FIREMON

STATE OF HYBRID CLOUD SECURITY: 2019

FIREMON

02 EXECUTIVE SUMMARY

04 INCREASING SCALE AND COMPLEXITY

11 LACK OF RESOURCES ALL AROUND

15 IS SHARED SECURITY RESPONSIBILTY REALLY SHARED?

19 APPENDIX: DEMOGRAPHIC DATA

20 CONCLUSION

Our inaugural survey of more than 400 security practitioners finds the acceleration of cloud adoption is outpacing security's time to protection. The path to securing hybrid cloud environments is paved with complexity as multiple disparate solutions are deployed across multiple environments without effective, integrated tools to manage them.

FIREMON

EXECUTIVE SUMMARY

We are pleased to share our inaugural 2019 State of Hybrid Cloud Security survey report. Our goal with this survey was to shed a light on the challenges security and network professionals are worrying about as they expand their hybrid cloud initiatives.

This report reveals new findings from surveying more than 400 security practitioners and surfaces three major themes affecting hybrid cloud security: scale and complexity, lack of resources and shared security responsibility.

FIREMON

KEY FACTS AND FIGURES

- The survey data suggests a rising trend of enterprises inadvertently introducing complexity into their environments by deploying multiple, disparate solutions on-premises as well as across multiple private and public clouds. Further analysis indicates that complexity is compounded by a lack of integrated tools and training needed to manage security across multiple environments effectively, leaving enterprises to resort to manual processes and inconsistent, multiple native security controls.
- 60% of respondents stated that deployment of their business services in the cloud has accelerated past their ability to adequately secure them in a timely manner.
- Security teams continue to do more with less. 57.5% of respondents indicated they spend less than 25% of their total security budget on the cloud and 52% of respondents say that their security teams include 10 people or less.
- In some cases, DevOps and security teams are fully aligned and working well together, but in other cases, the relationship between security and DevOps teams is inconsistent. This inconsistency can impact the coordination of security policies across the hybrid cloud as enterprises take more ownership of their security in the public cloud with their growing use of “as-a-Service” models (Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service).
- Compliance, migration issues, cyberattacks, lack of cloud expertise and infrastructure complexity emerged as top roadblocks to moving to the public cloud.

FIREMON

INCREASING SCALE AND COMPLEXITY

Enterprise hybrid cloud security responsibilities are increasing in scale and complexity.

Most network security teams are managing multiple solutions across multiple environments – on-premises as well as public, private and hybrid cloud – that have become rapidly and increasingly complex. Adding to the complexity, teams are using two or more different network security controls in the public cloud and have to resort to using native tools for each unique environment or manual processes to manage security across their hybrid environment.

Lack of visibility as a top challenge in securing the public cloud environment is a prominent theme that emerged from our research.

Our research found that

59%

of respondents use two or more different firewalls in their environment.

67%

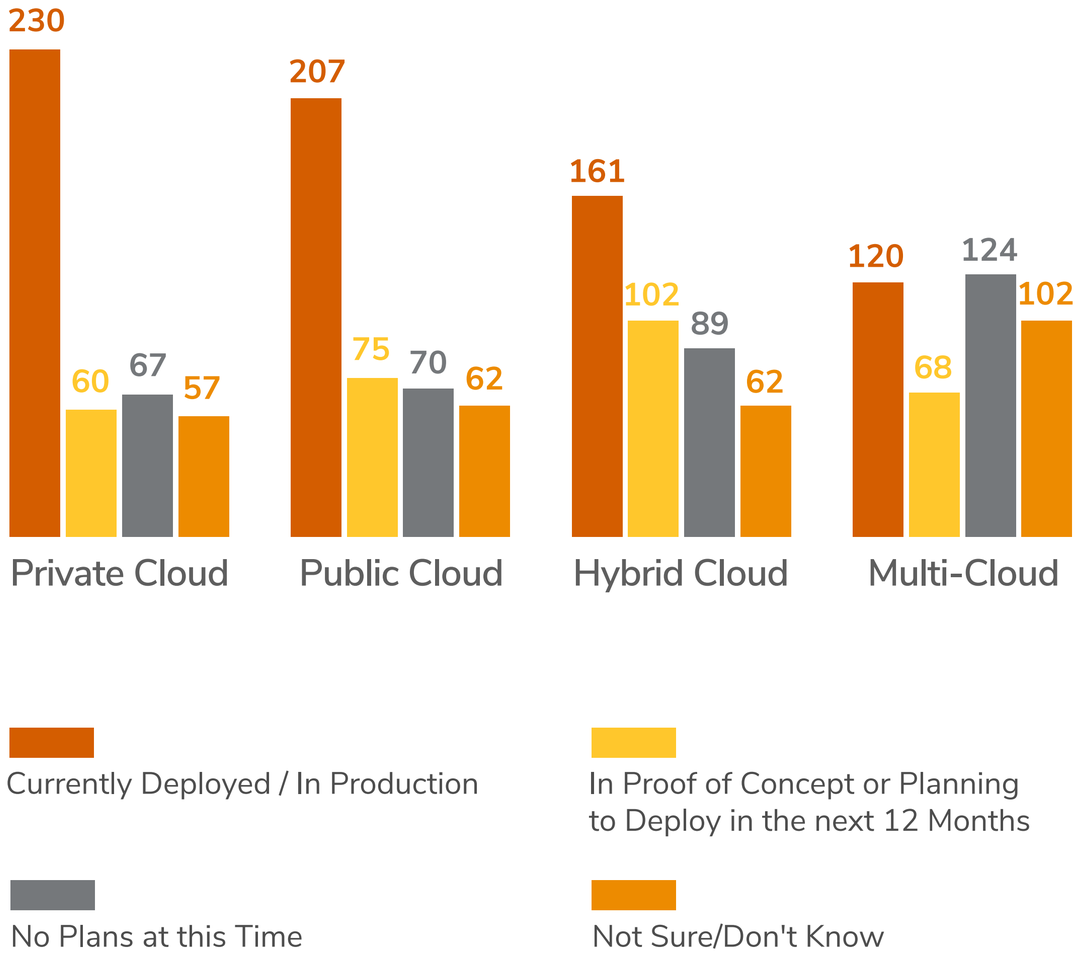
of those using two or more firewalls also use two or more public cloud platforms.

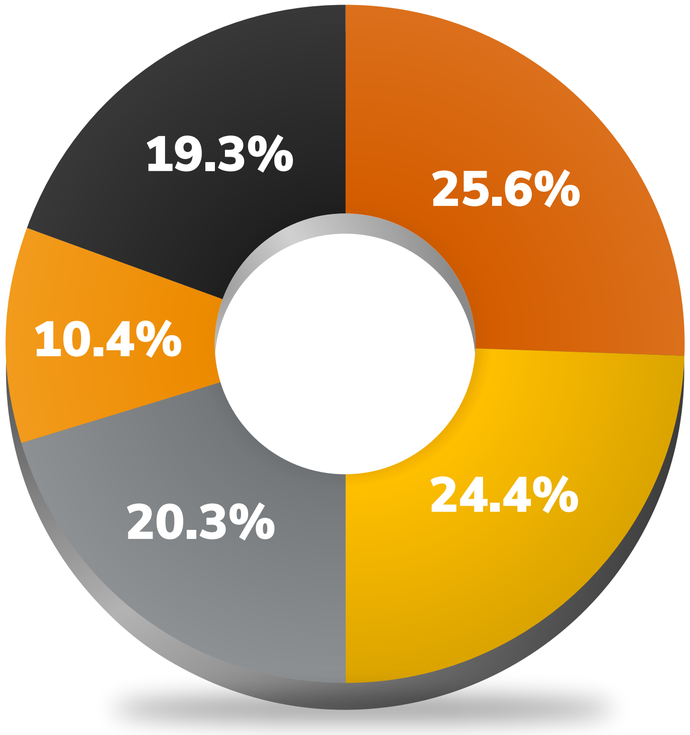
FIREMON

We found an increasing trend towards enterprises using more of the cloud. Most respondents are already deployed in cloud environments, with 50% having two or more different clouds deployed, while 40% are deployed in hybrid cloud environments, and 23% have two or more different clouds in the proof of concept stage or are planning to deploy in the next 12 months.

- 56% are in private cloud environments (15% in Proof of Concept)
- Half are in public cloud environments (18% in Proof of Concept)
- 40% are in hybrid cloud environments (25% in Proof of Concept)
- 29% are in multi-cloud environments (16% in Proof of Concept)

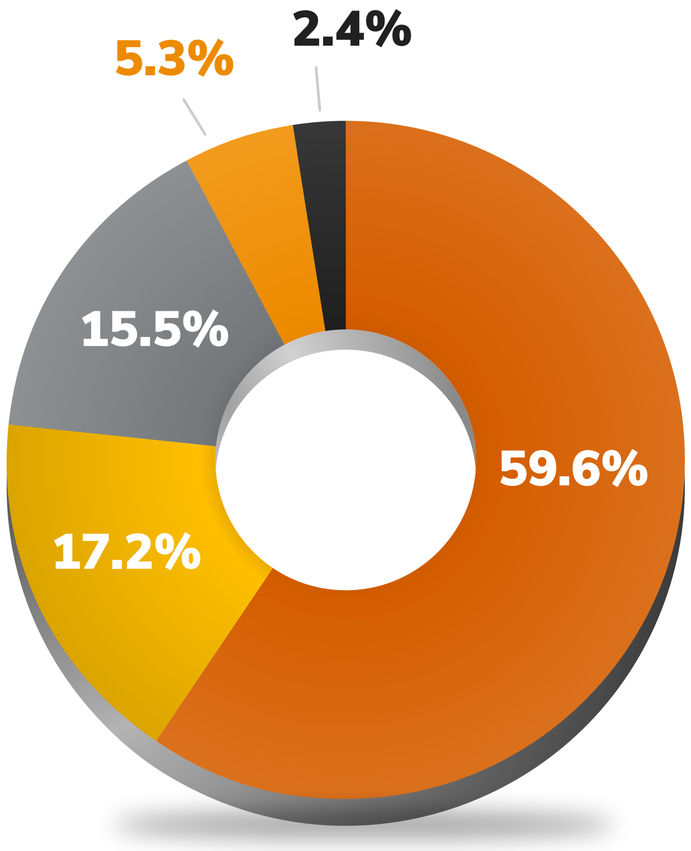
How are you currently (or planning to be) deployed in the cloud?





Number of Current Cloud Deployments

Zero | One | Two | Three | Four



Number of Cloud Deployments in POC or in Plan

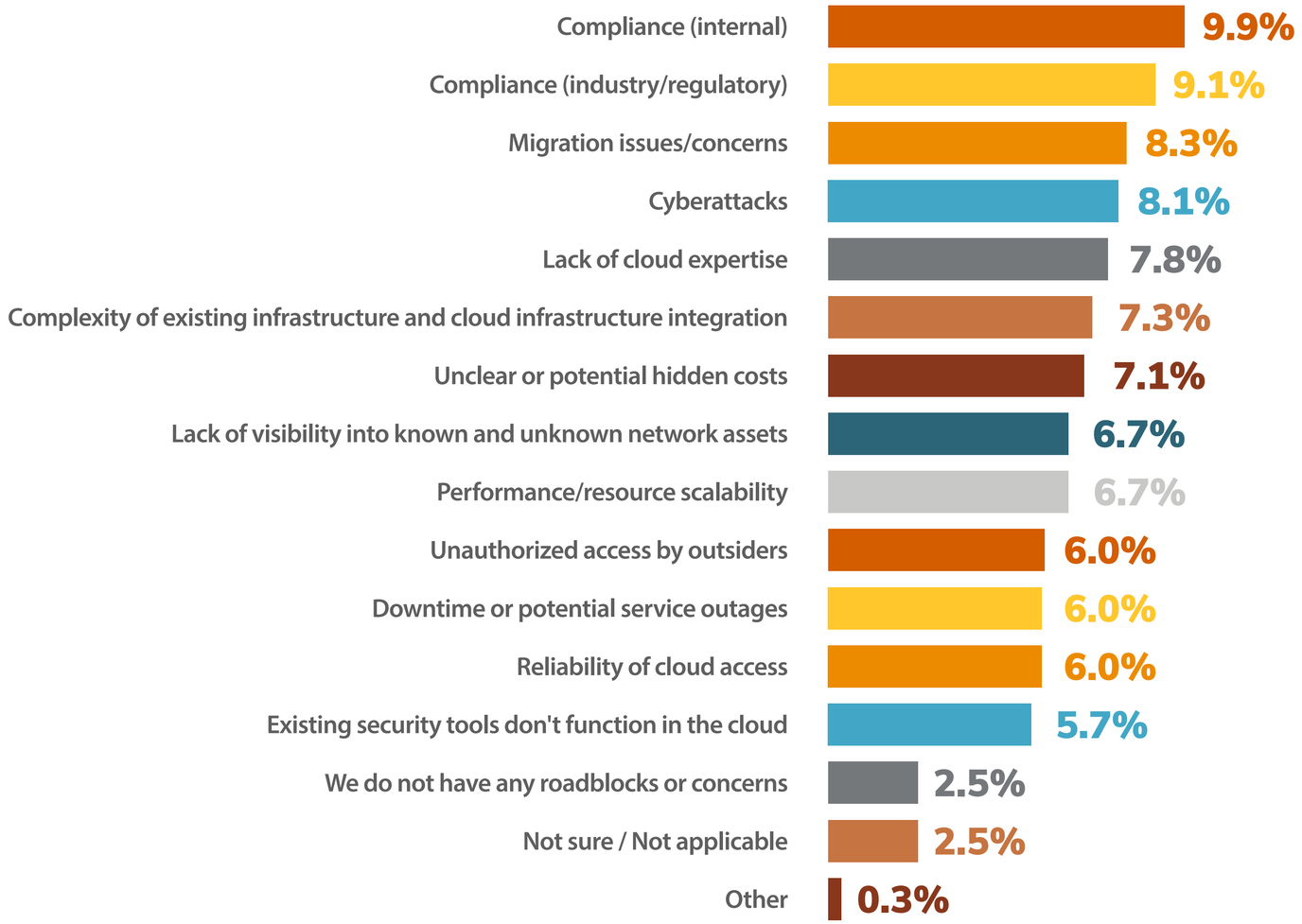
Zero | One | Two | Three | Four

FIREMON

The top five barriers keeping organizations from moving workloads to the public cloud include:

1. Compliance
2. Migration Issues/Concerns
3. Cyberattacks
4. Lack of cloud expertise
5. Complexity of existing infrastructure and cloud infrastructure integration

What roadblocks and concerns keep your organization from moving workloads to the public cloud?

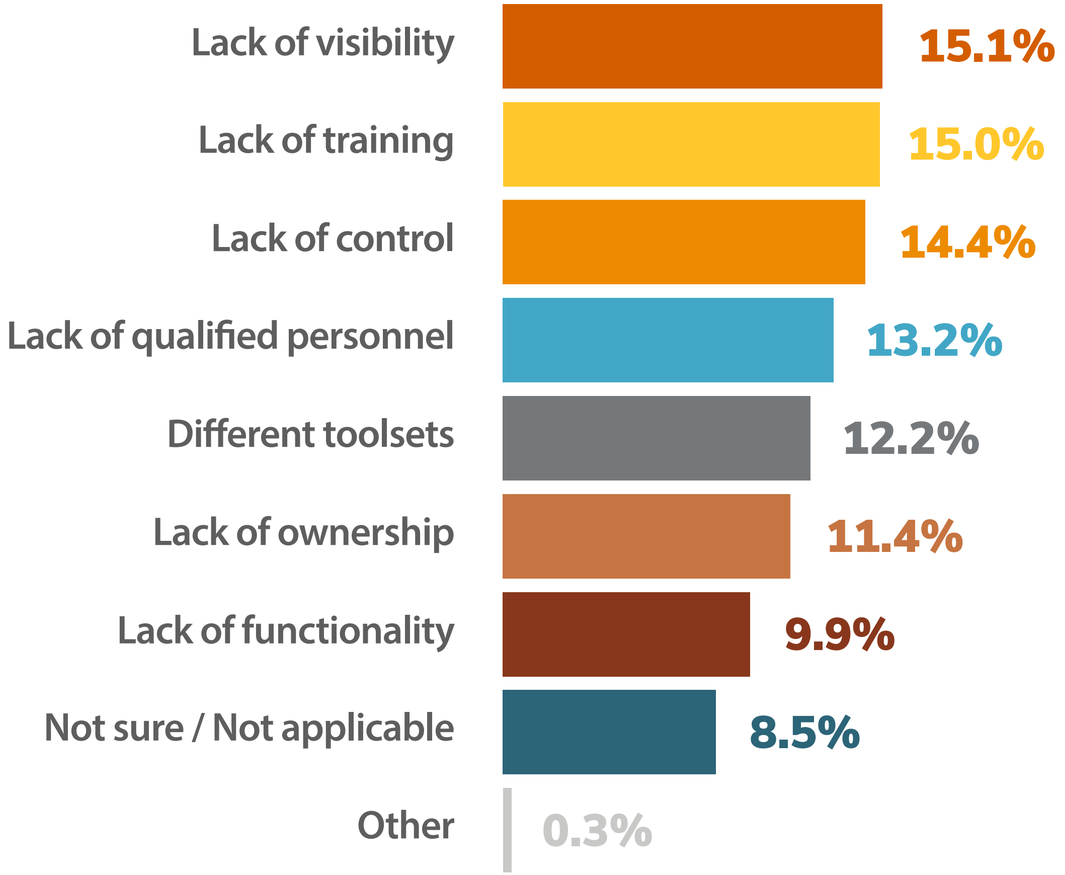


FIREMON

45% view the top three challenges to securing their public cloud environment as:

- Lack of visibility
- Lack of training
- Lack of control

What are your biggest challenges in securing your public cloud environment?

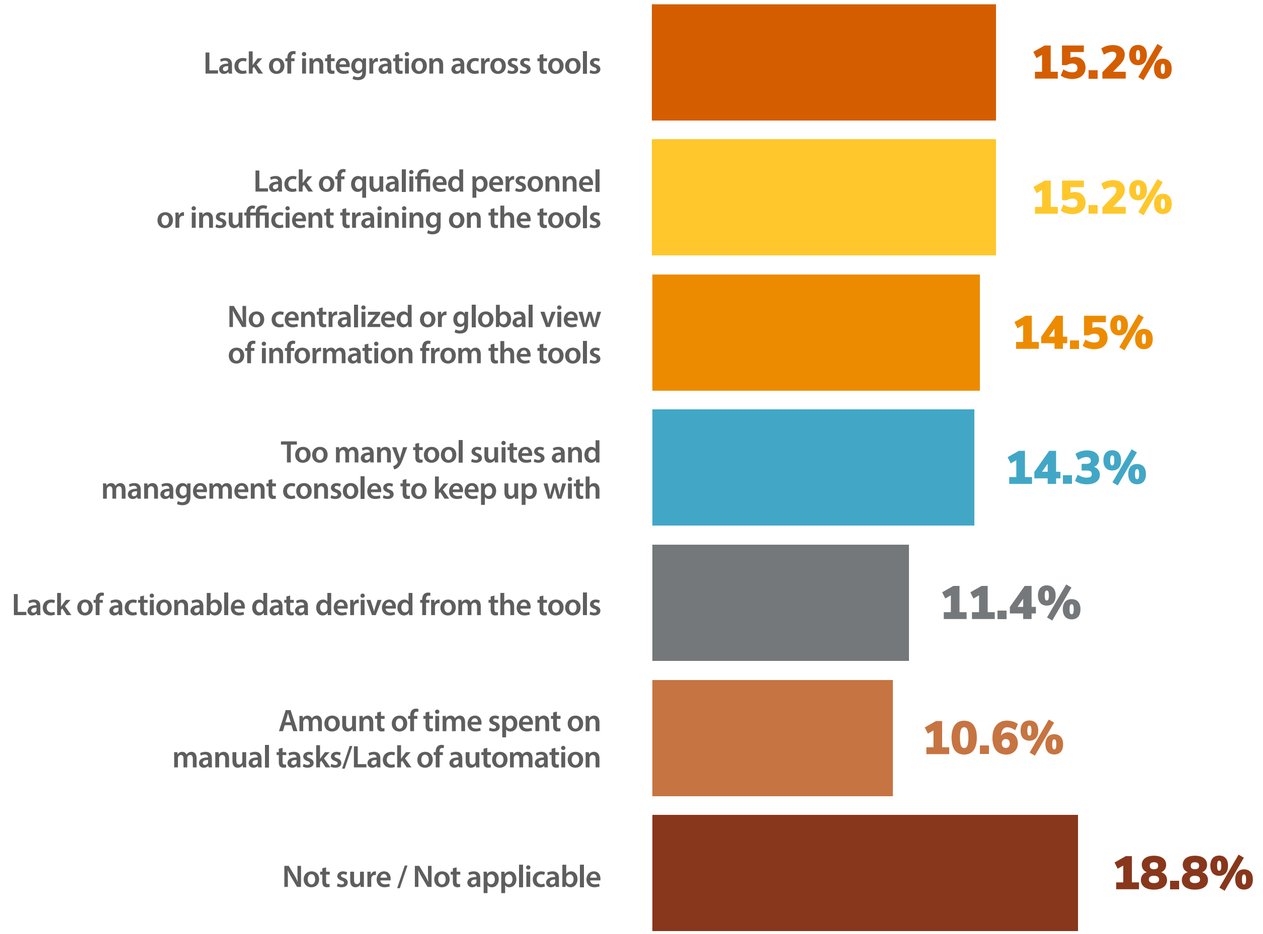


FIREMON

When considering all respondents, the top two biggest challenges in managing network security tools across hybrid cloud environments are the lack of integration across tools and the lack of qualified staff or proper training.

In contrast, among only the C-Level respondents, their biggest challenge cited was the lack of a centralized or global view of information across tools, followed by too many tool suites and management consoles to keep up with and lack of integration across tools.

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



FIREMON

LACK OF RESOURCES ALL AROUND

Given our survey finding that 60% of respondents believe that deployment of their business services on the cloud has accelerated beyond their ability to secure them, it makes sense to examine the budgets and human resources allocated to securing business on the cloud.

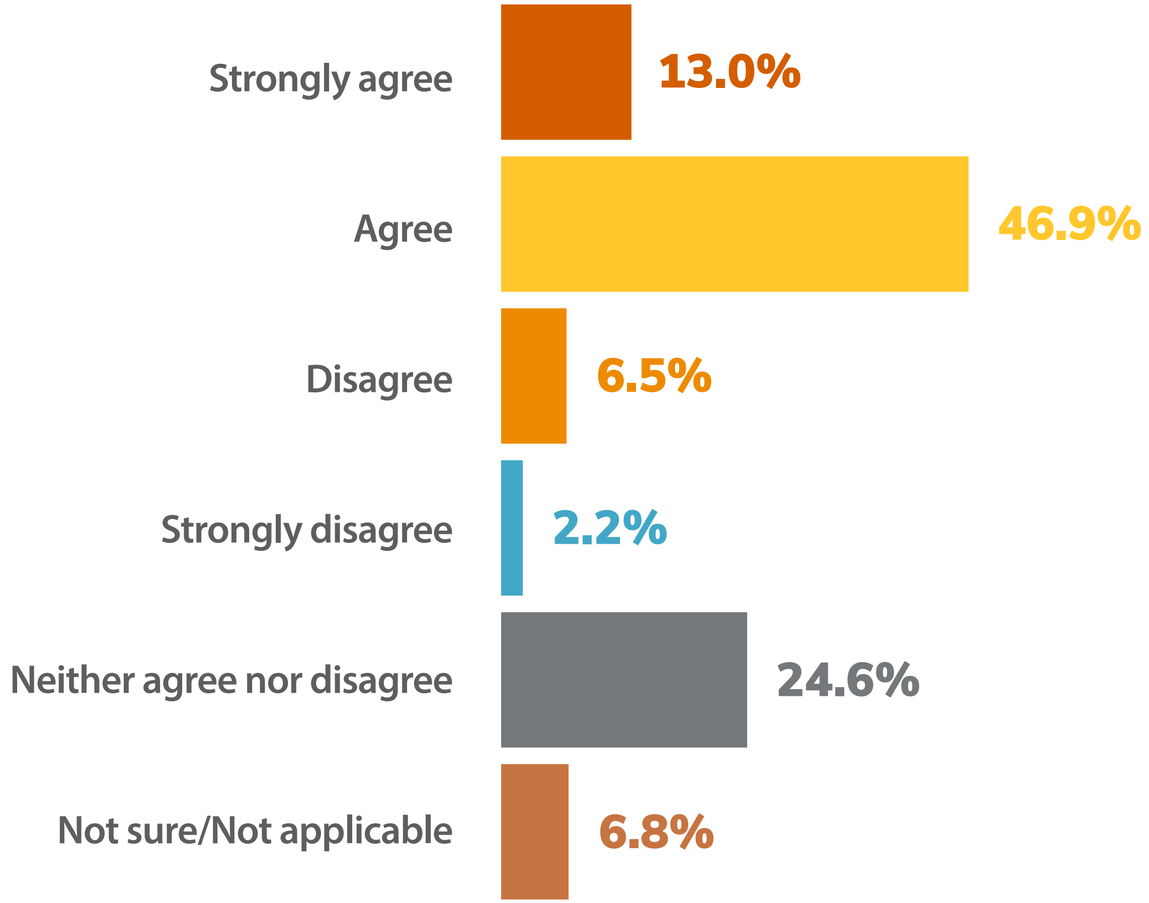
Over half of respondents spend less than 25% of their total security budget on cloud and rely on a security team of 10 people or fewer. Regardless of company size, resources are strained across the board.

It is also helpful to see how many people currently use tools that work across cloud environments. The number we uncovered is very low. The lack of integration across tools poses a problem for everyone, from network security managers handling the day-to-day to C-Level executives who need to report to their senior leadership or board of directors.

FIREMON

60% of respondents and over 60% of C-Level respondents agree or strongly agree that deployment of their business services in the cloud has accelerated past their ability to secure them in a timely manner.

Deployment of our business services in the cloud has accelerated past our ability to adequately secure them in a timely manner.

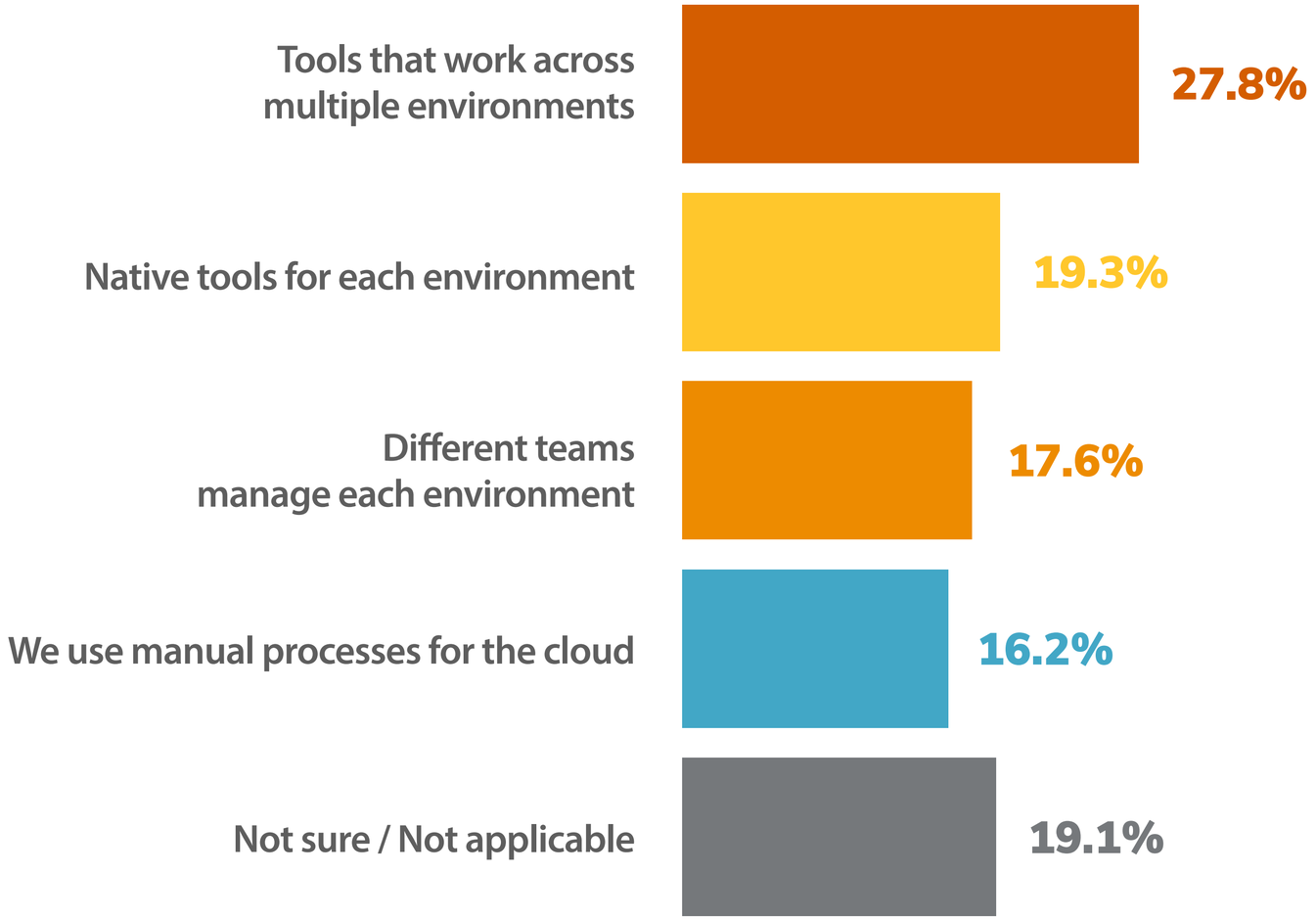


FIREMON

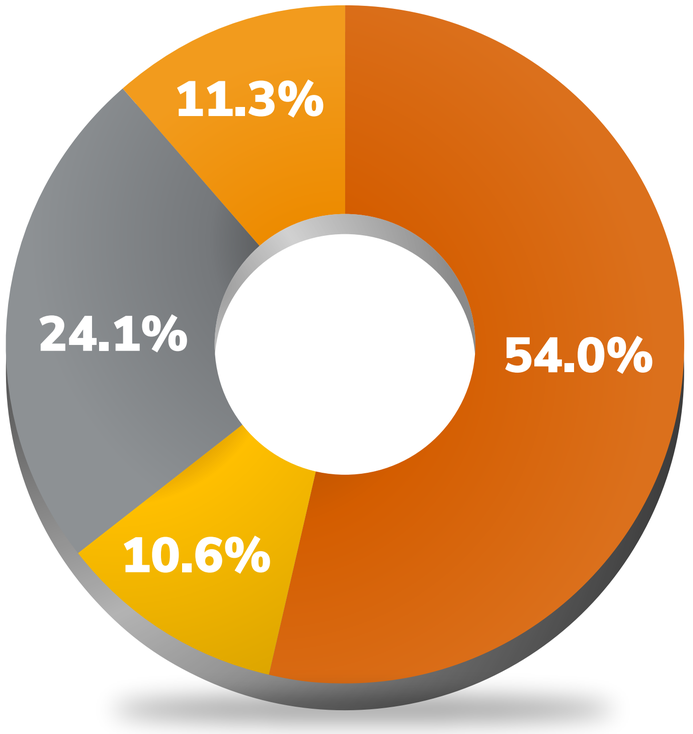
Among respondents, only 28% use tools that work across multiple environments to manage network security across their hybrid environments.

Almost 36% of respondents use either manual processes or native tools for each environment.

How does your organization manage network security across hybrid environments?



54% of respondents manage both on-premise network security and cloud security, demonstrating that their job has increased in complexity. Over half of those who manage both work at companies with fewer than 1,000 employees.



Do you (or your team) manage on-premise network security, cloud security or both?

Both | Cloud security | On-premise network security | Not sure Not applicable

FIREMON

IS SHARED SECURITY RESPONSIBILITY REALLY SHARED?

Enterprises are becoming more and more comfortable with deploying services in the cloud using models where security responsibilities are more shared, evidenced by the 39% of respondents using all three "as-a-Service" models concurrently, as well as the 23% using Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) concurrently -- models where more responsibility for certain areas (e.g. applications, data) falls to the user versus the cloud provider.

This trend reveals both a danger and an opportunity.

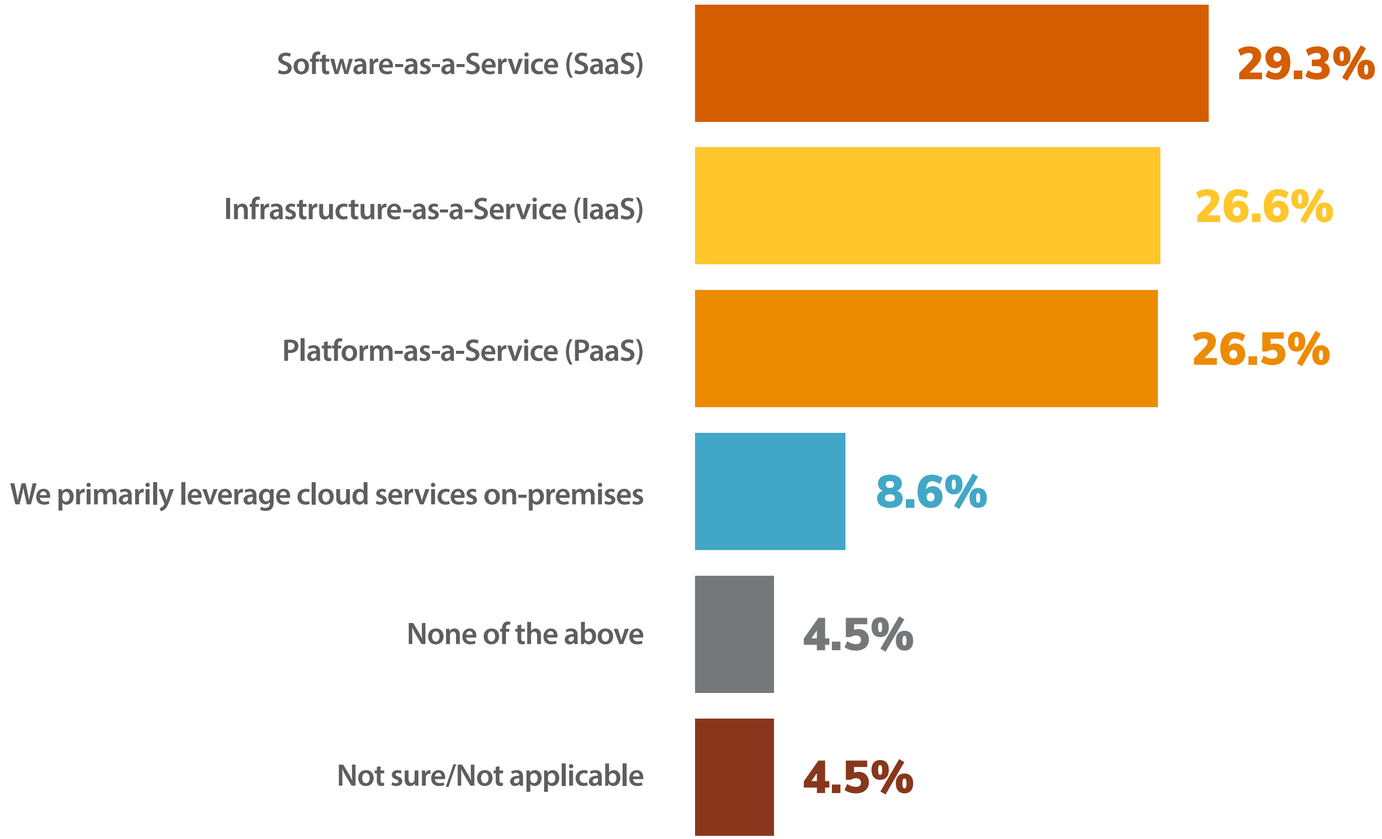
It is worthwhile to look into how well different teams within the organization are integrated with one another. While the acceleration of DevOps has positively impacted security operations for 44% of respondents, respondents' relationship with the DevOps/Application team is often complicated. Enterprises still have work to do to get everyone on the same page.

FIREMON

39% of respondents indicated they are using Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service models concurrently, while 23% of respondents are using Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) concurrently.

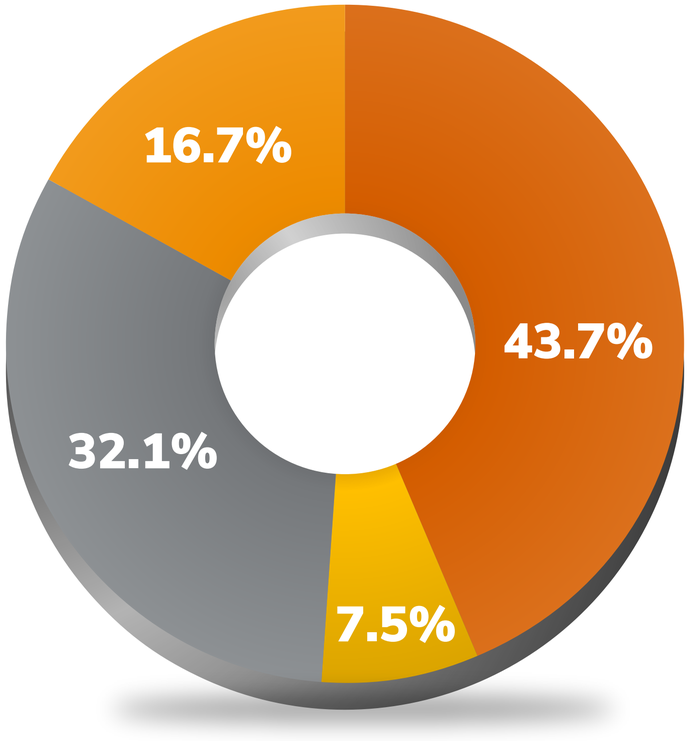
In areas with shared responsibilities versus clearly delineated roles and responsibilities, there is potential for confusion and increased risk.

How are you using the cloud?



FIREMON

DevOps is making a difference: almost 44% of total respondents and 46% of C-Level respondents state that the acceleration of DevOps has positively impacted security operations.



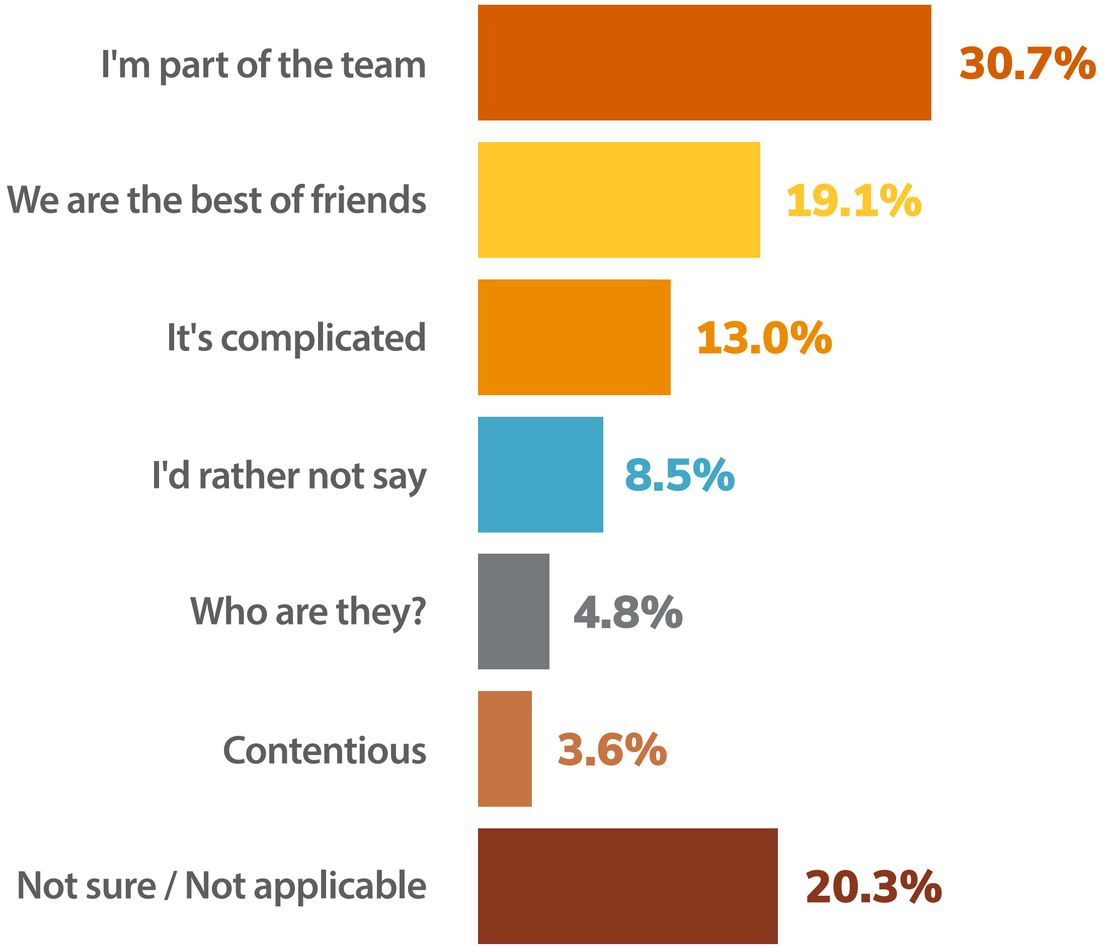
How has the acceleration of DevOps at your organization impacted security operations?

Positive | Negative | Neutral | Not sure Not applicable

FIREMON

On the other hand, 30% of respondents view their relationship with the DevOps/Application team as complicated, contentious, not worth mentioning or non-existent.

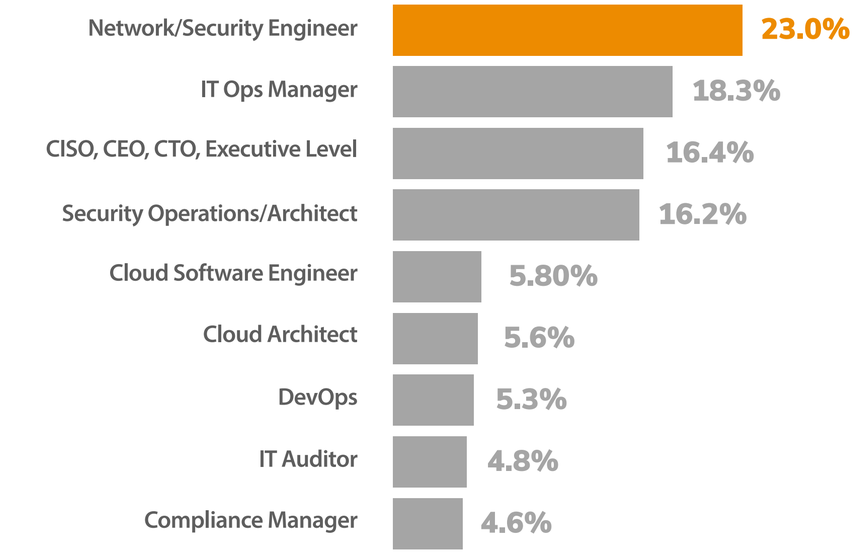
How would you describe your relationship with the DevOps/Application team?



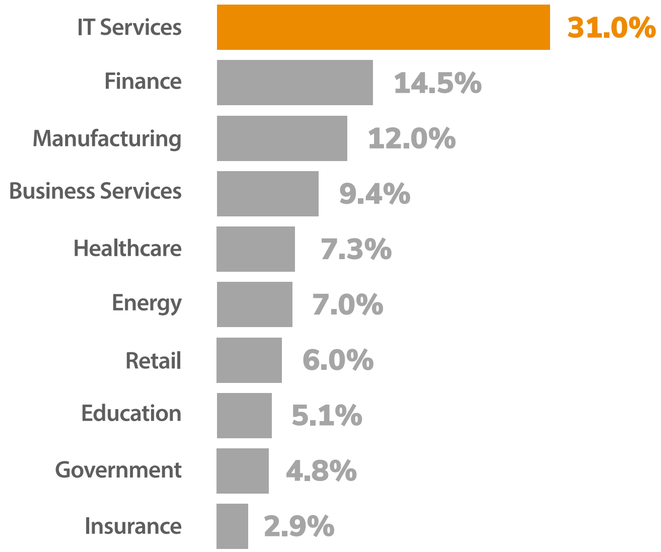
FIREMON

APPENDIX: DEMOGRAPHIC DATA

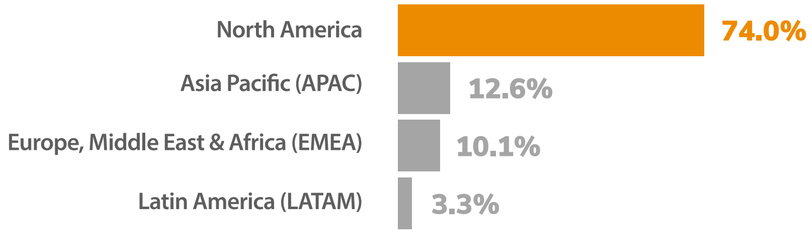
What best describes your position within your organization?



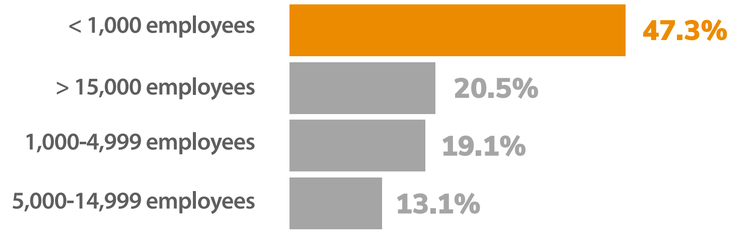
Which industry best describes your organization?



Which geographic region is your organization located in?



What is your company size by number of employees?



FireMon collected 414 responses between December 18, 2018 and January 16, 2019.

CONCLUSION

The data in this survey indicates that many enterprises are still in the early days of adopting hybrid cloud environments. They are embracing the cloud, but not necessarily using a single cloud vendor. This popular practice of relying on multiple vendors in a hybrid cloud environment, revealed through our research, shows that enterprises play an unintended part in adding to the complexity of securing their environment.

Budget and staffing constraints, lack of clarity around which team is responsible for cloud security, and the absence of consistent standards for managing security across hybrid cloud environments, compounded with the lack of integrated tools that can be used to manage security across multiple solutions and environments, sets the stage for costly breaches caused by misconfiguration errors.

Security responsibilities will continue to blur as more enterprises embrace multiple cloud platforms, but as the relationship between security and DevOps teams becomes more cohesive, we will likely see a growing emergence of DevSecOps teams that will streamline, while securing, the rapid development of business innovation.

ABOUT FIREMON

FireMon is the #1 network security management solution for hybrid cloud. FireMon delivers continuous security for multi-cloud enterprise environments through a powerful fusion of vulnerability management, compliance and orchestration. Since creating the first-ever network security policy management solution, FireMon has continued to deliver real-time visibility into and control over complex network security infrastructures, policies and risk postures for nearly 1,700 customers around the world.

Using the FireMon platform, today's leading enterprise organizations, government agencies, and managed security providers have dramatically improved the effectiveness of their network defenses, accelerating business agility and optimizing return on investment. For more information, visit www.firemon.com and follow us on Twitter at @FireMon.

FIREMON

Learn more about our solutions: **www.firemon.com | info@firemon.com**

8400 West 110th Street, Suite 500, Overland Park, KS 66210 | 5420 Lyndon B Johnson Freeway, Suite 375, Dallas, TX 75240