# 2020 STATE OF Hybrid Cloud Security

Our second annual survey finds no relief for enterprises dealing with increased complexity and scale of their hybrid cloud environments. Many enterprises are overburdened by the continuous onslaught of hybrid cloud security challenges including lack of automation and third-party tool integration, coupled with budget constraints and staffing shortages.

FIREMON

# Executive Summary

In the past 20 years, cloud computing has transformed from a niche concept to a ubiquitous standard, delivering groundbreaking technologies in cloud platforms and security solutions. While the advances in the cloud have enabled enterprises to venture into new areas for innovation and growth faster than ever, their efforts to secure their cloud environments effectively have come up short. Between the use of multiple cloud platforms and heterogeneous security solutions to the lack of qualified personnel needed to implement and manage them, enterprises find themselves compromising security to achieve their business objectives.

FireMon's second annual State of Hybrid Cloud Security report dives into how the proliferation of cloud environments is impacting enterprises and their ability to scale and protect them. We discovered across a survey pool of 522 IT and security professionals that the state of hybrid cloud security hasn't improved since our inaugural State of Hybrid Cloud Security report. Our findings have uncovered three main themes, which will be examined further in this report:

**1 Increased Complexity and Scale of Hybrid Cloud Environments**

Mainstream cloud adoption is leading to increasing hybrid cloud complexity and sprawl.

**2 Lack of Automation and Third-Party Tool Integration**

Manual processes and disparate tools leave security teams shorthanded in the race to innovation.

**3 Limited Budgets and Staffing Shortages**

Overstrained security teams are left to contend with limited staffing, reduced budgets and uncertain relationships with DevOps.

**While the mainstream adoption of the cloud brings new opportunities to drive innovation, it also leaves enterprises challenged by increased complexity, lack of automation and third-party tool integration, and limited staff and budget.**

CHAPTER 1

# Mainstream Cloud Adoption is Increasing Complexity and Scale of Hybrid Cloud Environments

The appeal of cloud computing is undeniable. Cloud-based applications and services have gone mainstream, with the promise of flexibility, convenience and speed to drive business initiatives. Through 2022, analysts project the market size and growth of the cloud services industry at nearly three times the growth of overall IT services. Enterprises are embarking on digital transformation projects to refresh their infrastructures, improve productivity and drive innovation in revolutionary ways.

But the rush to accelerate digital transformation efforts and beat the competition comes at a cost. According to ESG, 86% of IT professionals and application developers report their companies are under pressure to develop and launch new products and services at an accelerating pace. With no change from last year's report, **almost 60%** of this year's respondents say that deployment of their business services in the cloud has accelerated past their ability to adequately secure them in a timely manner. As enterprises attempt to protect their hybrid clouds using multiple security solutions, they inadvertently contribute to the increasing complexity of securing their environments.

**Within the past two years, the number of organizations committed to a hybrid cloud strategy has increased from 58% to 76%, according to ESG.**

CHAPTER 1

## Mainstream Cloud Adoption is Increasing Complexity and Scale of Hybrid Cloud Environments

The hybrid cloud is here to stay. While there are potential security challenges that come with moving to the cloud, enterprises are not deterred. Our report finds that 78.2% of respondents use two or more different enforcement points on their hybrid network, up 19.2% from 59% of respondents from last year's report (fig. 1).

In addition, enterprises have become more comfortable with the move to public cloud platforms, with almost 50% of respondents using two or more different public cloud platforms and 35.1% of respondents using two or more container platforms (fig. 2).

**Only 9.8% of respondents indicated they do not use any public cloud platforms, down 15.8% from 25.6% in 2019.**

**Fig. 1**
Number of Different Enforcement Points on the Network

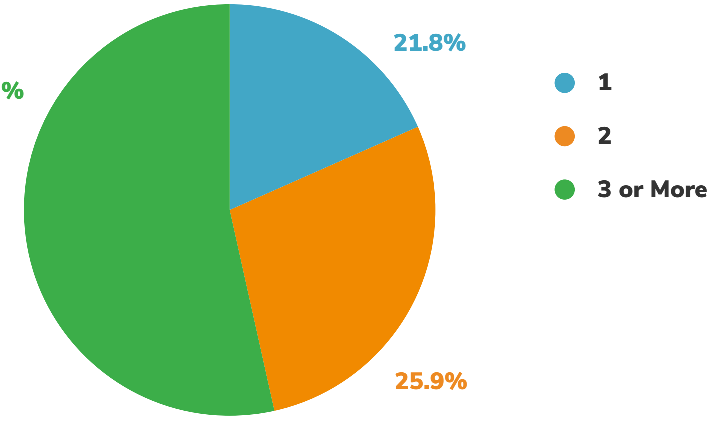
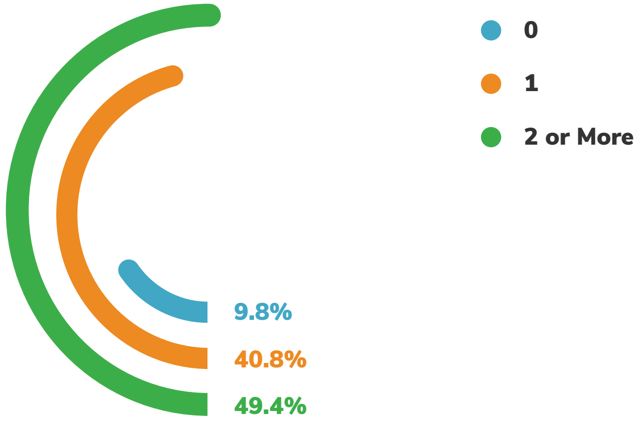


**Fig. 2**
Number Of Public Cloud Platforms Currently Being Used



## CHAPTER 1

### Mainstream Cloud Adoption is Increasing Complexity and Scale of Hybrid Cloud Environments

Enterprises are also embracing the hybrid cloud, with 41.4% of respondents indicating they have a hybrid cloud environment currently in production, an increase of 1.5% from last year. While 46.8% of respondents are deployed in public cloud (a slight decrease of 3.2% from last year), almost 25% of respondents are in proof of concept or planning to deploy in the next 12 months (up 6.4% from last year) (fig.3).

As more enterprises move to public cloud platforms, there is still some confusion on the shared responsibility security model and a lack of understanding on where security obligations fall. Our report finds that while respondents are using one or more "as-a-Service" models in tandem, those who do not understand the model or did not know responsibility was shared came in at 21.8% for Software-as-a-Service (SaaS), 20.7% for Platform-as-a-Service (PaaS), and 18.8% for Infrastructure-as-a-Service (IaaS) (fig. 4).

**Only 64.8% of respondents understand the shared responsibility security model for Software-as-a-Service (SaaS).**

**Fig. 3**
How are you currently (or planning to be) deployed in the cloud?

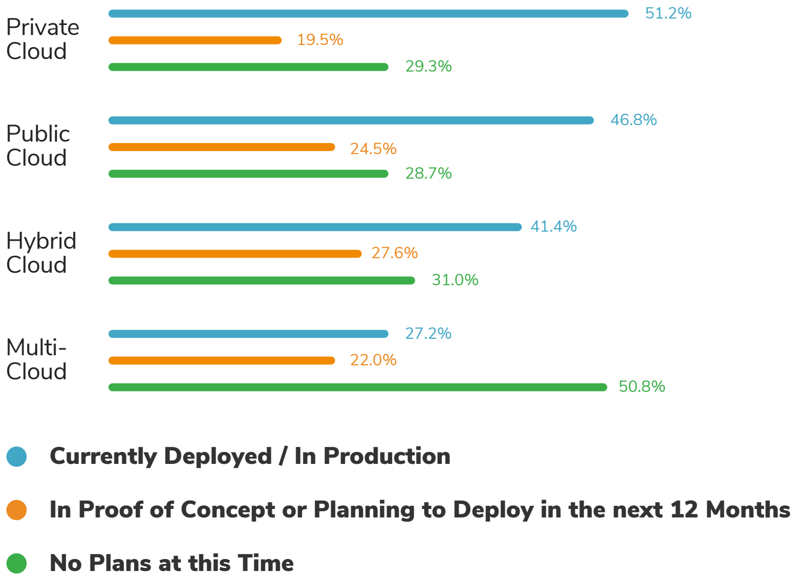
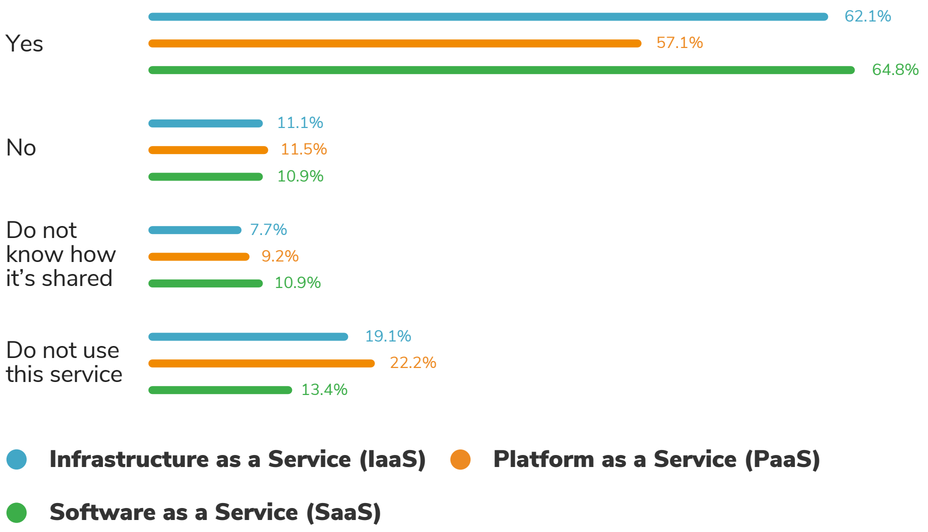


**Fig. 4**
Do you understand the shared responsibility security model for the following cloud services from your cloud provider(s)?



## CHAPTER 1

### Mainstream Cloud Adoption is Increasing Complexity and Scale of Hybrid Cloud Environments

Whether there is an understanding or not of the shared responsibility security model, enterprises find themselves exposed to many security challenges in their public cloud environment. 17% of respondents (and 17.8% of C-Level respondents) say that “lack of visibility” is their biggest challenge in securing their public cloud environment (up 1.9% from last year). 13.8% of respondents say “lack of control” and “lack of ownership/lack of integration with other tools” tied at 13% for the biggest challenge in securing their public cloud environment (fig. 5).

As hybrid cloud environments grow in scale and complexity, many enterprises find themselves challenged with maintaining the integrity of their overall security posture. Almost a third of respondents indicate that “misconfigurations/wrong set-up” is the biggest security threat to their hybrid cloud environment. 19.5% of respondents say that “unauthorized access” is the biggest threat to their hybrid cloud environment, followed by “ransomware/malware” at 13% (fig. 6).

**73.5% of those who indicated misconfigurations/wrong set-up was the biggest threat to their hybrid cloud environment are using manual processes.**

**Fig. 5**
What is your biggest challenge in securing your public cloud environment?

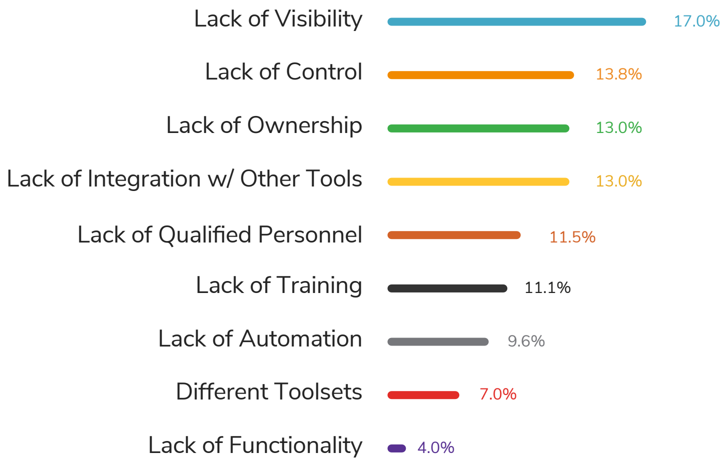
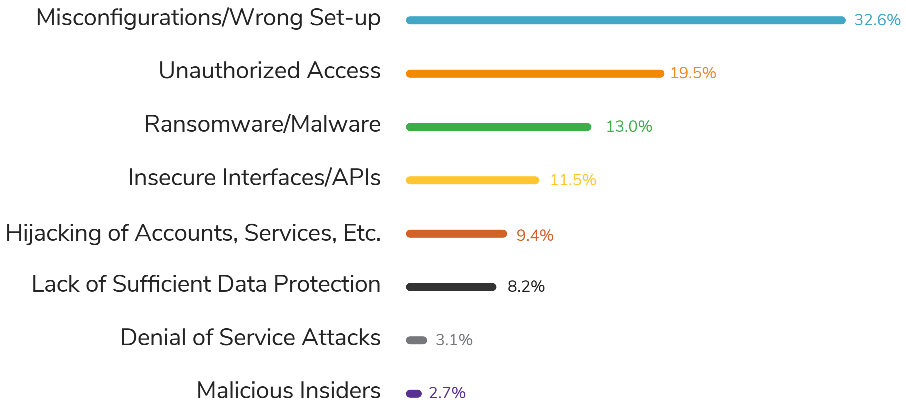


**Fig. 6**
What do you think is the biggest security threat to your hybrid cloud environment?



CHAPTER 2

# Lack of Automation and Integration of Third-Party Tools Complicate Security in a Fast-Moving Hybrid Cloud

The lack of security automation is posing issues for enterprises with complex, hybrid cloud environments. Overworked and understaffed, many security teams are left relying on time-consuming and error-prone manual processes. Misconfigurations have emerged as the primary reason for several high-profile security breaches, as security teams struggle with limited resources, too many disparate tools, lack of training, and hybrid network complexity.

The lack of third-party tool integration also introduces security implications in the hybrid cloud. According to the SANS Institute, integration requirements across the IT stack today are numerous, broad and complex, making it nearly impossible for operational teams to develop the unique plug-ins needed to orchestrate tasks across all the endpoints and security tools in place within their infrastructure. But with robust, open application programming interfaces (APIs), enterprises can adapt as their infrastructure and security demands change to ensure they incorporate the critical data they need to orchestrate their security tools across their entire hybrid network.

**According to the Ponemon Institute, 56% of organizations report a lack of in-house expertise is one of the biggest challenges impeding adoption of security automation.**

CHAPTER 2

## Lack of Automation and Integration of Third-Party Tools Complicate Security in a Fast-Moving Hybrid Cloud

Despite the growing need for security automation, many enterprises still use manual processes. Our survey finds that when asked about the level of security automation implemented in their hybrid environment, 65.4% of respondents indicated they use manual processes (fig. 7).

Respondents in this year's survey are at a low DevOps maturity level when it comes to ensuring that their disparate and/or siloed tools work together in a connected ecosystem through a converged toolchain. Our survey finds that only 36.8% of respondents say that their DevOps toolchain is integrated into their cloud deployments (fig. 8)

**35.4% of respondents do not have any level or security automation implemented in their hybrid environment.**

**Fig. 7**
What level of security automation do you have currently implemented in your hybrid environment?

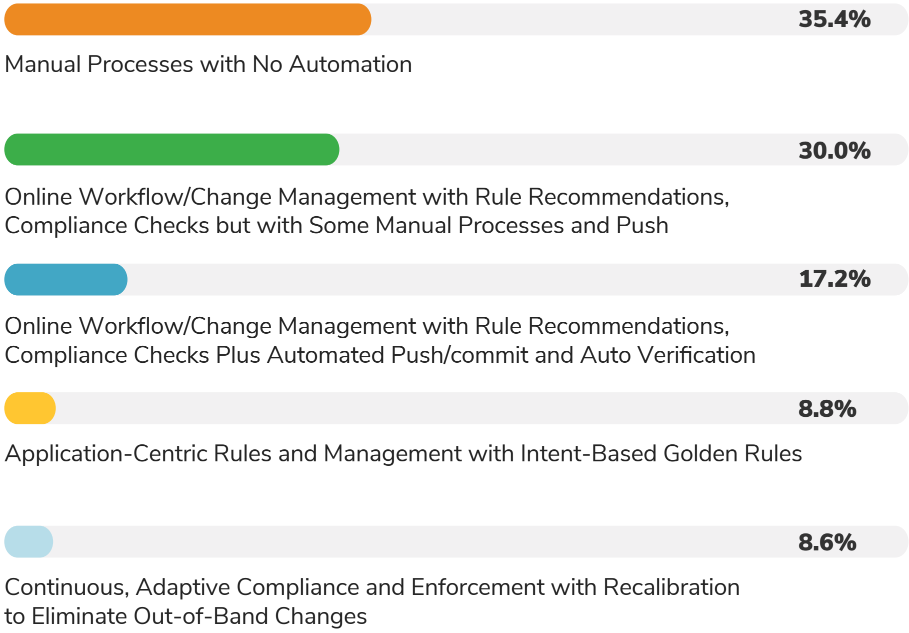
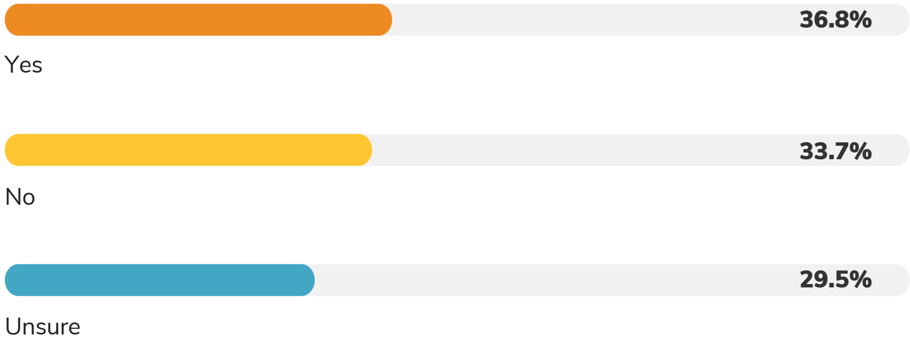


**Fig. 8**
Is your DevOps toolchain integrated into your cloud deployments using tools like Jenkins, Ansible, etc.?



CHAPTER 2

## Lack of Automation and Integration of Third-Party Tools Complicate Security in a Fast-Moving Hybrid Cloud

With the growing number of different security tools being used to protect hybrid environments, security teams are still feeling the pain associated with these tools not talking to each other. While 34.5% of respondents who manage network security across their hybrid cloud using tools that work across multiple environments shows a 6.5% improvement from last year, the percentage of respondents who use native tools for each environment jumped from 19.3% last year to 29.5% in this year's report (fig. 9).

Managing multiple network security tools across the hybrid cloud environment without adequate integration or automation poses several challenges for resource-strapped security teams. 24.5% of respondents say that their biggest challenge in managing multiple network security tools across their hybrid cloud environment is "No centralized or global view of information from the tools." 17.6% say there are "Too many tool suites and management consoles to keep up with" and 15.3% say there is a "Lack of actionable data derived from the tools" (fig. 10).

**40.4% of respondents are using two or more network security controls in their public cloud environment.**

**Fig. 9**
How does your organization manage network security across hybrid environments?

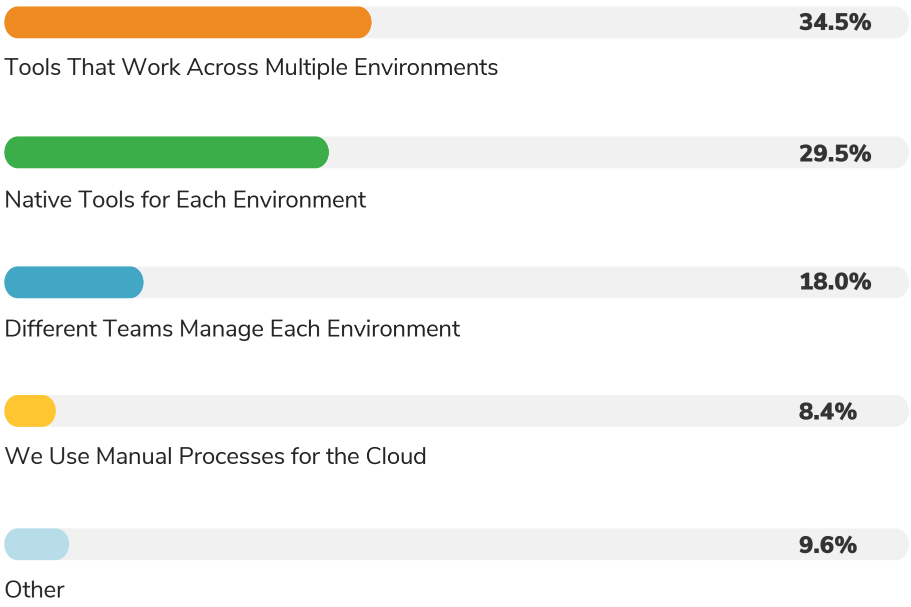
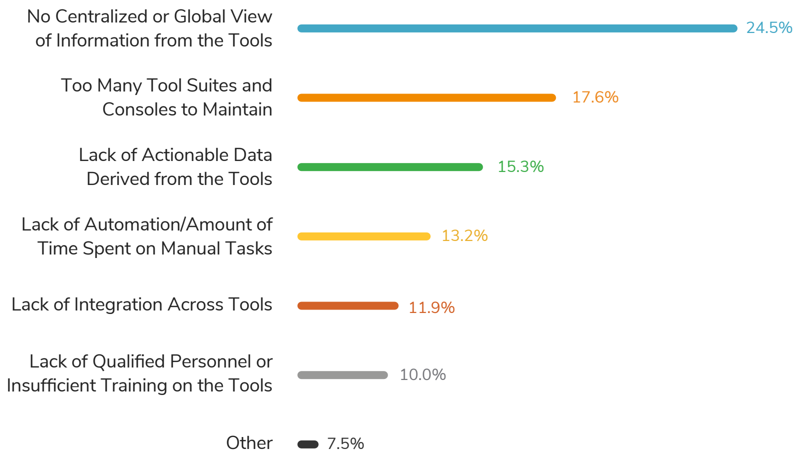


**Fig. 10**
What is your biggest challenge in managing multiple network security tools across your hybrid cloud environment?



## CHAPTER 2

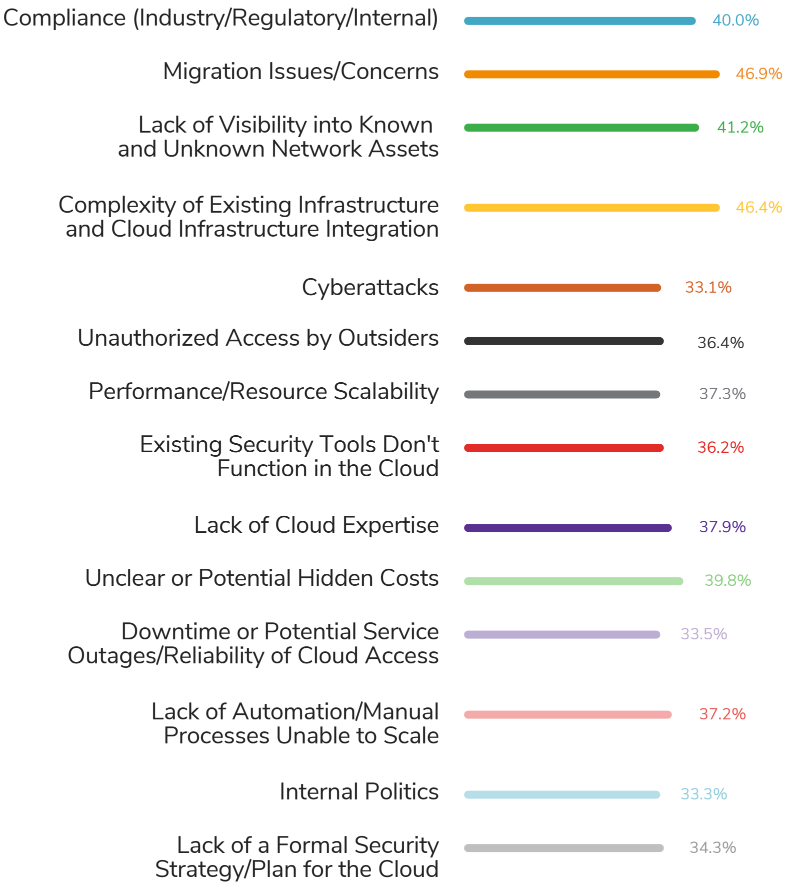
### Lack of Automation and Integration of Third-Party Tools Complicate Security in a Fast-Moving Hybrid Cloud

The roadblocks and challenges that keep enterprises from moving workloads to the public cloud touch across all the main themes uncovered in this year’s report. The top five that respondents say are “very challenging” include:

1. Cyberattacks
2. Compliance (industry/regulatory/internal)
3. Unclear or potential hidden costs
4. Lack of visibility into known and unknown network assets
5. Internal politics

Respondents were asked to rank each roadblock and challenge as very challenging, somewhat challenging, neutral, minimally challenging or not challenging at all. The highest ranking for each option across the board was "somewhat challenging" (fig. 11), highlighting the many challenges enterprises face when moving to the public cloud.

**Fig. 11**
What do you consider to be the biggest roadblocks and challenges that keep your organization from moving workloads to the public cloud? (Somewhat Challenging Responses)



**As seen in figure 11 above, the biggest roadblocks and challenges that keep enterprises from moving workloads to the public cloud in this year’s survey are all “somewhat challenging” for all 522 respondents.**

**CHAPTER 3**

# Decreasing Budgets and Staffing Shortages Continue to Overburden Security Teams

The cybersecurity staffing shortage continues to hit record levels. According to the InfoSec Institute, the shortage of cybersecurity professionals has grown to nearly three million globally, with approximately 498,000 openings in North America alone. Security teams are lean and their workloads have increased, and it's evident with the fact that only 26% of IT and cybersecurity professionals report that their organization sought cybersecurity staff augmentation services over the last 12-18 months, according to ESG.

Cloud security budgets are in transition as well, as enterprises work to restructure their budgets to accommodate different accounting rules for cloud services that do not apply to on-premises environments. According to the SANS 2020 IT Cybersecurity Spending Survey, there were some misguided perceptions that the cloud is inherently safe. This led some enterprises to defer investments in cloud security. In the end, when asked how they would allocate additional security budget, 32.7% of respondents say they would add more staff.

**Spending trends will transition from CapEx to OpEx in the "as-a-Service" era, but the pivot will not be seamless. Increasing cloud spend comes with add-ons which require enterprises to prioritize and manage digital technology.**

CHAPTER 3

## Decreasing Budgets and Staffing Shortages Continue to Overburden Security Teams

In this year's survey, 78.2% of respondents say that they spend less than 25% of their total security budget on the cloud, up 20.7% from 57.5% of respondents from last year's report. 44.8% of respondents spend less than 10% of their total security budget on the cloud (fig. 12).

While cloud security spending looks bleak, there is hope for cloud security budgets in the next year, with 55.2% of respondents indicating that their cloud security budget will increase in the next 12 months (fig. 13).

**While current spending levels are down for cloud security, 55.2% of respondents say their cloud security budgets will increase in the next 12 months.**

**Fig. 12**
What percentage of your total security budget do you currently spend on the cloud?

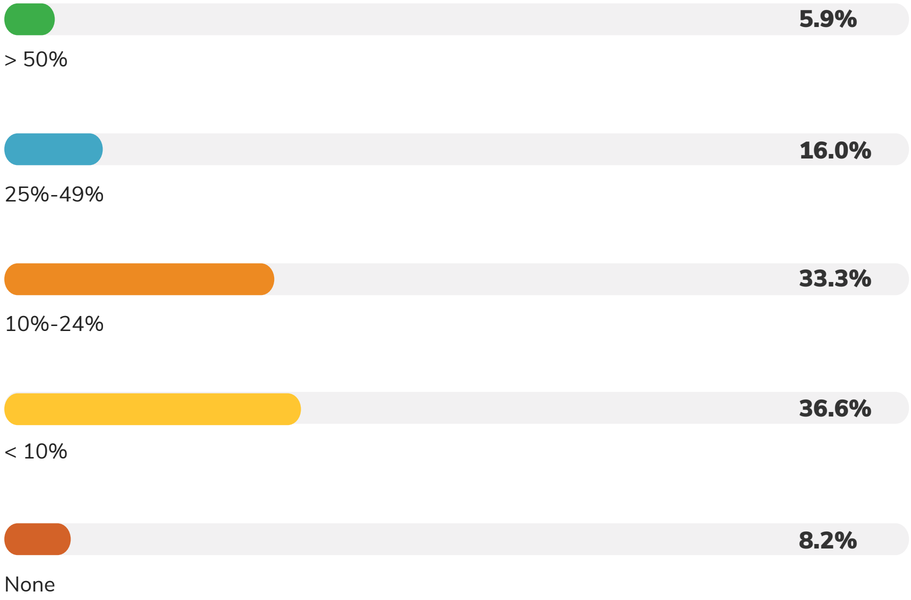
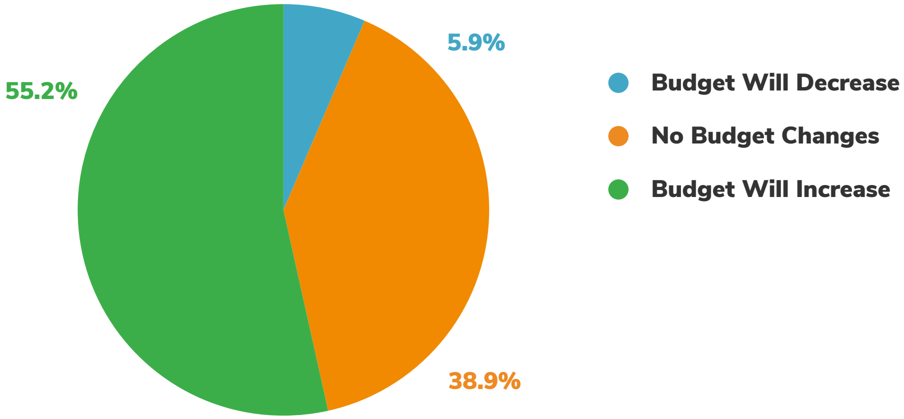


**Fig. 13**
How will your cloud security budget change in the next 12 months?



## CHAPTER 3

### Decreasing Budgets and Staffing Shortages Continue to Overburden Security Teams

While there is some hope for cloud security budgets, security staffing woes continue to challenge enterprises. Our survey found that 69.5% of respondents have a security team of 10 people or less (compared to 52% last year), with 45.2% of respondents indicating they have a security team of less than five people (compared to 28.5% last year) (fig. 14).

Lean security teams are also dealing with increased workloads and taking on more responsibility for different environments. Our survey finds that 59% of respondents manage both on-premises network security and cloud security for their organization (compared to 54% last year). Of the 59% of respondents who manage both, 66.4% work at organizations with less than 1,000 employees (fig. 15).

**30.7% say that the "IT/Cloud Team" is responsible for network security in the cloud, followed by the "Network Security Team" (22.2%), "Network Operations" (13.4%) and "Security Operations Team" (12.3%).**

**Fig. 14**
How big is your security team?

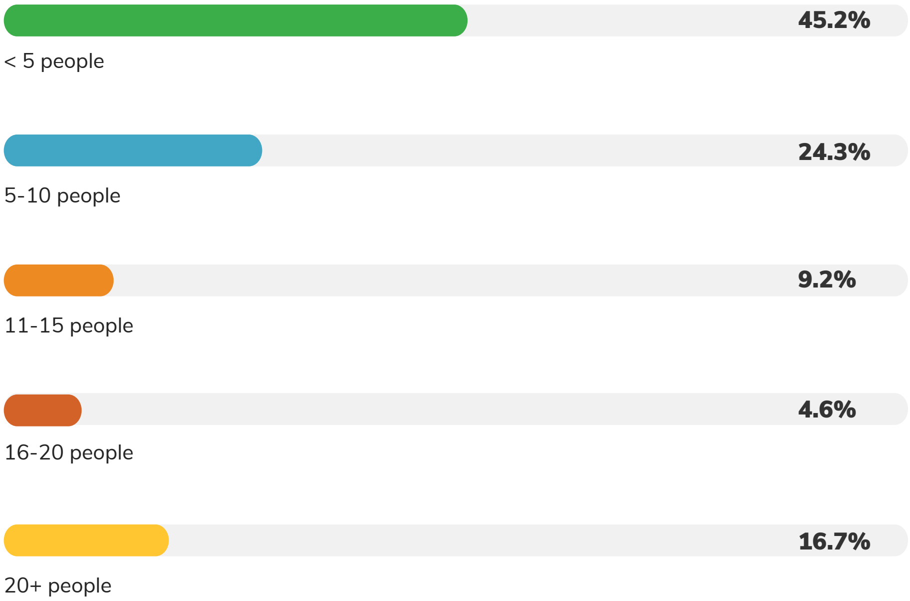
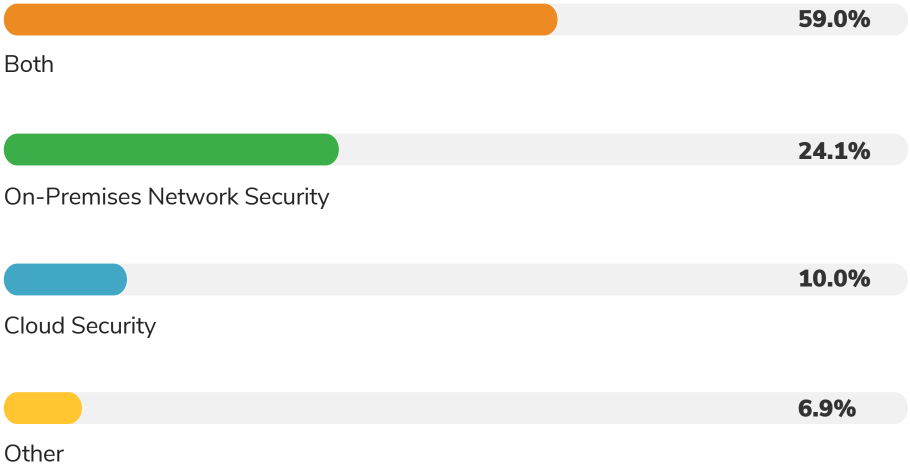


**Fig. 15**
Do you (or your team) manage on-premises network security, cloud security or both?



## CHAPTER 3

### Decreasing Budgets and Staffing Shortages Continue to Overburden Security Teams

With overburdened security teams and limited budgets, enterprises are also dealing with friction in the relationship between DevOps and security operations. When asked how the acceleration of DevOps impacted security operations, only 35.1% of respondents say that the impact has been positive (down 8.9% from last year) (fig. 16).

Adding to the tension between DevOps and security teams, collaboration is not getting any better – in fact, it is getting worse. 45.4% of respondents say that their relationship with the DevOps/Application team is either complicated, contentious, not worth mentioning or non-existent (up 15.4% from last year) (fig. 17).

**Only 23.3% of C-Level respondents say that the acceleration of DevOps has positively impacted security operations.**

**Fig. 16**

How has the acceleration of DevOps at your organization impacted security operations?

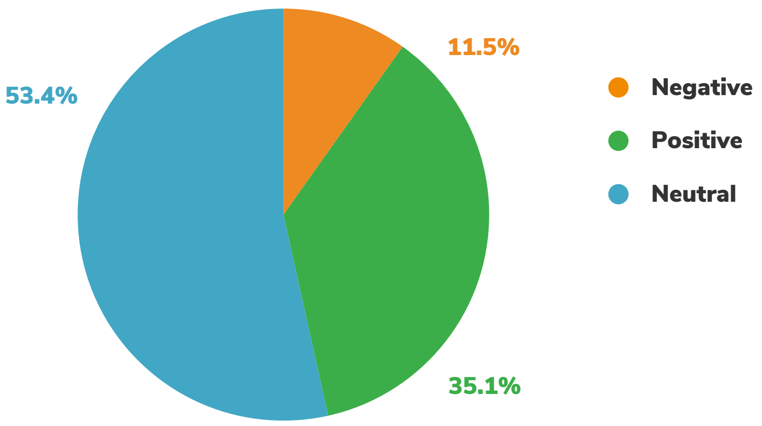
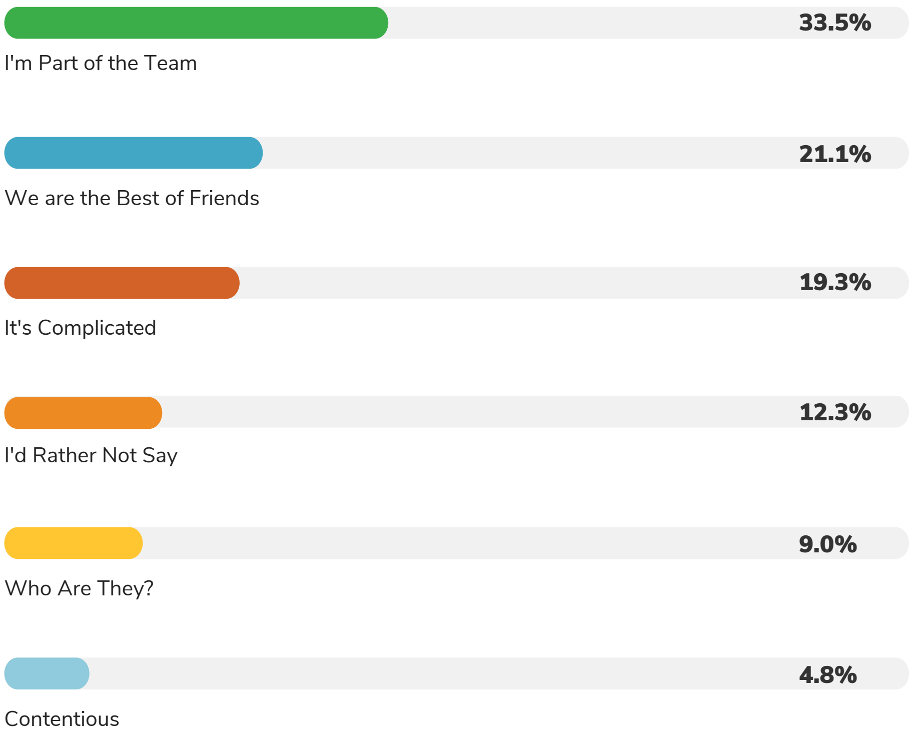


**Fig. 17**

How would you describe your relationship with the DevOps/Application team?



# Conclusion

The data in this year's survey shows that the current state of hybrid cloud security is not getting any better. From the percentage of respondents using two or more different enforcement points increasing almost 20% from last year, to less than a quarter of all respondents understanding the shared responsibility security model, it is clear that the task of securing hybrid cloud environments is plagued with increasing complexity and sprawl. The lack of integrated tools needed to manage security across the hybrid cloud environments is exasperated by the lack of automation and shortage of qualified security personnel, leaving enterprises with no choice but to rely on manual processes that can lead to costly misconfigurations due to human error.

Enterprises must explore the possibilities of automation to relieve their resource-constrained security teams and ensure that any misconfiguration errors do not result in headline-making news. Flexibility is key—there is no de facto standard for automation—enterprises should approach automation based on their unique needs, pace and confidence level. If implemented correctly, automation can deliver consistency, cost savings, ongoing visibility and assessment, and effective risk management across the hybrid cloud.

While there is still some work to be done to mend the relationship between security and DevOps teams, enterprises can work to alleviate the challenges of their hybrid cloud with the right strategy and tools. With well-defined, robust API structures, enterprises can integrate their multiple third-party security solutions to orchestrate the exchange of critical security data and optimize their security posture across their entire hybrid cloud environment to maximize their security investments and securely forge new avenues for business innovation and growth.

**Learn More about FireMon Automation.** SCHEDULE DEMO

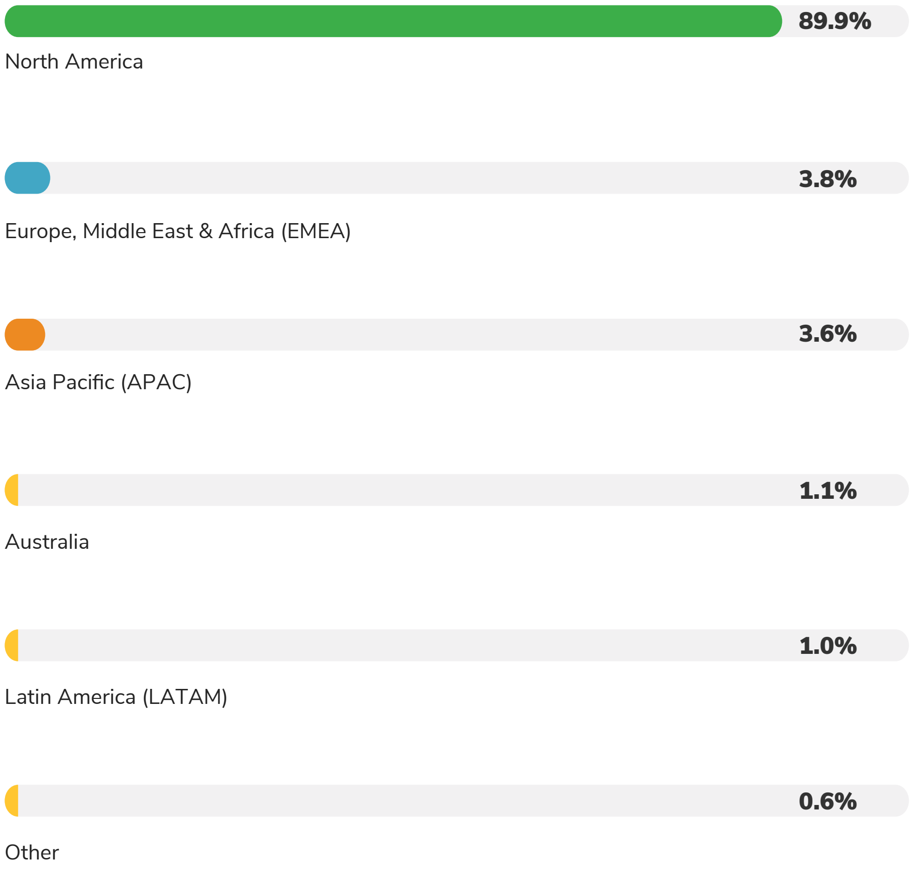
FireMon is the #1 network security automation solution for hybrid cloud enterprises. FireMon delivers persistent network security for multi-cloud environments through a powerful fusion of real-time asset visibility, compliance and automation. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world. For more information, visit www.firemon.com.

## APPENDIX

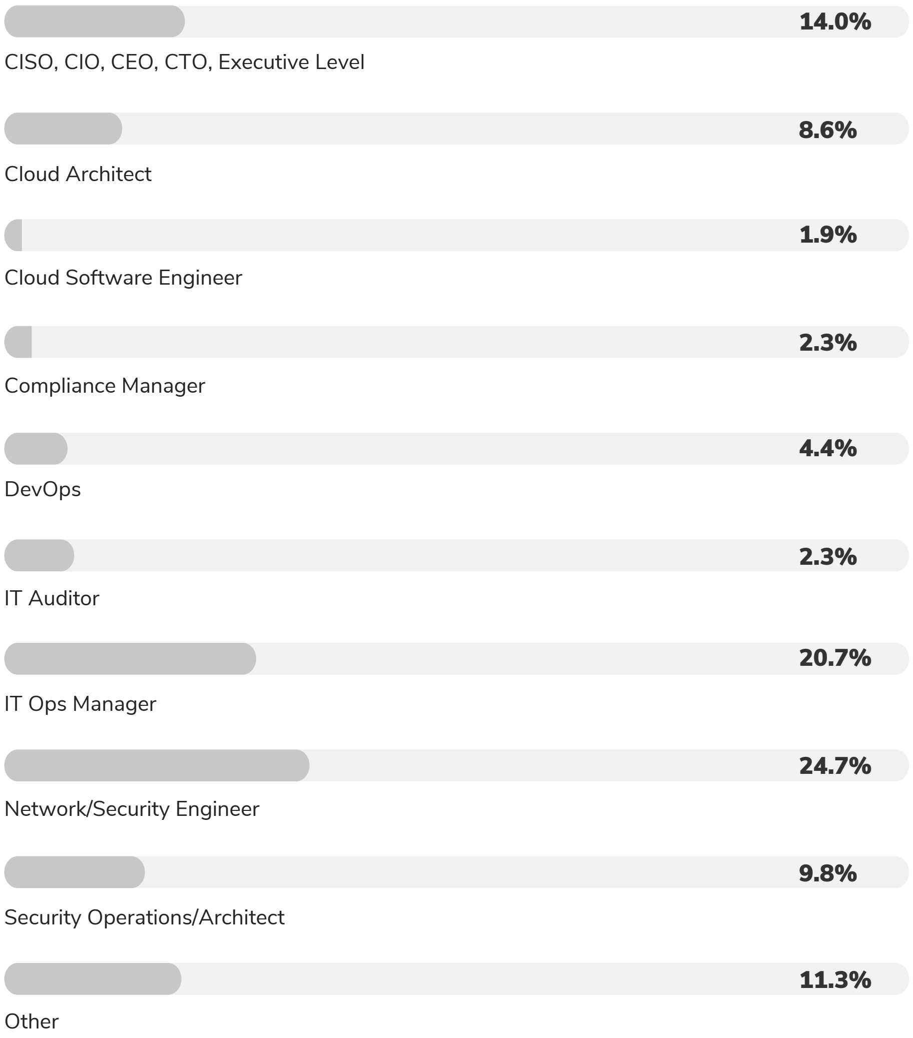
**The 2020 State of Hybrid Cloud Security survey was designed with a total of 31 questions covering demographics, operations, and hybrid cloud security challenges.**

**A total of 522 complete survey responses were collected from December 10, 2019 through January 17, 2020.**

### Which geographic region is your organization located in?

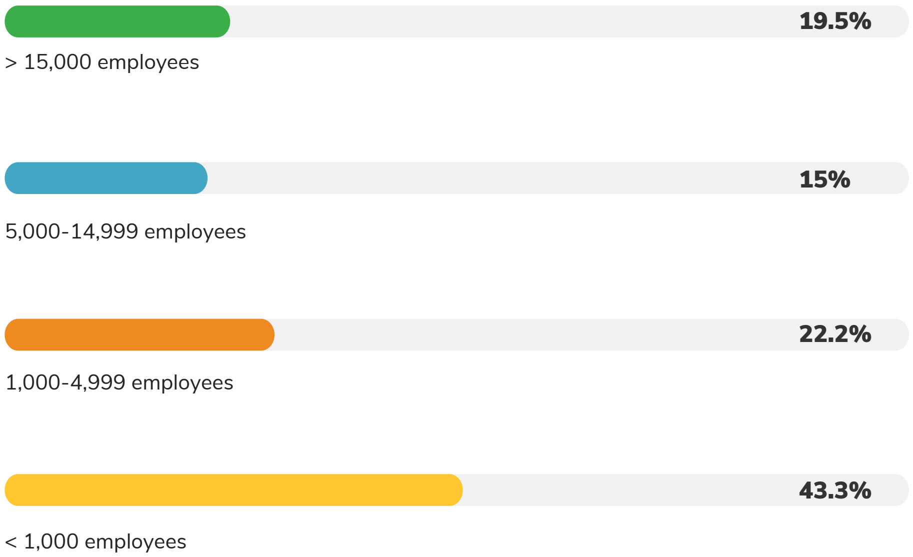


### What best describes your position within your organization?

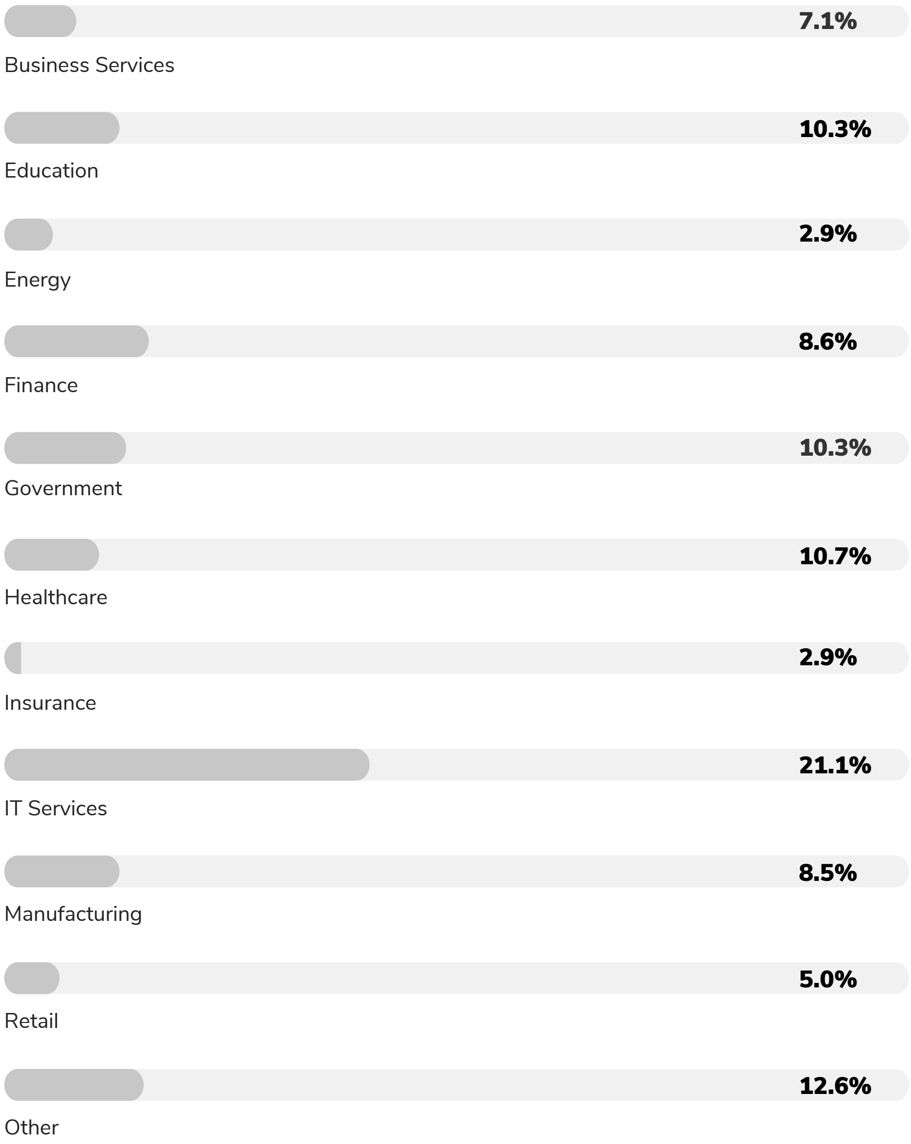


# APPENDIX

## What is your company size by number of employees?



## Which industry best describes your organization?


Business Services
Education
Energy
Finance
Government
Healthcare
Insurance
IT Services
Manufacturing
Retail
Other