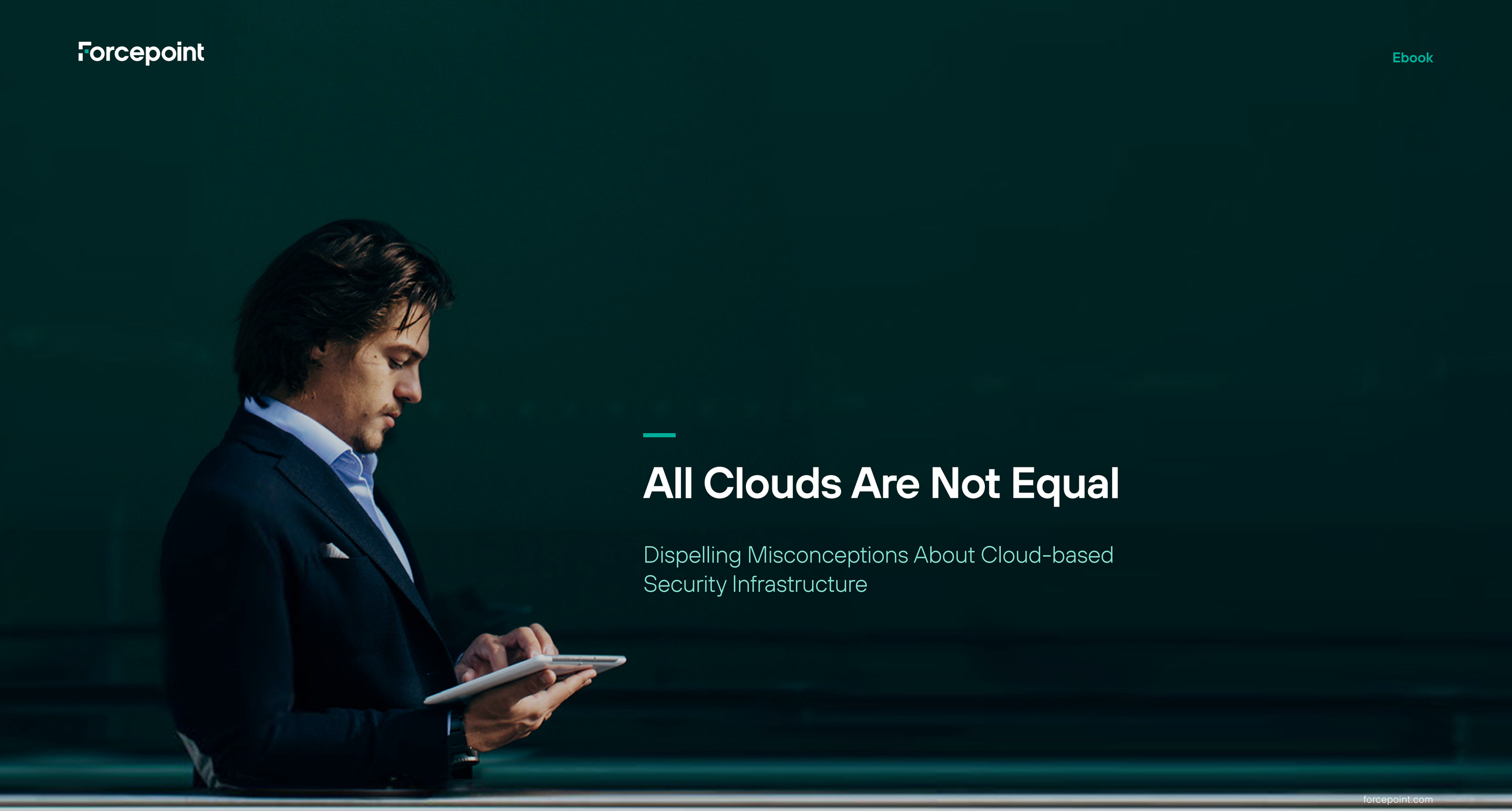
Forcepoint

Ebook



All Clouds Are Not Equal

Dispelling Misconceptions About Cloud-based Security Infrastructure

Table of Contents

Introduction

In the early days of cloud computing, security concerns prevented many organizations from moving their data, applications, and infrastructure off-premises. Today, however, most organizations realize the cloud can be a safe place for all three.

As everyone turns to the cloud for everything, security is no exception. More and more companies and government agencies are employing cloud-based security solutions to gain:

- → Security for all employees (including who are remote and roaming)
- → 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

Despite these advantages, certain misconceptions about cloud-based security infrastructure persist. Read on as we dispel them and detail what's actually important to look for in your own cloud-based security solution.

Misconception 01

Security certifications are only important for compliance teams.

Your compliance team checks certifications as part of its due diligence.

However, they're most likely checking on certifications for functions within your own business. Any organization you partner with (including your cloud-based security provider) has requisite certifications in its own areas—and those certifications need to be checked as well.

This means 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.

At minimum, you should look for:

→ Compliance with CSA STAR's additional layer of controls—an easy task, since CSA publishes a registry of companies that have passed the certification

→ Compliance with 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)

Be sure to check the scope statement or attestation: Does it reflect the services you're interested in consuming? Be wary of vendors that claim certification for their entire organization yet only include a single subset of operations in the compliance scope. And read the most current System and Organization Controls (SOC) 2 reports issued by the American Institute of Certified Public Accountants (AICPA), which can help illuminate glaring security-control issues.

Misconception 02

Cloud-provider datacenters are always more secure than corporate ones.

The cloud certainly offers benefits in the area of security. For providers to fully realize these benefits, however, they must put controls in place.

Many datacenters—both corporate owned and collocated—have strong control over their physical security. There's less consistency when it comes to implementing controls for data security. For sufficient assurance that your cloud security vendor's datacenters, servers, storage, applications, and customer data are secure and in compliance with all standards, regulations, and laws, they must have certification from a third-party auditor.

Keep in mind that a statement of compliance is not the same as certification. Without a certificate, you can't be assured that a provider has met every requirement to comply with a given standard. Additionally, certification doesn't mean that a cloud provider will handle all aspects of security. Most cloud service providers follow a shared-security model—so areas like user behavior, access and usage policies, and compliance are up to you. Since many cloud services are based on public cloud infrastructure, that underlying infrastructure has likely been audited and certified—but you still have to verify whether the same is true for the service itself.

Misconception 03

The more datacenters a cloud service provider has, the better the performance.

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.

Case in point? Microsoft Azure, which has just 30 datacenters globally. Lesser services with hundreds of datacenters can't begin to match Azure's throughput and performance.

While coverage helps with latency, peering is what makes the biggest difference in performance:

→ Cloud peering—which involves establishing a private, direct, and secure interconnection between your enterprise and a public cloud—ensures the best experience for your users

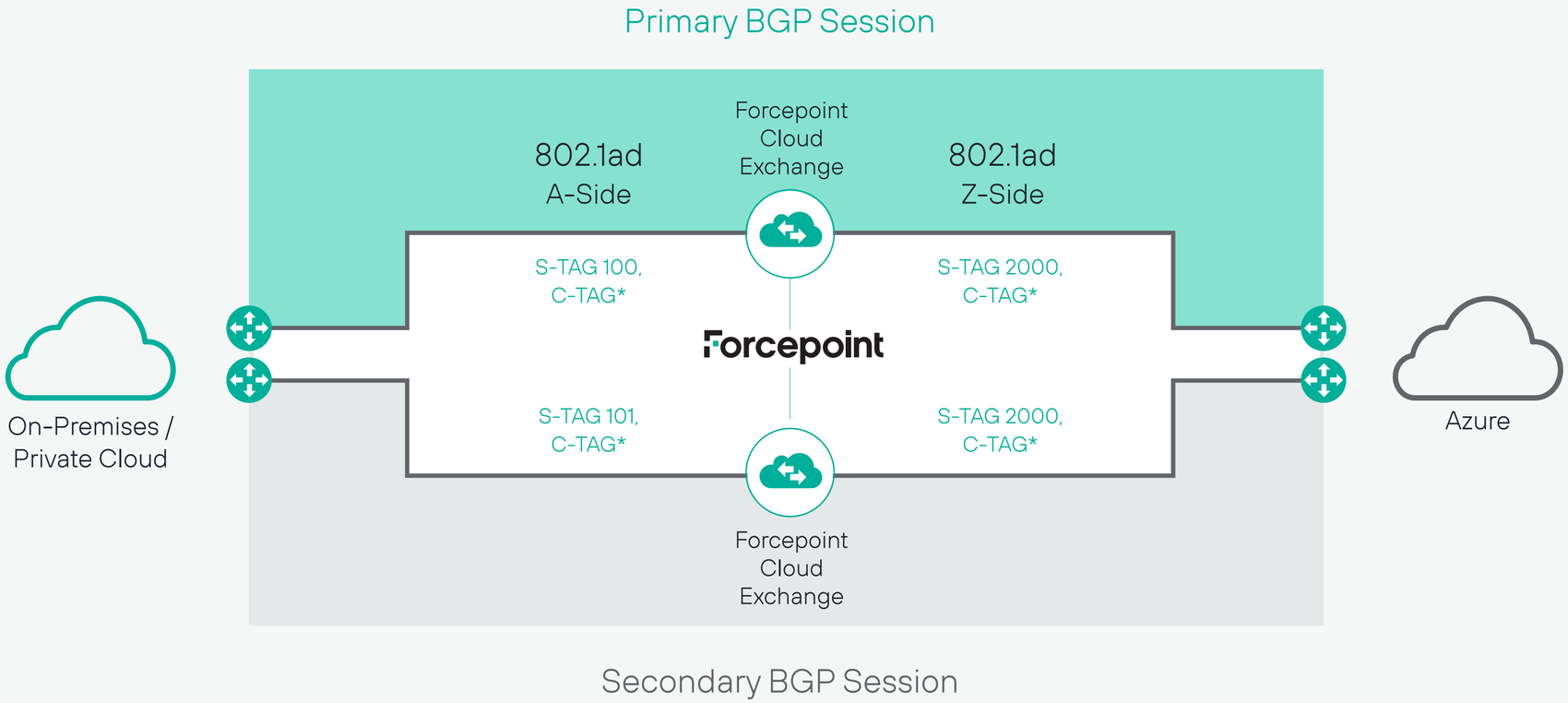
→ Datacenter peering exchanges enable better performance; internet service providers (ISPs) can interconnect these networks and exchange IP traffic

As a result, you'll experience lower latency with fewer network hops—providing faster, more direct data flows. An additional benefit is greater redundancy due to more available paths—improving routing, efficiency, and fault tolerance.

Misconception 03

The more datacenters a cloud service provider has, the better the performance.

Another important factor related 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), allowing the AS to remain connected to the internet in the event of a connection failure.



Misconception 04

The security of your cloud service provider doesn't impact your cybersecurity insurance costs.

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 properly secured.

You can also minimize your premiums by showing your insurance company that both parties subscribe 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.

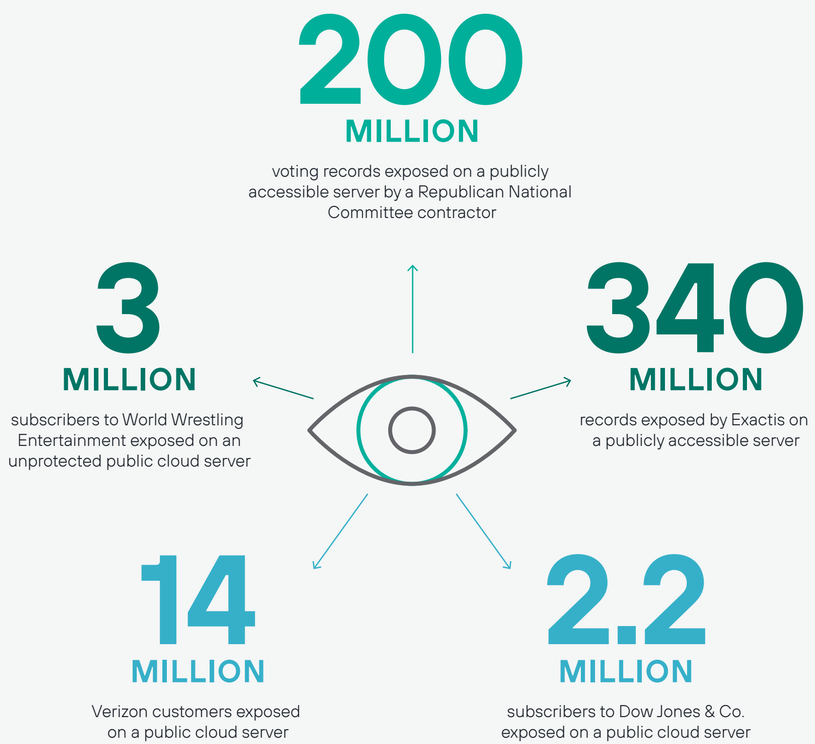
Misconception 05

Compliance is solely driven by external forces.

Governments and industries put in place regulations like HIPAA and PCI-DSS to protect privacy and personal data and ensure the preservation and integrity of data.

But your organization—with its unique needs, expectations, and sensitivities—has its own internal compliance drivers as well. External regulations don't address considerations such as protecting key intellectual property, strategic plans, business records, and the access restrictions you will define in support of those goals.

Compliance programs are increasingly becoming critical components of the business landscape, but they can be a significant challenge to establish and maintain. Policies form the cornerstone of your compliance and security program, and good policies take time to develop. Invest the time and resources necessary to set policies that will enable you to safeguard critical information and avoid the consequences of failing a compliance audit.



What to Look for in a Cloud-based Security Solution

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

Trust program certifications—not just self-audited compliance
ISO 27001, ISO 27018, CSA STAR, SOC 2 Type 2 report, and other relevant standards for your organization.

Compliance with relevant industry regulations
For example, HIPAA, PCI-DSS, and more.

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).

Carrier-grade, fully redundant data centers
For reliability and "five nines" (99.999%) service availability.

Multihomed autonomous systems
These should offer peering to other clouds for performance and reliability.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[All-Clouds-Are-Not-Equal-Ebook-US-EN] 24MAR2020