A Forrester Consulting
Thought Leadership Paper
Commissioned By Trend Micro

February 2015

Best Practices For Public Cloud Security

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

FORRESTER®

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.

Executive Summary

Security is, justifiably, a top concern about public cloud environments. Application developers are migrating to the cloud for the agility and speed that the cloud can provide. One thing that developers often do not account for in their cloud usage is the security of that cloud. It is up to cloud managers, with support from IT security, to ensure that their public cloud deployments are secure and that the data and workloads in that cloud are protected.

At the heart of public cloud security is a shared responsibility between the cloud vendor and the organization. Forrester calls this “the uneven handshake,” where the cloud service provider is only responsible for securing the data center, infrastructure, and hypervisor, while the end user organization is responsible for the operating system, applications, users, and data. Unlike in many hosting models, the cloud vendor isn’t responsible for solving all security requirements. Expecting security for the entire stack isn’t an option nor is it wise. Our survey of 321 IT professionals involved in public cloud security found that only 18% of respondents believe the native security capabilities of cloud providers are sufficient for their implementation.

Forrester believes that to ensure the data and assets in their public cloud environments are secure, cloud managers need to work with their security teams to adopt a Zero Trust security approach. A Zero Trust Model means the organization must: 1) verify and secure all resources; 2) limit and strictly enforce access control; and 3) log and inspect all traffic. However, in the public cloud, time-to-value for developers is the No. 1 priority, so risk must be balanced with agility when it comes to securing your public cloud. This requires special consideration on the part of cloud managers to preserve the tenants of Zero Trust without sacrificing the time-to-value of your public cloud.

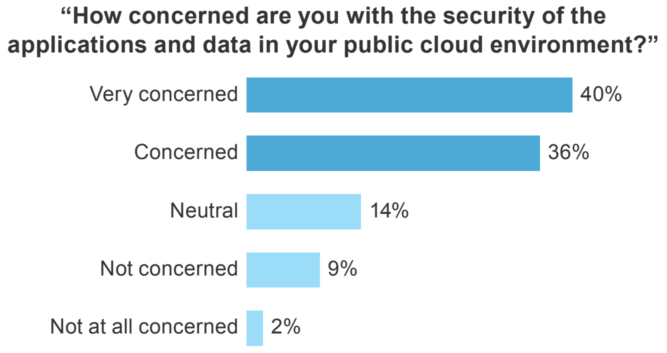
This paper is the third in a series of three on public cloud security practices. This paper follows “The Cloud Manager’s Balancing Act,” which describes the need for cloud managers to balance developer time-to-value with security risk and costs. Please see the methodology section of this paper for more details.

Security Remains A Top Concern About Public Cloud

In the public cloud model, responsibility for the security of the cloud is split between the cloud provider and the organization. The provider is responsible for securing the data center, infrastructure, and hypervisor, while the end user organization is responsible for the operating system, applications, users, and data. Forrester calls this “the uneven handshake.”

The security of data and other assets in the public cloud is a serious concern of cloud managers and IT security alike. Developers are concerned with their time-to-value, not cloud security. The responsibility for securing the cloud falls to cloud managers and IT security. Our custom survey shows that 40% of IT professionals involved in their organization’s public cloud security policies and tasks are very concerned, and an additional 36% are concerned, with the security of the applications and data in their public cloud environment (see Figure 1). This is a real and valid concern, and one that can keep companies from getting the most out of their public cloud environments.

FIGURE 1
Public Cloud Security Is A Concern Of Cloud Managers And IT Security Alike



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

Note: Percentages may not total 100 because of rounding.

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

Best Practices For Public Cloud Security

Cloud managers need to work with IT security to secure the users, data, and applications in their public cloud environments. To do so, Forrester recommends that they adopt a Zero Trust security model. There are three concepts that are the foundation of the Zero Trust security model that need to be incorporated into how cloud managers secure their public cloud environments today.[1] These are:

- **Verify and secure all resources.**
- **Limit and strictly enforce access control.**
- **Log and inspect all traffic.**

One issue in implementing Zero Trust practices in a public cloud setting is that the controls needed can be time-consuming — a nonstarter for savvy cloud managers. Therefore, cloud managers need to apply the tenants of Forrester’s Zero Trust security model without sacrificing the time-to-value of their developers. To do this, cloud managers should work with their security teams to leverage the following best practices (see Figure 2):

VERIFY AND SECURE ALL RESOURCES

To ensure public cloud resources are secure, be sure to:

- **Encrypt data intelligently.** Part of the “uneven handshake” of public cloud security is that the customer is responsible for the security of their data in the cloud. However, encrypting all of the data in your public cloud can be costly in terms of both time and money. To ensure your data is secure, you must, at a minimum, encrypt sensitive or “toxic” data before it enters the cloud. Our survey data shows that just over half of organizations (54%) using public cloud are encrypting sensitive data in the cloud today.[2] You should also control the encryption keys so you are not reliant on the cloud provider. Forrester terms this “bring your own encryption.” Consider the sensitivity and toxicity of your workloads before they enter the cloud, and encrypt intelligently using data protection technology.
- **Train developers to consider security.** While you do not want to burden your developers with time-consuming public cloud security processes, education and training can help ensure developer compliance with your cloud policies. Implement a secure development life cycle, and

use application scanning solutions that can be fully automated in the public cloud to detect known vulnerabilities. Our survey shows that 45% of organizations using public cloud are providing education to end users on public cloud safety, and 44% have made security training mandatory to accessing their public cloud.

LIMIT AND STRICTLY ENFORCE ACCESS CONTROL

To ensure only trusted users are accessing your public cloud data, be sure to:

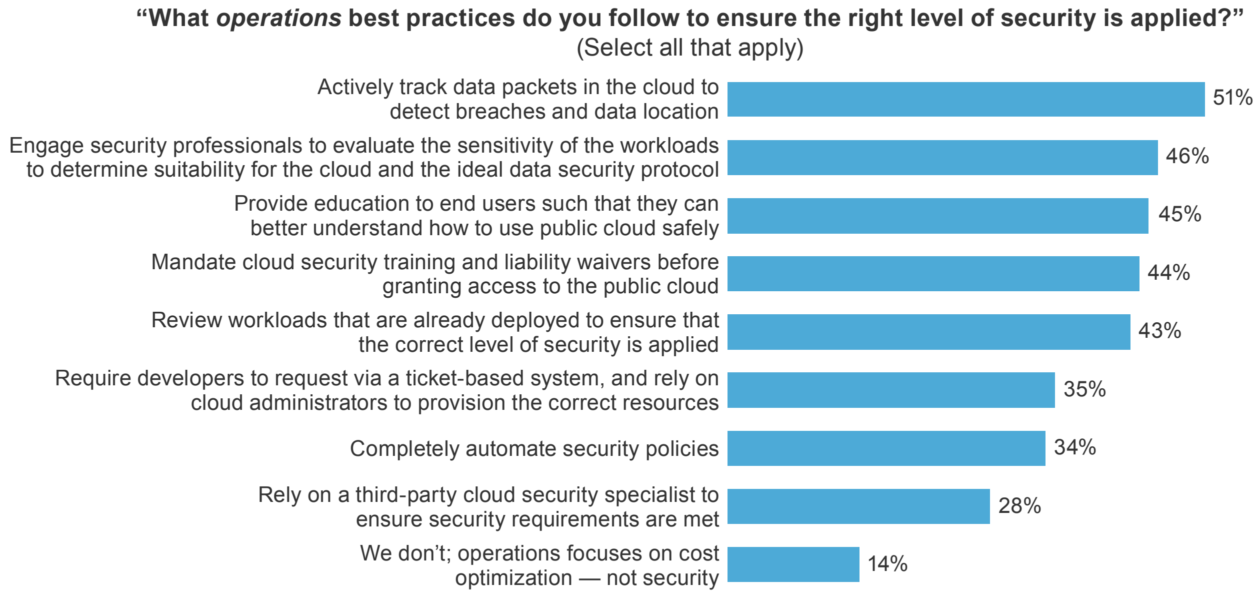
- **Get visibility into your public cloud.** To ensure safety, you need to know who is accessing your cloud, how they are accessing the cloud, and what resources are going into the cloud. Our survey shows that just over half (51%) of organizations using public cloud are actively tracking data packets in the cloud today. The goal is to identify threats and neutralize them with cloud-enabled versions of antimalware or host intrusion detection and/or intrusion prevention (IDS/IPS) solutions. In addition to monitoring the cloud, having limited access points to your public cloud allows you to control access using identity and access management technologies. However, you must be sure not to impede on your developers as they try to access the cloud.

LOG AND INSPECT ALL TRAFFIC

To secure your public cloud without impeding on your developers, be sure to:

- **Use tools that can automate security provisioning and track and monitor workloads.** To maintain your developers' time-to-value, use a tool that automates security provisioning for workloads. These tools should tag workloads before they enter the cloud, automatically assigning security policies across multiple controls based on predefined criteria. The goal is whenever you spin up a workload, it inherits the security policies automatically without creating a manual change management workflow, which slows provisioning. Once the data is in the cloud, continue to monitor workloads for unplanned or malicious changes using cloud-friendly log inspection and integrity monitoring solutions, and review the applied policy to ensure the proper level of security is in place. Our survey data shows that 43% of organizations are reviewing already deployed workloads to ensure the correct level of security is applied.

FIGURE 2
Operations Best Practices For Public Cloud Security



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

MAKE SURE YOUR SECURITY TEAM UNDERSTANDS THE CLOUD

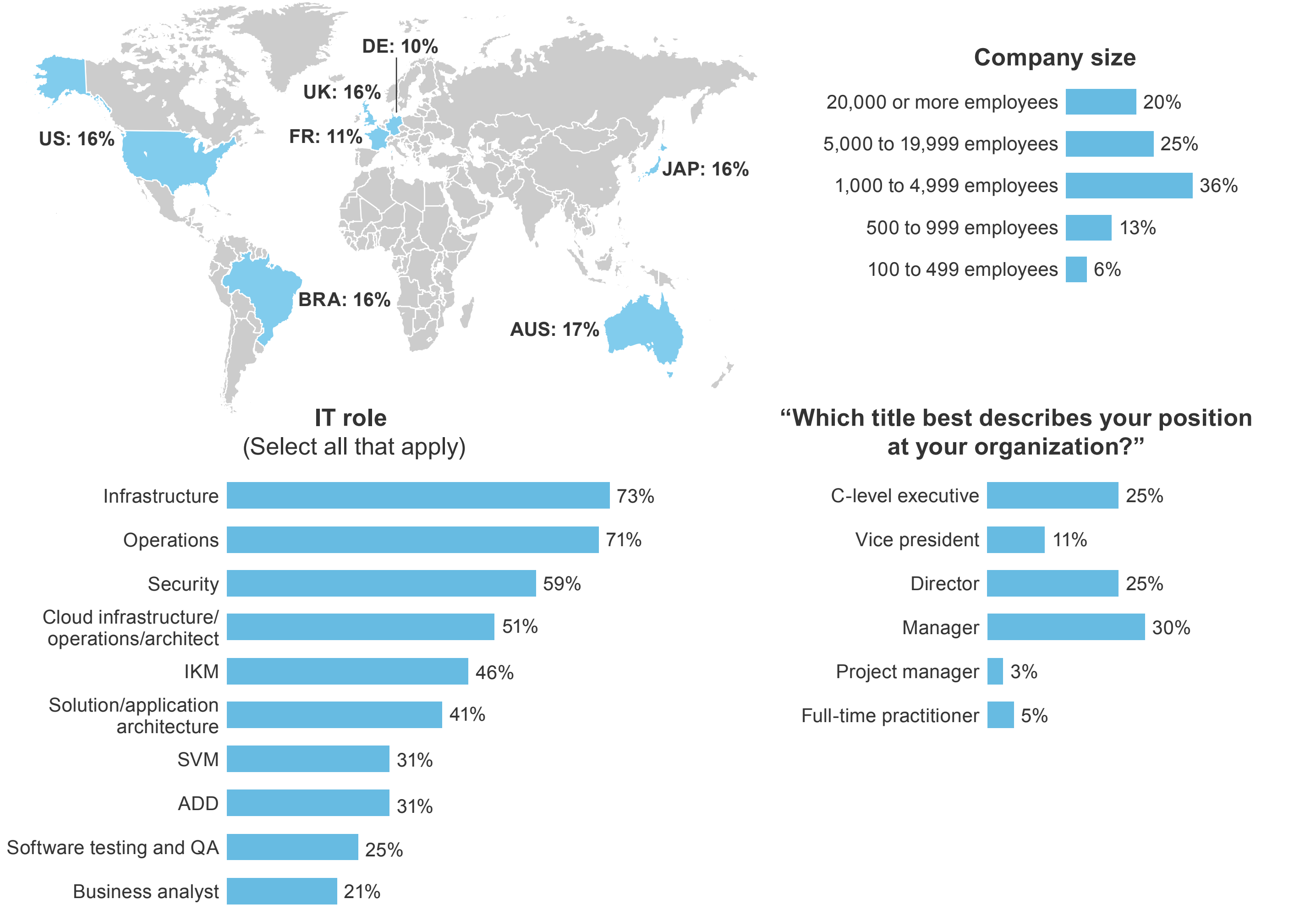
Your IT security team will be your key partner in protecting the cloud, provided they understand the importance of your developers’ time-to-value. Work with your security team to understand the unique challenges of cloud security, especially in the context of the shared security responsibility model, and how these challenges require different solutions. A good partnership between cloud managers and security will help to implement Zero Trust best practices for your cloud. Our survey shows that 46% of organizations are engaging their security team to evaluate workload sensitivity to determine cloud suitability and ideal protocols. However, if your security team does not understand the differences in securing the cloud, you risk the benefits of your investment.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 321 organizations of 100 or more employees spending more than an average of $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 3
Survey Demographics



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

Note: Percentages may not total 100 because of rounding.

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

Appendix C: Endnotes

[1] Source: “No More Chewy Centers: The Zero Trust Model Of Information Security,” Forrester Research, Inc., October 7, 2014.

[2] A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, May 2014.