A Forrester Consulting
Thought Leadership Paper
Commissioned By Trend Micro

September 2014

The State Of Public Cloud Security

Part One Of A Three-Part Series On Public Cloud Security

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Developers aren't waiting for enterprise-sanctioned cloud services. Savvy cloud managers have come to terms with developer independence. Rather than focusing efforts on limiting cloud usage, successful cloud managers concentrate on enhancing the developer experience in developer terms and not mandating restrictive policies and processes that slow down the experience. Staying in the conversation is dependent on delivering higher value without dictating terms that diminish productivity. Although developers often choose vendors and make other critical decisions by themselves, one decision that your developers should not be making on their own is how to secure your public cloud environment.

At the heart of public cloud security is a shared responsibility between the cloud vendor and the organization. Unlike in many hosting models, the cloud vendor isn't responsible for solving all your security requirements. In most cases, the vendor is only responsible for securing the data center, infrastructure, and hypervisor, while the organization is responsible for the operating system, applications, users, and data. Expecting security for the entire stack isn't an option nor is it wise.[1] The public cloud structure, especially for developer use cases, is more of a "take it or leave it" approach. Meeting your security requirements will mean layering your own security policies and processes atop the existing services. Forrester calls this "the uneven handshake."[2]

If left to their own devices, developers won't incorporate security measures. Developers don't have the training or the time to prioritize safer cloud practices nor will they continue to use your safer cloud services if it sacrifices their time-to-value. Cloud managers need to take control of public cloud security by finding a balance between security that is robust enough to protect your sensitive workloads and data, and security that is agile enough to support your developers. Traditional security practices can often restrict time-to-value for your developers, which risks them trying to circumvent your security practices in the name of efficiency.

In March 2014, Trend Micro commissioned Forrester Consulting to evaluate current and best practices in public cloud security. To do so, Forrester conducted an online survey with 321 IT professionals involved in their organization's public cloud security policies and tasks. The goal was to determine what enterprises are doing today to secure their public cloud environments and the best practices they should be following to make sure they have adequate security without sacrificing cost or time-to-value.

Forrester found that organizations today are ceding much of the control over cloud security to developers, who lack both the expertise and the desire to fully enforce cloud security policies, for fear of being left out of the conversation. Cloud managers often cited time as a critical factor for not implementing the ideal security tools, policies, and practices. Cloud managers need to rally forces with security professionals to craft cloud use policies. The challenge will be educating your security professionals on the importance of time-to-value and the need to automate and abstract security policies to ensure continued input on cloud usage and minimal circumvention. Establishing different levels of security for different workloads will help your organization find a balance between cost, time-to-value, and security.

KEY FINDINGS

Forrester's study yielded three key findings:

- **Developers are picking their own cloud tools.** Our survey shows that at 64% of organizations using public cloud, developers or non-IT professionals are responsible for selecting their public cloud vendors.
- **Security is not heavily involved in crafting security policies for public cloud.** Only 43% of organizations reported that their IT security team was heavily involved in crafting security policies for the public cloud.
- **Cloud managers should create workload-specific security policies and automate security within the provisioning process.** Cloud managers need to ensure that the proper level of security is applied to different workloads, without sacrificing the time-to-value that developers have migrated to the cloud for in the first place.

Current State

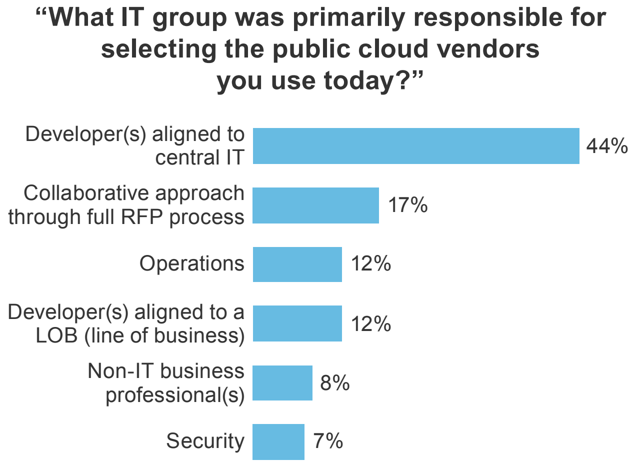
In order to discover best practices for public cloud security, we needed to profile secure public cloud environments and cloud managers. To do so, Forrester conducted a global survey in seven countries (see Appendix A) of IT decision-makers involved in their organization's public cloud security policies and tasks. These professionals mainly came from infrastructure or operations backgrounds, and 71% are in charge of the security policies and tasks applied to their public cloud environment. Essentially, all of these environments are organized enough to have a cloud manager.

In asking respondents about what their organization does today to secure their public cloud environment, we found:

- **Developers are selecting their own public cloud tools.** Developers were primarily responsible for selecting public cloud vendors for almost two-thirds of enterprises surveyed, with non-IT business professionals responsible for another 8% (see Figure 1). However, only 17% of organizations stated that they chose vendors using a collaborative approach with a full request for proposal (RFP) process, and only 19% of organizations stated that their operations or security professionals were primarily responsible for vendor selection. For organizations banking on vendor selection as the primary form of solving cloud security challenges, this serves as a reality check. Developers are dictating the tools and bringing cloud managers into the conversation retroactively. Developers don't consider security when evaluating cloud vendors, so a security approach that focuses on an "enterprise class cloud" or "secure cloud" will be short-lived if it does not include the tools that your developers know and want.
- **Over half the time, security is not heavily involved in crafting cloud security policies.** We asked respondents how involved their IT security team is in crafting security policies for the public cloud — not just if the security team is involved in cloud decision-making. The assumption is that every security team would be involved in creating any security policies, whether they are for cloud-based or non-cloud environments. Only 43% of respondents said their security team is heavily involved, with another 29% saying they are becoming more involved as the cloud matures (see Figure 2). Each and every one of the surveyed environments has a cloud manager, and yet less than half stated that the security team was heavily involved in

FIGURE 1

Sixty-Four Percent Of Organizations Report Developers/Non-IT Professionals Are Responsible For Selecting Public Cloud Vendors

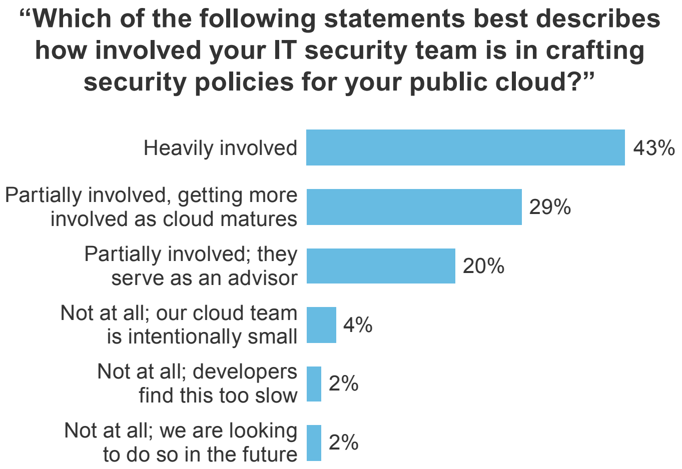


Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

FIGURE 2

Over Half The Time, Security Is Not Involved In Public Cloud Decisions



Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

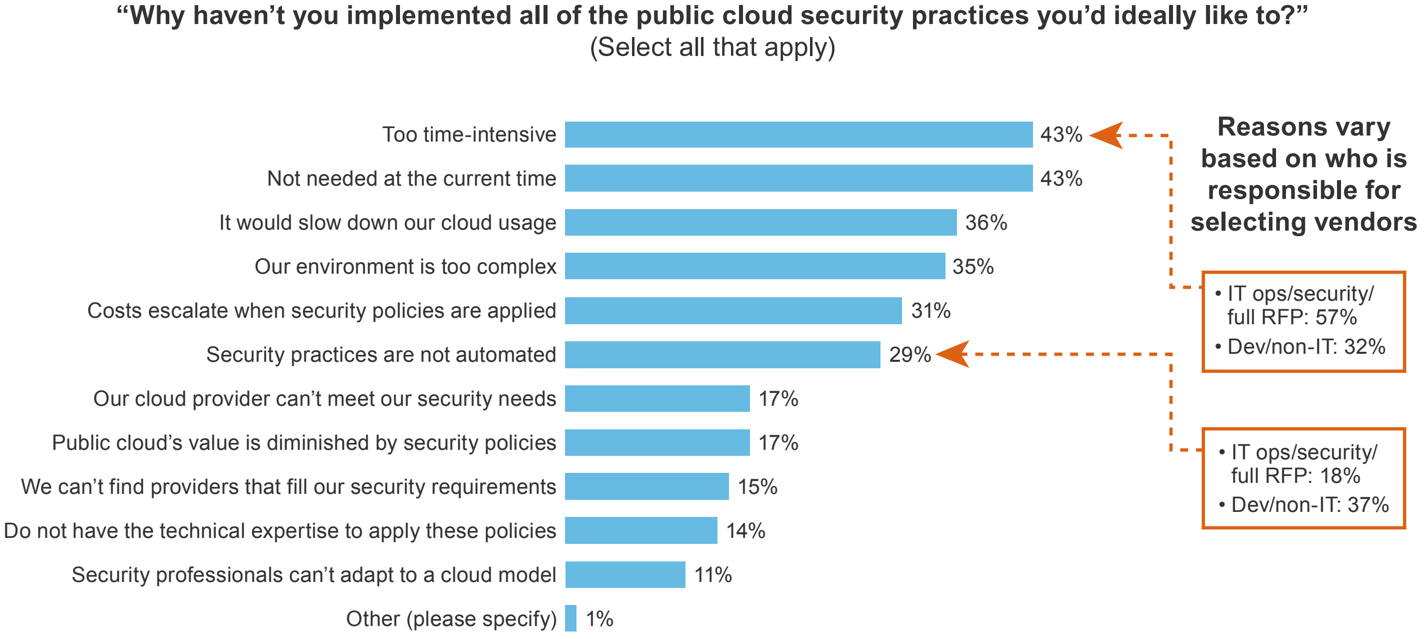
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

policy creation, with over one-fourth holding off. This shows a great reluctance to work with security teams regarding public cloud usage.

- **The top barrier to implementing desired cloud security services is that it is too time-intensive.** We asked respondents why they hadn't implemented all of the required security measures. The top two reasons selected were that the missing components were "too time-intensive" (43%) and that at the current time their existing offering was "good enough" (43%) (see Figure 3). Thirty-six percent of respondents said that additional security would slow down cloud usage, which jeopardizes the support of developers. These responses emphasize two attitudes among cloud managers: 1) Cloud managers are still getting in front of usage and don't want to risk a rollout that is too aggressive for ideal security practices and policies; simply remaining in front of cloud usage is of upmost importance and 2) some security practices will be applied once the environment, scenarios, or ability to provide automated versions of these security solutions matures.

- **Barriers to implementing desired cloud security services vary based on who is responsible for selecting public cloud vendors.** There were several noticeable differences in the top barriers based on whether developers or non-IT decision-makers were selecting cloud vendors, or whether IT operations/security were in control. Thirty-seven percent of respondents at organizations where developers/non-IT pros selected their cloud vendors said that a top barrier to ideal cloud security is that "security practices are not automated" versus only 18% selecting this as a top barrier when IT was in charge of cloud sourcing decisions. As we have seen, developers prefer that security is managed behind the scenes and does not intrude on their time-to-value in the cloud. One way to do this is through automation. Even if IT is in control of your cloud security, cloud managers should not overlook the benefits of automating public cloud security.

FIGURE 3
Top Barriers To Implementing Ideal Public Cloud Security



Base: 112 IT professionals involved in their organization's public cloud security policies and tasks

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

ENTERPRISES APPROACH CLOUD SECURITY FROM DIFFERENT VIEWPOINTS

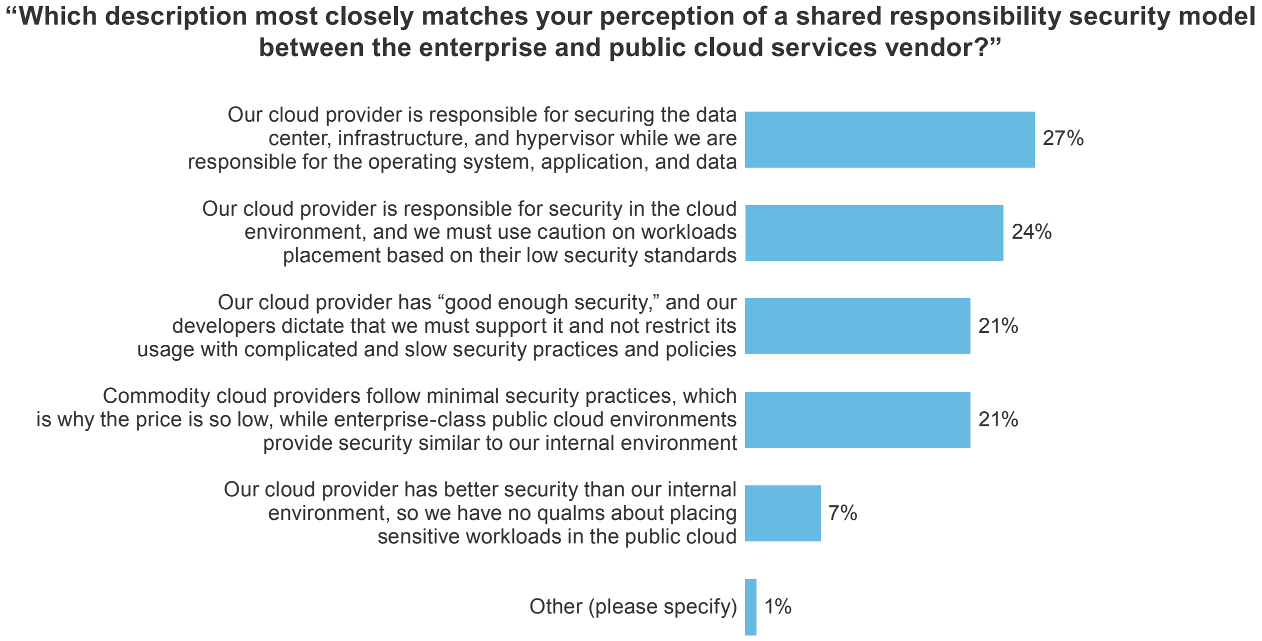
While a shared security model is at the heart of public cloud security, organizations have very differing views of what makes up that model. We asked respondents to select which description best represented their perception of the shared security model between a cloud vendor and the enterprise. We found that respondents were split fairly evenly between four different viewpoints:

- **Use a shared security model.** Only 27% of respondents correctly said that "the cloud provider is responsible for securing the data center, infrastructure, and hypervisor while we are responsible for the operating system, application, and data" (see Figure 4).
- **Minimize risk through app selection.** Twenty-four percent of respondents said that "the cloud provider is responsible for security in the cloud environment, and we must use caution on workloads placement based on their low security standards."
- **Something is better than nothing.** Twenty-one percent of respondents said: "Our cloud provider has 'good enough security,' and our developers dictate that we must support it and not restrict its usage with complicated and slow security practices and policies."
- **Use an enterprise cloud.** Twenty-one percent of respondents said: "Commodity cloud providers follow minimal security practices, which is why the price is so low, while enterprise-class public cloud environments provide security similar to our internal environment."

With only 27% of respondents selecting the correct version of a shared security model, it is clear that cloud managers need more education on the responsibility split between cloud vendors and their customers. Involving security in your public cloud can ensure that your organization can hold up its end of the agreement.

FIGURE 4

More Education Is Needed On The Components Of A Shared Responsibility Security Model



Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

Best Practices For Public Cloud Security

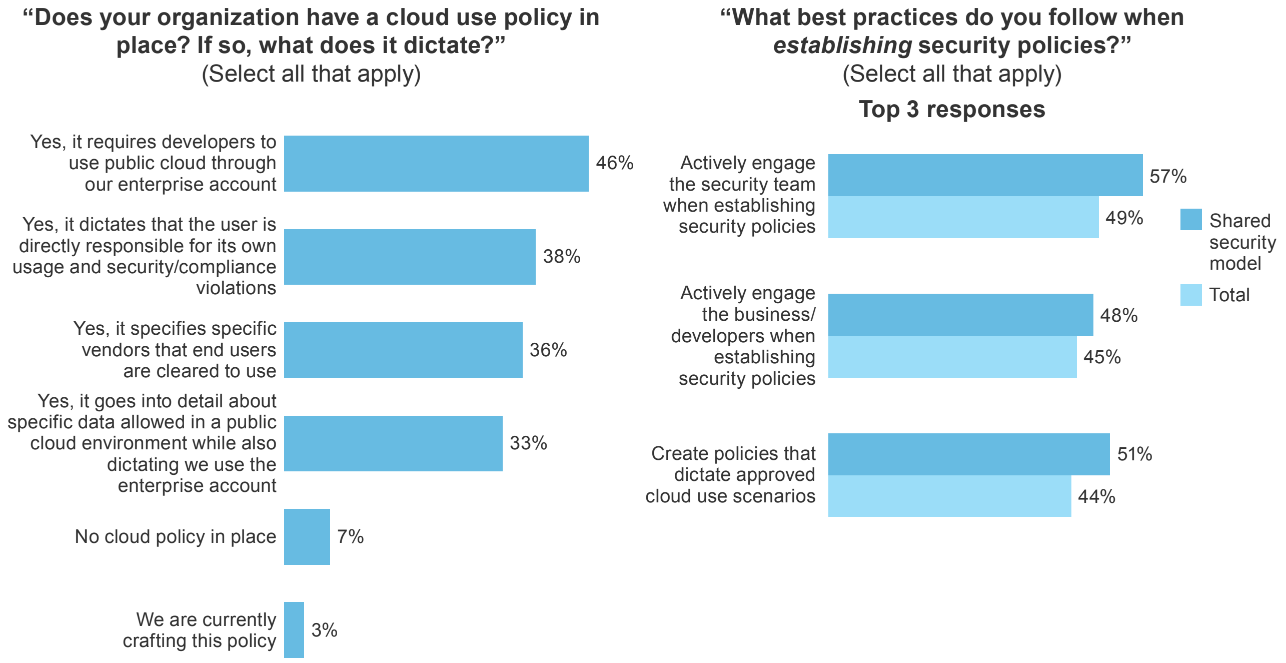
It's still in the early days of success for secure public cloud practices and policies. Although current practices today often don't reflect best practices, the survey results did highlight several important steps that cloud administrators can follow to ensure that your organization has sufficient cloud security without affecting the time-to-value of developers. These best practices are not always adopted by the majority of organizations we surveyed, but those organizations that understood and operated under a shared security model for the public cloud generally had higher adoption levels in these best practices that those that did not. Cloud managers should make sure:

- **Security is included in cloud use policies.** The good news is almost all organizations we surveyed have a cloud policy in place. However, 38% of respondents have cloud use policies that essentially hand over responsibility for security to the developers, making them directly responsible for their cloud usage and all security/compliance violations (see Figure 5). As we have seen, developers have neither the expertise nor the desire to ensure that ideal security practices are followed in the cloud. In order to make certain that proper security processes are followed, they should be included in your organization's cloud use policy. We also asked survey respondents what best practices they follow when establishing security policies. According to our survey, the policy should be created with input from both the security team (49%) and the business/developers (45%) and should dictate approved cloud use scenarios (44%). Respondents who operate under a shared security model for the public cloud follow these practices even more strongly, with 57% using input from their security team and 51% creating policies that dictate approved cloud use scenarios.

- **Security complexity is abstracted from developers, but remains compliant.** Developers are looking for security practices to be as minimal and unobtrusive as possible in their cloud user experience. At the same time, the policies still need to be managed by security and fully visible for auditing purposes. Currently, only 17% of respondents think that the ideal way for security to be built into the developer user experience is "completely

FIGURE 5

Cloud Security Policies Should Engage Both Security And Developers, Dictate Approved Cloud Use Scenarios



"Does your organization have a cloud use policy in place? If so, what does it dictate?"
(Select all that apply)

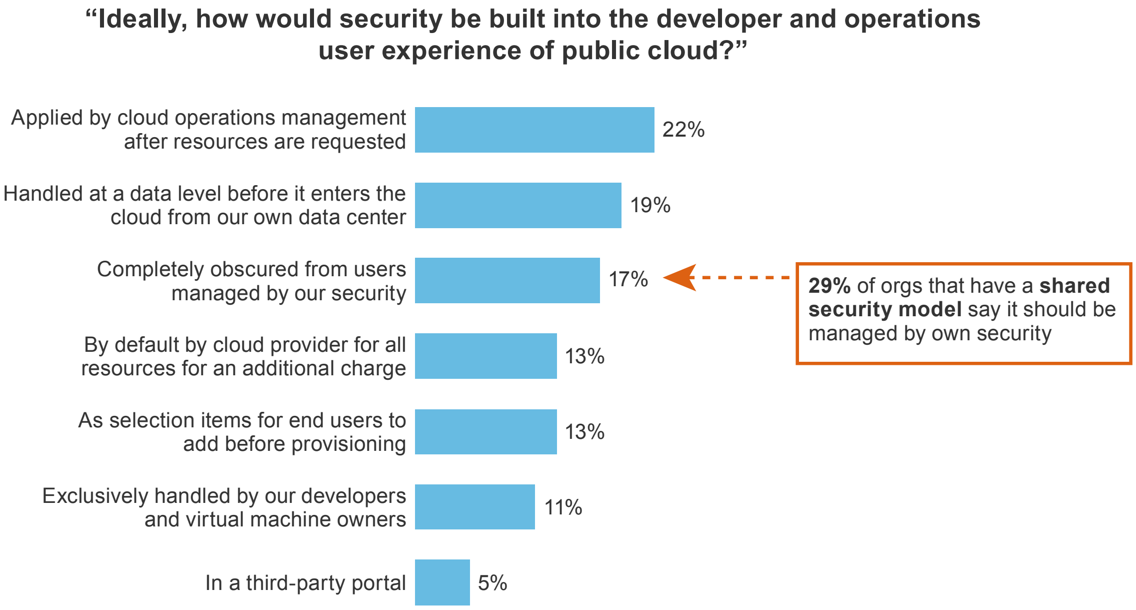
"What best practices do you follow when *establishing* security policies?"
(Select all that apply)
Top 3 responses

Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

FIGURE 6

User Experience Should Be Abstracted From Developers



Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

obscured from users and managed by our security" (see Figure 6). However, 29% of organizations that understand and operate under a shared security model follow this best practice, the No. 1 response.

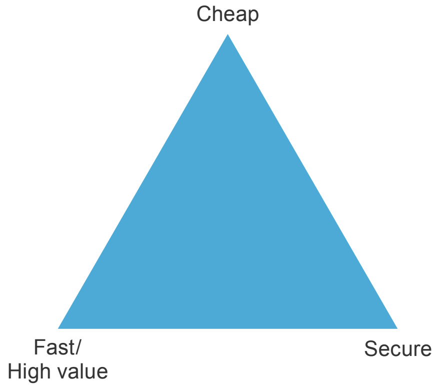
- **Different workloads mandate flexible security policies.** You need to secure everything you put in the cloud. However, a one-size-fits-all workloads approach is not the best approach. Not all workloads in the cloud will require the same levels of security capabilities. Workloads subject to compliance regulations have more complex and expensive requirements than a simple test/dev instance that only contains public data. Applying compliance-level security across all your resources is cost-prohibitive. In order to achieve a balance between cost, time-to-value, and security in your public cloud environment, consider a security policy that is flexible and can automatically apply different levels of security practices and policies to different workloads (see Figure 7).

- **To consider partnering with someone who knows both cloud and security.** We asked respondents how they view the native security capabilities of their cloud provider environment. Only 18% of respondents felt that the native security capabilities of their cloud provider are sufficient (see Figure 8). It is important to understand the extent of the cloud provider's security policies and service-level agreements (SLAs) and for enterprises to fill the gaps between their requirements and their cloud provider's offering. This is not always easy, and often leveraging a partner with both cloud and security backgrounds can make meeting those requirements easier and more effective. Fifty-nine percent of respondents thought that adding third-party security capabilities in addition to native security capabilities was sufficient. Finding a partner knowledgeable in security and the cloud who can be a trusted advisor can help you design a best-fit security solution for your cloud portfolio in less time and with higher accuracy.

The best practices featured in this paper are intended to assist cloud managers in securing their public cloud without alienating those who value the cloud most. The next papers in this series will dive into two essential best practices for public cloud security: 1) determining the most important components of cloud security and 2) balancing cost, time-to-value, and security.

FIGURE 7

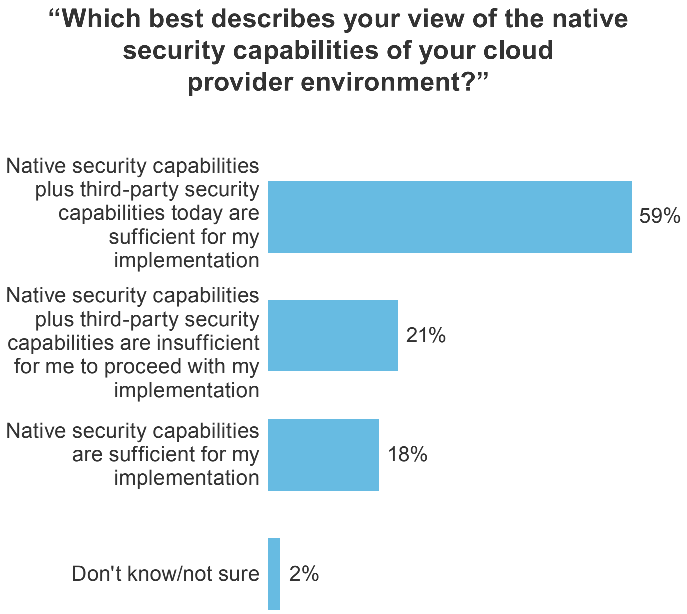
Cloud Managers Need To Balance Cost, Time-to-Value, And Security For Public Cloud



Source: Forrester Consulting

FIGURE 8

Native Security Of Cloud Providers Is Not Sufficient As A Standalone



Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

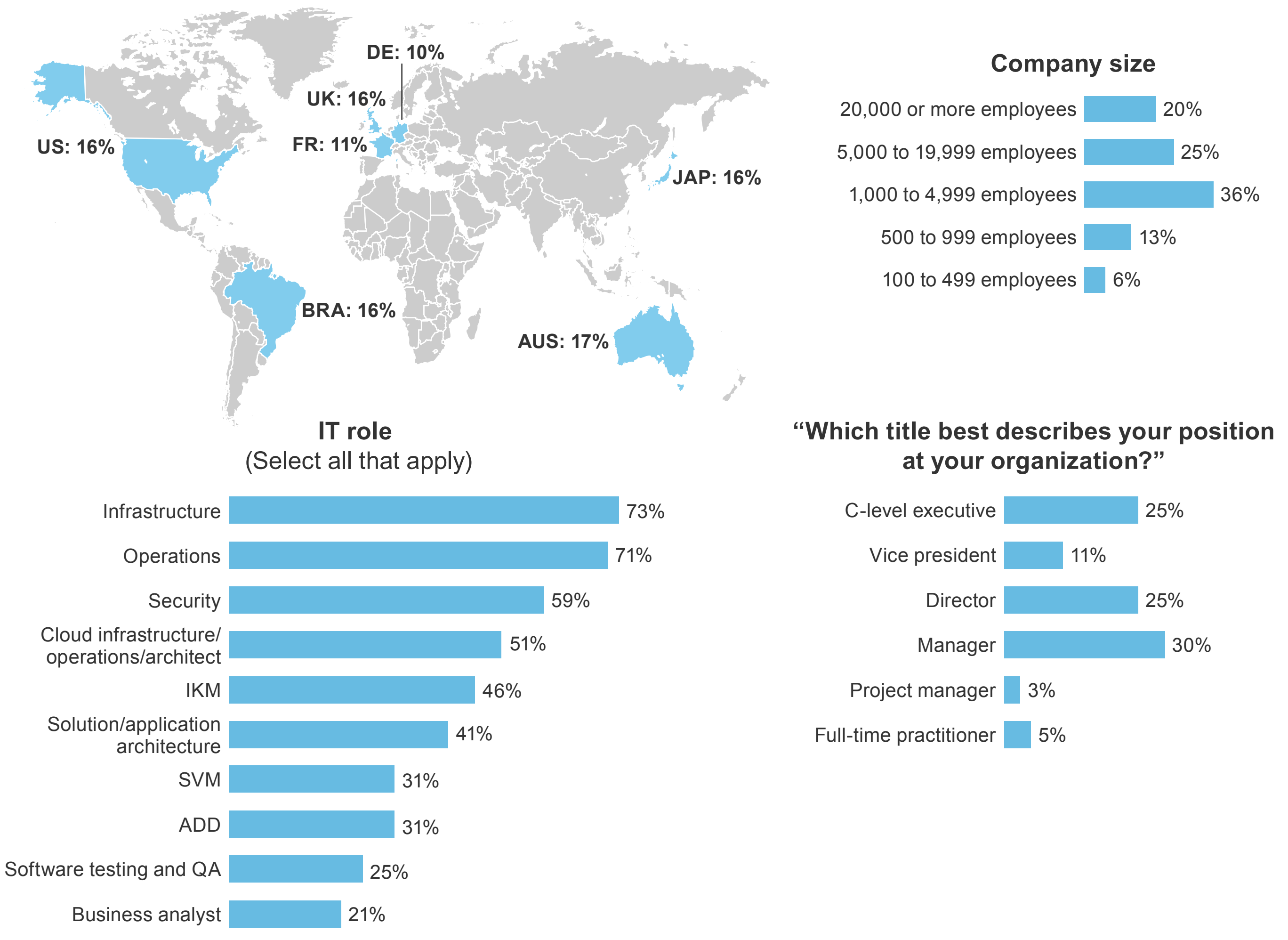
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

Appendix A: Methodology

In this study, Forrester conducted an online survey of 321 organizations of 100 or more employees spending an average of more than $5,000 per month on public cloud in Australia, Brazil, France, Germany, Japan, the UK, and the US to evaluate current and best practices in public cloud security. Survey participants included IT professionals involved in their organization's public cloud security policies and tasks. The study began in April 2014 and was completed in May 2014.

Appendix B: Demographics/Data

FIGURE 9
Survey Demographics



Base: 321 IT professionals involved in their organization's public cloud security policies and tasks

(Percentages may not total 100 due to rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014

Appendix C: Endnotes

[1] Source: “Understand The Cloud Service Provider Market Landscape,” Forrester Research, Inc., May 19, 2014.

[2] Source: “Make The Cloud Enterprise Ready,” Forrester Research, Inc., June 1, 2012.