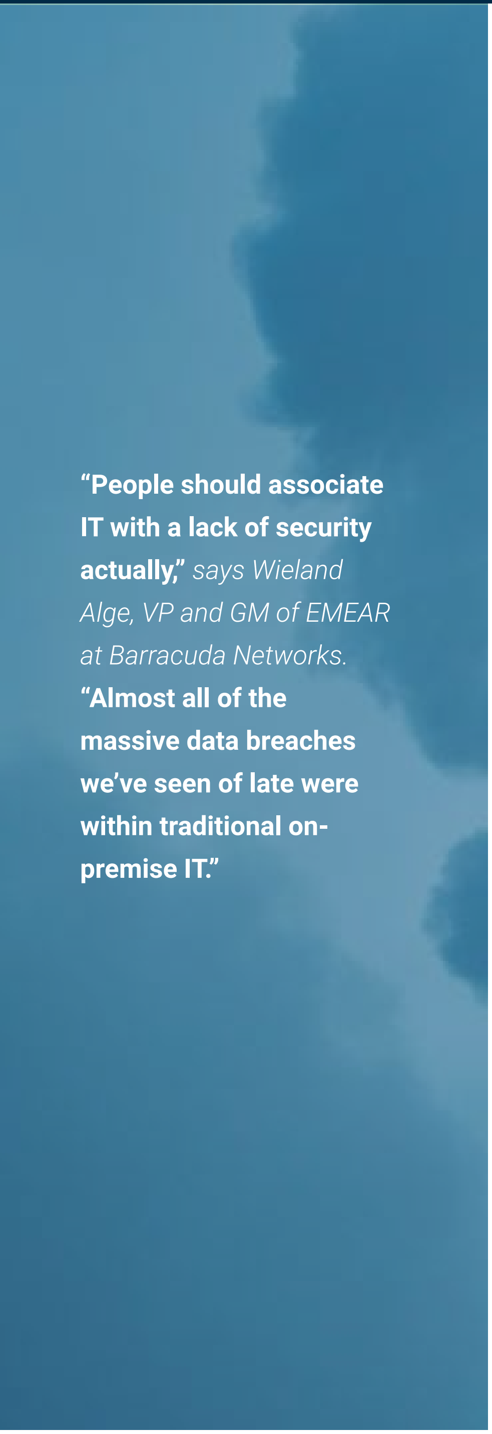
7 DATA SECURITY QUESTIONS TO ASK YOUR CLOUD PROVIDER

A Publication of

iCorps®
TECHNOLOGIES

7 DATA SECURITY — QUESTIONS — TO ASK YOUR CLOUD PROVIDER



“People should associate IT with a lack of security actually,” *says Wieland Alge, VP and GM of EMEAR at Barracuda Networks.* **“Almost all of the massive data breaches we’ve seen of late were within traditional on-premise IT.”**

ONE OF THE WORLD’S LEADING IT RESEARCH AND ADVISORY FIRMS, Gartner, describes cloud computing as “a disruptive phenomenon,” one that “promises economic advantages, speed, agility, flexibility, infinite elasticity, and innovation.” In the past several years, the cloud has evolved and delivered on its promise. Businesses of all sizes are already benefitting from the cloud – from Facebook, which moved all of its employees to Microsoft’s Office 365 cloud application suite, to a 65-employee technology firm that moved its critical business application to the cloud, saving $4,000 monthly.

Organizations have caught on to the benefits of the cloud, including high reliability, cost effectiveness, scalability, reduced strain on internal resources, and flexibility. One benefit, however, has taken critics by surprise: security. When cloud services first made their way onto the IT scene, the largest concern by far was data security driven by the fear of losing control over the data stored in public datacenters. But as consumption of the cloud has grown along with its capabilities, many cloud vendors have had no choice but to step up their security standards.

Security experts now argue that the cloud can provide businesses with more security than in-house (or on-premises) IT environments. They key word is “can” because not all cloud vendors are created equal.

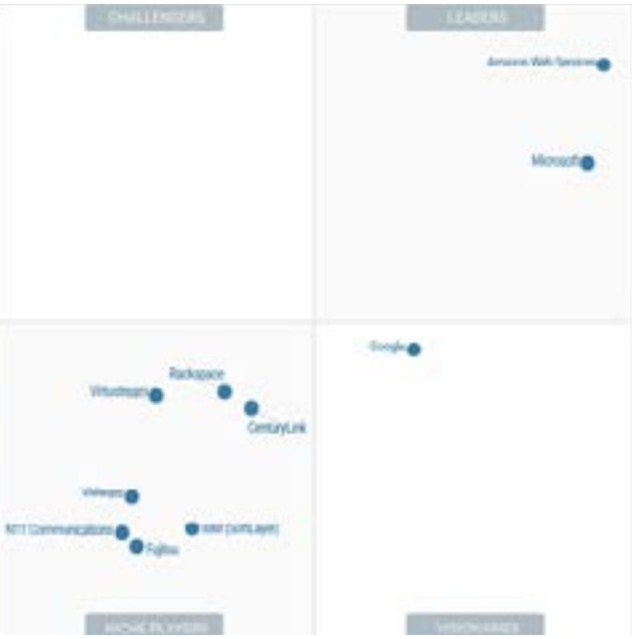
Many businesses already use entry-level cloud solutions, like Dropbox and Google Drive because of their convenience and affordability. You and your team might currently be using these same tools as well. While these options may be suitable for sharing family photos or storing research papers, their questionable security standards make them a risky tool for any business storing confidential data. Dropbox continues to make headlines for a data breach back in 2012, raising doubts even four years later about the company’s overall stance on security for its users. As your company grows, you’ll find that you need better options, with enterprise-level security to guard your data. This is when you should consider more robust cloud service choices, backed by more powerful measures, including Microsoft Azure and Office 365.

NOT ALL CLOUD PROVIDERS ARE EQUAL

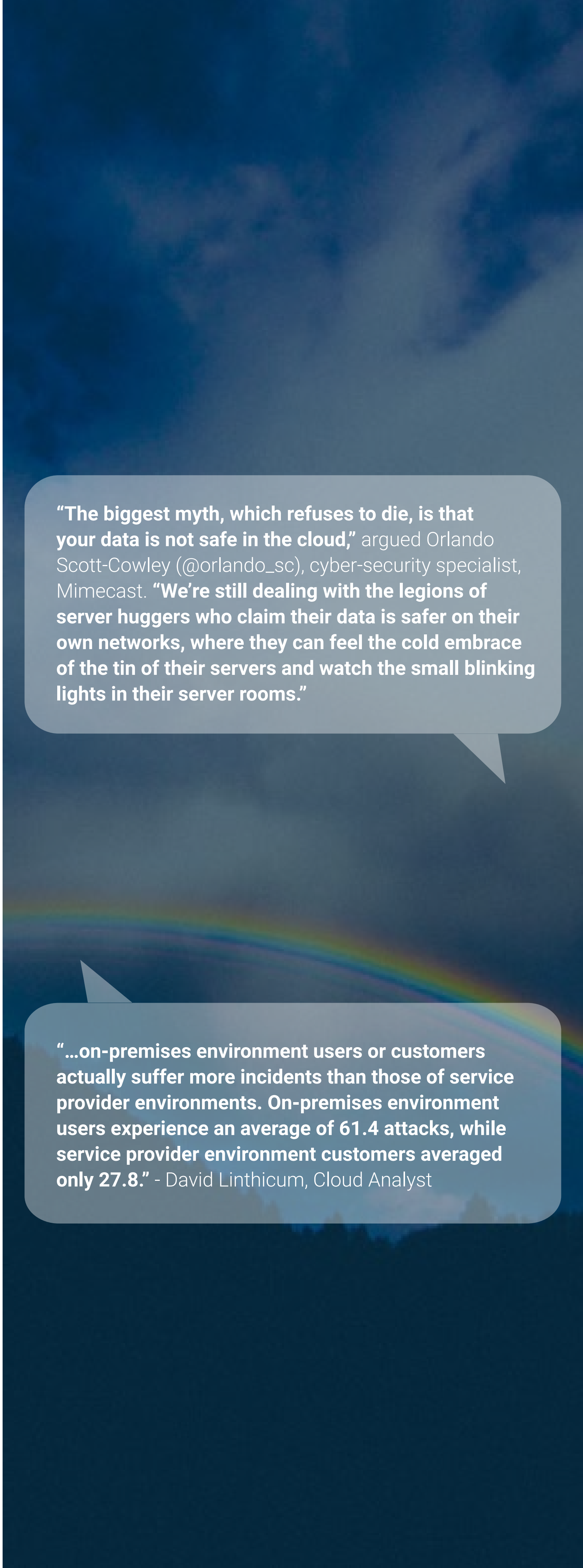
Each year, Gartner publishes its Magic Quadrant for Cloud Infrastructure as a Service. Gartner evaluates several cloud computing providers based on factors such as execution, service, availability, security and customer support.

MAGIC QUADRANT

Figure 1. Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide

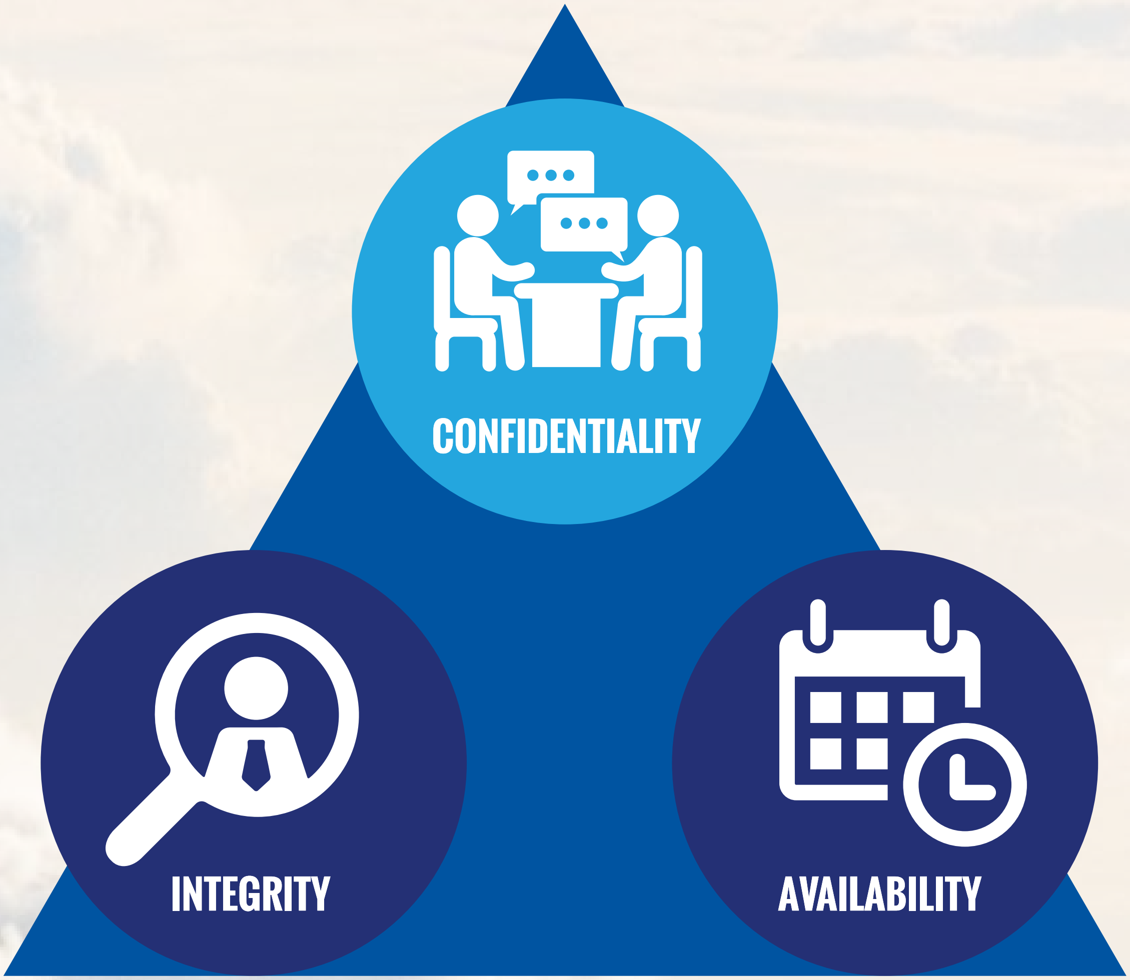


Amazon Web Services and Microsoft stand out as the leaders in the IaaS space (see Amazon Web Services vs. Microsoft Azure). Within its analysis, the research firm admits that while all the providers claim to have high security standards, the extent of the security controls varies significantly. While the Magic Quadrant is a good starting point for anyone researching cloud IaaS providers, each option much be carefully evaluated. All providers can meet common regulatory compliance requirements, but who goes above and beyond to ensure that YOUR business' data is being protected at every angle? Gartner also cautions that the future of cloud service providers other than the leading two (Amazon Web Services and Microsoft) is uncertain and "customers must carefully manage provider-related risks."



"The biggest myth, which refuses to die, is that your data is not safe in the cloud," argued Orlando Scott-Cowley (@orlando_sc), cyber-security specialist, Mimecast. **"We're still dealing with the legions of server huggers who claim their data is safer on their own networks, where they can feel the cold embrace of the tin of their servers and watch the small blinking lights in their server rooms."**

"…on-premises environment users or customers actually suffer more incidents than those of service provider environments. On-premises environment users experience an average of 61.4 attacks, while service provider environment customers averaged only 27.8." - David Linthicum, Cloud Analyst



ASK THE RIGHT QUESTIONS

A common misstep that many businesses make when migrating to the cloud is neglecting to ask the right questions of their vendors beforehand. Are you aware, for example, that some providers can potentially see the data you place in the cloud? That's client and project information, process documentation, budgets, HR records, and employee stats. Do you really want a third party to have a view into this sensitive material?

The security of information is often associated with the CIA triad: confidentiality, integrity and availability. The appropriate level of data security requires organizations – cloud providers included – to take measures and comply to these security controls. While some providers may offer bits and pieces of these three components, we'd argue that your data is most secure with a cloud vendor that can provide commitment to and proof of all three. Questions of confidentiality center around privacy - who has access to the information and what are the limitations of that access? Integrity essentially ensures that data cannot be altered by unauthorized people. Availability requires that access to data or services is available when needed. While the questions around proper bandwidth and keeping up-to-date hardware are important here, equally critical is having a backup plan should the hardware fail. Although public cloud outages are few and far between, your cloud provider should have a comprehensive disaster recovery plan and redundancy (i.e. datacenters in multiple geographies) to ensure continuity in case of a physical disaster.

With the CIA triad in mind, here are the questions every business should ask before entering into a partnership with a services provider:

How does the provider maintain the confidentiality of your data?

- Who has access to your data?
- How does the cloud provider ensure access is restricted to those who are authorized to view your data?
- How is your data accessed? What security layers and safeguards (e.g. firewalls, encryption, multi-factor authentication) are in place?

How does the provider maintain the integrity of your data?

- How do they encrypt your data?
- Who has the keys to your data?
- How does the provider keep unauthorized users from tampering with your data?
- Is there any verification of data?
- Are backups and redundancy in place?

How does the provider maintain the availability of your data in regards to data protection?

- Does the provider keep up to date on system upgrades?
- Does your provider have redundant data centers in geographically-isolated locations?
- What is their disaster recovery plan?

Who else's data will be co-mingling with yours?

- Are they at high risk for targeted hacking? For example: an online gambling site would be considered high-risk. Your data could be more susceptible just for being stored in the same place.

Does the provider meet compliance standards?

- How do they meet industry compliance standards (i.e. SOC, HIPAA, ISO, PCI)? Again, are they audited by an unbiased third-party?
- How often do they review their compliance?
- Have there been any past situations where customer data was compromised? What was done to rectify the problem?

Will your data remain your property alone?

- What happens if you want to leave the cloud?
- How will you get your data back?
- Will you always be in control of your data?

Is the provider you're considering certified?

- What are their certification standards?
- Do they self-certify or are they vetted by a third party?

The list can seem daunting but a trustworthy cloud provider will not shy from these necessary questions. As an example, Microsoft has taken efforts to provide cloud solutions that highlight not only high-powered usability, but also stringent security measures to defend their users against security threats. Their Azure cloud platform comes with a wealth of clearly stated and readily available material on their policies or procedures. These make it imperative for them to inform you, the customer, about how they help to secure your data, who accesses it, and under what circumstances. They also meet a wide array of industry-specific compliance standards, including ISO 27001, HIPAA, FedRAMP, SOC 2 and SOC 2, in addition to distinct international standards, like Australia IRAP, UK G-Cloud, and Singapore MTCS. When it comes to compliance, Azure excels at passing rigorous third-party audits performed by organizations like the British Standards Institute. Azure not only adheres to strict security controls and standards mandates, but is committed to transparency via third-party audit result requests to verify implementation.

Before committing to any cloud provider, make sure to do your due diligence by reviewing the contract in full (i.e. financial, technical and legal terms and conditions).

Scrutinizing a contract and the terms is important, and can answer some of the questions listed above, such as who owns the data and how you get it back. This should be called out in the service agreement, or service level agreement. Many leading cloud vendors already include language along these lines in their standard agreements.

EXAMPLES:

AMAZON WEB SERVICES: SECTION 10.2

‘Your Applications, Data and Content. Other than the rights and interests expressly set forth in this Agreement, and excluding Amazon Properties and works derived from Amazon Properties you reserve all right, title and interest (including all intellectual property and proprietary rights) in and to Your Content.’

MICROSOFT AZURE

Customer Data. You are solely responsible for the content of all Customer Data. You will secure and maintain all rights in Customer Data necessary for us to provide the Online Services to you without violating the rights of any third party or otherwise obligating Microsoft to you or to any third party.

YOUR RESPONSIBILITY

Leading cloud service providers will in general provide reliable security because it is in their best interest to do so. Having safeguards that are easily breached or exploited will not only endanger customer information, but may cause potential new customers to seek out other choices. However, don't use these industry-standard levels of attention to security as an excuse to overlook your own role in your business' security.

Cloud providers can only do so much, and total reliance on their security is a sure way to be caught unprepared in the event of a leak. There is also a burden on your team to be vigilant and enforce protocols to keep your information safe. This could mean bringing in a Managed Services Provider (MSP) to help implement password policies, end user education, multi-factor authentication, vulnerability monitoring, and other managed security duties. It's no secret that cybercrime has spiked in recent years. In 2015, ransomware attacks netted over $325 million from businesses around the world. It should be noted that insiders are the cause of 90% of security incidents, according to the Verizon 2015 Data Breach Investigations Report. Of those, 70% are unintentional. Company-wide cyber security education is key and should be committed to at all levels of your organization.

Your internal IT team may be doing an exemplary job, but we know from working with many departments that the concerns and duties of your in-house staff can quickly become overwhelming, especially in a small-to-midsize business. The daily demands of working through the end user issue queue, monitoring the network, answering tech support tickets, analyzing reports, and overseeing broader company projects doesn't leave much leeway for keeping up with security.

Due to circumstances that are hard to control and easy to overlook, your company may not be as prepared for a breach as you might think. Passwords strength and complexity requirements can go unobserved. Protocols intended to protect your employees and your data may not be enforced as thoroughly as they should be. It can be an easy, however unintentional, to slide into complacence, but today's cyber environment requires nothing less than proactive, multi-tiered approach to security.

Security is a shared responsibility; customers need to correctly configure controls and may need to supply additional controls beyond what their provider offers. – Gartner Research

> **“Looking at your task list and cross-correlating this with your IT staff bandwidth, you’ll likely draw the conclusion that managing the Cloud Handshake falls low on the priority list.”**
>
> – James Staten, Microsoft’s Cloud+Enterprise Chief Strategist

HOW AN MSP CAN HELP

As the business IT landscape becomes more complex and intertwined, businesses cannot be expected to master the mix of in-house, hosted, IaaS, and multiple cloud platforms on their own. “Looking at your task list and cross-correlating this with your IT staff bandwidth,” says Microsoft Chief Strategist, Cloud + Enterprise James Staten, “you’ll likely draw the conclusion that managing the Cloud Handshake falls low on the priority list. And this is exactly where the MSP can add the most value. And exactly where their business models are evolving.”

An MSP can serve your company as your entire IT department or as a complement to your internal staff, providing outside perspective on your existing practices. An MSP can help identify areas of vulnerability and provide the support you need for improvement. MSPs stay up to date on the latest threats, cloud vendor capabilities, industry best practices, compliance requirements, and emerging technology.

To get started in the cloud with better protection from the outset, find an MSP that specializes in providing cloud readiness assessments. Once the MSP has a thorough look at your IT infrastructure and business goals, they will be able to determine the type of security and cloud vendor that will provide optimal results. Because each business is different, each may require select measures to keep data secure. An MSP can provide the clearest picture of what cloud solutions are best for your company.