

# Overcoming the Top Three Challenges of the AWS 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.

### AWS: In a League of its Own

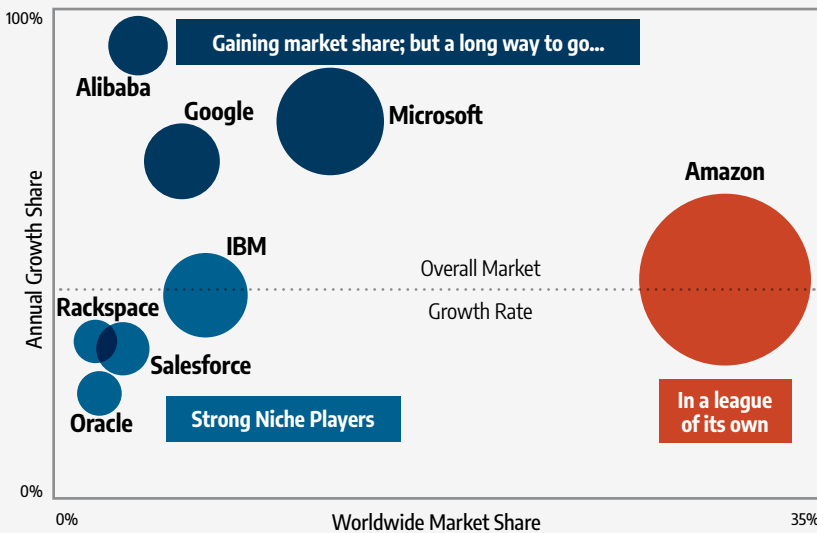
Amazon Web Services (AWS) was launched in 2006 as a web services platform for enabling businesses and developers to build scalable, sophisticated applications. Today, AWS is the undisputed leader in cloud services. While its three closest competitors, Microsoft, Alibaba and Google, are growing faster than the overall market, Amazon still managed to raise its market share up from 34% to 35% overall in the second quarter of 2018.<sup>1</sup>

AWS achieved success by providing a feature-rich public cloud, where customers could provision compute and storage capacity in a matter of minutes, paying for only those resources which they used. This model provides customers with a high degree of speed, agility and flexibility. AWS also shifted the burden of capital investment and maintaining data centers to Amazon, allowing enterprises to focus their efforts on building and running their business, not the data center.

However, as feature-rich as the AWS public cloud is, it can be complex to implement and administer. 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.

## Cloud Provider Competitive Positioning

(IaaS, PaaS, Hosted Private Cloud - Q2 2018)



Source: Synergy Research Group

<sup>1</sup>Synergy Research Group, Cloud Revenues Continue to Grow by 50% as Top Four Providers Tighten Grip on Market, July 2018.

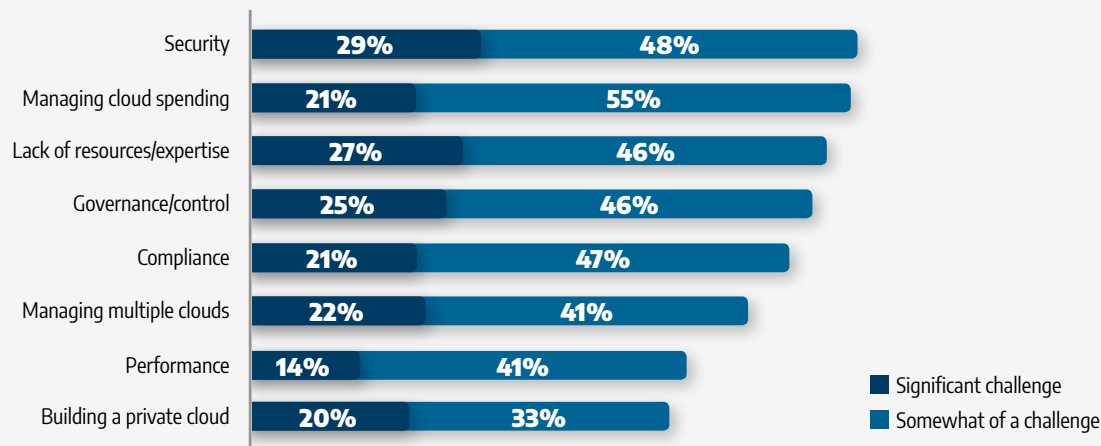
### Trust Increasing But Businesses Still Reluctant to Adopt the Public Cloud

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 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 finds 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 ask three main 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 AWS 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 AWS 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.** AWS 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 public cloud deployment and day-to-day administrative tasks to a qualified Managed Service Provider lets 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 old-fashioned physical theft of your data or accidental destruction through vandalism or a natural event is yours alone. AWS removes these concerns with state-of-the-art data centers that comply with industry best practices such as:

- Nondescript facilities that don't invite trouble.
- Strictly controlled physical access at both the perimeter and ingress points by multiple means: physical security staff, video surveillance, intrusion detection systems, etc.
- Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.
- All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
- Immediate revoking of credentials when an employee (or former employee) no longer has need for access privileges.
- Routine physical access logging and auditing.

Source: Amazon Web Services: Overview of Security Processes, May 2017

When it comes to cyber-security, AWS takes a more nuanced approach, distinguishing between security "of" the cloud and security "in" the cloud. 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 to AWS does not relieve you of this responsibility, nor can you fully transfer this responsibility to AWS partners.

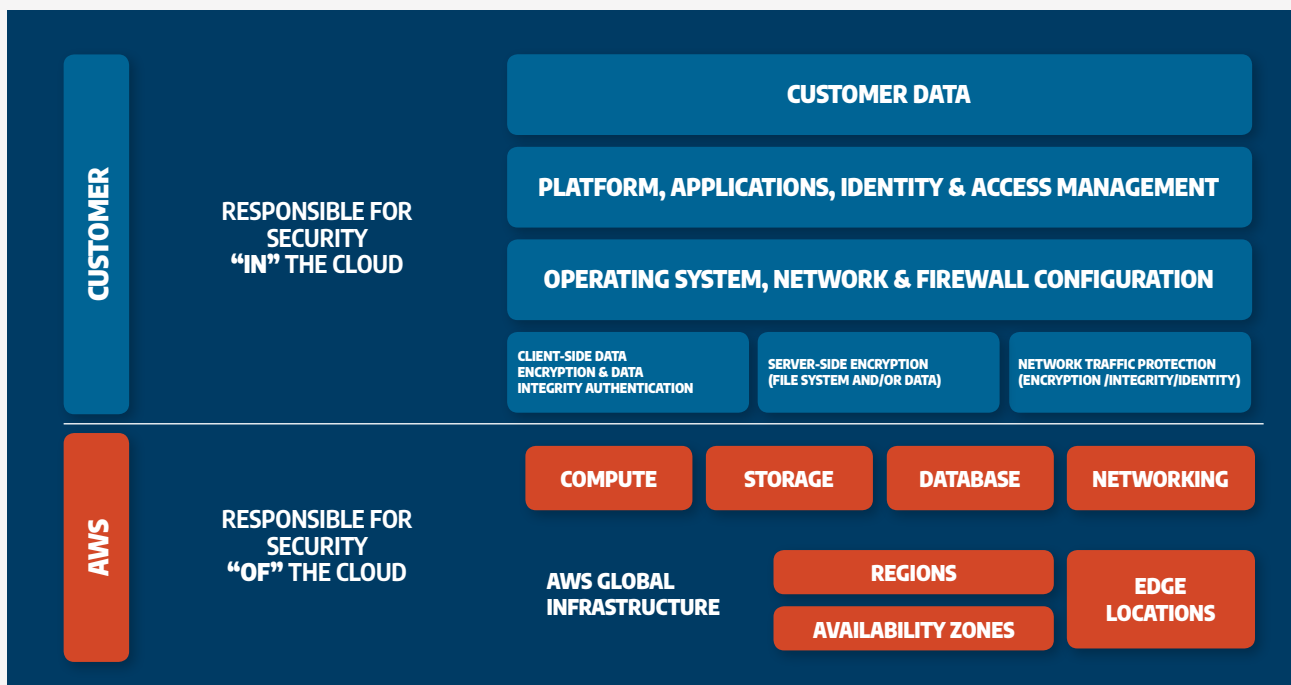
Improper security settings can lead to big problems when working within the cloud. You should regularly undergo security checks to ensure that permissions are set correctly and appropriate policies are in place. Important services like AWS CloudTrail, AWS Config and Amazon Virtual Private Cloud (Amazon VPC) flowlogs must be set up correctly. Security groups that allow dangerous ports or are open to the internet should be checked along with network ACL rules. You should ensure 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 AWS.

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

- A team that understands both your security and compliance requirements and the AWS 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.

## AWS Shared Responsibility Model



## Performance

Performance can include both availability of resources and speed. At 99.99%<sup>2</sup>, AWS's uptime SLAs are right in line with most reputable providers. In 2018, Amazon had a total downtime across all of their regions of only 108 minutes.<sup>3</sup> Downtime does happen, but Amazon is on par with, and depending on how you interpret the numbers, performing even better than its closest rivals.

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, AWS offers services like AWS Direct Connect, which lets you establish a direct connection to one of AWS's direct connect locations. They also offer specialized services such as High Performance Computing (HPC), a service designed for scientific and engineering applications that require high network performance, fast storage, large amounts of memory and very high compute capabilities.

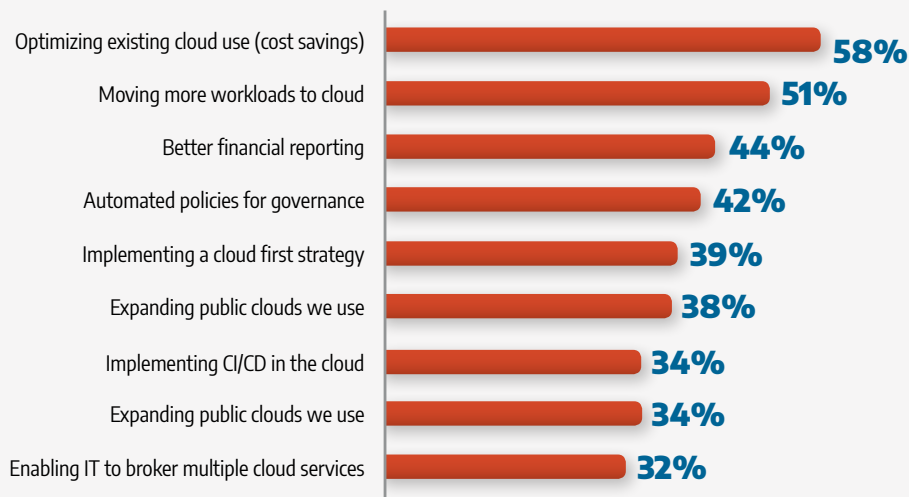
For the majority of users however, getting the performance you need out of AWS is a matter of understanding implementation best practices and knowing which features of AWS will allow you to get the most out of the cloud platform. Your infrastructure should also be regularly scanned to ensure that resources are properly configured and set up to take advantage of AWS's high availability architecture. Snapshots of Amazon Elastic Block Storage (EBS) volumes should be reviewed to make certain they are recent, and service limits should be monitored along with availability zone distribution of resources like Amazon Elastic Cloud Compute (EC2), Amazon Relational Database Service (RDS) and AWS Application Auto Scaling.

<sup>2</sup> As of February 12, 2018.

<sup>3</sup> The Information.com, How AWS Stacks Up Against Rivals on Downtime, Mar 2017.

Finally, with so many services within AWS, it can be a daunting task to ensure that all services are used correctly. Implementing checks to identify underutilized services like Amazon EC2, RDS and DynamoDB are critical. It is also important to ensure Application Auto Scaling launch configurations are configured correctly and unused resources like key pairs, security groups and Amazon CloudWatch alarms are identified.

## Cloud Initiatives in 2018



Source: RightScale 2018 State of the Cloud Report



## Cost-Optimization

Optimizing existing cloud use (cost savings) 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.

AWS 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 choosing options that aren'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. If you are not continuously monitoring resources like Amazon EC2, RDS, DynamoDB and others, you may be incurring unnecessary charges. For example, you may have Amazon EBS volumes which are not attached to any resources. And if you are not aware of older generation resources which may be migrated to a new generation, you may be missing out on more power at a lower cost.

All On-Demand Instances should also be reviewed regularly to see if they should be converted to Reserved Instances to take advantage of the lower pricing. On-Demand Instances that are stable and will be in use for at least six months are good candidates for conversion.

## The Bottom Line

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

There are some challenges, however, that must be considered to enjoy these benefits. Moving to and managing AWS environments requires a knowledgeable and available staff. Your environment must be continuously monitored to ensure it is performing as expected. Should problems arise, they need to be identified and resolved. 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 AWS allows for varying resource demand and capacity, left unchecked, your environment can cost you more than it should.

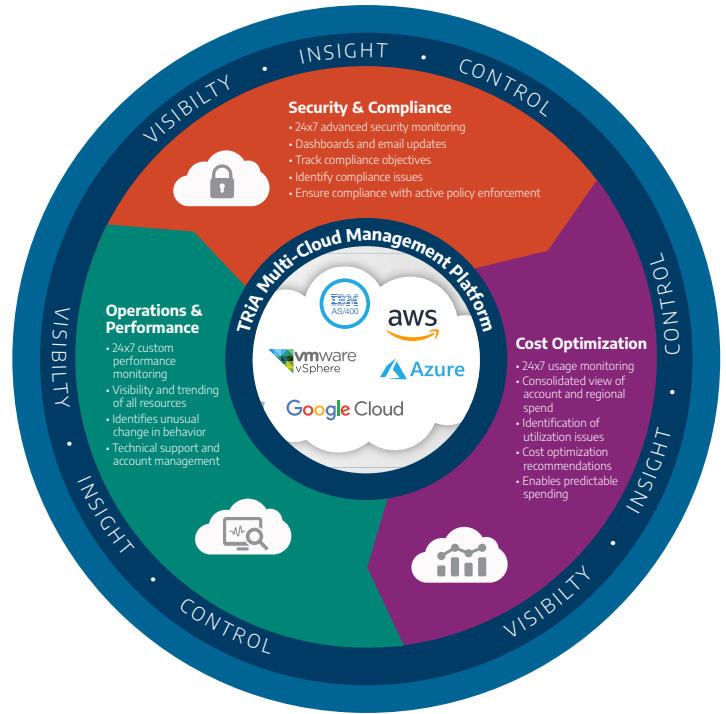
If you have the expertise and resources to address these concerns, you're in good shape. If not, you may wish to consider an AWS Managed Service Provider with the requisite knowledge and experience to assist you in getting the most out of your AWS environment. You'll find partnering with an expert, reputable provider to be a fraction of the cost of building these capabilities and staff on your 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 AWS 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.



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](mailto:sales@connectria.com).

