ALL CLOUDS ARE NOT EQUAL:

Disproving the Top 5 Misconceptions About the Infrastructure Behind Cloud-Based Security

FORCEPOINT
POWERED BY Raytheon

Contents

Introduction

"Growth in cloud-based security will remain strong, at about 19% through 2020."

Source: Gartner, "Market Trends: Global Demand for Cloud-Based Security is Growing Through 2020," April 5, 2017.

In the early days of cloud computing, security concerns prevented many organizations from moving their data, applications, and infrastructure off premises. Today, however, that thinking has come full circle, and most organizations realize that the cloud offers the potential to be a safe place for all three.

Indeed, according to a recent Intel Corp. report, people who trust public cloud now outnumber those who don't by a ratio of 2-to-1. And more than 62 percent of surveyed IT professionals now store their personal data on the public cloud.[1] It won't surprise you, then, to learn that global cloud traffic is expected to grow nearly fourfold to 14.1 zettabytes by 2020 (up from 3.9 zettabytes in 2015) or that the number of companies relying on traditional (on-premises) IT infrastructure is expected to drop by more than 30 percent over three years (from 77 percent in 2015 to 43 percent in 2018).[2]

In short, everyone is turning to the cloud for every*thing*, and security itself is no exception: Today, more and more companies and government agencies are employing cloud-based security solutions to gain:

- Security for *all* employees (including those on the go)
- Greater scalability and flexibility
- Security for applications, data, and systems (both in the cloud and on-premises)
- Reduced complexity (as compared with disparate, on-premises tools)
- Ease and speed of deployment
- Lower hardware and support costs

Obviously, you want your organization to gain these advantages as well, and the first step in getting there is choosing the right cloud security provider. But before you start ticking off items from your desired-security-features list, be aware that there are other factors you should take into consideration as well. For example:

- What do you know about the datacenters where the cloud-based security solution runs?
- What about the provider's security controls, data privacy, availability/reliability, and performance?
- And how do you know whether the provider's infrastructure will meet your company's needs?

Read on to discover five common misconceptions about cloud-based security infrastructure, and what you should *really* be looking for in your own cloud-based security solution.

1. Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2015-2020," 2016.
2. Pratik Dholakiya, "Five key cloud trends to look forward to in 2017: Containers, AI, and more," February 2017.

Important Security Standards for the Cloud

Before you can begin evaluating prospective providers of cloud-based security solutions, you need to have an understanding of the alphabet soup of existing security standards related to the cloud. Here's a brief run-down:

International Standards Organization (ISO) 27001

This security management standard specifies best practices and comprehensive security controls following the ISO 27002 best-practice guidance.

ISO 27018

This code of practice focuses on protecting personal data in the cloud. It provides implementation guidance on the ISO 27002 controls that are applicable to public-cloud personally identifiable Information (PII). It also provides controls and guidance on public-cloud PII protection requirements not addressed by the existing ISO 27002 control set.

Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)

Encompassing the key principles of transparency, rigorous auditing, and harmonization of standards, CSA STAR consists of three levels of assurance. These levels currently cover four unique offerings based on the cloud-centric control objectives in the CSA Cloud Controls Matrix (CCM).

American Institute of Certified Public Accountants Service Organization Control (AICPA SOC) 1/2/3

These standards establish the framework for examining controls at a service organization: SOC 1 reports focus on financial reporting, while SOC 2 and 3 reports focus on nonfinancial reporting controls relating to security, availability, processing integrity, confidentially, and privacy. SOC 2 also examines the details of datacenter testing and operational effectiveness.

Now that you've got that under your belt, let's start shattering some of those common cloud security misconceptions.

MISCONCEPTION 1

Security Certifications Are Only Important for Compliance Teams

Yes, your organization has a compliance team. And yes, that team is checking certifications as part of its due diligence. However, your compliance team is most likely checking on certifications for functions within your own business. Any organizations that you partner with—including your cloud-based security provider—should have the requisite certifications in their own areas, and those certifications need to be checked as well.

This means that your security team should be looking for certifications as part of their initial vendor selection process. If a cloud provider can't supply them, you have no assurance that it's complying with industry and government security standards. For example, without an ISO 27018 certification, you don't know whether a provider has controls in place for PII data (which is also a requirement for complying with the General Data Protection Regulation, or GDPR).

At minimum, your security team should also look for:

- Compliance with CSA STAR (for its additional layer of controls)—an easy task, since CSA publishes a registry of companies that have passed the certification
- Compliance with U.S. industry-specific regulations (such as Payment Card Industry Data Security Standard (PCI-DSS) for credit card transactions and Health Insurance Portability and Accountability Act (HIPAA) for healthcare)
- Compliance with local regulations in areas where your company does business (which may require that data remain within a region or country).

Finally, be certain to have your team check the scope statement on the certification or attestation: Does it reflect the services that you're interested in consuming? Be wary of vendors that are claiming certification for their entire organizations yet are only including a single subset of operations in the compliance scope. And read those SOC reports—they're not certifications, and they can contain glaring security-control issues.

COMPLIANCE VS. CERTIFICATION

Any company can implement a standard such as ISO 27001 and claim to be compliant. Certification by a third-party auditor, however, is the only way to prove conformance. This kind of audit requires time, resources, and money, and some providers may not want (or be able) to make the investment. Insist on a cloud-based security provider that ***has***. Carefully examine the scope of the provider's certification to make sure it covers the functions that your organization consumes. Be sure to ask for the provider's "Statement of Applicability."

MISCONCEPTION 2

Cloud-Provider Datacenters Are Always More Secure Than Corporate Ones

While cloud service providers like to point to breach after breach of private datacenters as evidence that their cloud-based infrastructures are more secure, this is not inherently true. Although the cloud certainly offers benefits in the area of security, providers need to put controls in place to ensure they're able to derive those benefits.

Many datacenters—both corporate owned and collocated—have strong control over their physical security (via key cards, biometric scanning, and so on). However, it's up to security managers to implement the controls needed for data security (for example, encryption, tokenization, and data loss prevention (DLP)). Certification from a third-party auditor is a must-have for the cloud security vendor to provide your company with assurances that their datacenters, servers, storage, applications, and customer data are secure and in compliance with all standards, regulations, and laws.

Be wary, though: A statement of compliance is not the same as certification. Unless a provider shows you a certificate, you cannot be assured that it has met all requirements to comply with a given standard. And don't be fooled into thinking that certification means that a cloud provider handles all aspects of security. Most cloud service providers follow a shared-security model—which means that areas such as user behavior, access and usage policies, and compliance are *your* responsibility, not the cloud service provider's.

WHEN SINGLE-SITE CERTIFICATION IS NOT ENOUGH

In addition to checking certifications for the cloud-based security provider, you should make sure that these certifications apply to ***all*** of the vendor's datacenters. A multi-site certification demonstrates that the vendor has consistent processes and procedures across all sites—an important distinction. Again examine the scope of the provider's certification to make sure it covers the functions that your organization will consume. Don't forget to ask for the provider's "Statement of Applicability."

MISCONCEPTION 3

The More Datacenters a Cloud Service Provider Has, the Better the Service's Performance and Resiliency

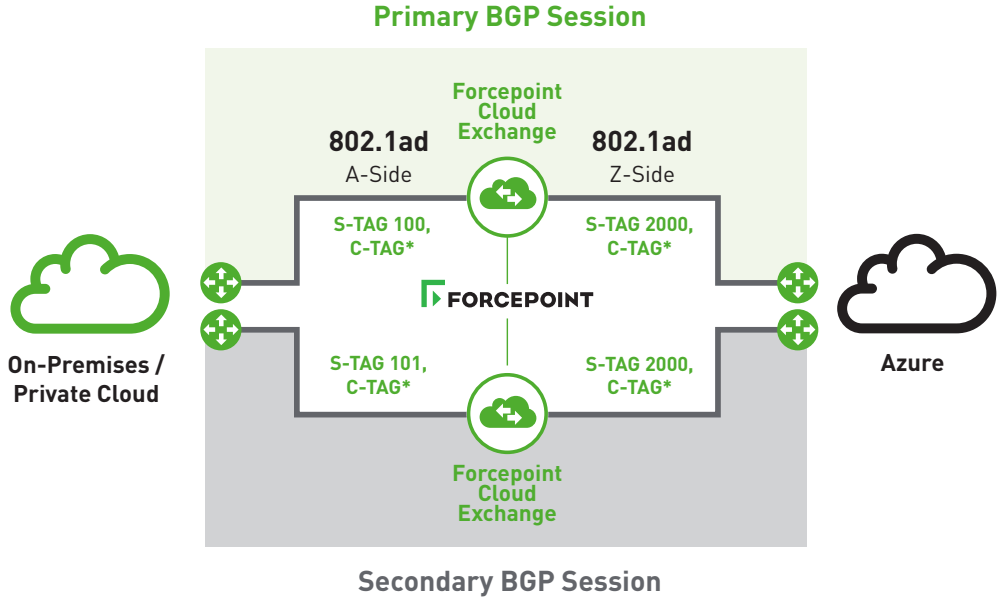
This is a fallacy. Although a cloud service should have a *minimum* number of datacenters globally, the number of datacenters has no direct bearing on the performance of the service. Take, for example, Microsoft Azure: it has just 30 datacenters globally. However, other lesser services with hundreds of datacenters cannot begin to match Azure's throughput and performance. So while global coverage does help reduce latency, it's something called *peering* that makes the biggest difference in performance.

Indeed, it is *cloud peering*—which involves an enterprise establishing a private, direct, and secure interconnection between itself and a public cloud—that will ensure the best experience for your users. And it is through *datacenter peering exchanges* that you can improve performance. Using an Internet exchange as a marketplace, Internet Service Providers (ISPs) can interconnect these networks and exchange IP traffic. The result is:

- Lower latency with fewer network hops—providing faster, more direct data flows
- Greater redundancy (because peering increases available paths)—improving routing, efficiency, and fault tolerance

Another important distinction when it comes to performance is whether the cloud security provider's facilities use multihomed autonomous systems. A multihomed autonomous system maintains connections to more than one other autonomous system (AS). This allows the AS to remain connected to the Internet in the event of a complete failure of one of the connections.

Example of Cloud Peering



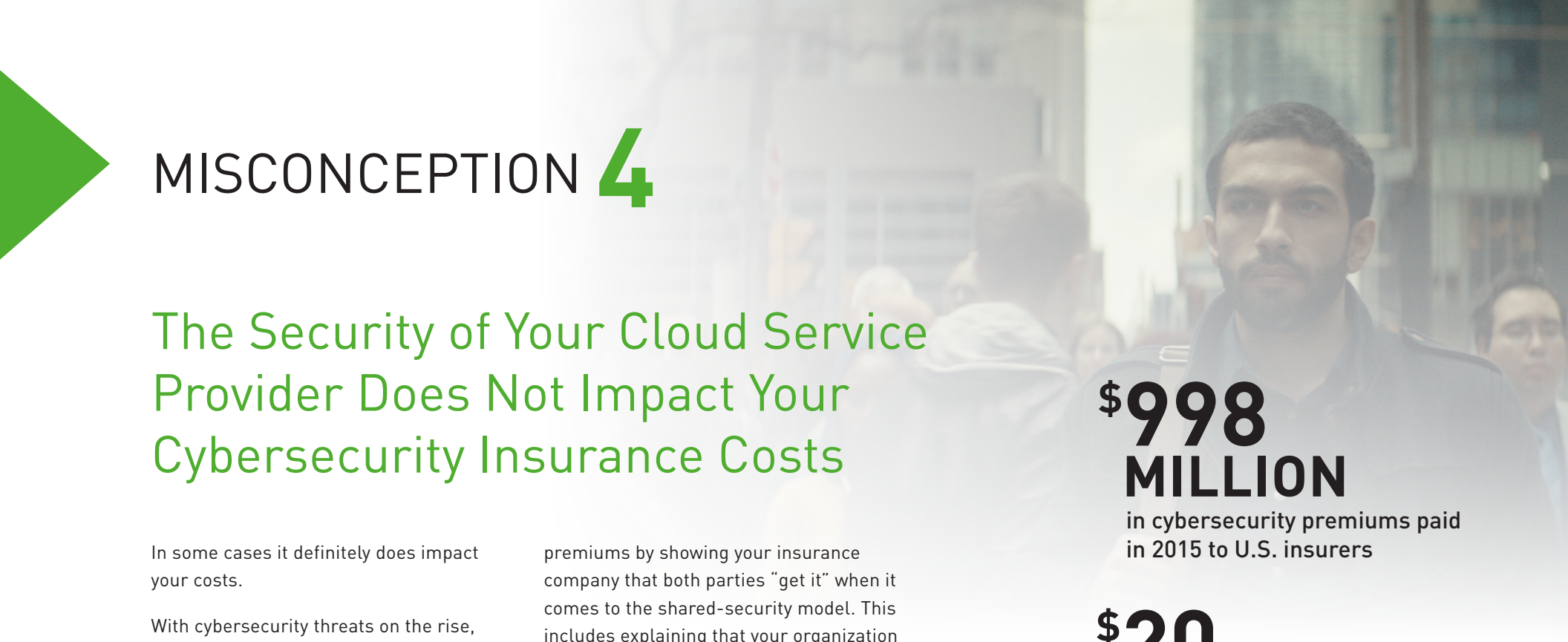
MISCONCEPTION 4

The Security of Your Cloud Service Provider Does Not Impact Your Cybersecurity Insurance Costs

In some cases it definitely does impact your costs.

With cybersecurity threats on the rise, cybersecurity insurance has become big business—earning U.S. insurers $1 billion in cyber-premiums last year.[3] This does not mean, however, that you need to pay more than necessary to protect your data and customer information.

If your company is investing in cyber insurance, you will likely pay a lower premium if your cloud providers can show certifications demonstrating that your sensitive data and customer PII are secured. You can also minimize your premiums by showing your insurance company that both parties "get it" when it comes to the shared-security model. This includes explaining that your organization and your cloud-service provider are actively mitigating cyber risks by having proper threat prevention, data security, and data protection in place—and that as a result, cyberattacks are minimized and recovery times are negligible.



$998 MILLION
in cybersecurity premiums paid in 2015 to U.S. insurers

$20 BILLION
in cyber insurance premiums by 2020

120
insurance groups offer cyber coverage

Source: Fitch Ratings, "U.S. Cyber Insurance Premiums Total $1B Per New Supplemental Filing," August 24, 2016.

3. fedscoop.com, "Survey: U.S. insurers earned $1B in cyber premiums last year," August 2016.

MISCONCEPTION 5

General Data Protection Regulation (GDPR) Compliance Only Impacts European Companies

With a primary objective of restoring citizens' and residents' control of their personal data, the GDPR is a regulation through which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. This does not mean, however, that only European companies need comply.

The truth of the matter is that *any* company processing personal data originating from the European Union (EU) (regardless of whether the data subject resides there or is a citizen) *or* from an EU resident (regardless of whether the company has operations in the EU) is subject to the GDPR.

So get ready: Come the May 2018 final implementation date, the GDPR will be mandating numerous privacy arrangements and controls designed to protect personal data. Because many of these controls are also recommended by ISO/IEC 27001:2013, ISO/IEC 27002:2013, and other "ISO27k" standards, organizations that already have an ISO27k ISMS (Information Security Management System) are also likely to have the GDPR requirements covered (though some adjustments might need to be made).

GDPR IS A TOP PRIORITY FOR U.S. MULTINATIONALS

In a survey by PwC of large American multinational companies, nearly all of the respondents (92 percent) considered compliance with Europe's landmark General Data Protection Regulation (GDPR) a top priority on their 2017 data-privacy and security agendas—with more than half naming it "the" top priority, and 38 percent putting it "among" top priorities.

Source: PwC, "Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets," January 2017.

A Checklist for Choosing a Cloud-Based Security Provider

Now that you know fact from fiction when it comes to the actual cloud infrastructure behind cloud-based security, here's a checklist of the things you should look for when selecting your provider.

- ☐ **Trust program certifications (not just self-audited compliance).** For ISO 27001, ISO 27018, CSA STAR, and others relevant standards for your organization.
- ☐ **Datacenters located in regions where your company operates.** This is necessary for both performance and compliance with local laws and regulations (which may require that data remain within a region or country).
- ☐ **Multihomed autonomous systems.** These should offer peering to other clouds for performance and reliability.
- ☐ **Compliance with relevant industry regulations.** For example, HIPAA, PCI DSS, and more.
- ☐ **Carrier-grade, fully redundant data centers.** For reliability and "five nines" (99.999%) service availability.

Selecting the Right Solution

Now that we've cleared up misconceptions about cloud-based security and you now know precisely what you should look for in a provider, read on to learn how Forcepoint delivers what you need.

With the industry's most trusted and robust cloud security services, Forcepoint provides:

High performance

With 27 globally distributed data centers, Forcepoint delivers highly available, globally distributed clusters with Tier 1 Internet and power feeds. As a result, Forcepoint's Top Tier 1 Wide Area Network (WAN) can reach every other network on the Internet without purchasing IP transit or paying settlements.

Forcepoint also offers multihomed ASN (Autonomous System Numbers) with peering—taking advantage of peering relationships with major peering exchanges and cloud providers to provide the best possible performance.

High availability

Forcepoint datacenter cooling equipment (including chillers and heating, ventilating, and air-conditioning (HVAC) systems) is independently dual-powered in a fault-tolerant site infrastructure with electrical power storage and distribution facilities. The result: expected availability of 99.999 percent.

Security and certifications

Forcepoint is the first and only cybersecurity company to incorporate all new ISO/IEC 27018 controls into its ISO 27001 program. (And we've been independently audited and certified to be in compliance with the new standard.) Forcepoint is also backed by:

- ISO 27001 multi-site certification for Development, Quality Assurance, Deployment, and Support Operations (for Forcepoint Cloud Web, Email, and Data Security). (Forcepoint undergoes annual independent audits to maintain its active certification.) Forcepoint has also attained ISO 27018 and CSA STAR certification.

- GDPR privacy controls compliance
- Secure cages, biometric access controls, CCTV-monitored datacenters 24/7/365
- Client-controlled log data and secure, compliant regional storage options

Learn More

For more information about Forcepoint cloud security, visit https://www.forcepoint.com/environments/cloud.

About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.Forcepoint.com and follow us on Twitter at @ForcepointSec.

FORCEPOINT
POWERED BY Raytheon