WHITEPAPER

Overcoming the Top Three Challenges of the Azure Public Cloud

At Connectria, integrity is everything.

When migrating your data and applications to the cloud, you have a lot of options to choose from. While we work with many different cloud vendors, we're not here to convince you that one platform is superior to any other. Instead, it's our mission to provide you with the information and guidance you need to make an informed choice. At Connectria, we know it's not just the integrity of your data on the line. It's our integrity as well. Thank you for choosing us to be part of your journey.

CONNECTRiA

Microsoft gaining ground

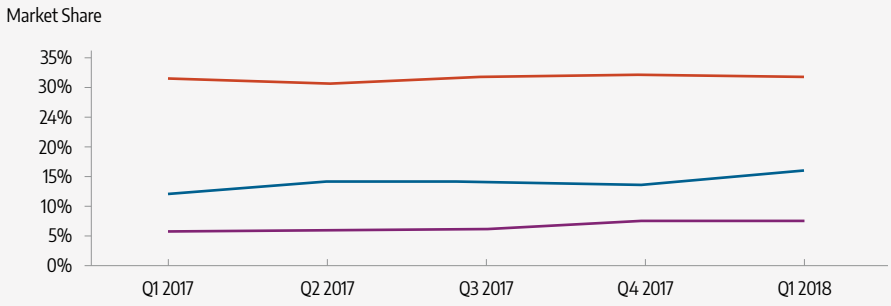
Microsoft Azure was launched in 2010 as a cloud-computing service enabling businesses and developers to build, deploy, and manage applications across a global network of Microsoft-managed data centers.

While Amazon AWS's significant head start in the market has translated into a substantial advantage in market share, Azure's growth now outpaces both AWS and Google. In their Q4 FY 2018 earnings statement, Microsoft reported that revenue generated from Azure had grown by 89% compared to Q1 FY 2017. This growth is similar to that which they reported the previous year and nearly double that of AWS for the same time period.[1]

The rate of Azure adoption is fueled by several factors:

- Microsoft has the advantage of an enormous installed base with strong enterprise ties.
- Many enterprises are drawn to a hybrid cloud platform that integrates well with their existing Microsoft-centric on-premises infrastructure.
- Microsoft continues to invest heavily in the Azure platform, adding new services to an aggressive roadmap.
- Microsoft is channel-friendly and committed to the success of its cloud resellers and the managed services providers (MSPs) that make Azure one of the most accessible public cloud platforms on the market today.
- Some customers view Amazon as a direct competitor in their markets, and therefore, don't wish to depend on a competitor for customer-direct services.

Top 3 players account for 55% of total market



Worldwide cloud infrastructure services

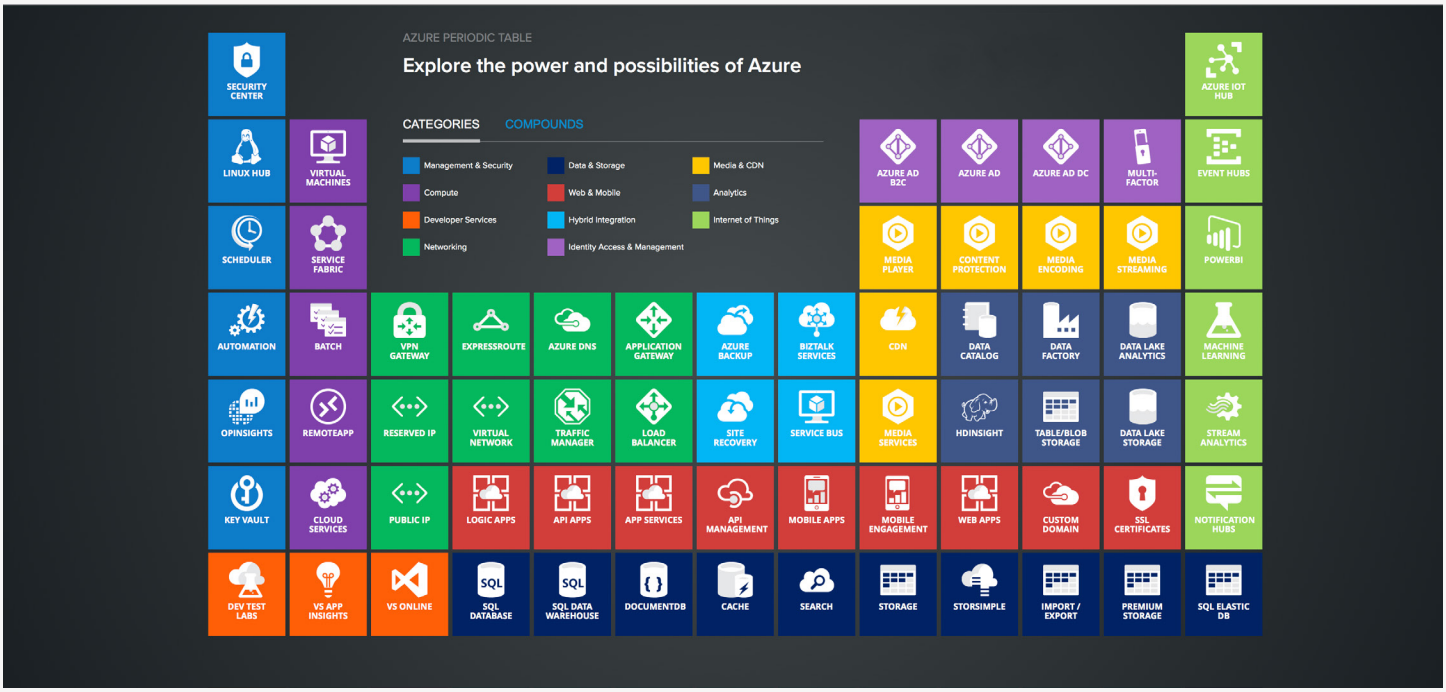
Q1 2017: **US$11.5 billion**
Q1 2018: **US$16.9 billion**
Growth: **46.8%**

Source: Canalys estimates, Cloud Analysis, April 2018

[1] McAfee, Cloud Market Share 2018: AWS vs Azure vs Google ¬– Who's Winning?

CONNECTRiA

However, as feature-rich as Microsoft Azure is, public clouds can be complex to set up and manage. This is especially true for enterprises that must maintain strict adherence to privacy regulations or other industry standards. The challenge is exacerbated by the current shortage of skilled technicians and the high cost of hiring and retaining qualified staff in full-time positions.



Source: Concurrency.com

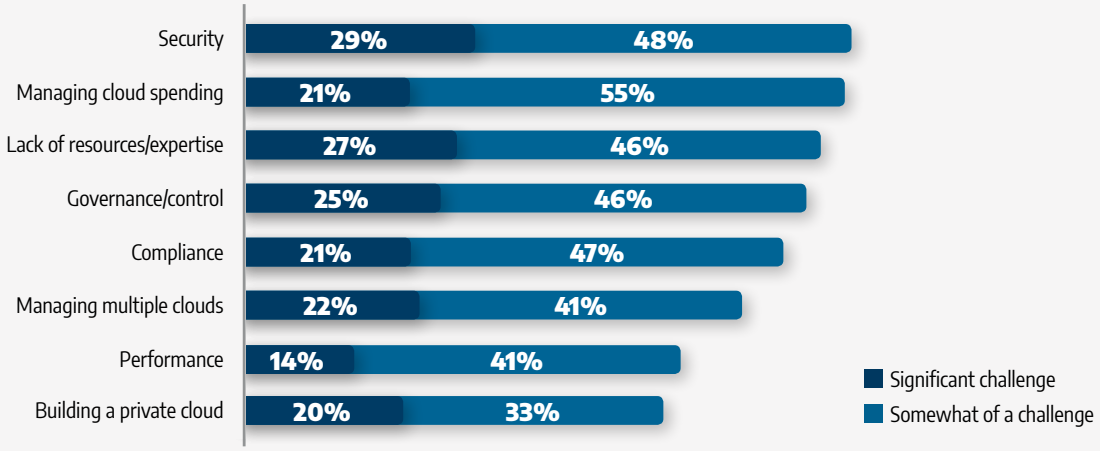
Trust increasing but businesses still reluctant to adopt the public cloud

There is no doubt that businesses are becoming more comfortable with the idea of placing mission-critical workloads in the public cloud. In a 2017 McKinsey study, less than half (40%) of companies had more than 10% of their workloads in the cloud. However, 80% planned to have more than 10% in the cloud within three years.

The low penetration of workloads in the public cloud is a sure sign that business leaders aren't yet as comfortable with the public cloud as they are with on-premises and private hosted clouds. However, the dramatic jump in the planned public cloud penetration shows that the benefits of the public cloud (flexibility, cost savings, etc.) are causing many to take a second look. In addition, the RightScale 2018 State of the Cloud Report found that 92% of businesses have at least some workloads in the public cloud, and 21% are using the public cloud only.

Clearly, trust in the public cloud is improving, but whether or not these business leaders realize their plans for leveraging the public cloud (or exceed them) will depend in large part of whether or not they can overcome their remaining concerns.

Cloud Challenges



Source: RightScale 2018 State of the Cloud Report

We can break these concerns down into three main categories: security and compliance, performance, and cost-optimization. When an organization considers moving a workload to the cloud (any cloud), they typically need to ask three primary questions:

- Can I meet my security and compliance obligations using this cloud?
- Will I get the performance I need?
- How can I be sure I am realizing the greatest return for my investment?

As you'll see from the rest of our discussion, a fourth, vital question that goes beyond the capabilities of the platform also needs to be asked:

- Do I have access to the in-house or 3rd party skills I need to stand up and maintain these cloud resources in a way that best helps me achieve my objectives and mitigate my risks?

In this white paper, we will address the three main concerns in the context of the Azure cloud platform by looking at the capabilities of the platform itself and the skills you will need to have or acquire in order to safely and securely take advantage of the Azure public cloud.

7 Signs You May Need Help With Your AWS Deployment

Deploying workloads in a public cloud can be hazardous if your team doesn't have the right skills and experience. Here are seven common scenarios where getting at least some outside help might be a good idea:

1. **This is your first foray into public clouds.** Azure offers hundreds of options. A qualified managed service provider can help ensure you get the features you need without paying for those you don't.
2. **You are in a highly regulated industry.** No cloud is inherently compliant. A managed service provider that understands BOTH the public cloud and your industry can help you avoid costly mistakes.
3. **Your IT team is already stretched thin, and IT infrastructure management isn't your forte.** Outsourcing some or all of your cloud deployment and day-to-day administrative tasks to a qualified managed service provider can help you better utilize your in-house resources and talent.
4. **You're having a hard time finding and retaining qualified talent.** A managed service provider who knows the public cloud can help you fill a need while you search for the right candidates.
5. **You don't have the resources to monitor your systems 24x7 for potential breaches and security violations.** When you're stretched thin, your team may not be as attentive as they need to be. A managed service provider can help you plug the holes in your security defenses.
6. **You want to spread workloads across multiple clouds while preserving connections between workloads.** This can be challenging even for a seasoned IT professional. Working with a qualified managed service provider can help you avoid spinning your wheels.
7. **You're thinking of migrating legacy workloads to the cloud.** A qualified managed service provider can help you find the safest, securest, most cost-effective cloud solution for these workloads and applications.

Security & compliance

We start with security and compliance because it is, hands down, the most pressing challenge for today's businesses. The consequences of failure are just too great.

Let's begin with an aspect of security that is often overlooked: physical security. If you're managing your own on-premises data center, the responsibility for guarding against the physical theft of your data or accidental destruction through vandalism or a natural event is yours alone. Microsoft removes these concerns with state-of-the-art data centers that comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability.

Microsoft's layered approach to physical security reduces the risk of unauthorized users gaining physical access to your data and data center resources. Data centers managed by Microsoft have extensive layers of protection including access approval at the facility's perimeter, the building perimeter, inside the building, and on the data center floor. In fact, Microsoft has an entire division devoted to designing, building, and operating the physical facilities supporting Azure.

Obsolete equipment can create a security risk, even if you're not the one responsible for disposing of it. Microsoft follows a rigorous disposal process that includes a NIST 800-88 compliant wiping solution. For hard drives that can't be wiped, Microsoft uses a through destruction process that destroys the drive and renders the recovery of information impossible.

When it comes to cyber-security, Microsoft takes a more nuanced approach that reflects their wide range of services across infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Many applications are subject to compliance regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for healthcare and the Payment Card Industry Data Security Standard (PCI DSS) for commerce. If your application handles protected health information (PHI) or data on credit card holders, failure to comply with regulations may result in significant fines or loss of business or reputation. Moving your workloads to Azure does not relieve you of this responsibility.

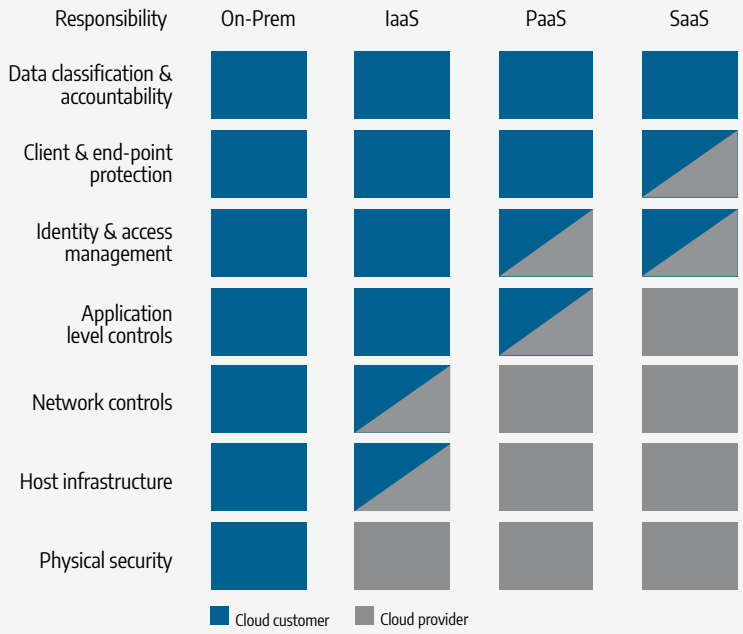
Improper security settings can lead to big problems when working within the cloud. You should regularly perform security checks to ensure that permissions are set correctly and that appropriate policies are in place. Security groups that allow dangerous ports or are open to the internet should be checked along with network access control list (ACL) rules. You should ensure that password policies are in place and encryption is being utilized.

With responsibility for their data, applications, etc. falling on their shoulders, business leaders need to make an honest assessment of their in-house security and compliance skill sets and tools before migrating workloads to Azure.

Here are just a few of the things you'll need:

- A team that understands both your security and compliance requirements as well as the Azure platform.
- 24x7 monitoring to alert you of potential intrusions into your cloud environment.
- Periodic vulnerability scans to identify weak points that need to be addressed.
- A comprehensive application, database, and OS management strategy that ensures the latest security updates are implemented in a timely manner.
- Antivirus and antimalware solutions for each of your instances.
- Scans and rescans of your instances after application installations or upgrades and for any discoveries to be remediated.

Shared responsibilities for different cloud service models



Source: Microsoft white paper: Shared Responsibilities for Cloud Computing, April 2017.

Performance

Performance includes both the availability of resources and speed. At 99.9%+ for the majority of Azure services,[2] Microsoft's SLAs are right in line with most reputable providers. While Cloud Harmony reports Microsoft's actual downtime for outages over the last three years to be higher than either Amazon or Google,[3] Microsoft claims the numbers to be misleading given that they have a far greater number of regions.

Microsoft issued a statement to that effect saying, "Microsoft has 34 Azure regions online worldwide, more than any other provider. When looking at average uptime across regions, rather than total downtime across a disproportionate amount of regions for each provider, Azure reliability is in line with that of the other cloud providers measured and in fact has consistently had global uptime upwards of 99.9979% for Compute in the past 12 months alone. What we hear from our customers is that uptime is a more useful measure of availability."

Our stance is this: Although all cloud providers are subject to unplanned outages, Azure's track record as of the publication of this paper exceeds its guarantees and is higher than the uptime found in most on-premises data centers.

Speed has historically been the greater performance concern when it comes to public clouds. The term "public" inherently means you are sharing resources as opposed to enjoying your own private, dedicated connections and compute resources. Noisy neighbors, other customers who periodically and unpredictably hog bandwidth, can lower your performance at times when you need it most.

To address the needs of customers with stringent performance requirements, Microsoft offers Azure ExpressRoute, which lets you create private connections with bandwidths speeds up to 100Gbps between Azure data centers and your on-premises or third-party infrastructure. With Azure DevOps you can also load test your applications before releasing them, helping you avoid performance issues and unplanned downtime due to application overload on day one.

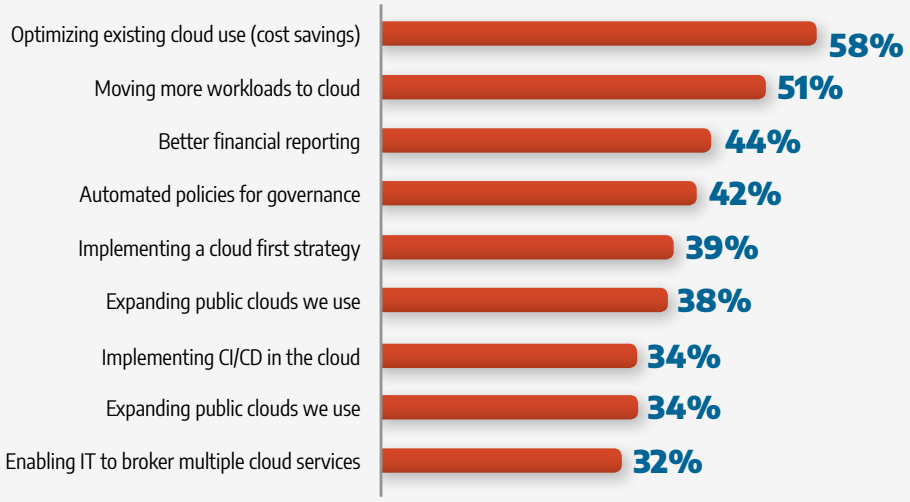
Microsoft may also have a slight edge in database performance as well, perhaps due to its decades of experience developing SQL tools. In tests performed by GigaOm Research, Azure SQL Data Warehouse ran 30 TB workloads at least 67% faster than Amazon Redshift.

For the majority of users, however, getting the performance they need out of the public cloud is a matter of understanding implementation best practices and knowing which features of Azure will meet their performance needs. Your infrastructure should be regularly scanned to ensure that resources are properly configured and set up to take advantage of Azure's high-availability architecture. Snapshots of Azure Storage resources should be reviewed to make certain they are recent. In order to ensure the high availability of resources, service limits, along with regional distribution of resources, should be monitored.

[2] As of March 2018, See the SLA summary for Azure services for more details
[3] How AWS Stacks Up Against Rivals on Downtime, The Information, Mar 7, 2017

With so many services within Azure, it can be a daunting task to ensure that all of them are used correctly. Implementing checks to identify underutilized services is critical. It is also important to ensure that Azure Autoscale launch configurations are configured correctly and that unused resources like key pairs, NSGs, and Azure Portal alarms are identified. These are only a few of the hundreds of checks that should be run against your Azure instances. Following best practices like these can greatly improve performance within your environment—and help you save money.

Cloud Initiatives in 2018



Source: RightScale 2018 State of the Cloud Report

Cost-optimization

Optimizing existing cloud use was the top cloud initiative cited by respondents to the 2018 State of the Cloud Report. That's not surprising given that respondents estimated they wasted approximately 30% of their cloud spend.

Azure offers a large number of services and an almost infinite number of ways to configure them around your application deployment. The challenge for most organizations is knowing how to configure the environment in the most cost-effective way, yet one that meets their security and performance requirements as well . The sheer number of options can easily lead to a configuration that isn't the most cost-effective.

Monitoring usage is also vital to cost-optimization. It can be easy to forget about a deployed resource that might no longer be needed, and you can easily rack up unnecessary charges. For example, you may have page blobs that are not attached to any resources. And if you are not aware of older generation resources which can be migrated to a new generation, you may be missing out on more power at a lower cost.

The bottom line

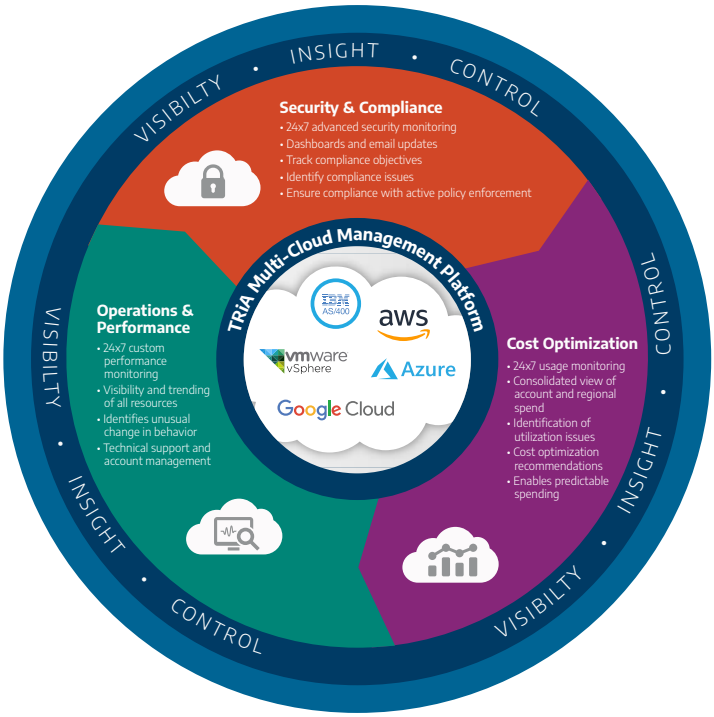
There are many benefits to moving workloads to Microsoft Azure. Within a matter of minutes, you can establish compute and storage capacity, paying for only the resources you use. Azure can provide your organization with a high degree of speed, agility, and flexibility for both development and production environments. Moving workloads to Azure allows you to shift the burden of capital investment and data center maintenance to Microsoft, leaving you to focus your efforts on building and running applications. And Azure can provide a cost-effective solution for disaster recovery that minimizes downtime and data loss.

There are some challenges, however, that must be considered. Moving to and managing Azure environments requires a knowledgeable staff. Your environment must be continuously monitored to ensure it is performing as expected. Should problems arise, root causes need to be identified and addressed. Your applications and data are crucial to your business and must be protected. Automation tools are great, but they will not address all security concerns alone. While Azure allows for varying resource demand and capacity, left unchecked, your environment can cost you more than it should.

If you have the expertise and resources to address these concerns, you're in good shape. If not, you may wish to consider an Azure managed service provider with the requisite knowledge and experience to assist you in getting the most out of your Azure environment. Many businesses find partnering with an expert, reputable provider to be a fraction of the cost of building these capabilities and staff on their own.

Managed clouds, powered by TRiA™

Connectria's Managed Clouds let you deploy your applications and data in the environment best suited to your needs without having to worry about staffing up resources to ensure you meet your compliance, performance, and cost objectives. Our team of AWS Cloud experts operates as an extension of your IT team, providing as much or as little assistance as you need. We will help you set up your Azure environment, choosing the options that meet your unique needs. And when your needs change, our cloud experts can help you transition workloads from one cloud to another.



All of our managed cloud solutions are powered by TRiA™, a unique multi-cloud platform that provides a single unified view of all of your cloud environments to provide ultimate visibility and control. With the TRiA Multi-Cloud Management Platform, you can monitor your systems 24x7 to track security and compliance and ensure real-time enforcement of policies as well as monitor the performance of your cloud assets, resource utilization, and regional spend.

Our team of experts will even help manage your costs by monitoring usage and looking for unused, underutilized, or inappropriately used resources. We then provide monthly reports and guidance on how best to optimize your spend, so you get the most for your investment.

About Connectria

From Fortune 100 enterprises to medium and small businesses, Connectria provides managed cloud, managed services, and compliant cloud security solutions to more than 1,000 global customers. Working as an extension of each customer's IT team, we deliver technology-agnostic solutions consistently, with depth and breadth of engineering expertise, scalable solutions, and speed to market. Our "No Jerks Allowed®" philosophy includes flexible terms, straight-forward pricing, and custom solutions. With a culture based on integrity and an unwavering employee commitment to treating every customer with a relentless focus on satisfaction, it's easy to do business with Connectria.

NO JERKS JERKS ALLOWED®

Connect with us today

Talk to one of our IT advisors by calling **800.781.7820** or reaching out to us by email: **sales@connectria.com**.

CONNECTRiA