RESEARCH REPORT

The Impact of Machine Identities on the State of Cloud Native Security in 2023

Venafi®

Introduction

To maximize competitive advantages, modern companies are evolving toward highly scalable, flexible, and resilient applications. This trend has driven widespread adoption of cloud native technologies like Kubernetes and microservices-based application architectures. But in their haste to transition to these modern environments, many organizations may not have fully considered unique security requirements, such as the impact of machine identities and their management.

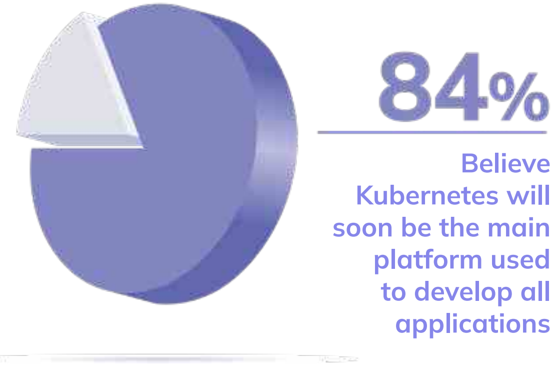
Machine identities are critical to secure sensitive microservices and resources that can be accessed from anywhere on the Internet. To properly implement the latest advances in technology, organizations need to establish the identity of cloud native machines such as containers, microservices, DevOps artifacts, API connections, and more. To function securely, all these interconnected cloud native machines must be able to rapidly verify their identities with each other. Yet, the management of this proliferation of machine identities can be challenging in cloud native environments and organizations may have trouble keeping up with today's rapid pace of continual innovation.

This report examines the top threats and challenges that are impacting cloud native security and emphasizes the foundational role of machine identities within cloud native security. To better understand the state of cloud native machine identity management, Venafi sponsored an independent survey of 800 security and IT leaders in large organizations across the U.S., U.K., France, and Germany. The goal was to gather data that revealed how companies are approaching cloud native security, where they are facing challenges, which trends they are adopting, and who is responsible for setting strategy and implementing security and machine identity management in cloud native environments.

Executive overview

In today's software-first, on-demand economy, competitive advantage can be measured in weeks, days, or even hours. Speed wins. Application development teams are moving faster and faster to keep their businesses in the lead. Gone are the days of lengthy application development and release cycles. Modern businesses simply can't afford to wait around for critical new features. So, they are turning to strategies like containerization and microservices, which have made rapid-fire application enhancements a reality. Seemingly overnight, Kubernetes has become the de facto standard of this cloud native world, with 84% of survey respondents believing that Kubernetes will soon be the main platform used to develop all applications.

Yet, this rapid growth has not come without its share of challenges. The focus and application of cloud native development are evolving at a breakneck pace.

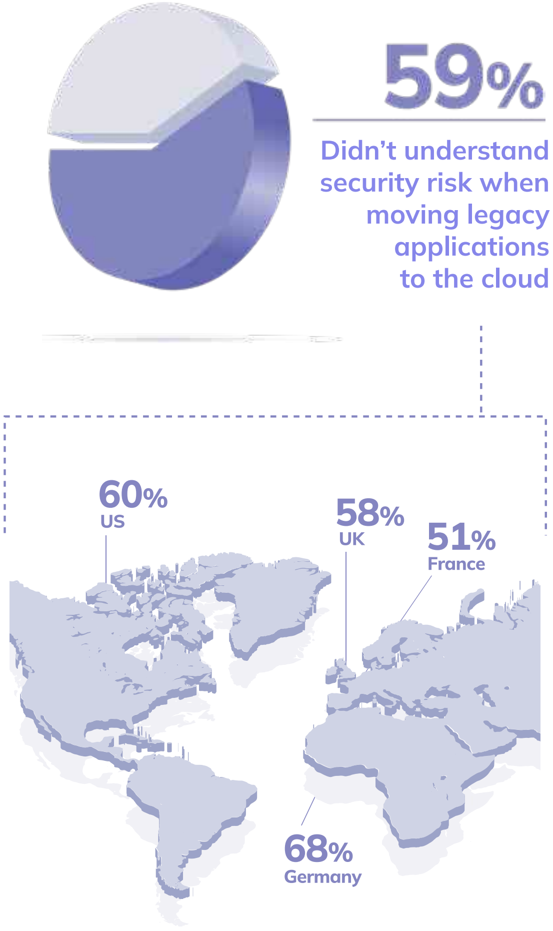


But in many cases, cloud native security is lagging behind. It's simply not top of mind for development teams. And there is little clarity on who should own the security function within engineering, platform, and development teams. Nowhere is this more apparent than in the use of machine identities in cloud native development. However, because they secure all communications and connections within a cluster, machine identities are the foundation of cloud native security.

Despite their relative importance, the application of machine identities in cloud native implementations—such as service meshes, software supply chain security and code signing of development artifacts—is often misunderstood.

Cloud adoption widespread, yet cloud native still lags

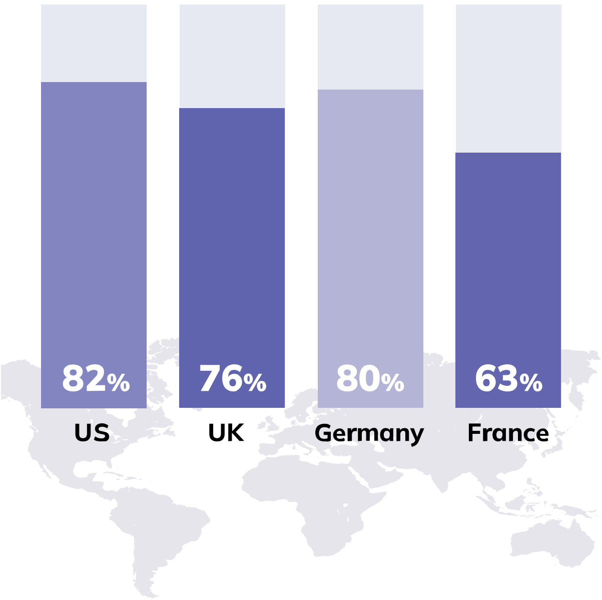
It's clear that organizations have recognized the benefits of moving to the cloud. Eighty-seven percent have started migrating their legacy applications. However, many are now realizing that they may not have spent enough time optimizing their approach for cloud native. Fifty-three percent did a lift and shift to the cloud with most application code remaining the same.



At the same time, nearly 59% of senior-level leaders admit they didn't understand the security risks when moving their legacy applications to the cloud. It's worth noting that this number varies by region and was significantly higher in Germany (68%) and lower in France (51%).

Many organizations also blindly migrated to the cloud without fully understanding the cost implications. Fifty-two percent have suffered from cloud sprawl and bill shock since moving legacy applications to the cloud. Seventy-seven percent of those impacted by cloud sprawl and bill shock have reconsidered moving applications to the cloud, although this was not as much of an issue in France, where only 62% admitted to reconsidering.

Reconsidered moving applications to the cloud



The bottom line is that organizations are eagerly adopting the cloud, but as the usage of Kubernetes increases and matures the resulting complexity of cloud native strategies becomes more visible. To manage these modern environments, organizations will need to promote proven patterns and tools that are unique to cloud native.

CLOUD SECURITY CHALLENGES

87% **have started to move legacy apps to the cloud**

53% **did a lift and shift to the cloud with most application code remaining the same**

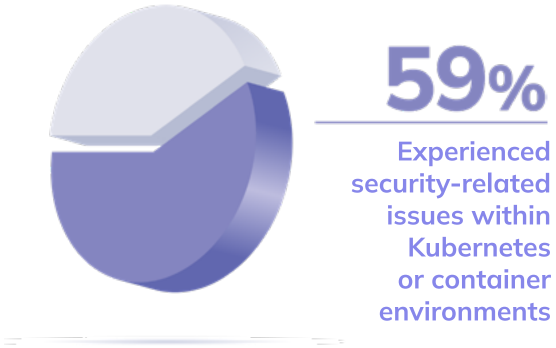
52% **have suffered from cloud sprawl and bill shock since moving legacy applications to the cloud**

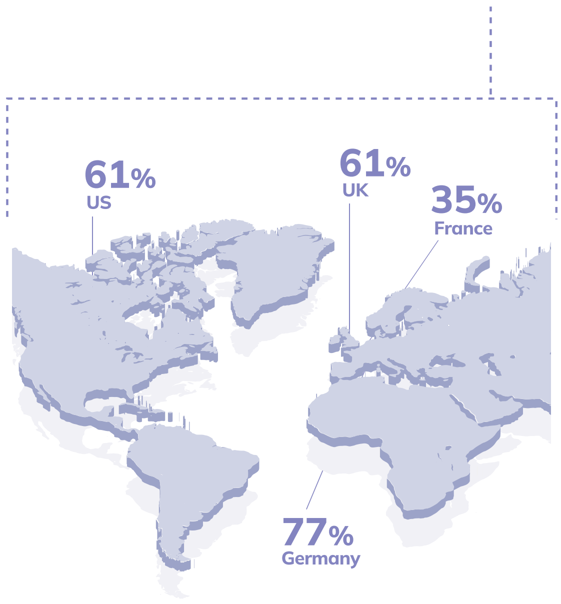
77% **of those impacted by cloud sprawl and bill shock have reconsidered moving applications to the cloud**

Organizations overconfident about maturity of their Kubernetes security

Even though most organizations failed to account for the unanticipated costs of cloud sprawl and bill shock, the vast majority believe that they have anticipated cloud native security issues and are prepared to counter them.

Yet reality may tell a slightly different story. Fifty-nine percent of respondents admit to having experienced security-related issues within Kubernetes or container environments. Again, security-related issues varied widely by region, with 77% in Germany and only 35% in France.

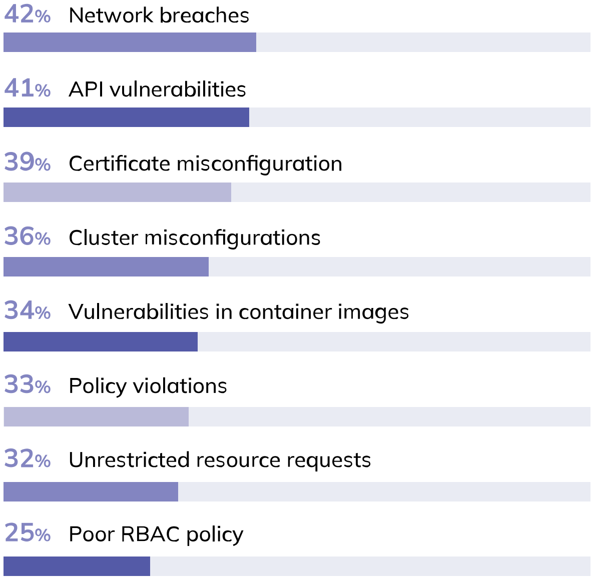




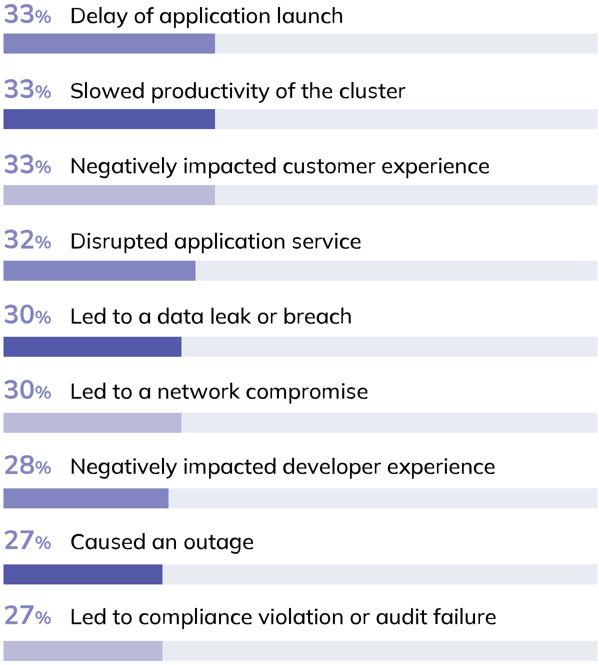
When queried about the main causes of security issues in Kubernetes or container environments, network breaches and API vulnerabilities topped the list. While machine identity challenges—such as certificate misconfiguration—came in third at 39% overall, they proved to be a more significant challenge in the US at 45%.

The consequences of these security issues can challenge the application development cycle in ways that many organizations may not have anticipated. For 33% of respondents, security issues delayed an application launch, while 32% experienced disruption to application services. Perhaps even more severe than these are the application outages that 27% of organizations experienced.

MAIN CAUSES OF SECURITY ISSUES



MAIN CONSEQUENCES OF SECURITY ISSUES IN KUBERNETES AND CONTAINER ENVIRONMENTS



Organizations grapple with unique risks of cloud native

Applications have become a primary target for attackers, and cloud native applications are no exception. Security teams are scrambling to secure these applications, which are evolving across architectures, and cybercriminals are adapting threat vectors to access them.

Even though organizations tend to be more than a bit optimistic about their cloud native security, they readily admit to a degree of uncertainty. However, cost is not the only unknown they have expressed concerns about. In fact, 76% agree that the world is heading towards a cloud reckoning in terms of both costs and security.

However, awareness and successful implementation of cloud native security remain lower than adoption rates should indicate. Seventy-five percent of respondents acknowledged that the speed and complexity of Kubernetes and containers create new security blind spots. To complicate matters even further, 69% believe that when moving to the cloud, they dragged a lot of old security problems with them.

CLOUD SECURITY CONCERNS

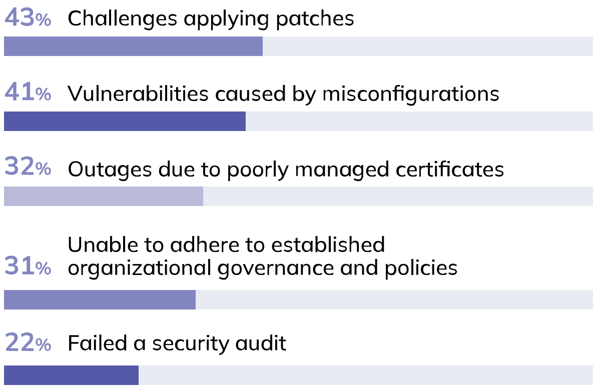
76% believe they are heading towards a cloud reckoning in terms of costs and security

75% believe that the speed and complexity of Kubernetes and containers are creating new security blind spots

69% acknowledge that when moving to the cloud, they dragged a lot of old security problems with them

While cloud native is touted as an enabler of competitive advantage, security issues can increase the risk of negative business outcomes—from downtime and lost revenue to data breaches and loss of customer trust. Among the top security challenges are vulnerabilities caused by misconfigurations and outages triggered by poorly managed certificates.

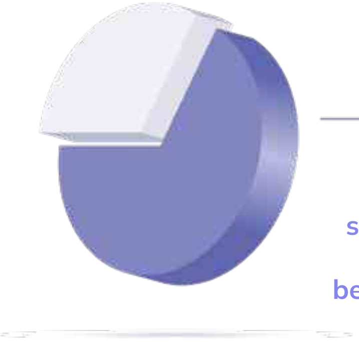
CLOUD NATIVE APP SECURITY ISSUES



Organizations disconnected from realities of cloud native security

Machine identity management is a critical requirement for Kubernetes clusters and workloads. Automating the creation and renewal of certificates is necessary to enable secure self-service for developers deploying applications on Kubernetes clusters. Far and away the most common tool that developers use for certificate management is the CNCF-backed open source solution cert-manager.

A recent CNCF survey indicated that 86% of new production clusters install cert-manager by default. Yet only 26% of security leaders were aware that their organization uses cert-manager to manage certificates in Kubernetes. It's no wonder that 73% believe it is hard for security teams to easily and securely meet developer-driven machine identity requirements for cloud native workloads. That may be one of the reasons that 68% of security leaders worry that delays in the process of issuing certificates may result in developers not using them at all.



68%

State that developers sometimes don't use certificates because issuance adds friction to developer processes

SERVICE MESH CHALLENGES

71% are concerned that service meshes just layer complexity on complexity

61% acknowledge they cannot issue certificates at the speed needed in Kubernetes and service mesh

61% confess that their certificate management system does not enable issuance for Kubernetes, CI/CD and service mesh

Complexity of cloud native security solutions is rising

Migrating from the data center to modern, cloud native environments has resulted in staggering levels of complexity in managing machine identities. This leaves many organizations overwhelmed by security needs that stretch across all aspects of the application life cycle. So, it's now more important than ever to keep abreast of cloud native security and how it's evolving to protect machine identities. Here is the state of security for some of the most common machine identity management trends for cloud native.

Service mesh: Does the complexity outweigh the advantages?

Organizations are looking to service mesh to gain observability into the communications between microservices. However, a service mesh can also help secure these communications by applying mutual TLS (mTLS) machine identities. This makes service mesh a valuable tool for cloud native security. But 71% of respondents admit that service meshes just layer complexity on complexity.

For some organizations, it's not a matter of overcoming complexity, but rather having the proper infrastructure to support a service mesh. Sixty-one percent acknowledge they cannot issue certificates at the speed needed in Kubernetes and service mesh. Perhaps these respondents are among the same 61% who confess that they don't even have machine identity management systems capable of issuing certificates for Kubernetes, CI/CD, and service mesh.

Software supply chain security highly valued, poorly implemented

The majority of organizations recognize the importance of software supply chain security as it can prevent unauthorized access and prohibit unsigned

SOFTWARE SUPPLY CHAIN CHALLENGES

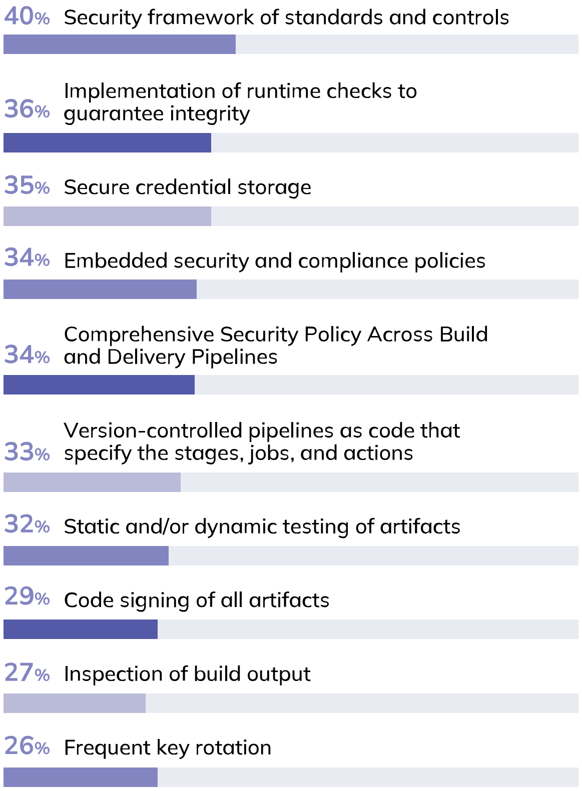
72% are concerned that third-party software is leaving gaps in security

70% believe that software supply chain attacks are their biggest security blind spot

61% worry that their organization isn't in a position to validate the security of all third-party software packages to run. Seventy percent of security and IT leaders believe that software supply chain attacks are their biggest security blind spot—and they are looking for viable solutions. Eighty-five percent believe that continuous security validation to the CI/CD pipeline is vital to reducing the risk of vulnerabilities going undetected during the software development lifecycle.

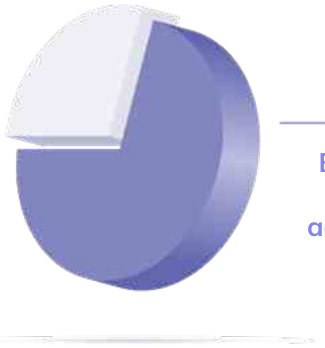
Although they acknowledge its importance, many organizations still struggle with implementing software supply chain security. Seventy-two percent are concerned that third-party software is leaving gaps in security, and 61% worry that their organization isn't in a position to validate the security of all third-party software.

HOW ARE ORGANIZATIONS PREVENTING SOFTWARE SUPPLY CHAIN ATTACKS?



Zero trust architecture vital, but ill-defined for cloud native security

Zero trust for cloud workloads enforces strict verification for any access to and from workloads to secure pods or nodes. Based on this critical function, 75% of security professionals believe the shift to cloud native accelerated their plans/adoption of zero trust.



75%

Believe the shift to cloud native accelerated their plans/adoption of zero trust

In a cloud native environment, the granular components of microservices are dynamic and short-lived—sometimes having a lifespan of only a few minutes. Perhaps that is why 88% of security and IT leaders also believe that the concept of machine identity is essential to the success of zero trust models.

In fact, 78% acknowledge that while centralized security teams may develop a zero trust strategy, they are not the ones to implement the controls that enable it. While this lack of ownership and enforcement may jeopardize the success of zero trust architecture in cloud native environments, that challenge was less of a factor in France (65%) than it was in the UK (86%).

ZERO TRUST CHALLENGES

79% admit that while zero trust is an essential way to approach security in modern distributed environments, it's too hard to implement

78% acknowledge that while centralized security teams may develop a zero trust strategy, they are not the ones to implement the controls that enable it

70% believe that while the idea of zero trust is logical, it's application often isn't

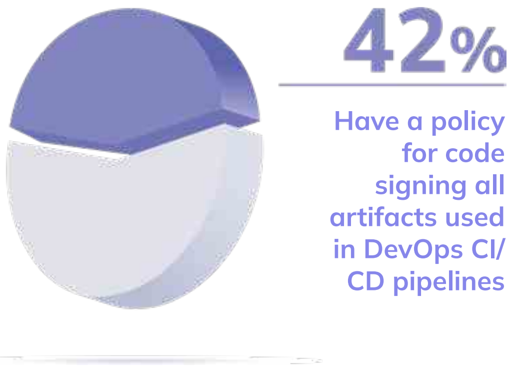
88% believe the concept of machine identity is essential to the success of zero trust models

Code signing of development artifacts gaining steady validation

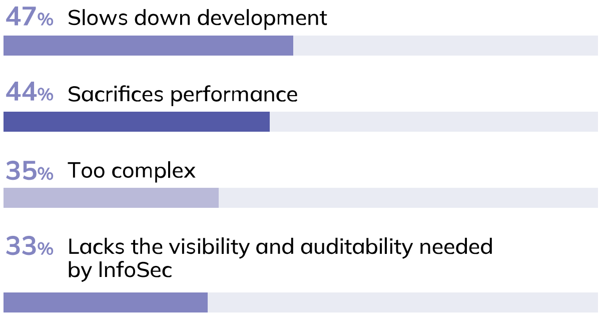
Development artifacts—including documents, files, scripts, libraries, and more—should be signed throughout the development cycle as a security best practice. Requiring developers to sign an artifact as they modify it helps prevent cybercriminals from accessing it and introducing undesirable components throughout the build process. Eighty-two percent of respondents say they sign at least some code, with 42% having a policy for code signing all artifacts used in DevOps CI/CD pipelines.

Organizations who are not signing all artifacts are concerned that such a policy could jeopardize the success of development cycles. Hence the age-old DevOps conflict between maximizing either security or performance, but not both.

Lack of clear ownership is further complicated by the fact that 90% admit that security teams need to increase their understanding of cloud native environments to ensure applications are secure.



REASONS FOR NOT CODE SIGNING ALL ARTIFACTS



Security teams also tend to be disconnected from the actual application and enforcement of the security policies that they set. Seventy-four percent worry that developers are challenged with several conflicting priorities, so security is not always top of mind.

In response, many organizations are moving security closer to developers. Eighty-nine percent believe platform engineering teams are or will be the next necessary evolution of DevOps. What's more, in 62% of organizations, it is the development or platform teams who are responsible for ensuring that the tools that allow cloud native security align with wider organizational governance and policies.

SECURITY TEAM OWNERSHIP

90% confess that security teams need to increase their understanding of cloud native environments to ensure applications are secure

85% allow security teams to set the strategy for managing security risk and governance across cloud native environments

PLATFORM OR DEVELOPMENT TEAM OWNERSHIP

89% believe platform engineering teams are or will be the next necessary evolution of DevOps

74% worry that developers are challenged with several conflicting priorities, so security is not always top of mind

62% trust development or platform teams to ensure the tools that allow cloud native security align to wider organizational governance and policies

What Security and IT Leaders Need to Know

The cloud has changed the application lifecycle in ways that many organizations did not anticipate. Development teams are now expected to deliver production code at warp speed, but security teams are struggling to keep pace. At the center of the tradeoff between speed and security is the management of machine identities.

Yet, many organizations are still trying to strategize the best ways to integrate machine identities into their cloud native application development cycles. They are unsure who should own the security of machine identities going forward, although many are shifting priorities to move security closer to the development process. Here are some key takeaways to keep in mind as you plan your cloud native machine identity management strategy moving forward.

- Machine identity management has become the foundation of cloud native security with 88% believing that it is essential to the success of zero trust models
- Organizations are reevaluating their cloud strategies to maximize the advantages of cost and security
- Cloud native-focused attacks are on the rise with 59% experiencing security-related issues within Kubernetes or container environments
- Security teams are ill-prepared to protect against cloud native attacks with 90% of professionals admitting that they need to increase their understanding of cloud native environments to ensure applications are secure
- Security teams are hampered by lack of enforcement within development teams, with 68% worried that the latency of issuing certificates means that developers may not use them
- 74% worry that because developers are challenged with several conflicting priorities, security may not always top of mind
- Many organizations are moving security closer to the development process with 62% turning to development or platform teams for the cloud native security tools that align to wider organizational governance and policies
- Service mesh is recognized as a valuable cloud native strategy, but suffers from complexity that dampens adoption efforts
- Organizations are concerned about software supply chain attacks, but are not confident in their prevention methods
- Code signing development artifacts is acknowledged as a successful security practice for preventing software supply chain attacks

Venafi is the cybersecurity market leader in identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. **To learn more, visit venafi.com.**