algosec

Managing Security at the Speed of Business

Examining Security Policy Management in Hybrid Cloud Environments

An AlgoSec Survey | Fall 2014

Share this Research

Executive Summary

Many enterprises are now making the strategic decision to adopt a hybrid cloud environment in order to maximize business agility and reduce costs. In fact, according to Gartner nearly three-quarters of large enterprises will have hybrid cloud deployments in 2015[i]. Not surprisingly, network security for business applications on a public IaaS platform is a primary concern for organizations of any size, yet it is also one of the most complex functions to migrate and manage.

In August 2014, AlgoSec surveyed 363 IT professionals to find out more about the key challenges organizations face when securing their business applications across hybrid on-premise/public cloud environments. Two thirds of these individuals are currently deploying or planning to deploy business applications on an IaaS platform within the next 12-36 months, and their responses reveal some key insights about network security across hybrid cloud environments:

- **Visibility and network security policy management remain huge challenges**. Overall four out of five respondents who have already deployed or expected to deploy business applications on a public IaaS platform said they need better visibility into network security across on-premise and public cloud environments. Two-thirds of those respondents agree or strongly agree that extending the corporate security policy to the public cloud poses a significant challenge.

- **No one type of network security control dominates for public IaaS.** Of those currently running business applications in public clouds, just one-third use a commercial network firewall, while another 25% use provider controls. For those planning to migrate business applications to a public IaaS platform over the next 12-24 months, more than a third are uncertain what tools they will use to manage their security policies in the public cloud.

- **Lack of processes hinders cloud management and compliance**. Nearly two thirds of respondents noted the lack of operational workflows to manage security in a hybrid environment. Demonstrating compliance on IaaS compared with on-premise data centers was another major issue, with half of those surveyed claiming difficultly.

- **Large and small companies differ in who handles public cloud security.** In large organizations, cloud security falls to the Information Security team, whereas at small companies it tends to be the responsibility of IT Operations.

The hybrid cloud environment amplifies the security policy management challenges of the on-premise data center, such as business continuity, change management and compliance. However, as the survey highlights, the fragmented variety of security controls for IaaS, poor visibility, and lack of processes currently make it very difficult for organizations to enforce network security consistently across their entire environment.

To successfully extend the corporate policy across a hybrid environment, organizations first need an in-depth understanding of the network security controls used in the public cloud. Then they need to select controls that will integrate with their security policy management platform, and enable holistic, unified visibility and management across the entire environment. Additionally, organizations should look for ways to extend existing network security processes, especially compliance processes, across the hybrid environment through new workflows, so they can continue to protect the enterprise and ensure effective network security.

Poor Visibility and Disparate Policies Hamper Network Security in Hybrid Environment

The majority of organizations that currently operate in a hybrid environment agree or strongly agree that it is difficult to unify network security policy management across on-premise and public cloud environments. Nearly three-quarters agree or strongly agree that they need better visibility across on-premise and public cloud environments, while nearly two-thirds say that it is more difficult to demonstrate compliance on public IaaS platforms than on on-premise data centers.

Extending the corporate security policy to the public cloud causes problems for 54% of respondents currently using a public IaaS platform and about the same percentage said they lack the operational workflows needed to effectively manage security in a hybrid environment.

The complexity of network security policy management in the public cloud is seen as a significant challenge by 62% of respondents currently operating in a hybrid environment (Figure 1).

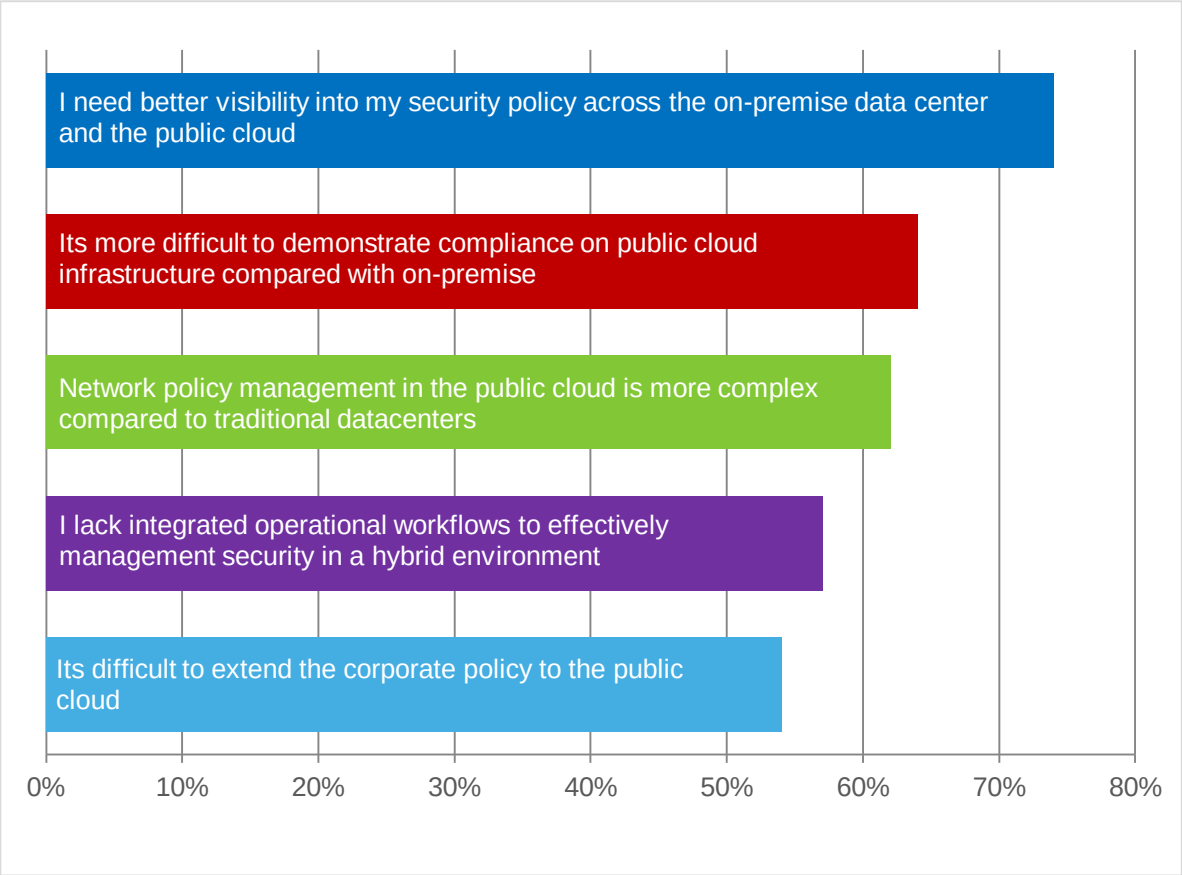

Figure 1: Security policy management challenges experienced by organizations currently using a public IaaS platform.

Respondents who plan to deploy business applications on a public IaaS platform in the future are more concerned about extending corporate policies (75%) and having visibility across platforms (83%) than those who already operate in a hybrid environment.

Security Concerns Aren't Slowing Down the Adoption of IaaS

Despite the challenges experienced and anticipated with network security management across hybrid platforms, most organizations surveyed are already using or planning to use public IaaS to host at least some of their business applications—and the pace seems to be accelerating.

Just one-third of all 363 respondents do not expect to run any business applications on a public IaaS in the next three years, while nearly 30% of them already use public IaaS and 37% expect to migrate their business applications to a public IaaS within the next 36 months (Figure 2).

Figure 2: Percentage of organizations deploying or planning to deploy business applications in a public IaaS.

Many of the respondents who use or plan to use public IaaS expect it to be a significant platform for them. Overall seventy percent anticipate that they will have 10% to 60% of their business applications on public IaaS platforms in the next three years and 14% predict that more than 60% of their business applications will run on public IaaS platforms by 2017 (Figure 3).

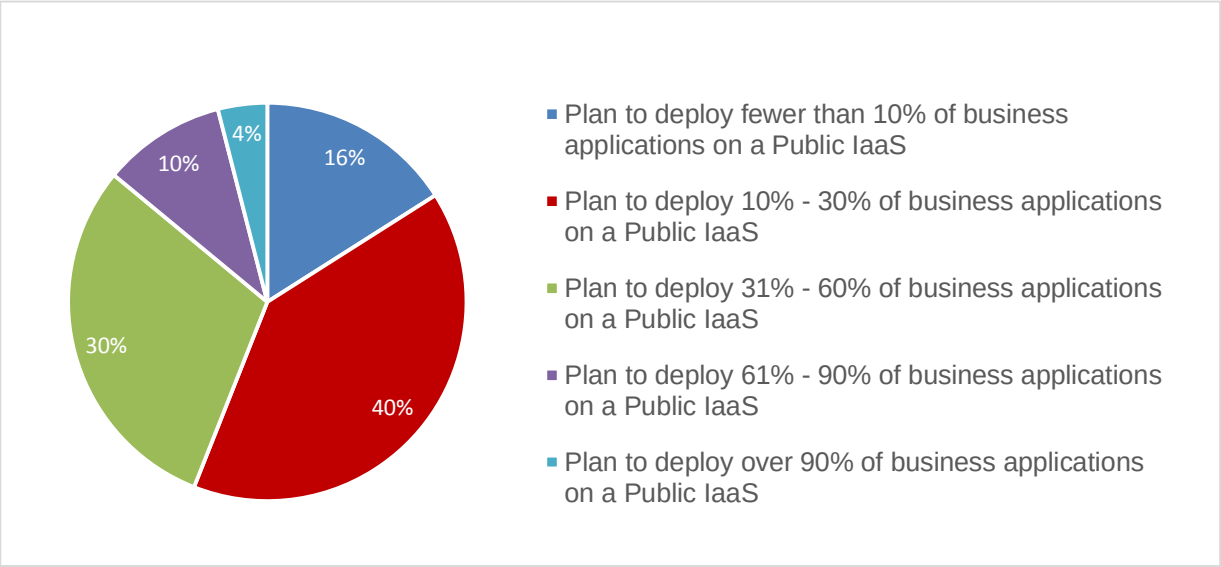

Figure 3: Percentage of business applications expected to run on a Public IaaS by 2017.

Larger organizations are the most likely to expect to operate in a hybrid environment, with 74% of respondents in organizations with more than 2,000 employees planning to run 10% to 60% of their business applications on public cloud infrastructure, compared to 65% of those in organizations with fewer employees.

Those who currently use IaaS are a bit more bullish than the total group, with 22% expecting at least 60% of their applications to use public cloud infrastructure within three years and 8% predicting that nearly all of their business applications will run on public IaaS in that time frame.

Use of IaaS Network Security Controls is Fragmented and Unclear

Unlike on-premise data centers, where commericial firewalls are predominantly used to control network access, fragmentation and uncertainty characterize the IaaS network security arena today (Figure 4). Only a third of survey respondents use or expect to use commerical network firewalls, while a quarter rely or will rely on provider controls such as AWS Security Groups.

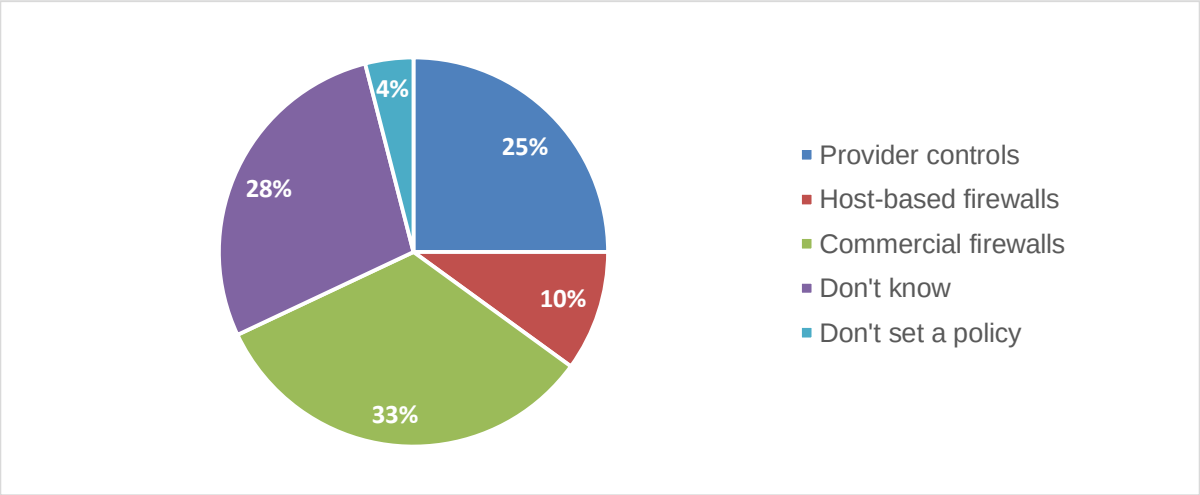

Figure 4: Controls currently used/planned to define network security policies for public IaaS platform.

Those currently using public IaaS platforms are slightly more likely to depend on host-based firewalls such as Linux IP Tables (13%) than those who plan to use public infrastructure platforms in the next few years (10%), and they use provider controls at a slightly higher rate as well (31%).

More than a quarter of all respondents report that they are unsure what to use to define network security policies for public IaaS. That uncertainty is not restricted to small companies. Thirty-four percent of those who do not know what to use to manage security policies are companies with fewer than 500 employees, but half have more than 2,000 employees.

The lack of clear choice for network security policy definition is not limited to those still in the planning stages. While 33% of those who expect to migrate some business applications to a public infrastructure platform don't know what they will use, neither do 18% of those respondents whose organizations currently use public IaaS platforms.

Data and Network Security are the Most Challenging Functions to Migrate

Respondents across all organizations say that network security and data security are the two most challenging security functions to migrate to public clouds (Figure 5), though their ranking varies with the size of the company. Smaller organizations find network security the slightly more difficult function to migrate, whereas larger companies say that data security is the more difficult by a margin of nearly 2 to 1.

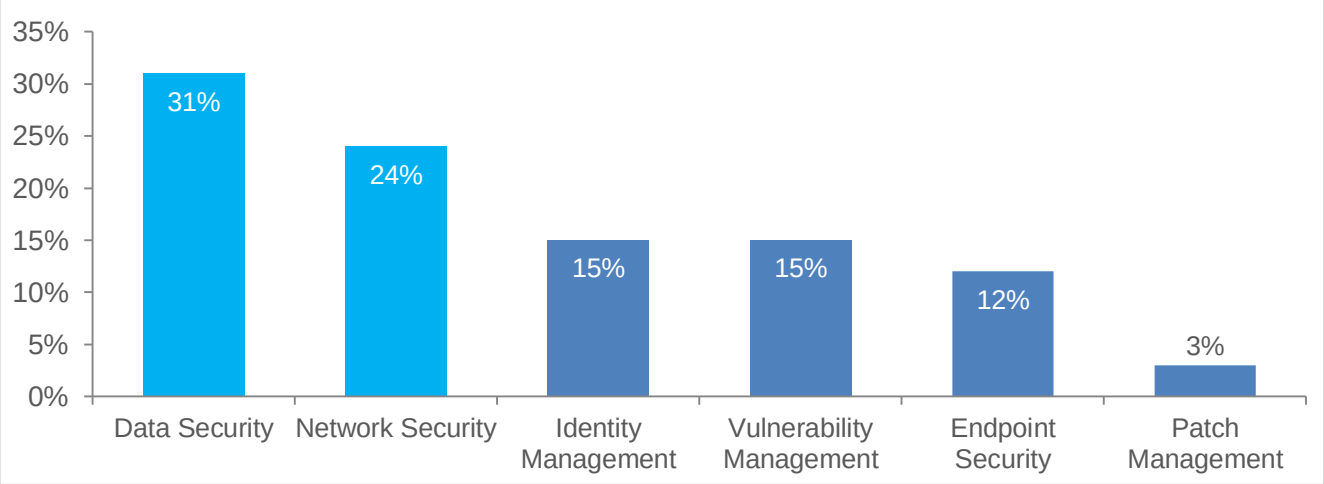

Figure 5: The most challenging security function to migrate to the public cloud across all companies.

Security: Who's in Charge?

The team responsible for managing the organization's security policy for public IaaS platforms depends on the size of the respondent's company. While slightly more than half of all respondents who use or plan to use public IaaS task the Information Security team with managing the security policy in the public cloud. Drilling down by company size reveals a sharp distinction: 70% of those who work for organizations with 500 or fewer employees report that the IT Operations team handles public cloud security, whereas at 72% of larger companies, the responsibility falls to the Information Security team.

AWS and Azure Dominate

Amazon Web Services (AWS) and Microsoft Azure lead the pack among public IasS platforms, claiming 53% and 44% of respondents, respectively (respondents were allowed to select multiple IaaS providers). Respondents were more than twice as likely to say that they use or expect to use AWS or Microsoft Azure as the next most popular platform, Rackspace (19%) or Google Compute Engine (17%). Eight percent say they use or will use Verizon Terremark and respondents also named more than 20 other platforms, most used by just one or two respondents. (Figure 6).

Microsoft Azure seems to be gaining ground, especially among the largest companies. Notably, many organizations report using or planning to use multiple IaaS platforms with a mix of AWS, Microsoft Azure, Rackspace and Google Compute Engine.

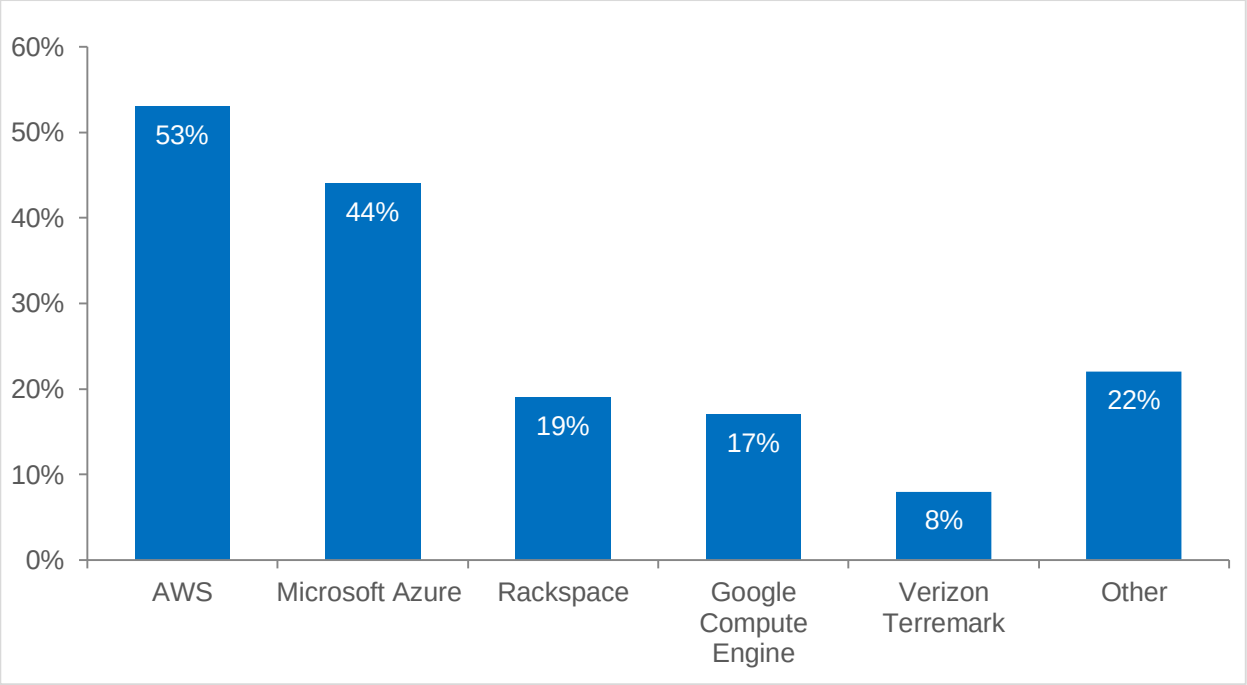

Figure 6: Public IaaS in use/planned.

Conclusions

The migration to the cloud, particularly a public IaaS platform, continues to pick up speed. As most companies expect to have a significant percentage of their business applications hosted on a public IaaS platform within the next 12-36 months, organizations will need to come to terms with the challenges of extending and maintaining network security in a hybrid environment. The ***lack of visibility and increased complexity associated with multiple environments remains a significant concern for organizations***, even as they commit to migrating more of their applications.

At the same time, IT organizations struggle to determine who should manage security for public IaaS platforms—IT operations, information security or perhaps the platform providers. Workflows must shift to accommodate the public model as well, though many organizations report that the changes necessary to support the new environment have yet to occur. *For IT professionals,* ***the rapid movement to a hybrid environment means significant changes in team structure and responsibilities need to happen just as fast*** to enable the organization to maintain agility and security.

As challenging as determining who manages public IaaS security organizations in the planning stages as well as those who have already deployed business applications on a public IaaS platform continue to wrestle with whether they should use commercial network firewalls, provider controls or other methods. This uncertainty may be exposing organizations to significant risk if indecision leads to inaction.

With increased adoption of hybrid environments, organizations should focus efforts on aligning IT and information security roles and responsibilities for the new realities, codifying security management processes that work across on-premise and cloud environments, and improving visibility of policies in public IaaS platforms. These changes will enable them to work more effectively and ensure security in the new paradigm, while taking advantage of the flexibility and cost benefits public IaaS platforms offer.

About the Survey

The Security Policy Management the Hybrid Cloud Environments survey was conducted in August 2014 and surveyed 363 IT professionals worldwide. Of the 239 (66%) who had or planned to deploy business applications in the cloud, 40% primarily had responsibility for information security, 16% were in network operations, 13% were C-level executives, 9% were data center architects and 22% worked in other roles (Figure 7). In addition, survey respondents represented businesses of all sizes (Figure 8).

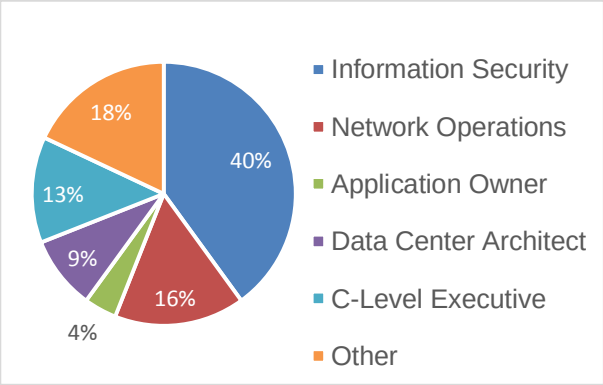

Figure 7: Breakdown of roles that completed the survey.

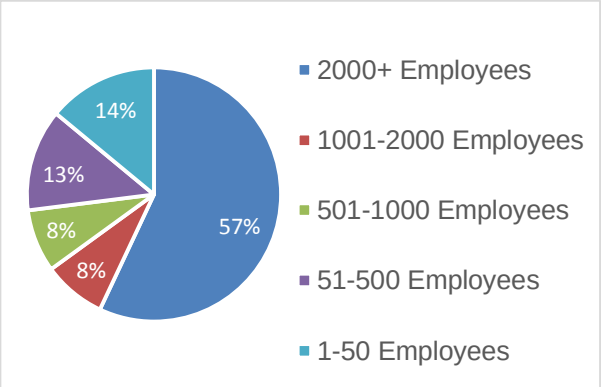

Figure 8: Organization size.

About AlgoSec

AlgoSec is the market leader for security policy management, enabling organizations to simplify and automate security operations in evolving data centers and networks. More than 1,000 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec for faster security provisioning of business applications, streamlined change management, continuous compliance and tighter security.

AlgoSec's application-centric approach orchestrates the management of complex policies across firewalls and related network devices, aligning IT teams for improved business agility. AlgoSec is committed to the success of every single customer, and offers the industry's only money-back guarantee. For more information, visit www.AlgoSec.com.

---

[i] Source: Gartner, Private Cloud Matures, Hybrid Cloud is Next by Thomas Bittman, September 6, 2013.

265 Franklin Street
Boston, MA 02110
USA

T: +1-888-358-3696
F: +1-866-673-7873
E: info@algosec.com

AlgoSec.com