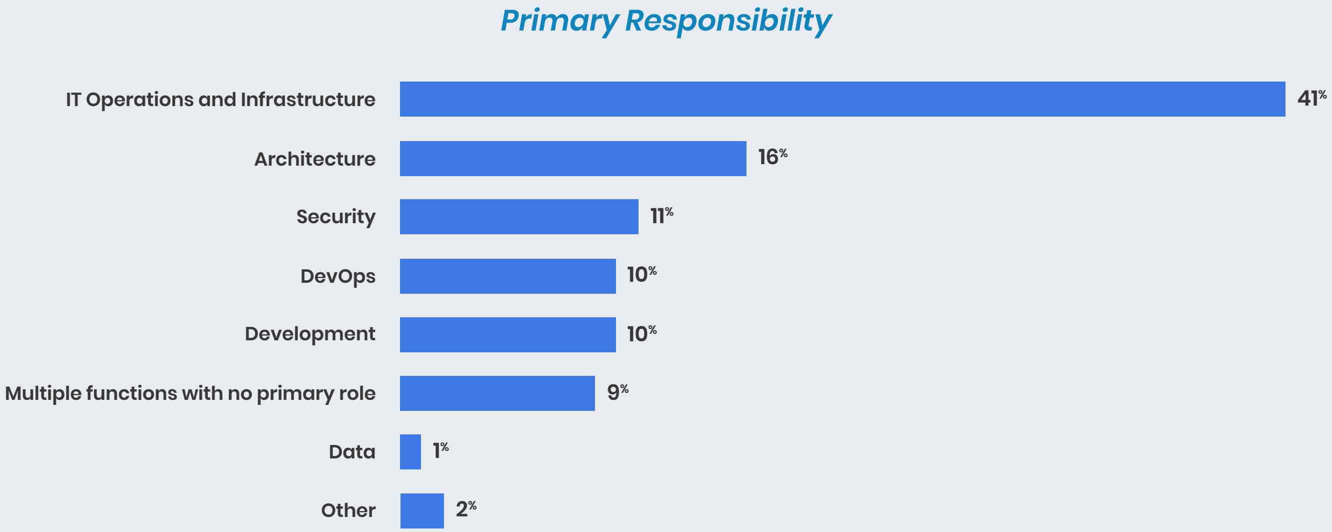
ABOUT OUR RESPONDENTS

Our survey focused on individuals with container responsibilities at companies with 10 or more employees.

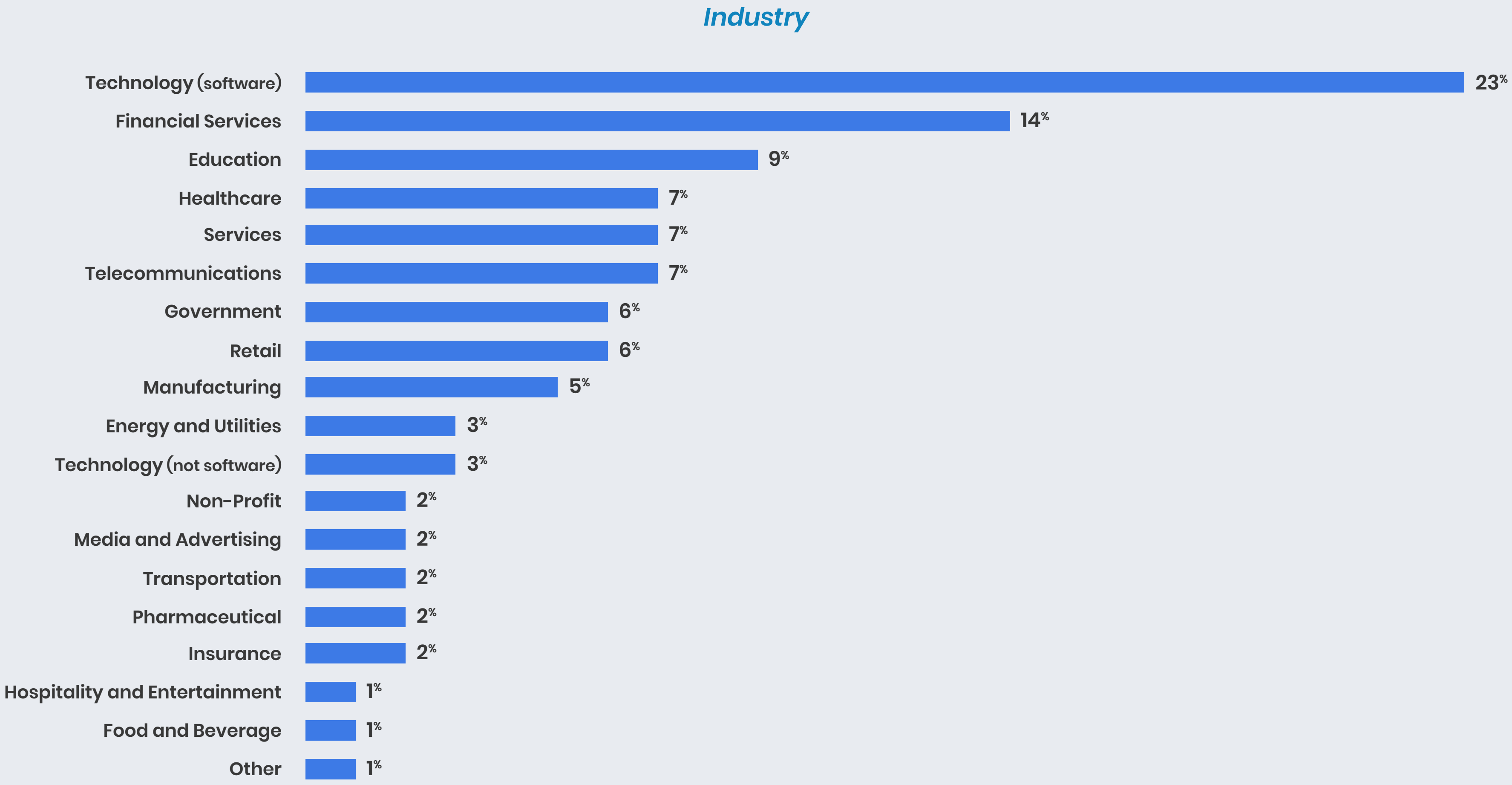
Tigera commissioned Dimensional Research to survey 304 qualified security professionals in a variety of roles, seniority levels, industries, and regions. All respondents had direct container responsibilities.







Although our sample leans heavily toward the technology (23%) and financial services (14%) industries, all major sectors are represented. This includes education (9%), healthcare (7%), telecommunications (7%), government (6%), transportation (2%), pharmaceutical (2%), and insurance (2%). In all, respondents represented more than 20 industries from 5 continents.



IMPLICATIONS AND RECOMMENDATIONS

According to our report, the move to cloud-native applications has strong momentum, but companies need tools to increase visibility and provide security at the container, application, and network levels. These tools need to remove barriers and delays during development and deployment, while also reducing the risk from delayed time to market, security vulnerabilities, and compliance violations.

The findings of this survey make it clear that organizations need advanced security and observability capabilities. We offer the following recommendations to address these needs.

1. Threat prevention: Reduce application attack surface with zero trust

> Start by focusing on threat prevention, using zero-trust controls to reduce the attack surface. This can be done by implementing granular, zero-trust workload access controls (e.g. DNS policies, NetworkSets) to control the flow of data between workloads and external resources. Use microsegmentation to isolate workloads based on environments, application tiers, compliance needs, user access, and individual workload requirements.

2. Threat detection: Monitor for both known and unknown vulnerabilities and malware

> To protect containerized workloads from external threats and lateral movement, implement image assurance and runtime application-level security. Use a tool that:
>
> - Ingests threat feeds and offers the ability to create custom threat feeds to detect threats
> - Monitors inbound and outbound traffic (north-south) and east-west traffic
> - Identifies anomalies based on process, syscall, file system access, and network behavior
> - Uses machine learning to identify zero-day threats
> - Offers workload-based deep packet inspection to inspect network data in detail and perform signature-based detection of potential threats
> - Provides advanced anomaly detection capabilities to identify, quarantine, and remediate attacks from unknown actors

3. Threat mitigation: Mitigate risks from exposure

The best way to mitigate breaches is by dynamically responding to threats. To do this, you need a detailed runtime visualization of your environment in order to observe microservice behavior and interaction, quickly troubleshoot connectivity issues, and identify performance hotspots. You should use a tool that:

- Allows you to create a security moat around critical workloads to mitigate risk
- Offers the ability to deploy honeypods to thwart zero-day attacks
- Automatically quarantines potentially malicious workloads
- Enables you to configure alerts to trigger automated remediation

Want to learn more about zero-trust security? Discover best practices and core principles in our zero trust guide.

→ Learn More

ABOUT TIGERA

Tigera provides active, zero-trust based security for cloud-native applications running on containers and Kubernetes. Our Cloud-Native Application Protection Platform (CNAPP) prevents, detects, troubleshoots, and automatically mitigates exposure risks of security issues in build, deploy, and runtime stages.

CALICO CLOUD

Ready to see Calico Cloud in action?

Try Calico's active, zero-trust based security for cloud-native applications with a free, 14-day trial.

Try Now