Welcome to our 2018 report on the state of securing cloud workloads

A summary of the responses of close to 350 professionals whose primary areas of responsibility within their organizations include this important task.

Cloud workload security is at an important juncture. DevOps has revolutionized the velocity at which apps are deployed and updated, while containers and functions-as-a-service (serverless) result in highly distributed and modular apps that are hosted on complex hybrid and multi-cloud infrastructures. Traditional perimeter-based approaches cannot meet the security requirements of these next-generation apps, and we’re seeing new paradigms based on a shift-left approach that bring security to the app layer early on.

The emergence of reliable, scalable automation and orchestration solutions was essential for DevOps, containers, and serverless to become mainstream technologies. In order to close the security gap for cloud workloads, a similar ecosystem is required that can support consistent implementation of security policies at scale and provide visibility across the entire service mesh.

Yet, the results of our survey indicate that, in 2018, cloud workload security workflows are still highly fragmented. Enterprises of all sizes are, for the most part, manually configuring security for their different workloads. At a time when security and privacy requirements are becoming even more stringent, manual workflows are a constraint on business velocity. Thus, there is still an unmet need for end-to-end platforms that can support DevOps and security professionals in securing cloud workloads in a way that accelerates business outcomes and enhances their enterprise’s competitive edge.

Top Five Survey Highlights

53% of respondents have a hybrid cloud setup, while 19% are running multi-cloud

67% believe serverless environments are "very" or "completely" secure, but only 7% believe their organizations are "serverless pros."

28% are already using serverless, and only 20% have no plans to look at it over the next year.

75% of respondents will increase the number of security tools they rely on over the next 12 months.

60% of organizations still manually configure security policies for apps.
All Key Findings

What’s Happening in Cloud Environments

- Securing cloud workloads is still largely the responsibility of the corporate IT security team, but there is a growing trend towards more specialized DevOps and DevSecOps teams taking over these tasks.

- A little more than three out of every four organizations, across all company sizes, distribute their cloud workloads across a complex infrastructure—either hybrid (~57%) or multi-cloud (~19%).

- IT specialists are embracing containers, serverless, and service-mesh as security enablers rather than security obstacles.

Cloud Security Stack and Controls

- The stack used to secure cloud workloads is highly fragmented. The larger the organization, the higher the fragmentation.

- Across all company sizes and job types, 75% of the respondents expect their cloud security stack to increase during the next 12 months—either “significantly” (20%) or “somewhat”.

- Security groups and host-based threat protection are the most prevalent cloud workload security controls in use across enterprises of all sizes.

App Security Configuration

73%

Of security pros are still configuring application security policies manually.

Most configurations are highly decentralized: 44% of medium-large enterprises and 74% of very large enterprises have 3 or more people involved in the configuration of security policies for any given app.

Serverless Computes

- Three out of four enterprises are running their serverless computes in production environments, while one out of five run serverless only in production.

- 44% of IT specialists consider their enterprise’s serverless computes to be only “somewhat secure.”

- With only 7% believing that their enterprise has a high level of serverless expertise, these respondents are aware that there is still a learning curve in terms of understanding how and when to apply effective security controls in serverless apps.
Methodology

This online survey was conducted by Informa Engage on behalf of IT Pro Today, a leading content portal for the IT industry, and Alcide, a cloud-native security platform for even the most complex deployment architectures.

During August 22-28, 2018, 346 responses were gathered from IT Pro Today subscribers who have direct involvement in data center selection and management in their organizations. Their primary areas of responsibility and IT job functions were as follows:

![Primary Areas of Responsibility Chart]

- **IT administration**: 41%
- **IT leadership**: 13%
- **IT MANAGEMENT (Director level)**: 35%
- **Other**: 11%

![Primary IT Job Function Chart]

- **Operations**: 48%
- **Development**: 15%
- **Security**: 12%
- **Other**: 6%
- **Cloud architecture**: 11%
- **DevOps or DevSecOps**: 8%

What’s Happening in Cloud Environments

**Level of Personal Involvement in Cloud Environments**

*Q: What is your level of involvement in architecture, development or security of your company’s cloud environments?*

Regardless of enterprise size, for a little more than 90% of the respondents, the enterprise’s cloud environment is either their primary responsibility (21%) or among their responsibilities. The remaining 6% consider themselves influencers, i.e., they are not directly involved in implementation but they have a say in cloud-related decisions and policies.
Security Ownership: Functional Ownership of Securing Cloud Workloads

In your organization, who is primarily responsible for securing cloud workloads?

Not surprisingly, in almost half of the organizations surveyed, regardless of size, the corporate security team (46%) is responsible for securing the enterprise’s cloud workloads. However, in a little more than 34% of the organizations, it is a more specialized DevOps or DevSecOps team that takes on this responsibility. We will continue to track this metric in future surveys, which we believe will show that this trend towards specialization is deepening.

Workload Distribution Across Cloud Infrastructures

How does your organization currently distribute workloads?

A little more than three out of every four organizations, across all company sizes, distribute their workloads across a complex infrastructure—either hybrid (53%) or multi-cloud (18%). These results are fully consistent with what Alcide sees among its customers, and it is generally accepted within the IT sector that the implementation of hybrid and multi-cloud infrastructures will continue to grow.
Usage of Cloud Compute

Q Which of the following cloud computes does your organization use? (Select all that apply.)

- Virtual machines (VMs) 81%
- Containers 33%
- Serverless 26%
- Bare metal 22%
- Service-mesh 18%
- Other 3%

Not surprisingly, in almost half of the organizations surveyed, regardless of size, the corporate security team (46%) is responsible for securing the enterprise’s cloud workloads. However, in a little more than 34% of the organizations, it is a more specialized DevOps or DevSecOps team that takes on this responsibility. We will continue to track this metric in future surveys, which we believe will show that this trend towards specialization is deepening.

Focus on Serverless Environments: Security & Motivation

Running Across Production/Development - Serverless Compute Use Cases

Q Do you run serverless in production or development stages?

Three out of four enterprises are running their serverless computes in production environments, while one out of five run serverless only in production. These results are a clear indication that serverless architectures have gone mainstream. We expect this trend to continue.
Primary Motivation for Using Serverless

Q What is your organization’s primary motivation for using serverless?

- Reducing operation costs: 39%
- Improved utilization: 29%
- Hybrid-cloud applications: 27%
- Testing it out: 10%

There are three leading motivations for using serverless, with reducing operation costs a little bit ahead of improved resource utilization and managing apps in a hybrid cloud environment.

Security Perceptions - Security of Serverless Computes

Q In your opinion, how secure are your serverless computes?

Almost 60% of all respondents and IT security pros consider their organization’s serverless computes to be very secure. However, none (0%) of the IT security specialists were prepared to declare serverless computes as "completely" secure (vs. 10% of all responses), and more of them perceive the organization’s serverless computes as "somewhat" secure vs. the full pool of respondents (44% vs. 32%).

Just as containers were not fully understood when they first went mainstream about two years ago, security issues associated with serverless computes are not yet fully understood. In containerized apps, developers have learned how to effectively secure the OS and hardware layers that are shared across multiple containers. The serverless architecture offers developers a similar security opportunity across the abstracted application and web server layers. However, there is still a learning curve in terms of understanding which security controls to implement at which app lifecycle stages.
Level of Expertise in Serverless Environments

Q Do you believe your organization has the expertise to run serverless environments?

- 7% We’re serverless pros
- 40% We’re fairly competent
- 34% We’re fairly competent
- 20% Serverless is not on our radar this year

There seems to be a sizable gap between the proliferation of serverless computes (see Running Across Production/Development) and the expertise required to manage and secure them. Only 7% of the respondents believed that their organizations had reached a high level of serverless expertise, while another 40% of respondents believed that their organizations had reached competency. Emerging next generation serverless automation and orchestration tools can help close this gap.

Securing Cloud Workloads

Cloud Security Controls in Use

Q Which of the following cloud security controls does your organization currently use? Select all that apply.

- Security groups: 63%
- Host-based threat protection: 59%
- File integrity monitoring: 44%
- Account compliance features: 42%
- Visibility tools: 38%
- Other: 3%

Organizations must deploy a wide range of solutions in order to secure their cloud environments. Security groups and host-based threat protection are the most prevalent cloud security controls in use across enterprises of all sizes.
Number of Cloud Solutions Used

How many cloud computing solutions does your organization use to secure your cloud workloads (application security, CASB, other cloud-based security services)?

In general, the results reflect a high level of fragmentation in the cloud stack used to secure workloads. **The larger the organization, the higher the degree of fragmentation.** A little more than one in five (22%) of very large enterprises (1000+ employees) are using 10 or more solutions to secure their cloud workloads compared to only 3% of the medium-large organizations (100-999 employees).

It is also telling that fairly high percentages of respondents are not sure how many solutions are being used to secure cloud workflows in their organizations. Fragmented stacks and poor visibility into deployed solutions are very often constraints of business velocity, due to the difficulties in scaling securely and reliably.
Expected Change in Number of Cloud Security Tools (By company size)

Q Over the next 12 months, how do you expect the number of cloud security tools your organization uses to change (decrease somewhat, remain the same, increase somewhat, increase significantly)?

Across all company sizes and job types, 70% of the respondents expect their cloud security stack to increase during the next 12 months—either "significantly" or "somewhat". The other 25% expect it to remain the same. No respondents chose the option "decrease somewhat."

In other words, the current challenges in managing a wide array of cloud security solutions (see Number of Cloud Solutions Used) are only going to be exacerbated as the stack becomes even more fragmented. Winning enterprises will be seeking overarching platforms that can give them full visibility into, and centralized control over, their cloud security policies and implementations.
Securing Applications

Prevalence of Manual Configuration by Primary Job Function

Q Does your organization need to manually configure security policies for applications?

Quite shockingly, according to the security pros among the respondents, the vast majority of organizations (73%) are still configuring application security policies manually. In our highly automated DevOps world, time consuming and error-prone manual security processes are unacceptable constraints on business velocity for organizations of all sizes. Alcide’s platform is purpose-built to open this bottleneck.

Number of Employees Involved in Configuring Security Policies

Q On average, how many people in your organization are involved in configuring security policies for a given app?

We were very surprised by these results: 44% of medium-large enterprises and 74% of very large enterprises have 3 or more people involved in the configuration of security policies for any given app. As we saw in Prevalence of Manual Configuration and Number of Cloud Solutions Used, most of that security configuration work is done manually with a highly fragmented stack.

The bottom line of all these data points is that cloud security as it is implemented today can be a significant constraint on business velocity. However, organizations that succeed in using next generation security tools to automate and streamline their security processes will benefit from a strong competitive edge.
Summary

Our survey results clearly indicate that, in 2018, cloud security has not yet benefited from the great strides that have been made in automating the security and management of resources and the continuous deployment of apps. Almost one out of four (73%) organizations are still manually configuring their application security policies and are using a highly fragmented stack to do so. In fact, a little more than one in five (22%) of the very large enterprises (1000+ employees) surveyed are using 10 or more security solutions—a combination that has the potential to slow down business-critical initiatives. And, regardless of company size, 75% of respondents expect their cloud security stack to increase during the next 12 months.

The trend towards complex cloud infrastructures, such as hybrid-cloud and multi-cloud (53% and 18% respectively of the organizations surveyed), as well as the trend towards microservices and serverless (with 75% of enterprises running their serverless computes in production environments) have rendered traditional security paradigms ineffective. Organizations are on a steep learning curve, with 44% of IT specialists considering their serverless computes to be only "somewhat secure" and only 7% believing that their enterprise has a "high level" of serverless expertise.

Innovative, cloud-native, cross-environment security solutions are required to provide effective management and real-time responses to a wide range of attack scenarios with a unified security controls that span over the cloud infrastructure, workloads, and services. Automation is critical in order to consistently implement corporate security and compliance policies within a holistic yet simple and agile framework.

How Can We Help?

Alcide is the cloud-native security company with the mission to empower DevSecOps and security teams, to manage application and networking security through the intelligent automation of security policies applied uniformly, regardless of the workload and infrastructure.

Book your personal demo today