CLOUD AND HYBRID ENVIRONMENTS: THE STATE OF SECURITY

AN ALGOSEC SURVEY

BUSINESS-DRIVEN SECURITY MANAGEMENT

www.AlgoSec.com

EXECUTIVE SUMMARY

AlgoSec recently surveyed 450 C-level executives and senior security and network professionals to investigate the hybrid cloud security strategies of their organizations. The survey revealed that many organizations are embracing hybrid cloud as part of their enterprise infrastructure, and plan to increase their adoption of cloud platforms over the next three years. However, the majority of enterprises do have some serious security concerns and encounter significant challenges when managing security across hybrid environments, both during and after cloud migrations.

Key insights include:

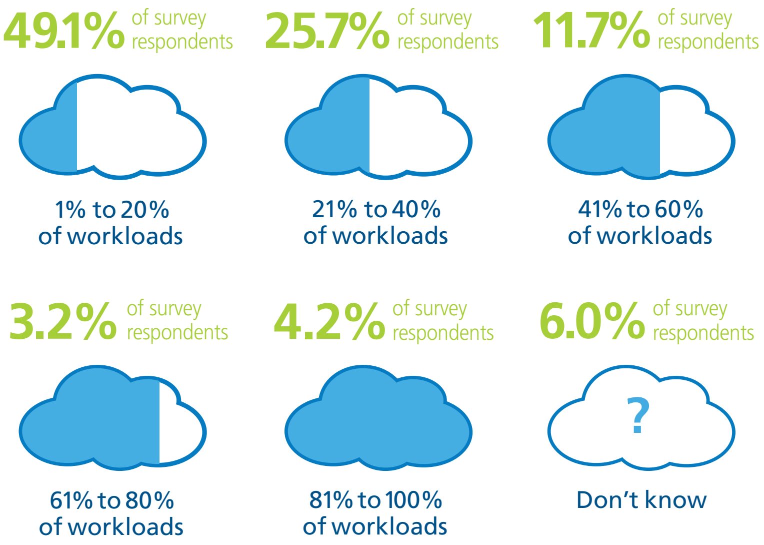
- **Security concerns are front and center:** respondents' greatest concerns about their applications in the cloud are cyber attacks (58%) and unauthorized access (53%), followed by application outages and misconfigured cloud security controls. These concerns are hampering wider use of public clouds, with nearly 40% of respondents saying security is inhibiting further adoption of cloud platforms.
- **Cloud obscures visibility, hampers management:** the biggest security management challenges enterprises face in hybrid environments are a lack of visibility (63%) and managing security policies consistently (61%). Demonstrating compliance and managing a mix of traditional and virtual firewalls and cloud security controls were also cited as major issues. These challenges highlight the need for solutions that can manage and automate security processes holistically across both cloud and on-premise networks.
- **Manual cloud migration mishaps:** respondents reported a range of problems when migrating applications to public clouds. 44% had difficulty managing security policies post-migration, 32% had difficulty mapping application traffic flows before starting a migration project, and 30% reported their applications did not work after the cloud migration: emphasizing the need for automation solutions that can manage this highly complex process end-to-end to ensure business continuity.
- **Automation benefits in hybrid clouds:** 26% of respondents said they use automation to manage security in their hybrid environments, with 20% using manual processes. Enterprises that used automation said the top reasons for doing so were speed and accuracy of security changes, ability to speed up migrations to the cloud, providing audit reports and enforcing compliance, and helping to overcome staffing limitations — highlighting the security and operational benefits of automation.

The survey clearly shows that most enterprises are driving their business transformation strategies by expanding their usage of public cloud infrastructure. But they also have significant security concerns about how they will secure and manage their increasingly hybrid environments. As organizations increase their public cloud deployments and migrate applications to the cloud, it's essential that they have complete visibility across both their on-premise and cloud networks, together with the ability to automatically and holistically manage security policies. This enables them to better protect the business and fulfill compliance demands, while taking full advantage of the cost savings and agility offered by the hybrid cloud model.

HYBRID IS HERE AND NOW

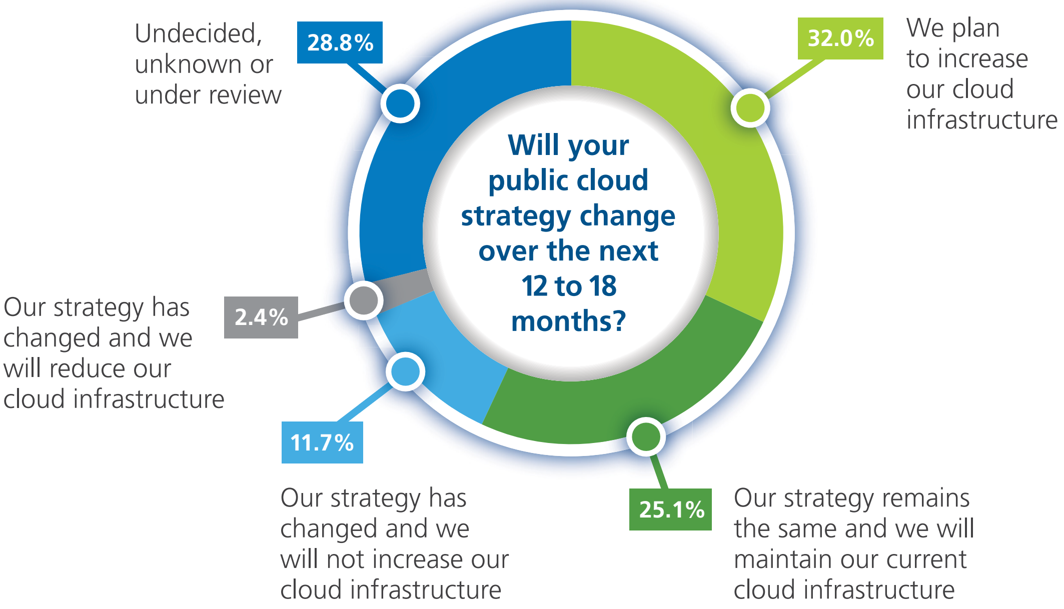
All the organizations that participated in the survey are using public cloud services for some of their business applications. Nearly half of the respondents (49%) said their organization was running up to 20% of its business workloads in the public cloud, while a quarter (26%) use public cloud for between 21 and 40% of workloads. 7% use public cloud services for between 61 to 100% of their workloads.

Percentage of workloads in the cloud



Larger organizations tend to run a higher proportion of their workloads in the cloud, compared with smaller enterprises: 45% of organizations with 5,000 to 10,000 employees and 40% of organizations with over 10,000 employees run between 21% and 60% of their workloads in the public cloud (compared to 37% overall).

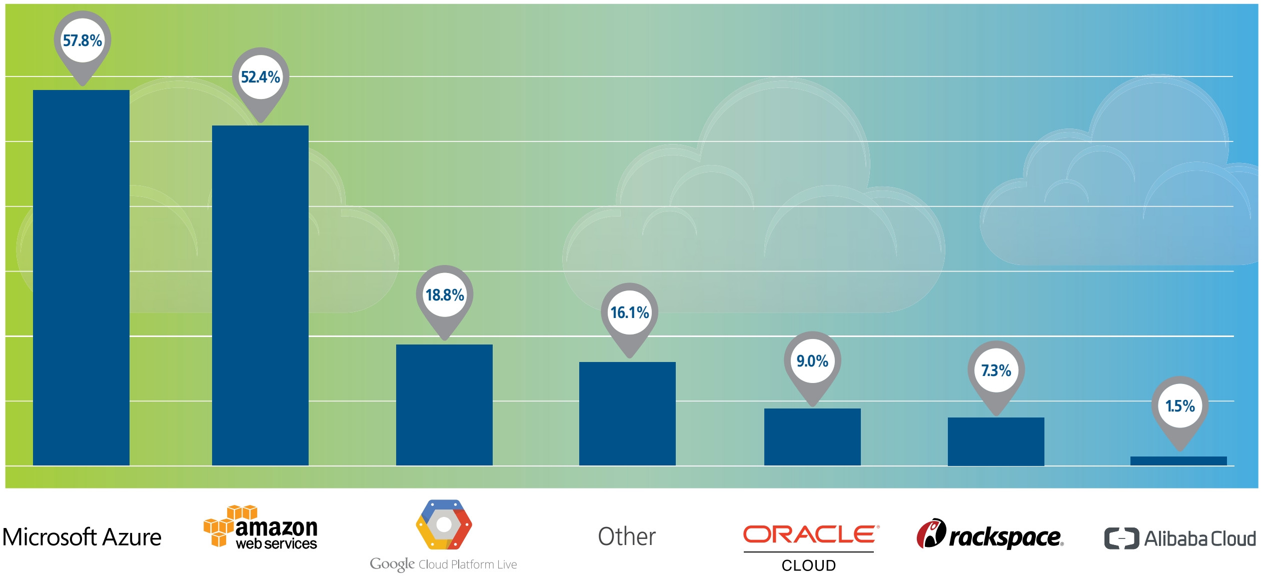
What's more, hybrid cloud environments are here for the long run. 32% of organizations said they plan to grow their public cloud infrastructure over the next 12-18 months, and 25% expect to maintain it at its current level. Just 2% said they plan to reduce their public cloud usage.



AWS AND AZURE STILL LEAD THE PACK

Interestingly, the survey showed that many organizations are increasingly adopting a multi-cloud approach using multiple cloud vendors to support their infrastructure. 58% of survey respondents use Microsoft Azure, and 52% of respondents use Amazon Web Services as their cloud platforms. Additionally, 19% use Google Cloud, 9% use Oracle Cloud, and 7.3% use RackSpace.

Which public cloud platform does your organization use?



The same holds true for security controls. 58% of respondents use the cloud provider's native security controls to secure their cloud deployments while 44% said they also use third-party firewalls deployed in their cloud environment (specifically Cisco Adaptive Security Virtual Appliance, Palo Alto Networks VM Series, Check Point vSEC, Fortinet FortiGate-VM and Juniper vSRX), thereby creating a mixed estate of traditional and virtualized firewalls, and cloud security controls.

The additional advanced security features provided by these third-party next-generation virtual firewalls, such as application and user awareness, enable a more granular approach to application security which becomes critical as enterprises move more of their mission-critical applications to the public cloud.

SECURITY CONCERNS ARE STILL FRONT AND CENTER

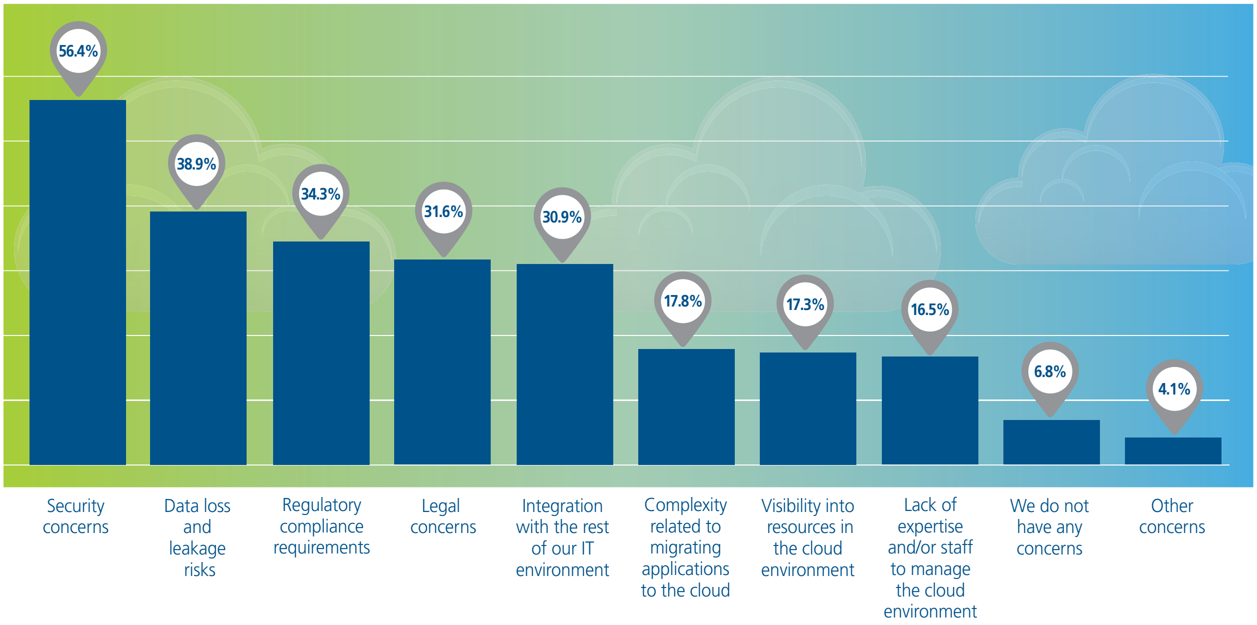
Despite the growth trends, organizations still have significant concerns related to security in the public cloud, which is impacting a wider adoption of public cloud platforms.

The greatest concerns for organizations currently running applications in public clouds center on their exposure to cyberattacks, the risk of breaches and outages, and the challenges and complexity of managing security effectively in the public cloud.

59%	1	Cyberattacks
53%	2	Unauthorized access by an outsider
46%	3	Downtime or outages
41%	4	Misconfiguration of cloud security controls leading to security holes
37%	5	Inability to meet compliance requirements
30%	6	Unauthorized or risky security changes
29%	7	Managing hybrid on-premise and cloud environments consistently
29%	8	Another cloud tenant accessing my corporate data

By far the greatest concern impacting the wider adoption of public cloud platforms for enterprise applications, cited by 56% of respondents, is security. Other significant concerns were the risks of data losses and leaks, meeting compliance requirements, legal issues, and integration with existing IT estates.

What's holding your organization back from wider adoption of public cloud?



Respondents also expressed concerns about the complexity of migrating applications to the cloud, gaining visibility into their cloud estates, and a lack of expertise or resources to manage the cloud environments.

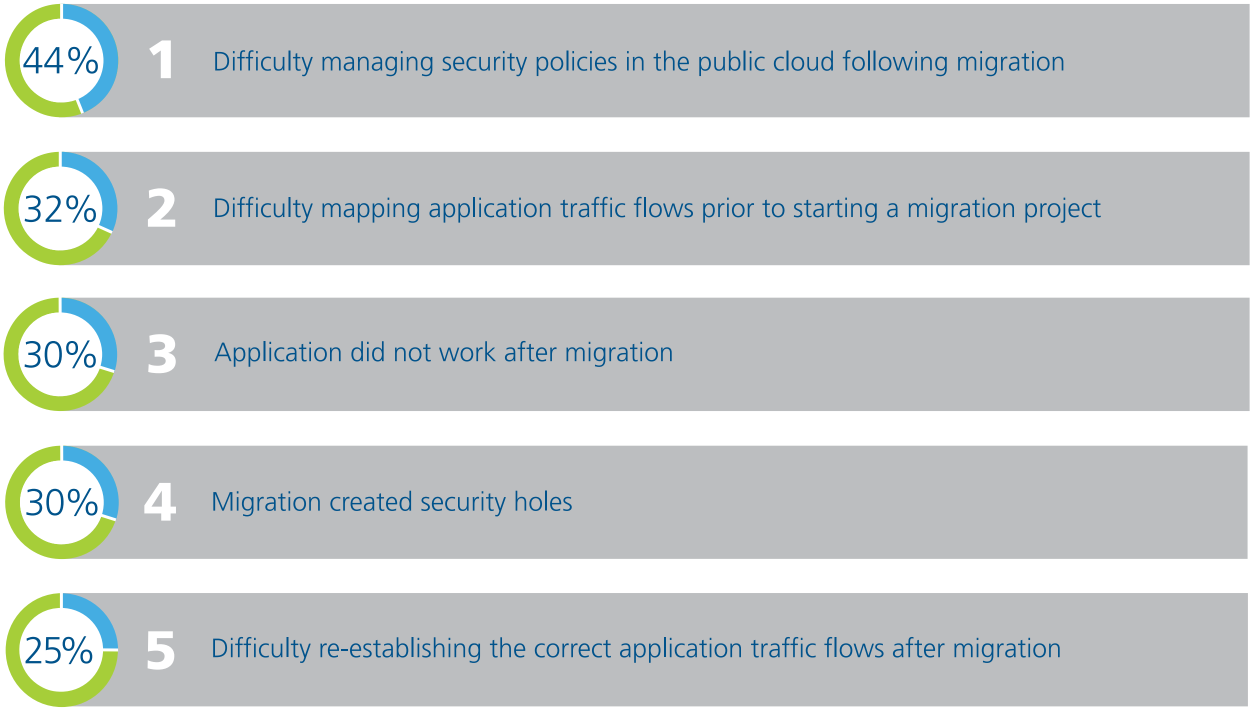
Just 7% of respondents stated they had no concerns over wider cloud adoption.

Over 41% of respondents from larger organizations (those with 5,000 employees and above) rated meeting regulatory compliance requirements as their second greatest concern, compared with 34% of overall. This is likely due to the fact that larger organizations are typically subject to more stringent regulatory compliance requirements and run a higher percentage of their workloads in the cloud.

Respondents with the role of CIO or CISO expressed higher levels of concern regarding security, the risks of data loss and leaks and meeting compliance requirements. This reflects the fact that C-level respondents are likely to have direct executive responsibility and accountability for maintaining security and compliance across their organizations.

MOVING TO THE CLOUD ISN'T SMOOTH SAILING

Organizations are migrating their business applications to public clouds for a variety of reasons, including cost savings, flexibility, improving business agility and to take advantage of digital transformation initiatives. However, the migration process is not smooth sailing. The survey uncovered a range of challenges that companies experience when migrating network connectivity and security policies to public clouds including:



44% 1 Difficulty managing security policies in the public cloud following migration

32% 2 Difficulty mapping application traffic flows prior to starting a migration project

30% 3 Application did not work after migration

30% 4 Migration created security holes

25% 5 Difficulty re-establishing the correct application traffic flows after migration

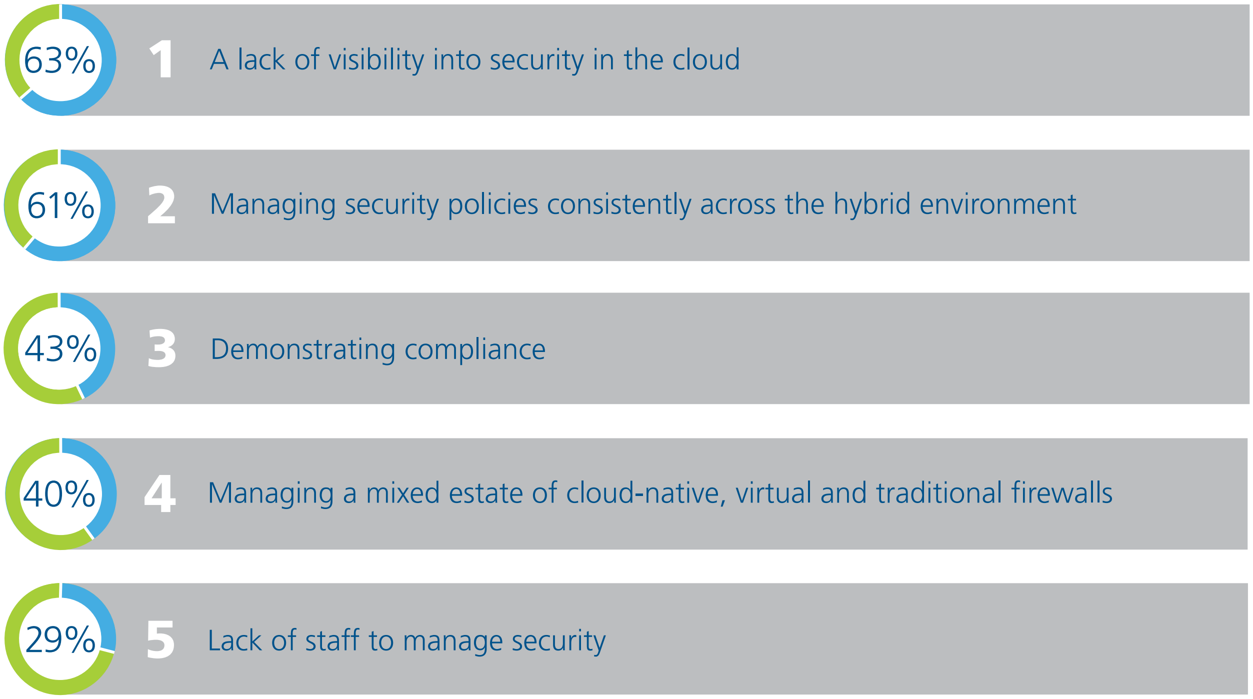
Only 17% reported that they encountered no problems during migrations.

These challenges are not surprising. Migrating applications is a complex, tedious and error-prone process that requires detailed preparation if it is to proceed smoothly without compromising security, compliance and business agility.

Understanding and mapping existing application connectivity flows for complex enterprise applications pre-migration — which is critical in order to re-establish the correct traffic flows following migration — is extremely difficult. There is usually little to no up-to-date documentation on existing application connectivity and it can take months to gather the necessary information, understand the requirements and then painstakingly adjust and migrate every firewall rule, router ACL and cloud security group to the new environment. A single mistake can cause outages, compliance violations and create holes in the security perimeter.

LACK OF VISIBILITY STILL HAMPERS SECURITY MANAGEMENT ACROSS THE HYBRID ENTERPRISE

Once in the cloud, the greatest challenges encountered when managing security across hybrid cloud environments includes:



63% 1 A lack of visibility into security in the cloud

61% 2 Managing security policies consistently across the hybrid environment

43% 3 Demonstrating compliance

40% 4 Managing a mixed estate of cloud-native, virtual and traditional firewalls

29% 5 Lack of staff to manage security

Examining the survey results by organization size and respondents' roles, highlighted several interesting variations. Nearly half (49%) of mid-size companies (between 1,000 and 5,000 employees) found that 'managing a mixed firewall estate' was a major security challenge (compared with 40% overall) — highlighting the need for more expertise or better management tools within these organizations.

As stated earlier, compliance was found to be a much bigger issue for organizations with 5,000 to 10,000 employees (60% compared with 43% overall), demonstrating the increasing pressure on larger enterprises to ensure they maintain regulatory compliance.

Little Has Changed Since 2014

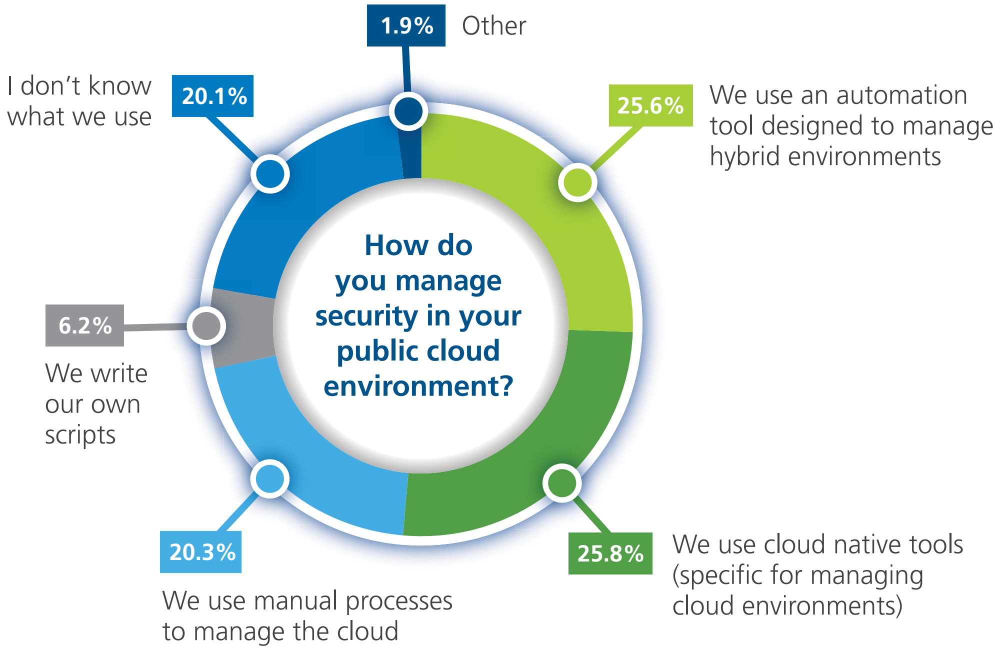
In AlgoSec's 2014 survey *Examining Security Policy Management in Hybrid Cloud Environments*, respondents stated that visibility into security was their greatest challenge, followed by maintaining and demonstrating compliance, and difficulties in extending security policies to the public cloud, thereby highlighting that organizations' use of public clouds continues to surpass their current abilities to effectively manage and secure those environments.

SECURITY MANAGEMENT PROCESSES ARE FRAGMENTED

We previously looked at the challenges faced by organizations when managing security across their hybrid cloud environments. Some of these challenges can be attributed to the fact that security teams use a variety of disparate management tools for their cloud and on-premises environments: 26% of respondents said they use automation tools designed for hybrid environments, while a further 26% use cloud-native tools for their cloud environment. 20% reported using manual processes to manage their cloud environment.

The situation is further complicated when organizations use multiple public cloud platforms, which requires the use of different native tools for each cloud platform, in addition to managing their on-premise security controls.

In organizations with more than 10,000 employees, 31% use automation to manage security. In contrast, SMBs were more likely to use manual processes.



Interestingly, companies gave somewhat similar reasons for why they do, or do not use automation solutions. Deploying any new IT solution involves time to configure and rollout, however once deployed, respondents found that automation solutions significantly helped improve the accuracy and speed of application migrations and security changes, maintain compliance as well as overcome staffing limitations.

Why use automation to manage security?

60%	1	Enhances the speed and accuracy of security changes
43%	2	Improves application migrations to the cloud
36%	3	Helps maintain compliance with industry regulations
33%	4	Helps overcome staffing limitations
27%	5	Helps enforce security policies for any provisioned resources

Why not use automation to manage security?

36%	1	Time involved to deploy
35%	2	Concerns about accuracy and false positives
34%	3	Concerns about supporting compliance with industry regulations
32%	4	Lack of staff to manage the automation solution
32%	5	Lack of products that provide the necessary automation capabilities

CONCLUSION AND KEY RECOMMENDATIONS

Hybrid cloud is now a reality in most enterprise IT environments and, despite the challenges, a significant percentage plan to increase their public cloud usage by the end of 2018 to drive digital transformation initiatives as well as improve business continuity.

The security challenges facing organizations when migrating to and managing their hybrid cloud environments, stem from a lack of visibility and difficulty in managing the array of security tools and policies consistently. This highlights the need for organizations to adopt solutions that help them simplify and intelligently automate security policy management processes holistically and consistently across both on-premise and cloud environments — from application discovery, through migration, change management and decommissioning.

Our key recommendations for improving security policy management across hybrid clouds are:

Get clear, holistic visibility

Lack of visibility was one of the biggest underlying security challenges cited in the survey. Therefore, it is critical to use a security management solution that provides holistic visibility of security across both on-premise and cloud security controls, via a single pane of glass.

Automate security processes

Together with visibility, managing security policies across the entire hybrid environment was a significant concern for survey respondents. Security automation is the key to managing a hybrid network environment efficiently, especially when there's a mix of security controls and platforms. Automation provides the speed and accuracy required to manage security changes — helping to prevent security gaps, misconfigurations, outages and compliance violations, as well as accelerate migrations to the cloud, and overcome staffing limitations.

Choose the right security management solution

With many organizations using a mix of security controls — from their cloud providers' own security controls, to host-based and on-premise firewalls — managing policies consistently is a huge challenge. What's needed is a security management automation solution that can optimize and manage all of the organization's security controls from a single console, using a single set of commands. This enables security policies to be applied consistently, without duplicating efforts using multiple management tools or attempting time-consuming and error-prone manual processes.

Map before you migrate

As the survey showed, organizations are struggling to migrate their applications to the cloud. It's a complex, tedious and error-prone process that is often severely hampered by a lack of visibility into and understanding of the applications' connectivity requirements.

To streamline the process, enterprises need to map existing applications, their connectivity flows and all their dependencies — before migration. With this information in hand, connectivity flows can be defined/adjusted to support the infrastructure and security devices used in the cloud.

Additionally, users should proactively simulate and assess the impact of any network connectivity changes on performance and compliance, and make any adjustments to help to avoid outages, misconfigurations and compliance violations once the application is deployed in the cloud. Once the migration is complete, it is vital to remember to decommission or remove redundant security policies from the on-premise security devices, in order to plug any inadvertent gaps in the network perimeter.

Link cyberattacks to impacted applications for faster mitigation

Cyberattacks and breaches were found to be one of the greatest concerns for organizations running business applications in the cloud. Security policy management solutions that integrate with SIEM solutions can help address this challenge.

Exploit kits and malware often spend months on enterprise networks, stealthily moving laterally, often from the cloud to the on-premise network, in order to reach and then exfiltrate high-value data. According to a recent report by Trustwave, the median number of days from intrusion to detection of malware is now 49 days.

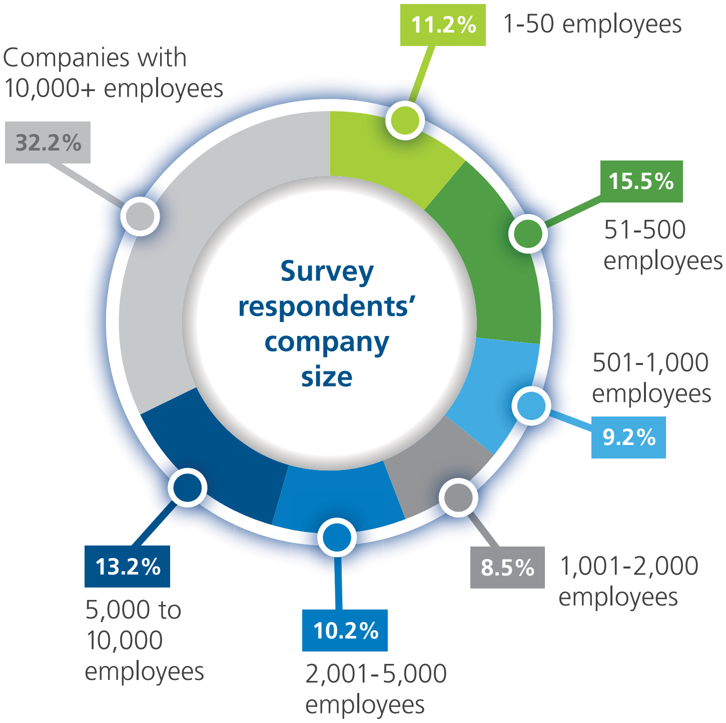
Therefore, as soon as malware is detected, it's imperative identify all of the business applications and servers impacted — whether in the cloud or on-premise — and map the lateral movement of the infection. Once identified, the security management solution can mitigate the risk of a cyberattack by automatically isolating any affected (or potentially affected) servers or devices from the network.

By focusing on improving overall network security visibility, and standardizing and automating security management processes across their hybrid cloud environments, organizations can better protect their business, and comply with regulatory requirements, while taking full advantage of the cost savings and agility offered by the hybrid cloud model.

ABOUT THE SURVEY

The *Cloud and Hybrid Environments: The State of Security* survey included 450 C-level executives and senior security and network professionals from a range of industry sectors and organizations worldwide. All of the companies that participated in the survey were required to have at least some of their business workloads in the cloud.

41% of respondents were based in North America, 21% in Europe, 28% in Asia-Pacific and 10% were from other regions.



ADDITIONAL RESOURCES

- Why hybrid cloud is here to stay
- Don't get lost in translation when managing mixed firewall estates
- Cloud atlas: how to accelerate application migrations to the cloud
- The ripple effect of public cloud outages
- Public cloud security: virtualized firewalls or native controls?

ABOUT ALGOSEC

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With AlgoSec, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyberattacks to business processes and intelligently automate network security changes with zero touch — across their cloud, SDN and on-premise networks. Over 1,500 enterprises, including 20 of the Fortune 50, utilize AlgoSec's solutions to make their organizations more agile, more secure and more compliant — all the time. Since its inception, AlgoSec has offered the industry's only money-back guarantee.

Global Headquarters
65 Challenger Road, Suite 310
Ridgefield Park, NJ 07660
USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
+44-207-099-7545

APAC Headquarters
Centennial Tower, Level 21
3 Temasek Avenue
Singapore 039190
+65 6549 7415

AlgoSec.com