cloud security alliance®

Cloud Security Complexity:

Challenges in Managing Security in Native Hybrid and Multi-Cloud Environments

Sponsored by algosec

SURVEY CREATION AND METHODOLOGY

The Cloud Security Alliance is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is comprised of a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

AlgoSec, a leading network security solution provider, commissioned CSA to develop a survey to add to the industry's knowledge about hybrid-cloud and multi-cloud security, and to prepare this report of the survey's findings. Algosec financed the project and co-developed the initiative by participating with CSA in the development of survey questions addressing hybrid cloud security. The survey was conducted online by CSA, from December 2018 to February 2019, and was submitted to nearly 700 IT and security professionals from a variety of organization sizes and locations. Approximately 500 organizations answered the majority of the 20-question survey. The data analysis here was performed by CSA's research team.

ACKNOWLEDGMENTS

Lead Authors:

Hillary Baron
Sean Heide
Shamun Mahmud
John Yeoh

Special Thanks:

Yitzy Tannenbaum, Product Marketing Specialist, AlgoSec

TABLE OF CONTENTS

INTRODUCTION

Year after year, the adoption of cloud technologies continues to increase. Companies of all sizes are taking advantage of the value in cloud with its improved security, agility, and flexibility all of which are crucial for success in today's market. However, like any technology, cloud comes with particular concerns and complications, especially when integrating multiple different cloud services with legacy IT environments. To complicate things further, cloud platforms include ecosystems of services that aren't always fully compatible with each other, causing data ownership and interoperability issues. Today's cloud adoption requires focused attention on data migration, expert levels of knowledge per service, and understanding of vendor security and responsibility.

One of the challenges with this multi-cloud integration is assigning assets to different types of cloud environments, including public and private cloud services, as well as multiple cloud public platforms and services. The various cloud options must also be integrated with on-premise networks and other third-party services. To top it all off, the final computing environment your organization achieves, regardless of its complexity, must be able to remain secure and stay current with regulatory compliance protocols.

To get a better understanding of information security concerns in this complex environment, the Cloud Security Alliance (CSA), in cooperation with AlgoSec, surveyed 700 IT professionals about the following topics related to cloud usage within their enterprises:

- Types of cloud platforms in use
- Proportion of workloads actively in the cloud
- New workloads expected to be moved into the cloud
- Anticipated risks and concerns about potential migrations to the cloud
- Challenges managing security after adopting cloud technologies
- Methods for addressing these security challenges
- Challenges related to network or application outages
- Methods for and results of addressing outages and security incidents

KEY FINDINGS

This survey demonstrated the complex nature of today's cloud computing environment, and with it, attendant concerns about managing security risks. The survey also identified potential disconnects and misinformation in the industry related to the importance of visibility into critical cloud resources and necessary professional security expertise when using cloud services. The survey illustrates the need within our industry to better address these issues before adopting cloud technologies in order to create practical and manageable network environments--rather than simply putting out fires as they arise after deploying new technologies. And the need to maintain cloud service specific knowledge during the growth of the service in order to stay current with new features and functionality.

Lack of Visibility into Cloud Resources

Organizations adopting new technologies in the public cloud may not be considering the potential risks

related to visibility until they eventually encounter security problems in practice. A third of respondents (39%) identified visibility as a concern that has arisen when their organization considered adopting a public cloud. However, more than three-quarters of respondents rated visibility as a challenge related to managing their security once in the public cloud. When asked the level of challenge presented by lack of visibility into the entire cloud estate, 44% reported this issue to be a moderate security challenge, and 36% reported it as a maximum challenge.

Cloud Computing Complexity

More than half of survey respondents operate within a complex cloud computing environment, including multiple clouds (66% of respondents) and hybrid clouds (55%). Many also rely on a combination of hybrid and multi-cloud technologies (36%). Of the nearly 700 people who were given the survey, less than 10% of the enterprises reported that they do not use any public cloud services. Meanwhile, many respondents expect to increase their use of cloud computing technologies by 2020. The number of enterprises that host more than 40% of their total workloads in a public cloud should double within one year according to their reports.

Lack of Security Expertise

While a third of respondents reported lack of expertise as a concern when considering moving to the public cloud, nearly three-quarters of respondents already using the cloud cited this same concern as a challenge for security management. When asked to rate the level of challenge to managing security that is posed by a lack of expertise in cloud-native security constructs, 43% of respondents rated it a moderate challenge, and 30% a maximum challenge.

The importance of staff security expertise is emphasized once again with regards to network and application outages. More than 200 survey respondents indicated their organization had experienced an outage in the previous year. When surveyed about the causes, most respondents reported they did not know its cause (potentially a visibility issue). Another 20% identified the cause as operational human errors and mismanagement of devices. Together, these findings indicate that adequate security expertise may often be an afterthought.

Regulatory Compliance and Legal Concerns

When enterprises are deciding whether to move their critical resources into a public cloud platform, one of the top three concerns they report is regulatory compliance, with legal concerns following closely after. More than half of survey respondents (57%) reported these concerns about regulatory compliance, and nearly half indicated a similar unease about legal concerns (44%) when adopting public cloud services.

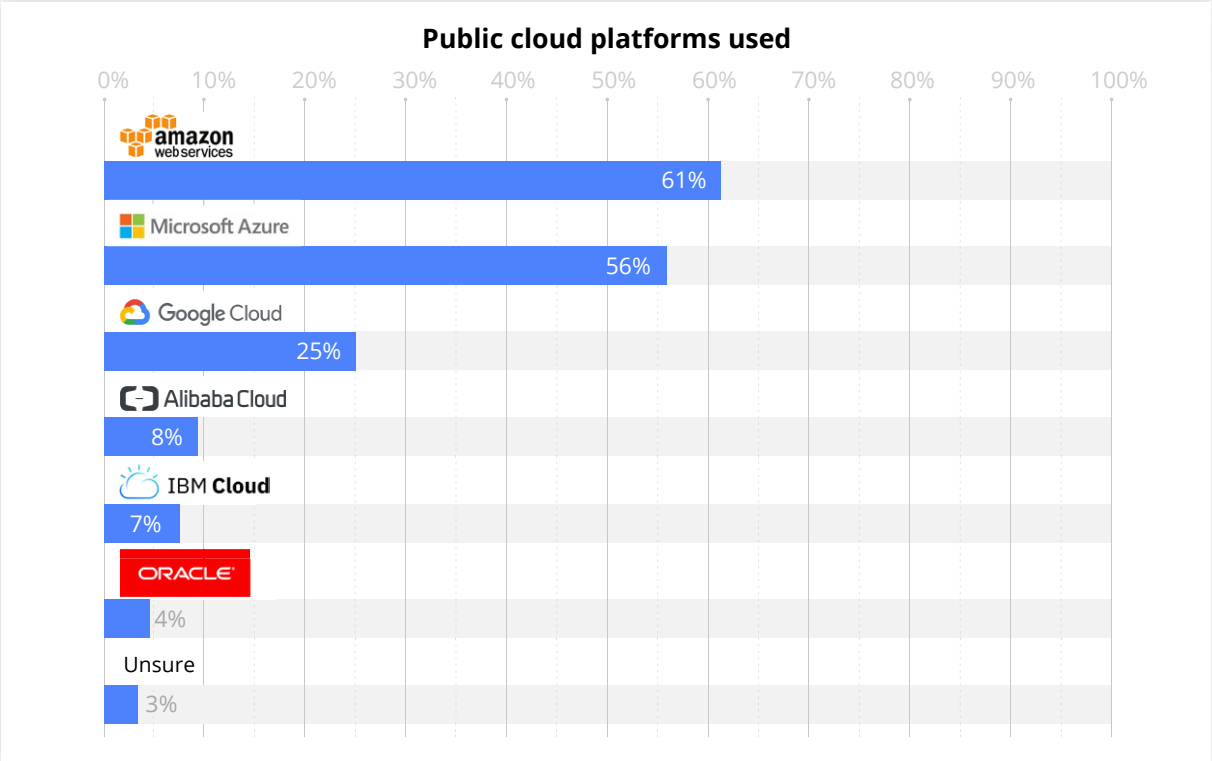
These issues remain at the forefront of an organization's security posture after cloud computing services are adopted. More than three-quarters of respondents found compliance and preparing for audits to be a challenging aspect of managing the security of their public cloud resources (with 45% reporting this to be a moderate challenge and 31% reporting maximum challenge).

BACKGROUND ON THE CLOUD TODAY

In order to reduce costs, increase scalability, and avoid relying on a single provider for all network needs, many organizations use multiple different cloud providers.

- Most survey respondents (66%) use multiple clouds (defined as a multi-cloud environment). In fact, more than a third (35%) of respondents using cloud leverage 3+ cloud platform vendors[1].
- In addition to this complexity, organizations may use both public and private clouds. More than half (55%) operate in a hybrid-cloud environment (using at a minimum at least one public and at least one private cloud service)[2].
- More than a third (36%) have a combination of multi-cloud and hybrid-cloud environment[3].

This trend of using both a hybrid cloud and multi-cloud strategy continues to rise as is predicted to increase significantly in the next three years[4].

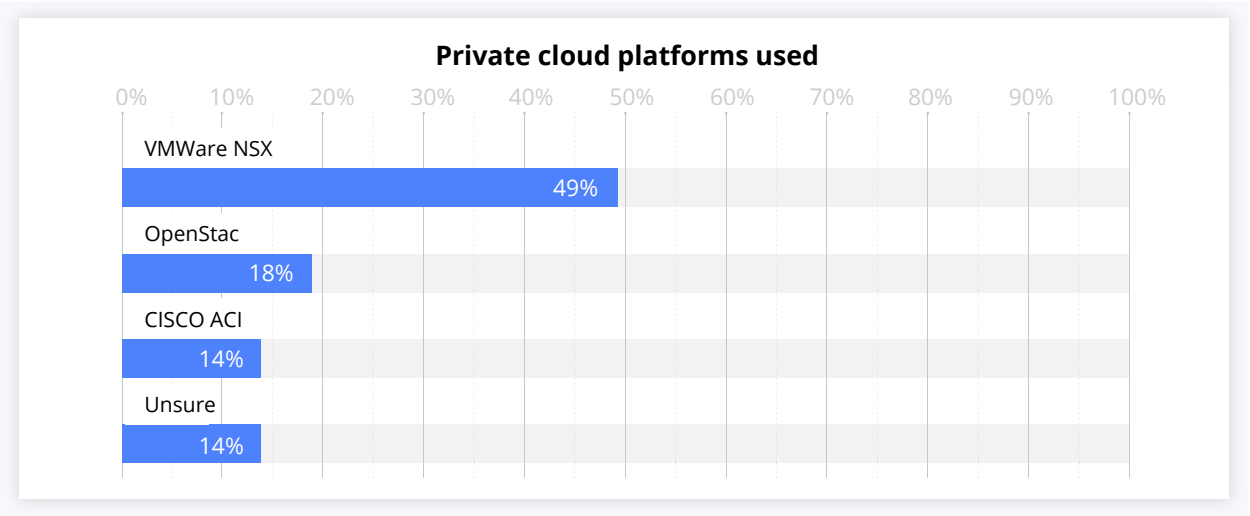


[1] Data was obtained by identifying the percentage of respondents who selected more than one provider on either of the questions: Which public cloud platforms does your organization use? or Which private cloud platforms does your organization use?

[2] Data was obtained by identifying the percentage of respondents who selected at least one public and one private cloud provider from the questions, Which public cloud platforms does your organization use? and Which private cloud platforms does your organization use?

[3] Data was obtained by identifying the percentage of respondents who selected at least one public and at least one private cloud provider, and also selected more than one public or private cloud provider for the questions, Which public cloud platforms does your organization use? and Which private cloud platforms does your organization use?

[4] https://www.ibm.com/thought-leadership/institute-business-value/report/multicloud



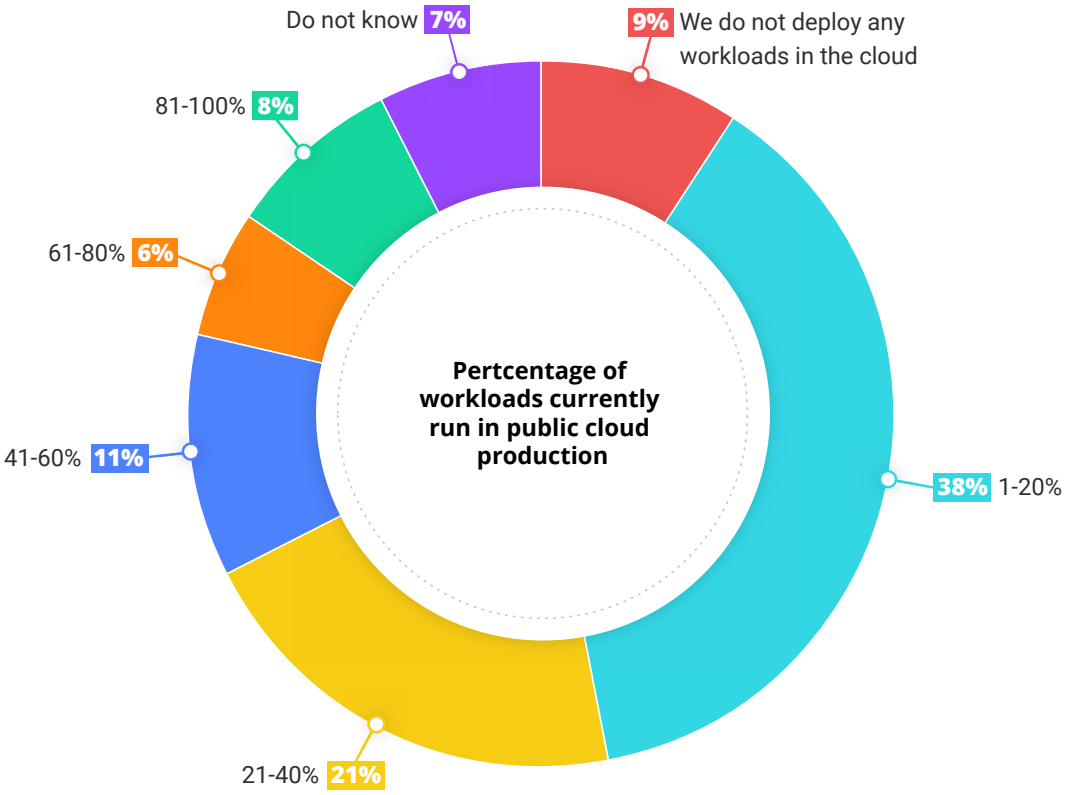
Over the past decade, enterprises have made plans to move their workloads from data centers to the cloud, and the past two years were no exception. The percentage of enterprises with a majority of their workload in the public cloud (61-100% of workload) has doubled from a survey conducted in 2017[5] to 14% today.

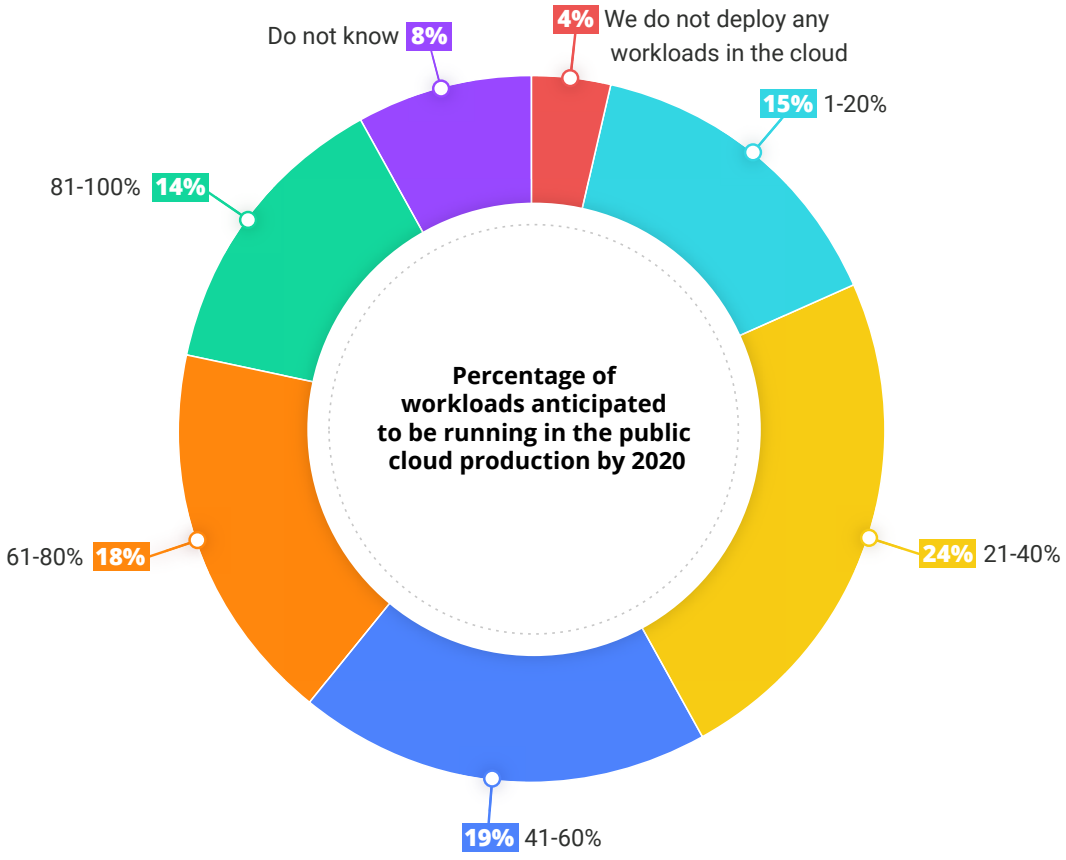
When asked what percentage of workloads an organization is operating in the public cloud, 0- 20% was the most commonly selected response (38% of respondents). About a quarter of respondents (21%) reported hosting between 20 and 40% of their workload in the public cloud, while another quarter (25%) reported already having more than 40% of their total workload in the public cloud. A small sample of highly regulated industries like healthcare and financial services more frequently reported having less of their information (up to 20% of workload) in the cloud, when compared with other industries[6].

Respondents were also asked to predict the percentage of workload their organization plans to move to the public cloud by the end of 2020. Respondents indicated they expect these workloads to increase, with an approximate doubling of the number of organizations who would likely be hosting more than 40% of their total workloads in the public cloud. While 9% of respondents reported currently not using the cloud for any workload at all, that percentage dropped to 4% in their projections for 2020. Those in the IT industry were more likely to select 81-100% of workload in the cloud (20%) than those in regulated industries like healthcare (7%) and financial services (8%).

[5] https://www.algosec.com/wp-content/uploads/2017/10/171029_algosec_hybrid_cloud_survey.pdf

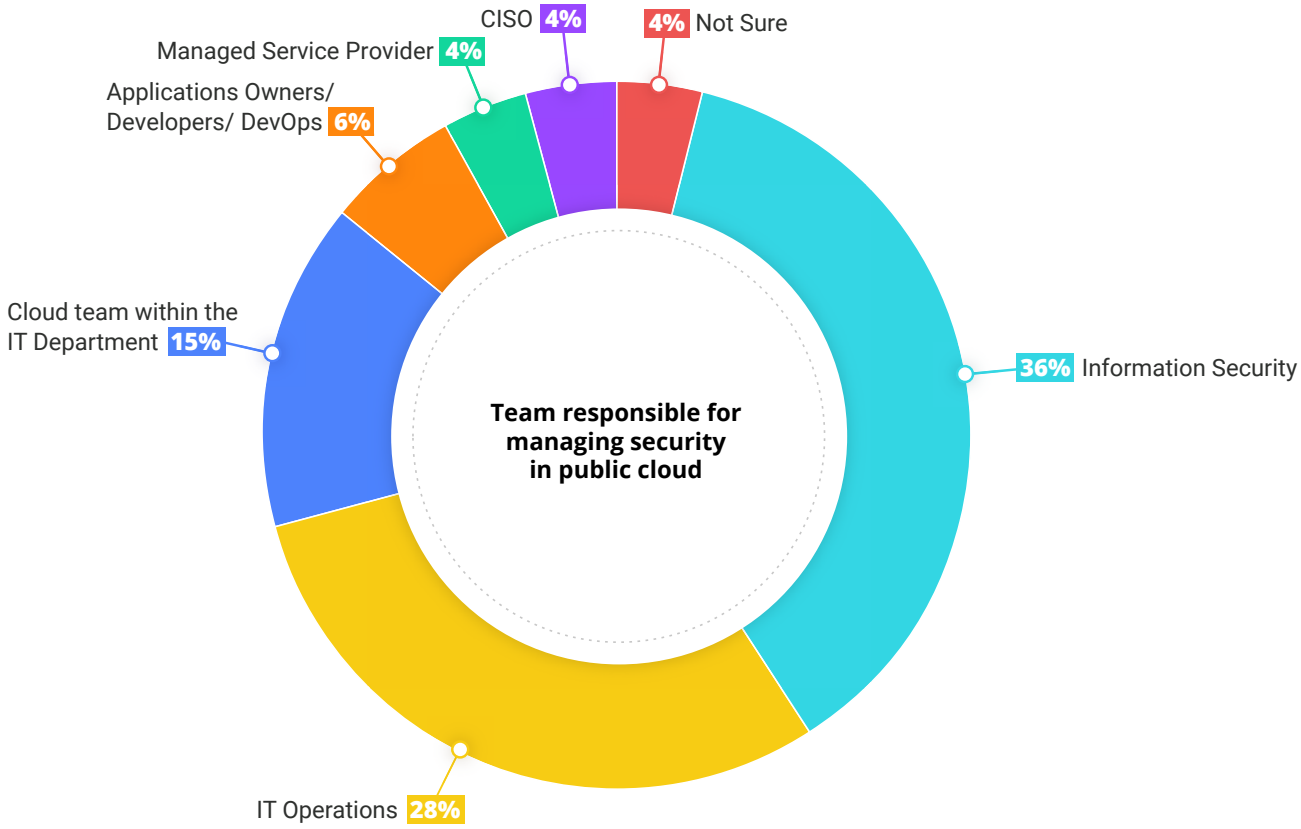
[6] The sample size for healthcare was 35 respondents, and finance was 74 respondents.





CONCERNS AND CHALLENGES: ENSURING SECURITY AND COMPLIANCE

With easy accessibility to cloud services, each separate business department in an organization has more control and ownership over the services they use. With this increased use, organizations must identify which department(s) will be responsible for security. Most survey respondents (79%) indicated that their IT department held this jurisdiction. Of those responses, just 15% had nominated a dedicated cloud security team within their IT department. Meanwhile, the remaining respondents relied on other security services, such as DevOps or a managed service provider. As easily available as cloud services are and the speed in which they are being adopted, responsibility for security should be considered shared throughout the organization with each business unit understanding the security issues around each service they are using.



The vast majority of respondents (81%) expressed concerns about security when considering moving data to the cloud. Respondents' concerns about data loss and leakage risks were also high (62% of respondents) when considering moving to the public cloud. Companies already face security issues with on-premise solutions. Moving to the cloud can further expose these vulnerabilities, making the need to protect data before migration an important task. The majority of respondents had high levels of concern for security when adopting public cloud platforms, however, more research needs to be conducted to better understand how these concerned users are using their cloud platforms. Using cloud platforms as a hosted service can amplify existing vulnerabilities when directly migrating enterprise applications. Building or re-building within the cloud platform allows enterprise applications to take advantage of cloud native features including security.

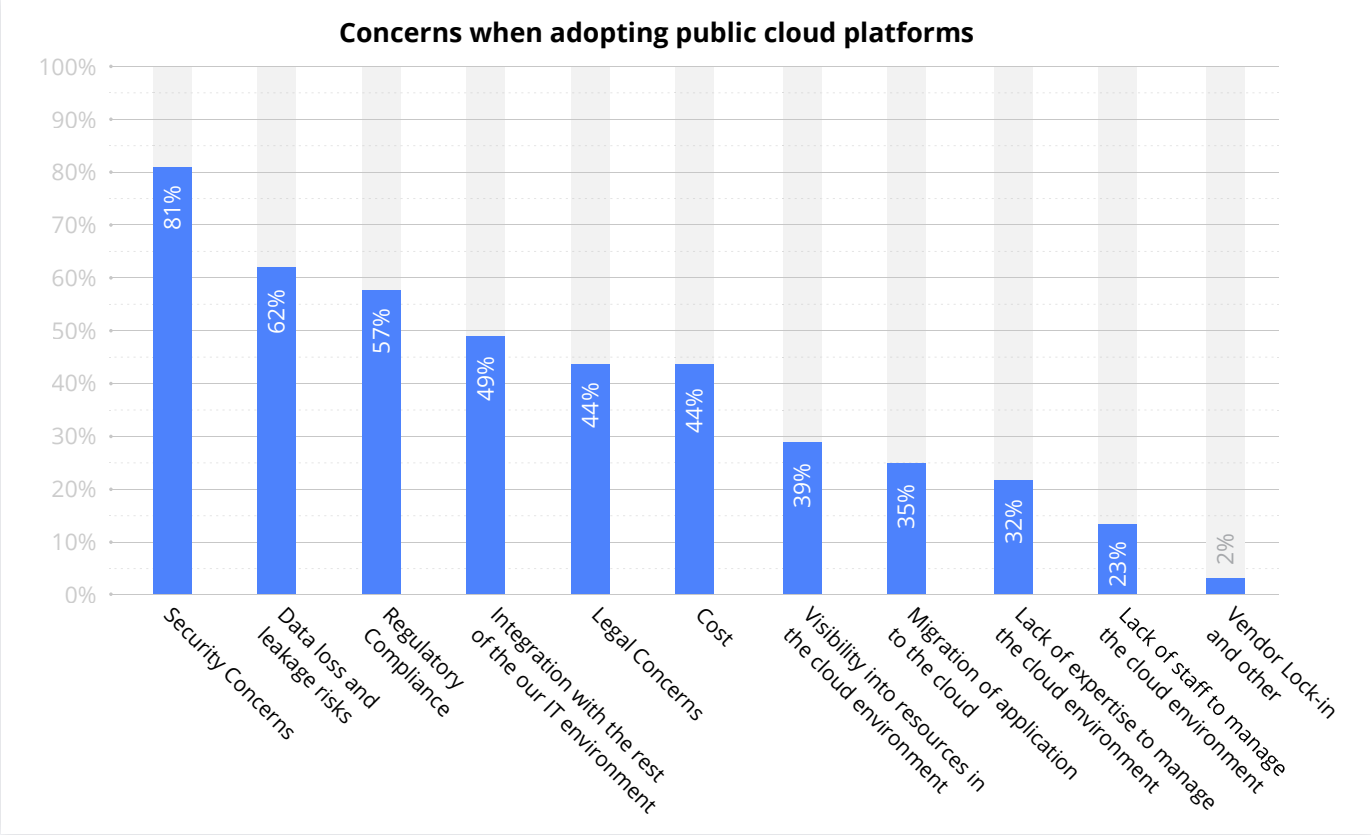
In addition to common compliance frameworks (e.g. ISO 27001, PCI-DSS, HIPAA, SOX, NIST 800-53), cloud providers are continuously upgrading services and platforms to be compliant with new regulatory policies and industry standards, such as the new European General Data Protection Regulation (GDPR) and CSA Security, Trust, Assurance, Risk (STAR). In recent years, we have seen increased enforcement and greater penalties for security violations. Meanwhile, customers using cloud services may be uncertain about who is liable for any such security violations. More than half of survey respondents (57%) reported concerns about regulatory compliance, and nearly half indicated unease over legal concerns (44%) when adopting public cloud services. There is still ambiguity on how customers leverage these platforms for compliance and who is liable for regulatory violations.

Many respondents (39%) indicated that one of the items of concern when moving towards public cloud adoption is visibility into resources in the cloud environment. In a 2017 survey, this concern was significant enough to keep organizations from adopting the public cloud[7]. The need for cloud visibility has given rise to new security tools and vendor solutions to add to the cloud platforms and services that are already being utilized. Leveraging existing standards and open tools can guide organizations for measuring the security, transparency, assurance, and risk of each service. Even with the rise in available security tools, consumers will likely need to push their cloud service providers (CSPs) for higher transparency and accountability.

Organizations may also be scrambling to train and acquire talent to manage security skills gaps related to the use of public clouds. These concerns need to be addressed equally by customers and cloud service providers if the industry hopes to achieve robust security and transparency as a whole. About a third of respondents reported a lack of expertise and a quarter reported lack of staff to manage their cloud environments. Half of this survey's respondents expressed concern about integrating the public cloud with their current IT infrastructure. Additionally, the above-mentioned 2017 survey found that 61% of respondents already using a hybrid cloud reported that consistent management of security across the hybrid environment is one of their organization's greatest challenges. With the apparent rise in multi-cloud platform usage and the move to public cloud environments, the skills gap concern will need to address management guidelines for their programs, which includes proper use of provider security tools and default configurations.

Less than 2% of respondents mentioned vendor lock-in as a major concern. This correlates to the rise and practice of hybrid cloud and multi-cloud environments, as indicated from earlier analysis.

[7] https://www.algosec.com/wp-content/uploads/2017/10/171029_algosec_hybrid_cloud_survey.pdf



Respondents were asked to rate the level of challenge several different issues posed to managing security in the public cloud (no challenge, minimum challenge, moderate challenge, maximum challenge). The issue found most frequently to be a maximum challenge was proactively detecting misconfigurations and security risks, and was followed by a lack of visibility into the entire cloud estate.

Other interesting findings:

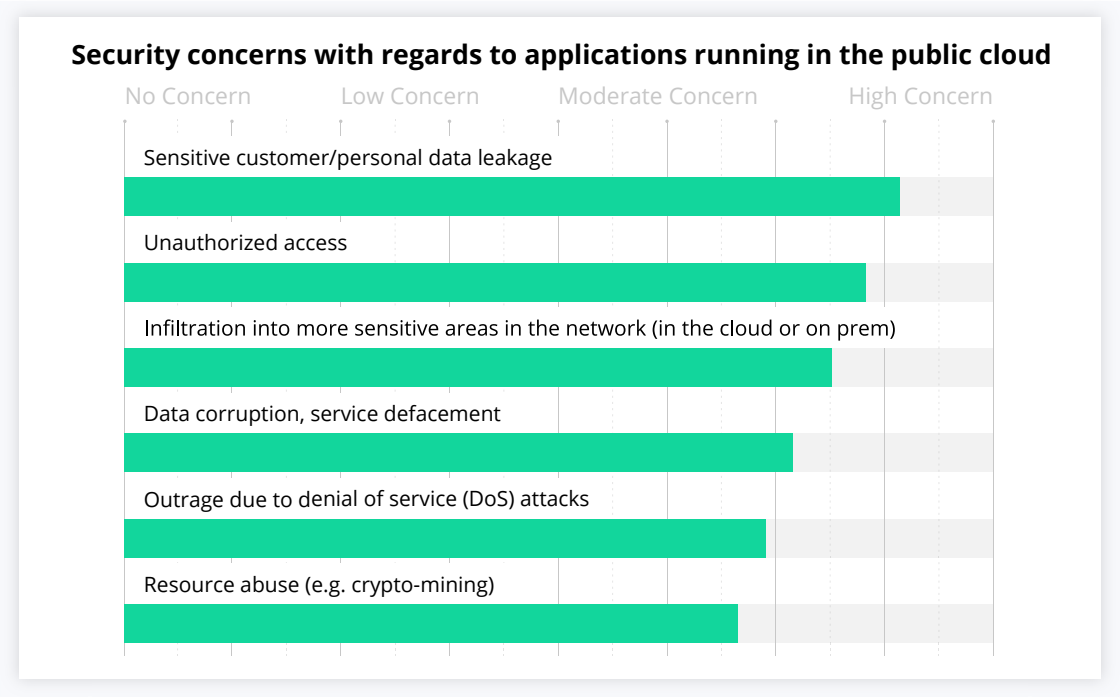
- Respondents who reported experiencing a cloud-related security incident in the past 12 months were more likely to report lack of staff to manage the cloud environment as a concern (44%) when compared with those who had not experienced a security incident (17%).[8]

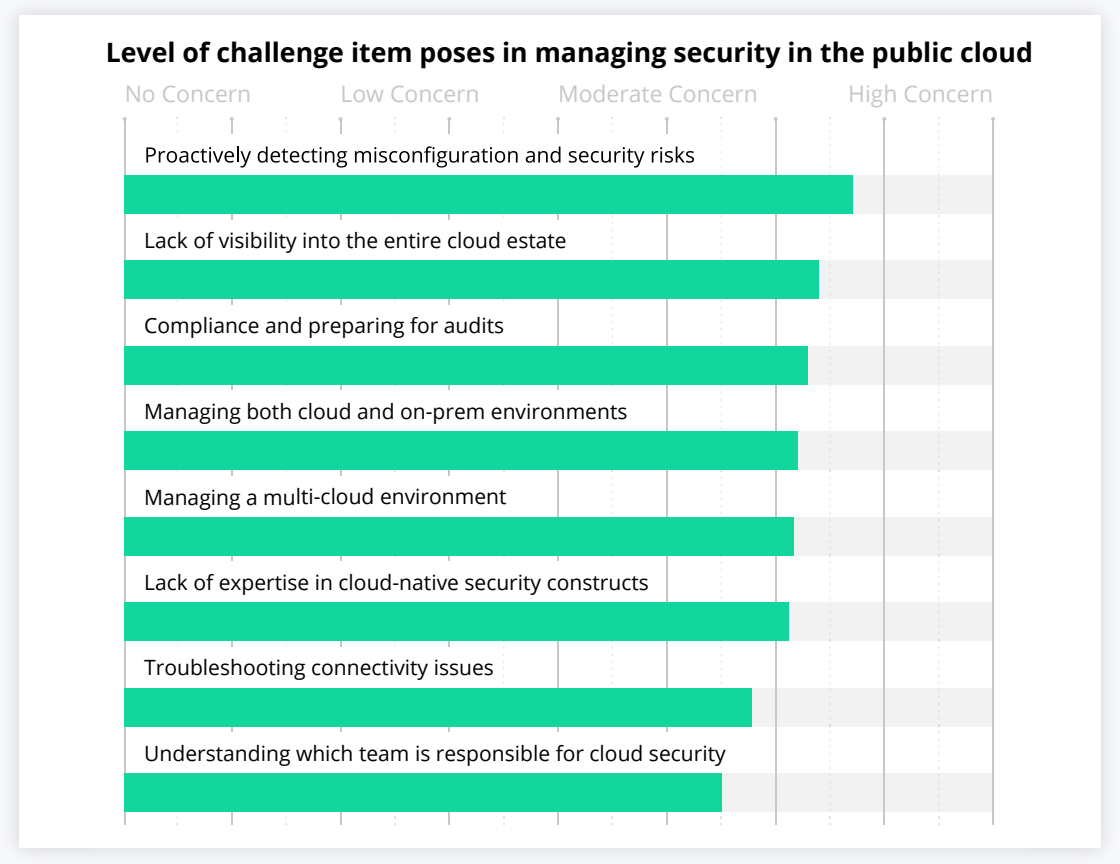
These challenges, if not managed correctly, can lead to many important security problems. When asked to rate security concerns related to running applications in the public cloud, the highest rated concerns were sensitive customer/personal data leakage, unauthorized access, and infiltration in more sensitive areas in the network (in the cloud or on-prem).

Security in the public cloud remains a shared responsibility of providers and end users. To ensure adequate management of security, providers must continue to implement secure default

[8] Of the 58 respondents that recorded experiencing a cloud-related security incident in the past 12 months, 25 reported lack of staff to manage the cloud environment as a concern. Of the 461 respondents that did not record having experiencing a security incident in the past 12 months, 56 reported lack of staff to manage the cloud environment as a concern.

configurations for their customers and alert customers systematically and reliably when these configurations are altered. Meanwhile, when organizations adopt cloud services, it will likely be necessary to acquire tools and staff to manage security properly in these new environments.

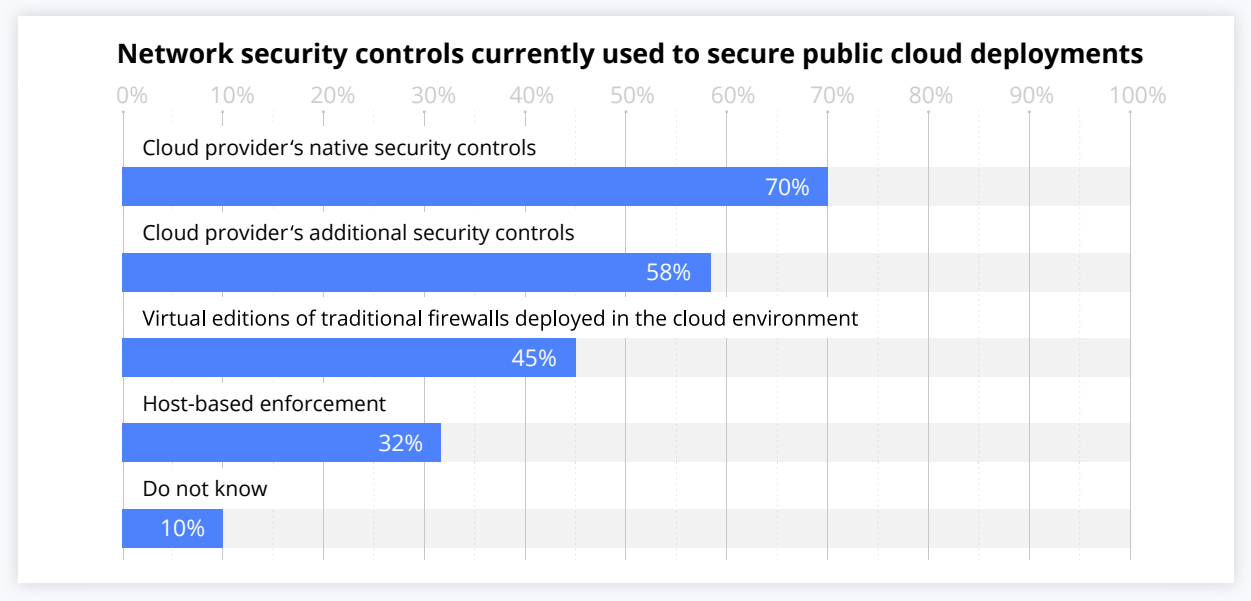


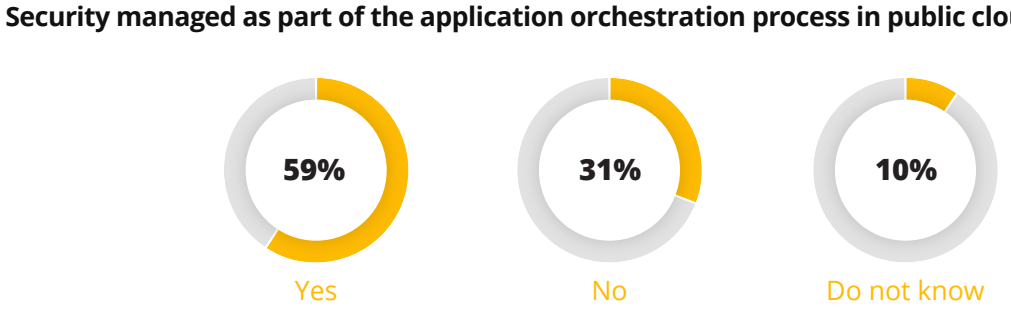


SECURITY MANAGEMENT: TOOLS AND COUNTERMEASURES

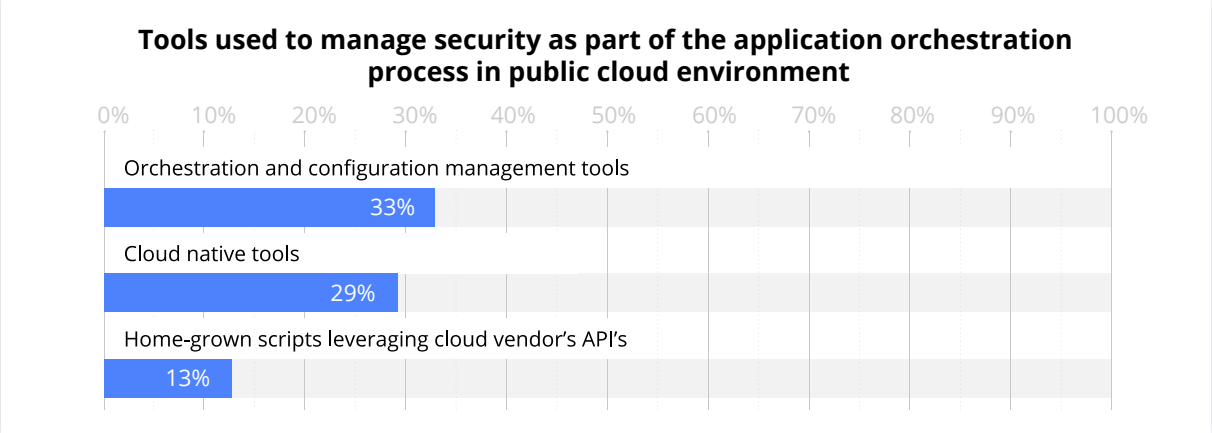
The use of multi-cloud and hybrid cloud environments can provide many benefits, it also increases the complexity of securing these environments. To better understand how organizations are navigating these complexities, survey respondents were asked what network security controls they use to secure their public cloud deployments. The majority of the respondents reported using more than one security control to manage their public cloud deployments, with the most popular choice being cloud-native security controls (70%). In a similar study performed in 2017[9], only about a quarter of respondents were using their cloud providers' native security tools. This indicates a significant increase in the use of CSP's native security controls.

There was also a significant number of respondents who reported using cloud provider's additional security controls (58%) and virtual editions of traditional firewalls (45%). Far fewer, reported the utilization of host based enforcement (32%).

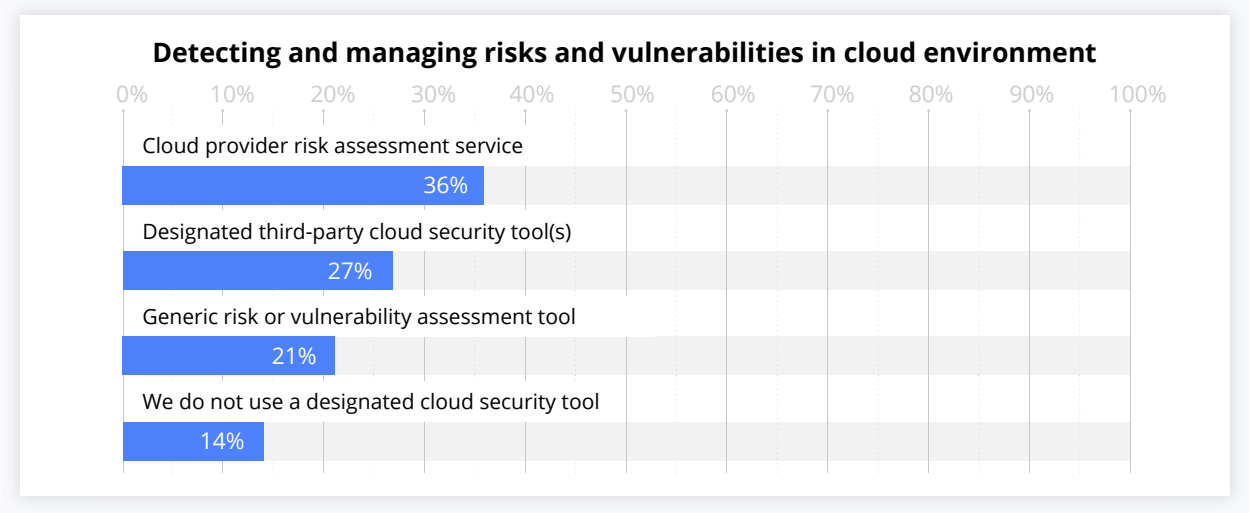




[9] https://www.algosec.com/wp-content/uploads/2017/10/171029_algosec_hybrid_cloud_survey.pdf



Security management can take many forms within security application orchestration. Respondents were asked whether they currently manage security as part of their application orchestration process, the majority 59% reported yes. To follow up, respondents were then asked what they use to manage security as part of their application orchestration process in public cloud, the responses were mixed. The most common response was orchestration and configuration management tools (33%). Another common responses include cloud native tools (29%). Less common was the use of home-grown scripts leveraging cloud vendor's APIs (13%).



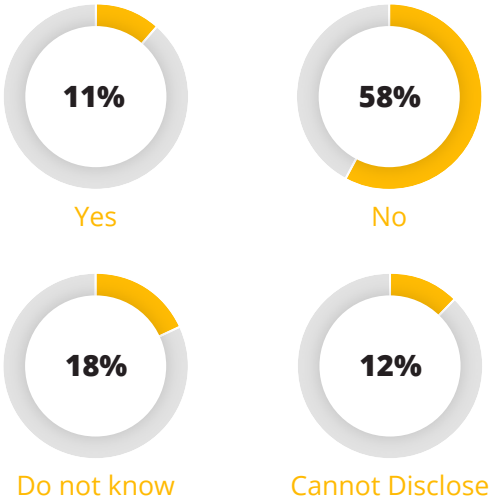
Early detection of potential security risks continues to be an important aspect of security management. The tools utilized to detect and manage these risks or vulnerabilities are vital to early detection. In this survey, about a third of respondents use their cloud providers' risk assessment service to detect and manage vulnerabilities, while close to a quarter use designated third-party security tools. Another fifth of respondents use generic risk or vulnerability assessment tools. This indicates that less than half are utilizing tools above and beyond what is provided by the CSP. By doing this, organizations's trust is heavily placed on CSPs assessment services without validation and could leave the organization vulnerable.

SECURITY INCIDENTS AND CLOUD OUTAGES: PREPARATION AND RECOVERY

When asked about security concerns related to applications in the public cloud, nearly 90% of this survey's participants reported moderate or high concern about data leakage; unauthorized access; and infiltration of sensitive network areas. About two-thirds reported the same levels of concern about outages due to DoS attacks; data corruption; and resource abuse.

Many enterprises are ill-prepared for security incidents, such as breaches and outages. When asked whether their organization had experienced a cloud-related security incident in the last 12 months, 11% reported definitively having had a security incident, and another 30% were either unsure or could not disclose. In the last year, 43% of respondents' organizations have experienced a network or application outage.

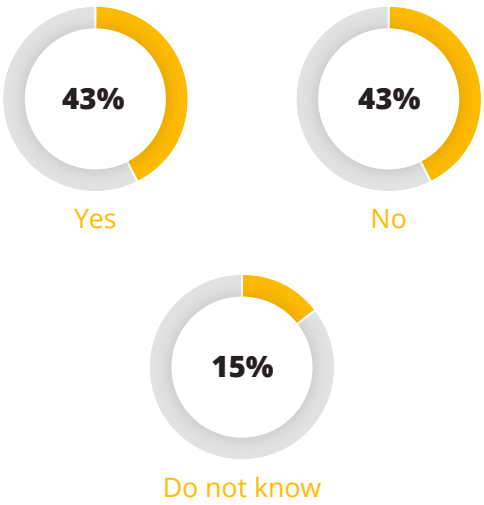
Experienced cloud-related security incidents



Other interesting findings:

- Respondents from Asia were more likely to report experiencing a cloud-related security incident in the past year (17%) than were respondents from the EU (5%) or the US (8%).

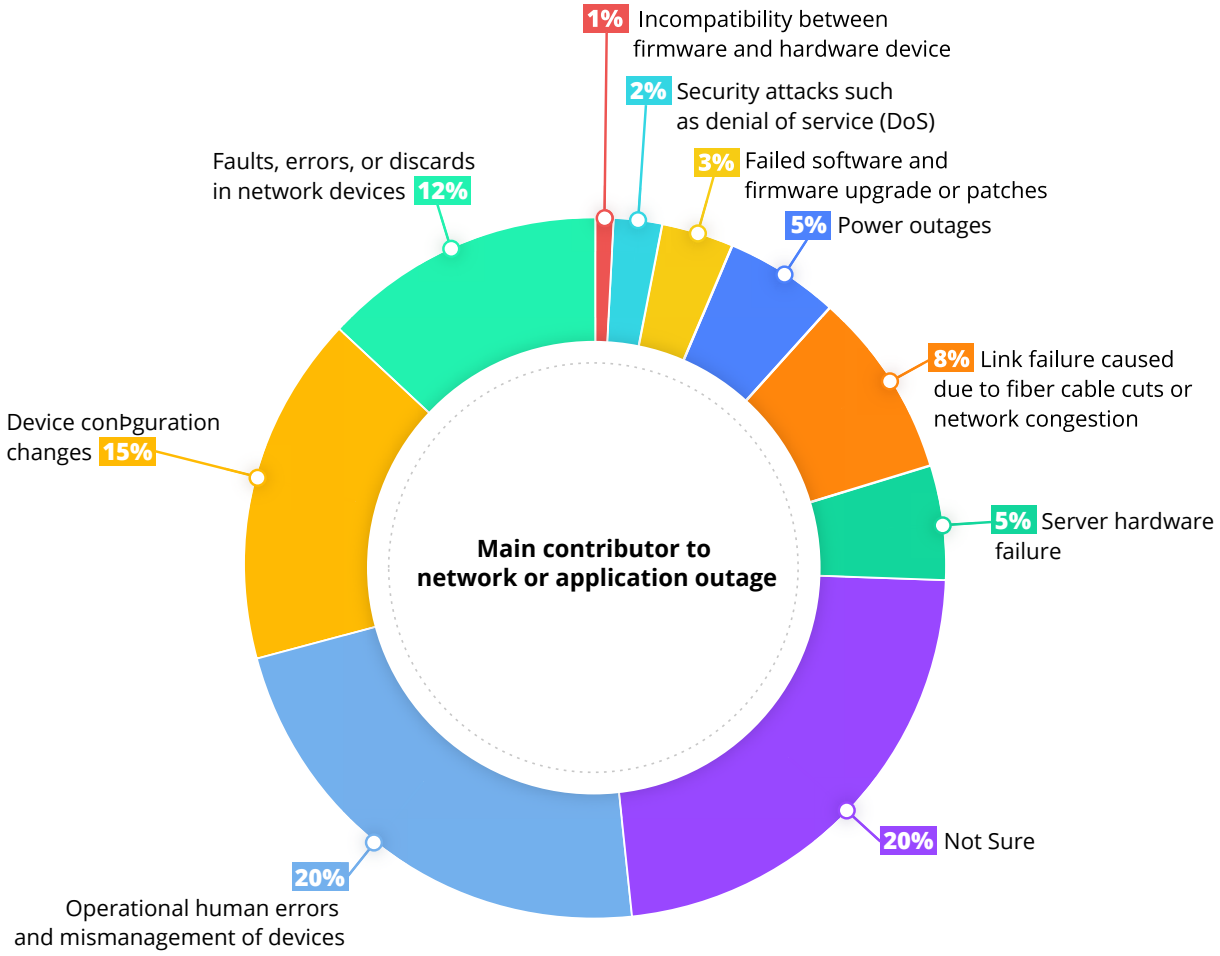
Experienced a network or application outage



Other interesting findings:

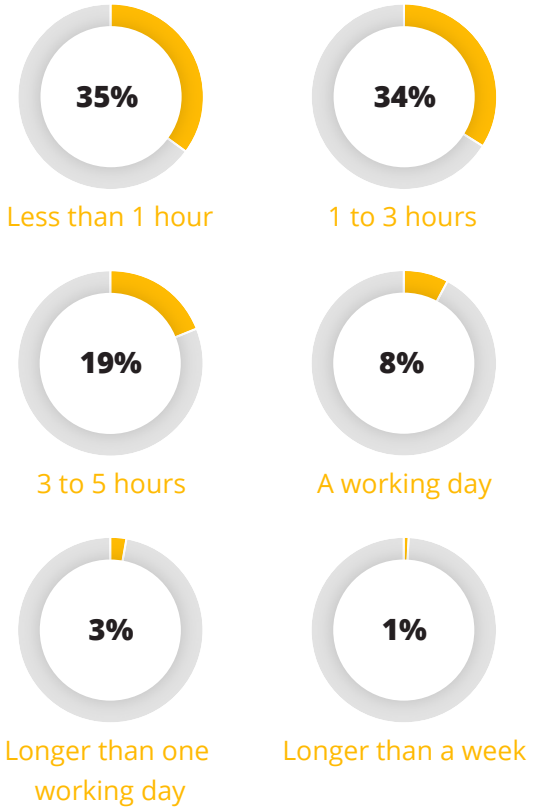
- Respondents in a small sample of regulated industries like healthcare (53%) and financial services (52%) were more likely to report having experienced a network or application outage than those in other industries (33%).

The contributors to these outages included both human error and numerous technical problems, such as power outages and hardware failures. When asked to identify the primary contributor to one recent outage, most respondents were unsure of its cause (which may indicate a problem related to visibility). The next most popular answers were operational human errors and mismanagement of devices (20%) and device configuration changes (15%).



For over 25% of respondents, it took over 3 hours to restore normal operation. Significant delays could lead to significant revenue loss for an organization through operational inefficiency, lack of productivity, and leaves the organization vulnerable.

The length of an experienced network or application outage



Other interesting findings:

- Those who reported having experienced a network or application outage were less likely to have had their outage resolved within an hour (10%), when compared with those who reported having an application outage but no security incidents (42%).
- Ninety-seven percent of respondents reported their outages were resolved within one working day.

CONCLUSIONS AND RECOMMENDATIONS

Many organizations are migrating more and more of their workloads to cloud-based resources, including hybrid environments, multi-cloud environments, and combinations of the two. These organizations also are working to integrate various applications from public and private cloud providers with their own on-premise resources. As cloud computing environments become even more complex, it is critical for IT professionals to have visibility into their cloud-based resources and to be able to trust the expertise of their own security staff and their cloud provider's staff. These concerns are underscored by the many new regulatory compliance and legal obligations, making it absolutely necessary for these responsibilities and liabilities to be clearly designated.

Build in Security and Compliance

The use of multiple cloud platforms and services offers best in breed capabilities and reduces the reliance on a single vendor. The added need for visibility of data across multiple services has given rise to even more security tools and vendor solutions. This increased adoption of services, combining traditional on-prem and multiple cloud offerings, adds to an already complex environment. This complexity in a cloud environment increases the level of expertise needed to manage and secure these services.

Organizations will need to understand how to leverage cloud platforms and use provider tools in order to maximize the full benefits of the cloud. Cloud providers continue to offer native tooling with added

visibility and security, often meeting or exceeding other traditional (on-premise and third-party) security controls. Cloud provider platforms and services meet some of the more strict compliance requirements for industry and government regulations. Architecting your IT environment to the services and platforms that are being used allows cloud customers to use cloud native tools for improved security and built-in compliance across complex environments. "

Take Responsibility for Security Internally

The cloud service provider and customer IT management teams should be able to articulate their security objectives and establish a baseline level of security requirements that can be measured and shared by both. This shared responsibility approach can go a long way in bolstering transparency and assisting with additional adherence to security regulations and best practices. It is essential for customers to build trust with cloud service providers before migrating any of your organization's vital resources to the provider's cloud.

Today's cloud adoption model doesn't always allow a procurement team to stand between the company data and cloud services being used. The easy adoption and accessibility to cloud services leads to business units throughout organizations using services that are unknown and often undiscovered by IT management and cloud procurement teams. In addition to establishing shared security responsibility with cloud providers, each separate business unit should have a level of awareness of the security objectives established by their organization. Identifying a department responsible for cloud security, establishing cloud security policies across business units, and raising the level of education and awareness for all employees completes the modernized shared responsibility model. The data owner can take responsibility for data security that includes external business partners and internal business units. "

While many capabilities expand in the cloud, existing and future security risks and vulnerabilities unfortunately may also expand. Cloud providers continue to offer more security features and end users are working to increase staff and expertise to manage these tools.

Detecting Misconfigurations and Security Risks

Training and acquiring staff to manage security remains a challenge for properly implementing cloud services. In addition to staying up-to-date on security best practices, cloud customers struggle to keep up with the rapid advancement of features constantly being added to the cloud services. The cloud providers need to play a role in both securing the cloud services and ensuring that customers are using the services securely.

As cloud services evolve, new features are added to improve functionality and security of cloud services. Customer awareness of these features and the training of secure operation should be a priority for the cloud provider upon releasing updates to their services. Additionally, safe and secure default configurations should be implemented to ensure exposed features aren't turned on without the acknowledgement or understanding of the customers. Finally, customer notification of misconfigurations of publicly exposed services, insufficient credentials, and misuse of any features should be a built in part of the service. Cloud customers and providers need to work together to improve the overall operation, management, and security of cloud services."

When to Automate

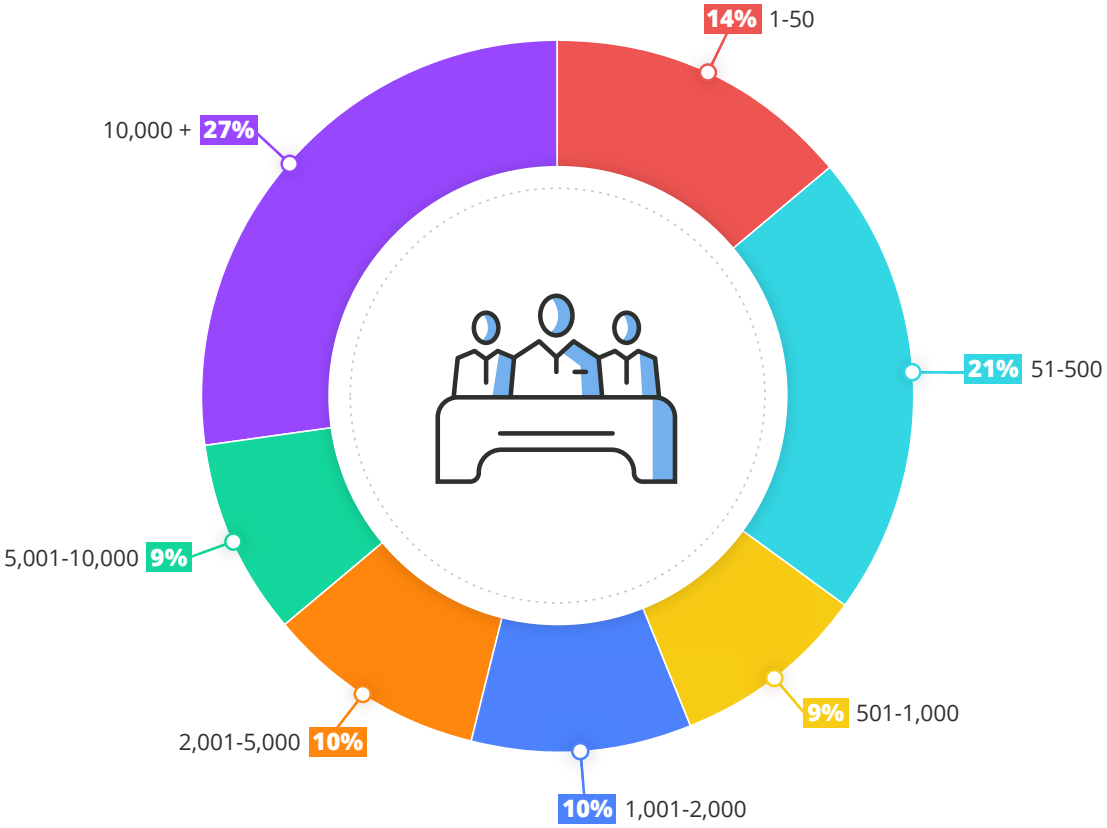
The increased adoption of cloud services and features must be met with a skill set that matches the complex cloud environment. The skills to increase visibility and security in cloud service operations involves the training of people toward the management of each service and the ability to automate features when possible. Automating components of your security aids in the lack of expertise and staff to manage a complex cloud environment. Log activity, data aggregation, threat detection, and security policy management are just a few pieces of where automation can help more quickly and accurately identify security gaps, compliance violations, service misconfigurations, service outages, and other anomalous behaviors. As we look to accelerate the use of new technologies, devices, and users in the cloud environment, automation promises to help organizations and their staff keep up with the security and operational demands of tomorrow's cloud."

Organizations are continuing to migrate more of their workload into complex cloud environments such as hybrid, multi-cloud, and a combination of the two. These environments are the new reality for organizations and addressing security concerns and challenges, discovered through this survey, is of the utmost importance. Security challenges arise in these complex environments due to several factors including lack of visibility, regulatory compliance and legal concerns, and lack of staff expertise. Organizations are able to remedy the situation building in security and compliance, proactively taking responsibility of security, establishing safe and secure default configurations, and utilizing automation.

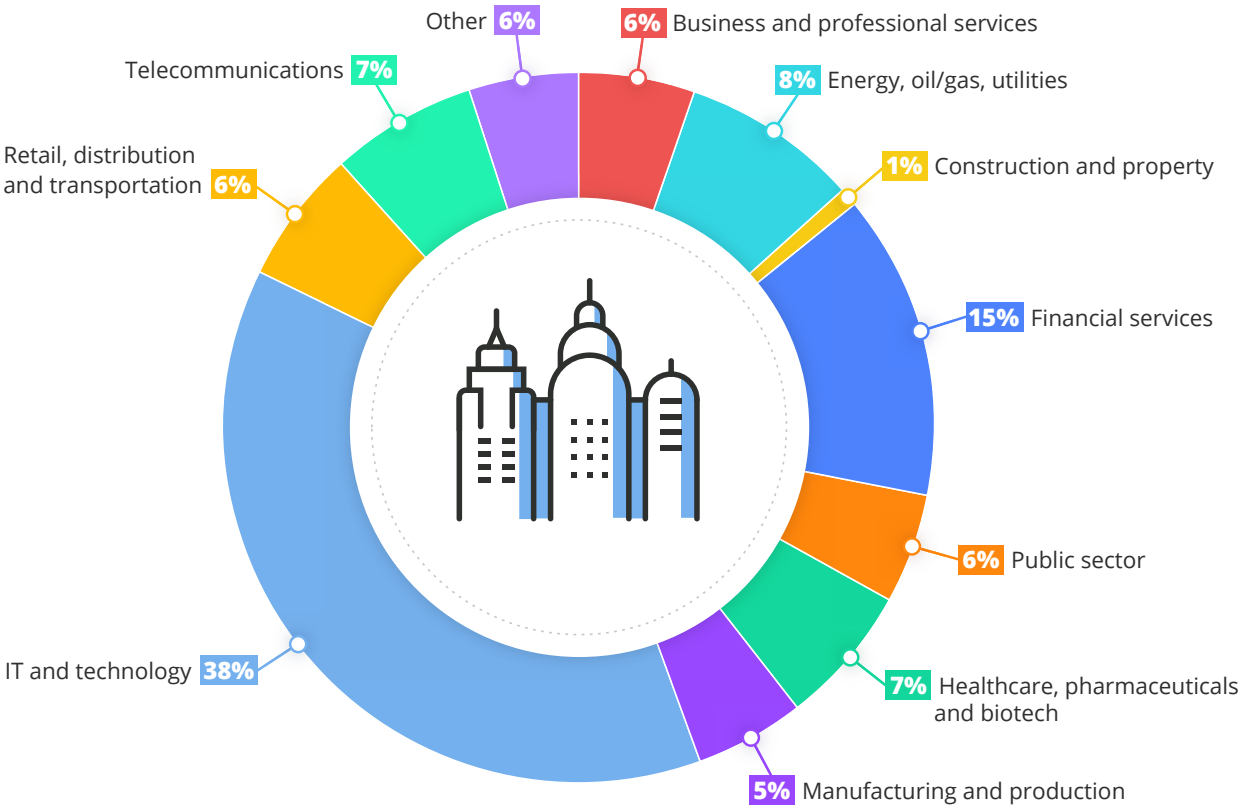
SURVEY PARTICIPANT DEMOGRAPHICS

This survey was conducted from December 2018 to February 2019 and gathered 700 responses from IT and security professionals from a variety of organization sizes, industries, locations, and roles.

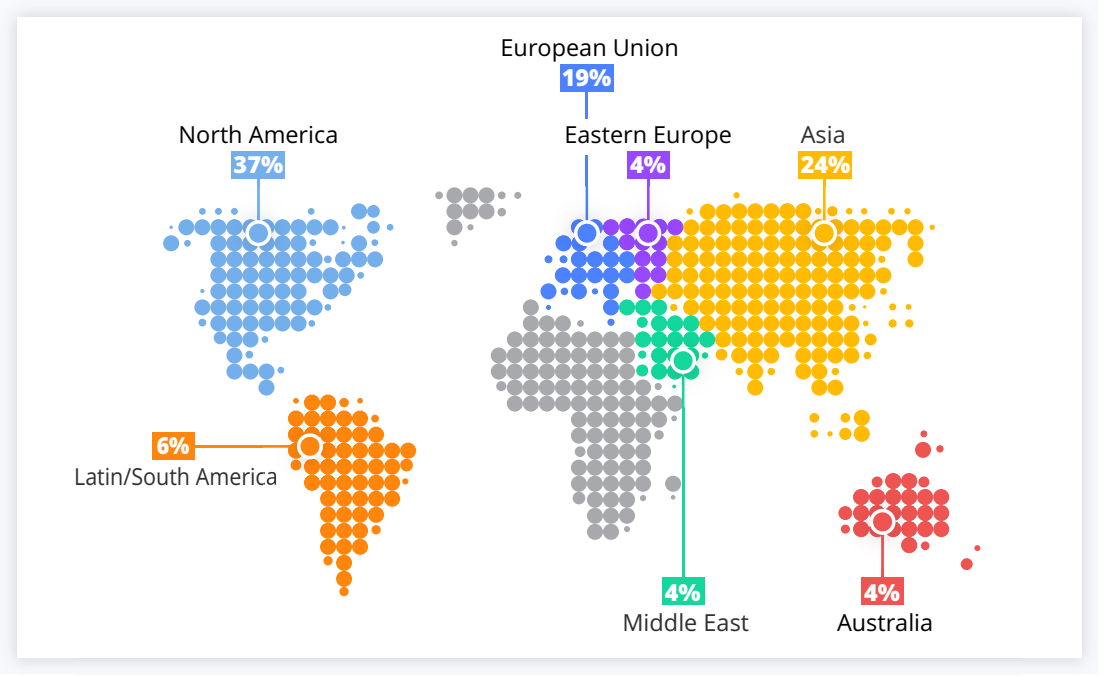
The size of your organization



Select the option that best reflects your companies industry



Location



Primary roles