Amazon Web Services Information Package Canada

June 2017

This Amazon Web Services, Inc. (AWS) package is provided for informational purposes only. The services included in this package are standard commercial services and due to the unique nature of the services, AWS's standard terms and conditions must govern any use of and access to AWS services and are available at http://aws.amazon.com/agreement/. For current prices for AWS services, please refer to the AWS website at www.aws.amazon.com.

Table of Contents

Tables & Figures

1.0 AWS Overview

Amazon has a long history of using a decentralized IT infrastructure. This has enabled our development teams to access compute and storage resources on demand, increasing overall productivity and agility. By 2005, Amazon had spent over a decade building and managing the large-scale, reliable, and efficient IT infrastructure that powers one of the world's largest online retail platforms. Amazon launched Amazon Web Services, Inc. (AWS) so that other organizations could benefit from Amazon's experience and investment in running a large-scale, distributed, transactional IT infrastructure. AWS has been operating since 2006 and currently supports an almost limitless variety of workloads for millions of customers worldwide.

The University of Western Australia
NDI
GeoNet
Transport for London
Open Universities Australia
esa
Singapore Post
東京大学 The University of Tokyo
swisstopo
City of Melbourne
echo360
MIT Massachusetts Institute of Technology
PBS
JustGiving
CDC
UCAS
NREL
National Institutes of Health
Multnomah County
Zooniverse
FDA
USDA

Figure 1 – Snapshot of Public Sector Customers

The AWS Cloud is uniquely positioned to provide scalable, cost-efficient solutions to the Canadian public sector, helping find ways cloud services can be employed to meet mandates, reduce costs, drive efficiencies, and increase innovation. Over 2,300 government agencies are already using AWS to address a diverse set of use cases, from complex government systems to mission-critical intelligence projects dealing with large volumes of sensitive data. The AWS Cloud is also used by 7,000 educational institutions and 22,000 nonprofits. Case studies about government agencies and educational institutions migrating to the AWS Cloud can be found at https://aws.amazon.com/solutions/case-studies/government-education/.

AWS offers a broad set of global compute, storage, networking, database, analytics, application services, deployment, management, developer, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid and enterprise applications, all of which are listed at http://aws.amazon.com/products/. **Figure 2** on the following page is a simple view of the AWS Cloud and associated services. AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS Application Programming Interface (API)-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools: http://aws.amazon.com/tools/.

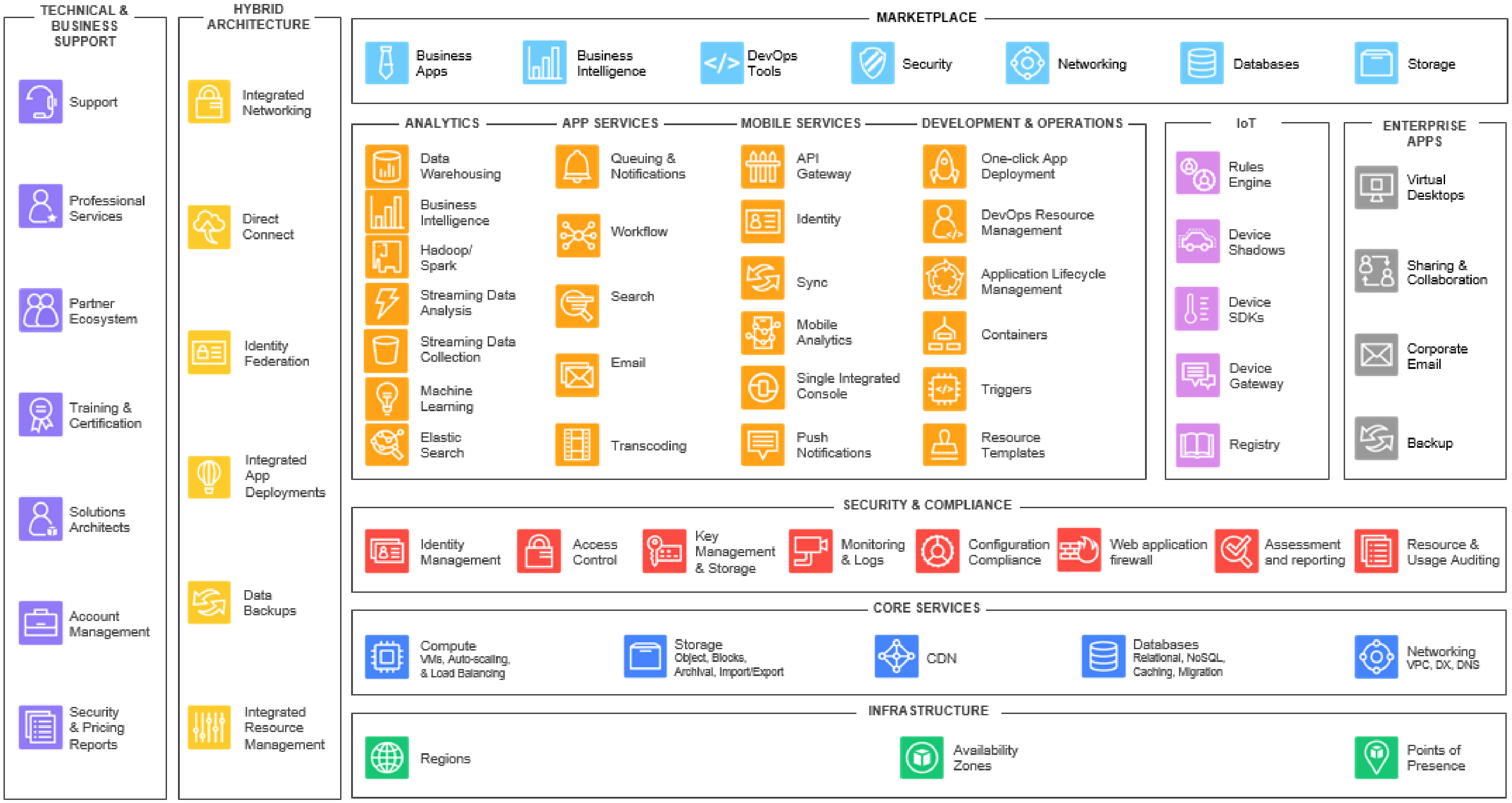


Figure 2 – High-Level View of the AWS Cloud

All of AWS' cloud services are hosted within our global data centre footprint, allowing customers to consume services without having to build or manage facilities or equipment. AWS Cloud services are offered in separate Regions in a number of separate geographic areas. A Region is a physical location in the world where we have multiple, isolated locations known as Availability Zones (AZs) that are engineered to be isolated from failures in other AZs (see **Figure 3** below). AZs consist of one or more discrete data centres, each with redundant power, networking, and connectivity, and housed in separate facilities.

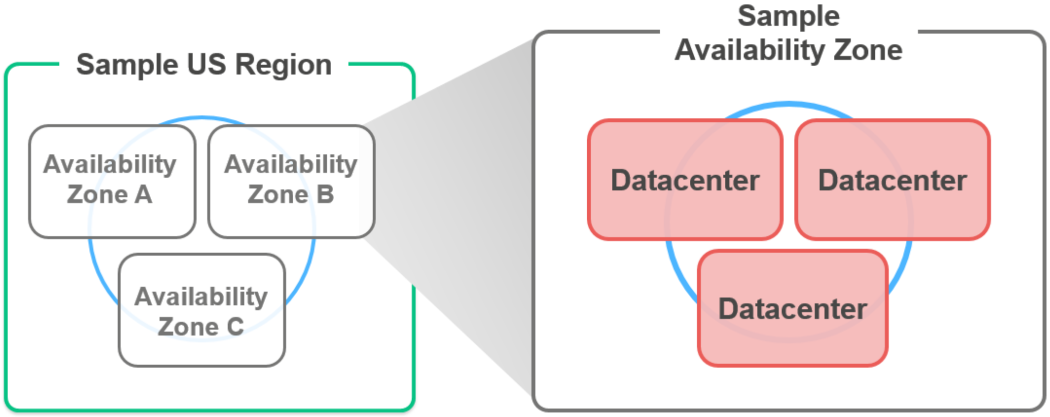


Figure 3 – AWS AZs consist of 1+ data centres. Every AWS Region contains 2+ AZs. Some Regions have as many as 5 AZs.

AZs are engineered to be isolated from failures in other AZs, and to provide inexpensive, low-latency network connectivity to other zones in the same Region. By launching instances in separate AZs, you can protect your applications from the failure of a single location. AZs offer the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data centre.

AWS provides customers with six North American Regions:

- Canada (Central)
- US East (Northern Virginia)
- US East (Ohio)
- US West (Northern California)
- US West (Oregon)
- AWS GovCloud (US)

AWS North American Regions and Amazon CloudFront Edge Locations

AWS provides customers the flexibility to place instances and store data within multiple geographic Regions as well as across multiple AZs within each Region. You decide which AWS Region(s) house your data, and it resides only in the Region(s) you specify, for as long as you choose. For example, AWS has the capability to host and provide services in Canada via the Canada (Central) Region in Montreal, Québec.

The Canada (Central) Region is carbon neutral, and continues AWS' focus on delivering cloud technologies to customers in an environmentally friendly way. In fact, AWS data centres in Canada draw power from a regional electricity grid that is 99 percent powered by hydropower. Additionally, Canada is home to Amazon CloudFront edge locations in Toronto, Ontario, and Montreal, Quebec, which is important for customers delivering websites, applications, and content to Canadian end users with low latency.

Network latency metrics to other Canadian cities are:

- 9 ms to Toronto
- 14 ms to Ottawa
- 47 ms to Calgary
- 49 ms to Edmonton
- 60 ms to Vancouver

Metrics to locations in the US:

- 9 ms to New York
- 19 ms to Chicago
- 16 ms to US East (Northern Virginia)
- 27 ms to US East (Ohio)
- 75 ms to US West (Oregon)

We are steadily expanding global infrastructure to help our customers achieve lower latency and higher throughput. As our customers grow their businesses, AWS will continue to provide infrastructure that meets their global requirements. The AWS products and services that are available in each Region are listed at http://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/.

Figure 4 displays AWS' 16 global Regions and 43 Availability Zones. At least 4 more AWS Regions (and 11 Availability Zones) in France, Sweden, Hong Kong, and China are coming online throughout 2017 and 2018.

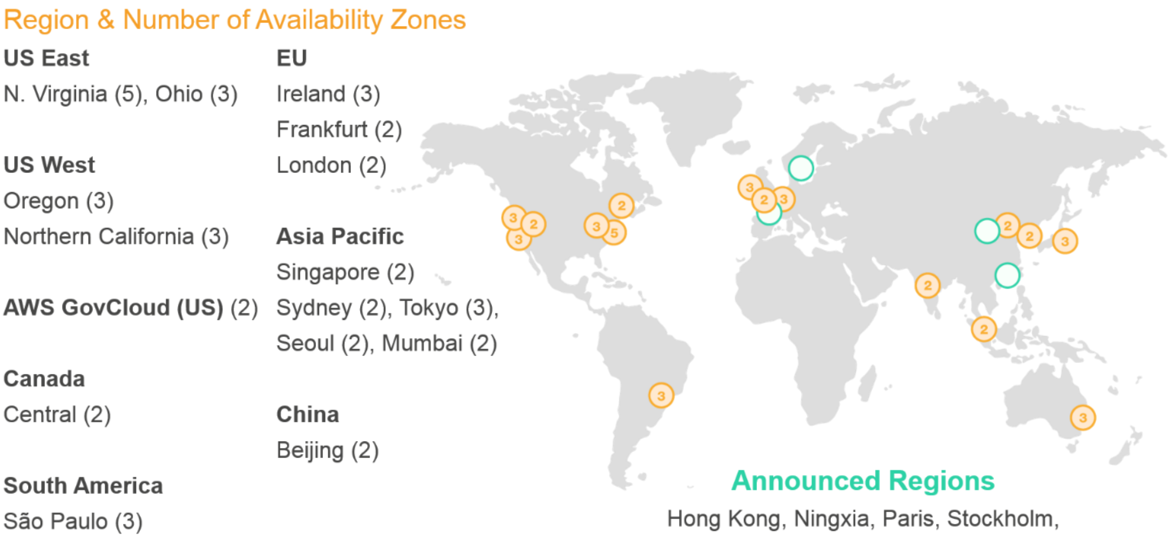


Figure 4 – AWS' Global Infrastructure Consists of 16 Regions and 43 Availability Zones.

2.0 Benefits of Cloud Computing

Table 1 highlights the benefits of cloud computing, many of which are unique to the AWS Cloud.

Table 1 – Benefits of the Cloud

Benefit of Cloud	Benefit to Customers
Trade Capital Expense for Variable Expense	The fundamental difference between cloud computing and traditional IT is that in a cloud model customers are not buying physical assets. Instead of having to invest heavily in data centres and servers before you know how you're going to use them, you can use cloud computing and only pay for the resources you consume. The primary benefit of this approach lies in optimization, and not having to invest heavily in physical data centres and servers, which inevitably leads to limited capacity or idle resources.
Access to Greater Service Breadth and Depth	Cloud computing allows you to access industry-shaping technology quickly, at an affordable cost, no matter what the scale. AWS has developed the broadest collection of services available from any cloud provider. We have been continually expanding our services to support virtually any cloud workload, and now have more than 90 services that range from compute, storage, networking, database, analytics, application services, deployment, management, IoT, AI, mobile and more. Refer to the Gartner: Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, August 2016 for a third-party assessment of AWS' broad service offerings.
Scalability	When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little as you need and scale up and down as required with only a few minutes' notice. Combining software-defined infrastructure with AWS products featuring modern programming methods lets you design your computerized systems to

rapidly scale resources (and costs) up or down based on actual demands on the system.

Increase Speed and Agility

In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

Global Footprint

Cloud computing allows you to easily deploy applications in multiple Regions around the world with just a few clicks, providing lower latency and a better experience at minimal cost.

AWS' approach to Regions and Availability Zones provides global coverage for high-availability, low-latency applications. As noted above, an AWS Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centres, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data centre.

AWS currently has 16 Regions and 43 Availability Zones throughout the world (with at least 11 more Availability Zones and 4 more Regions coming online throughout 2017 and 2018). Information on each Region can be found at http://aws.amazon.com/about-aws/global-infrastructure/.

Benefit from Massive Economies of Scale

By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from millions of customers is aggregated in the cloud, AWS can achieve high economies of scale, which translates into lower, pay-as-you-go prices.

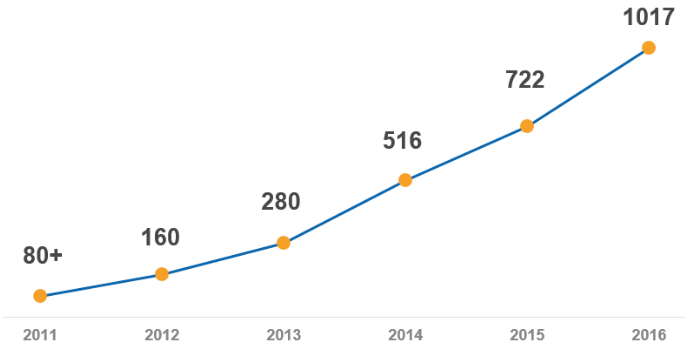
AWS continues to lower the cost of cloud computing for our customers. We continually focus on reducing our data centre hardware costs, improving our operational efficiencies, lowering our power consumption, and passing savings back to customers. We have a history of continually lowering prices, and have reduced prices 61 times since AWS launched in 2006.

Pace of Innovation

AWS is proud to be known as a "disruptor." Since our inception, AWS has been an innovator in defining cloud computing by working to get new products in the hands of customers quickly and then rapidly iterating and improving on those products based on customer feedback.

Because AWS Cloud services are provided on an on-demand basis, we endeavour to earn this customer trust one hour at a time. We focus on providing innovative services to our customers that make them want to continue to use AWS.

Our continual innovation ensures that customers maintain state-of-the-art IT infrastructure without having to make recapitalization investments. In addition, our rich ecosystem of third-party applications also



AWS has launched more than 3,000 new features and/or services since 2006.

	provides complementary functionality that further extends the power and breadth of the AWS environment.
Partner Ecosystem	Having consulting and technology partner support in place makes it much easier to deploy, adopt, and/or shift workloads to the cloud, and the strength of a partner ecosystem is crucial when selecting a cloud service provider (CSP). AWS has the largest ecosystem in the cloud, and it continues to grow at a rapid pace. The AWS Partner Network (APN) includes tens of thousands of the world's largest technology and consulting companies. AWS Marketplace offers 35 product categories and more than 3,800 software listings from more than 1,170 Independent Software Vendors (ISVs).
Security and Compliance	AWS customers obtain greater security in the cloud than is available in traditional data centres. The AWS Cloud infrastructure has been designed and managed in alignment with many regulations, standards, and industry best practices. AWS is under a constant state of audit to comply with multiple risk management and compliance regimes, all of which are described on the AWS Compliance page.
Segregation of Duties	Separating physical infrastructure responsibilities from customer virtual infrastructure and software responsibilities provides a critical data integrity control by ensuring that those with physical access are completely isolated from those with logical access to data.
Auditability	The message-based interoperability of web services allows customer configuration and use of AWS products to be uniformly logged, monitored, and audited.
Focus on Core Competencies	The ultimate benefit of the cloud is that customers can spend less time on undifferentiated tasks and more time focusing on the core competencies that add value to their organizations.

3.0 Cost Benefits of the Cloud

AWS offers a pay-as-you-go approach to pricing for over 90 cloud services. With AWS, you pay only for the individual services you need, for as long as you use them, without requiring long-term contracts or complex licensing.

Given that AWS has over 90 services, we advise customers to view the AWS Pricing webpage https://aws.amazon.com/pricing/ for pricing of each service, and to view the AWS whitepaper *How AWS Pricing Works*, which summarizes AWS' pricing methodology.

Some AWS pricing principles include:

- **Pay as You Go –** No minimum commitment or long-term contract is required. You can turn off cloud resources and stop paying for them when they are not needed, maximizing Return on Investment (ROI) through full utilization.
- **Pay Less When You Reserve –** For certain AWS products, you can invest in reserved capacity, paying a low up-front fee to receive a significant discount. This results in overall savings of up to 60% (depending on the type of instance reserved) over equivalent on-demand capacity.
- **Pay Even Less Per Unit by Using More –** AWS pricing is tiered for storage and data transfer, so the more you use, the less you pay per gigabyte.

Considerations regarding the cost savings benefits of the AWS Cloud compared to on-premises infrastructure include:

- **Stop Spending Money on Data Centre Operations –** Cloud computing vendors do the heavy lifting of racking, stacking, and powering servers, so you can focus on your customers and core business rather than on IT infrastructure.
- **Do more for less –** Moving to the cloud is not just an effort to increase cost savings and avoidance for the sake of the obvious monetary value; it is also about the increase in technological competitiveness that comes with it. If you can deliver twice the capability at the same cost, that equates to savings.
- **Benefit from economies of scale –** Millions of customers are aggregated in the AWS Cloud, which translates into lower, pay-as-you-go prices. We continually focus on reducing our data centre hardware costs, improving our operational efficiencies, lowering our power consumption, and passing savings back to customers. AWS has a history of continually lowering prices and has reduced prices 61 times since AWS launched in 2006.
- **Move from a forecast-procurement model to a consumption model –** Instead of investing more in optimizing data centres and servers, pay only for the resources you consume and increase or decrease usage depending on need, not elaborate forecasting. For example, development and test environments are typically only used for eight hours a day during the work week. You can stop these resources when they are not in use for a potential cost savings of 75% (40 hours versus 168 hours).
- **Transparently attribute expenditure –** The cloud makes it easier to identify the cost of a system and attribute IT costs to individual business owners. This helps measure ROI and gives those owners an incentive to optimize their resources and reduce costs, an important capability that allows oversight on IT revenue and expenditures.
- **Use Managed Services to Reduce Cost of Ownership –** In the cloud, managed services remove the operational burden of maintaining servers for tasks like sending email or managing databases. And because managed services operate at cloud scale, they can offer a lower cost per transaction or service.
- **Continuously Reevaluate Design Choices –** Unlike traditional IT infrastructure approaches where you are required to make large capital investments in hardware and software, AWS offers pay-as-you-go pricing for most of its services. This means you are not bound by decisions made at a design level at the beginning of a project’s lifecycle. This reduces the risks of overprovisioning or not being able to meet unexpected demand. You can continually reevaluate your design decisions. You can also explore the use of new AWS products to see if they lead to even greater efficiencies.

Additional considerations regarding the AWS pricing model and optimizing spend include:

- Compare the projected costs of both planned and new IT initiatives over 1, 3, 5 years (or whichever timeframe is appropriate for the initiative). Take into account that the costs that come with initial migration efforts (such as System Integrators [Sis] or managed services engagements) and how overall IT costs will normalize in the longer term.
- Consolidate accounts. When AWS customers consolidate accounts under a single bill it allows them to designate one account as a payer account and link other accounts to it. This provides a combined view of AWS charges incurred by all accounts, as well as a cost report for each individual account associated with a payer account. A benefit of this approach is that it treats all of the accounts on the consolidated bill as one account, meaning that all accounts on a consolidated bill can receive the hourly cost benefit of reserved resources purchased by any other account.
- Analysing spend and forecasting usage leads to predictable cloud budgeting. Monitoring tools and services (native AWS services such as Amazon CloudWatch and Cost Explorer, or third-party tools like Splunk, CloudCheckr, or Data Dog) can be used to analyze cloud usage and spending, and customers can build-in alerts to notify them when they approach customized usage thresholds and projected/budgeted spend. Such alerts enable customers to determine whether to reduce usage to avoid overages, or prepare additional funding to cover costs that exceed projected budget.
- Utilize AWS tools that automate service provisioning. This allows for optimal resource utilization, scaling up resources when needed then scaling down resources when they are not being used. The use of tools such as AWS Config, Amazon CloudWatch, AWS OpsWorks, Auto Scaling, and AWS CloudFormation will help ensure that resources are being used efficiently, but cost optimization is achieved through a continuous cycle of assessment, benchmarking, and integration with operations. More information on cost optimization is found in the AWS whitepaper Cost Optimization with AWS.
- Calculating a total cost of ownership (TCO) at the beginning of a cloud migration will help customers understand the costs and savings of the migration and to plan for them. AWS provides a TCO calculator to enable customers to compare the cost of running applications in an on-premises or traditional hosting environment to the cost of AWS. Customers can describe their on-premises or hosting environment configuration to produce a detailed cost comparison with AWS.

According to a 2015 International Data Corporation (IDC) report commissioned by AWS, “on average, organizations will reduce data centre hosting and infrastructure costs by 64.3%” by moving to the AWS Cloud. AWS’ TCO Team and Solutions Architects are happy to work with customers in estimating the potential cloud savings benefits of migrating to AWS in relation to customer targets.

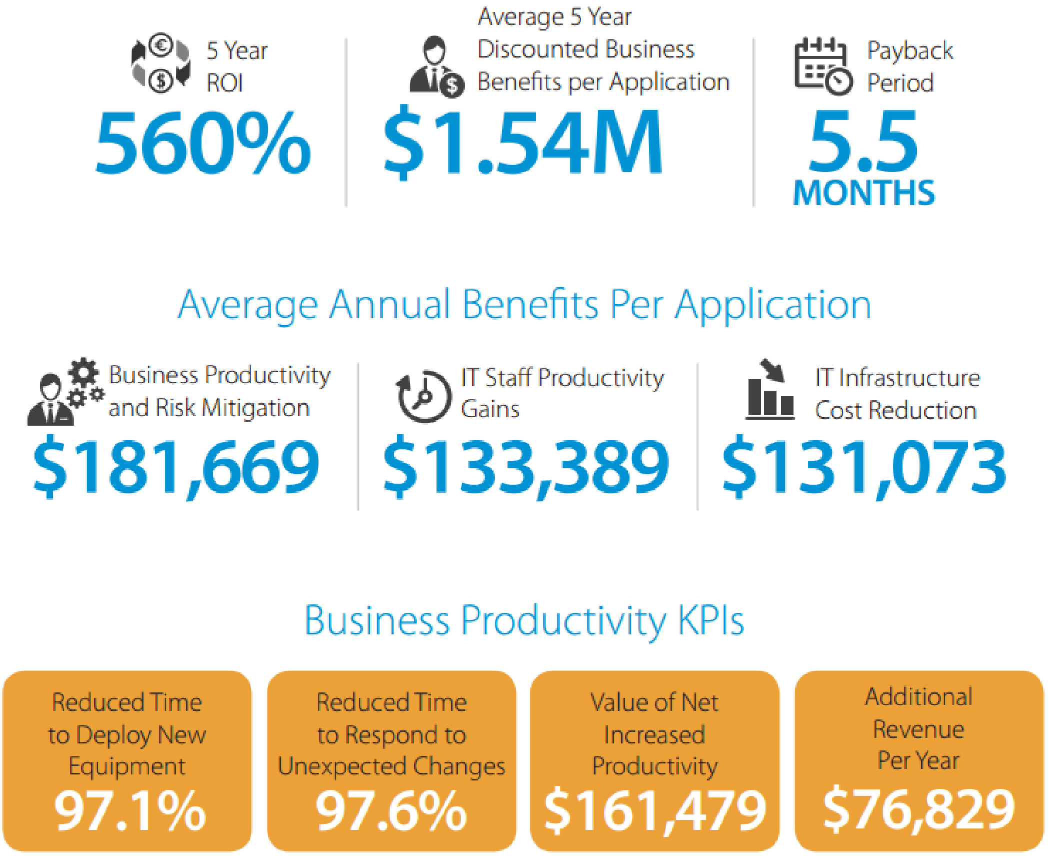


Figure 5 – IDC Whitepaper, sponsored by AWS, “Quantifying the Business Value of Amazon Web Services,” May 2015

3.1 Reserved Instances

As an example of paying less when you reserve, AWS customers can look to Reserved Instances to optimize costs in a cloud model. An AWS compute "instance" is a virtual server with CPU, memory, storage, and networking capacity. AWS offers four ways to pay for instances. In this example we focus on "On-Demand" instances and "Reserved Instances."

- With **On-Demand** instances, customers pay for compute capacity by the hour with no long-term commitments or upfront payments. You can increase or decrease compute capacity depending on the demands of an application, and only pay the specified on-demand hourly rate for the instances used. In essence this is the simple cloud pay-per-use model.

- **Reserved Instances** are best suited to customers with predictable compute usage, allowing you to reserve compute capacity and receive a discount on usage compared to running On-Demand instances. The discounted usage price is reserved for the duration of the contract, allowing customers to better predict compute costs over the term of the contract.

With Reserved Instances, customers can save up to 75% over equivalent on-demand capacity. Reserved Instances are offered on a 1-year or 3-year term, and are available in 3 options—all up-front (AURI), partial up-front (PURI) or no upfront payments (NURI). The larger the upfront payment, the greater the discount a customer receives. When the term of the Reserved Instance ends and a customer does not renew by purchasing another Reserved Instance, they can simply continue to use the same compute instance without interruption (it will then be charged at the On-Demand rate).

Additionally, AWS provides customers with a Reserved Instance Marketplace, so that if they find they have excess Reserved Instance capacity they can list it on the Marketplace and sell it to someone who needs additional capacity (an optimization of IT assets not possible in a traditional on-premises model). By advancing pay for IT (such as in the Reserved Instances example above) customers can predictably manage part of their IT budget in a fashion that is not too dissimilar to an on-premises model, while also gaining the cost savings and vast technological benefits of the cloud.

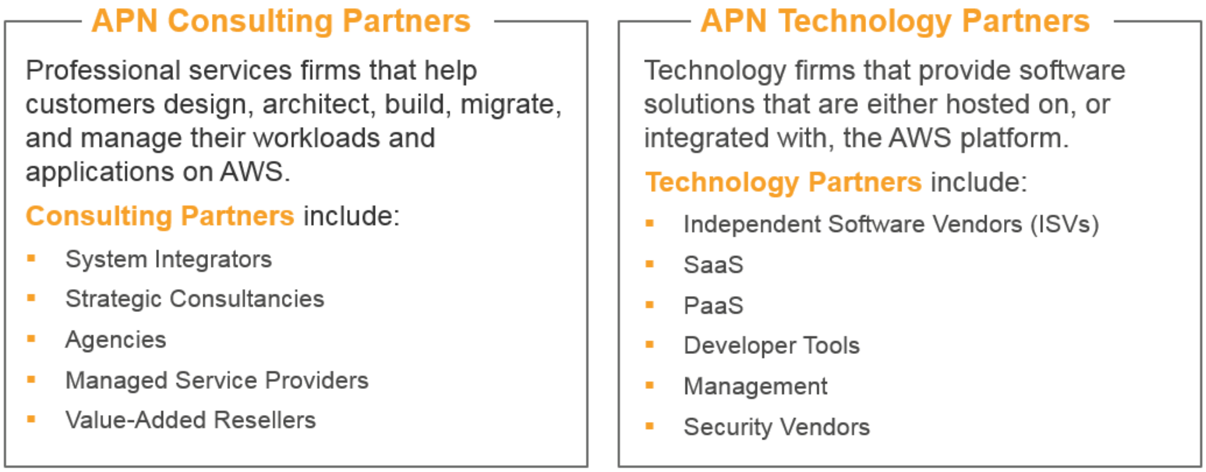
4.0 Case Studies

AWS has dedicated teams focused on helping our customers in government organizations pave the way for innovation and, ultimately, making the world a better place through technology. The AWS website contains information detailing AWS customer success stories in the Canadian public sector at https://aws.amazon.com/canada/. Below are a few examples:

- Banro Corporation
- BC Hydro
- British Columbia Institute of Technology (BCIT)
- Desire2Learn
- International Civil Aviation Organization
- Jour de la Terre
- Municipal Property Assessment Corporation (MPAC)
- National Bank of Canada
- The Globe and Mail
- Toronto Star
- University of Alberta
- Vancouver International Airport

5.0 Partner Ecosystem and AWS Marketplace

AWS has the largest partner ecosystem in the cloud (see **Figure 6** below), and it continues to grow at a rapid pace. It is very likely that the System Integrators (SIs) and Independent Software Vendors (ISVs) that you already work with are in the AWS Partner Network (APN).



APN Consulting Partners

Professional services firms that help customers design, architect, build, migrate, and manage their workloads and applications on AWS.

Consulting Partners include:

- System Integrators
- Strategic Consultancies
- Agencies
- Managed Service Providers
- Value-Added Resellers

APN Technology Partners

Technology firms that provide software solutions that are either hosted on, or integrated with, the AWS platform.

Technology Partners include:

- Independent Software Vendors (ISVs)
- SaaS
- PaaS
- Developer Tools
- Management
- Security Vendors

Figure 6 – AWS' Extensive Partner Ecosystem

Having consulting and technology partner support in place makes it much easier to deploy, adopt, and/or shift workloads to the cloud, and strength of partner ecosystem is crucial when evaluating a CSP. APN partners bring unique and proven experience in helping you design, architect, build, migrate, and manage your workloads and applications in the cloud.

- The **AWS Consulting Partner Program** is a global network comprising thousands of professional services firms that have invested in their AWS practice. They have experience in deploying customer solutions on AWS, a bench of trained and certified technical consultants, expertise in project management, and a financially stable consulting business on AWS.

- **APN Technology Partners** provide software solutions that are either hosted on, or integrated with, the AWS Cloud. APN Technology Partners include ISVs, Software as a Service (SaaS) providers, Platform as a Service (PaaS) providers, developer tool providers, and management and security vendors. APN Technology Partners gain access to a variety of tools, training, and support that enables them to more efficiently build their solutions on AWS.

The AWS Public Sector Partner Program enables partners to accelerate their business growth on AWS through alignment with our public sector sales, marketing, partner, and bid teams; designation as a public sector partner in our APN Partner Solutions Finder; and eligibility for further unique benefits and differentiation programs.

Additional APN partner programs such as the AWS Channel Reseller Program, AWS Managed Service Program, AWS Competency Program, and AWS SaaS Partner Program (to name only a few) are listed on the AWS website at https://aws.amazon.com/partners/programs/.

5.1 Salesforce and AWS

Salesforce and AWS extended their global strategic alliance in December of 2016 when they announced they will deliver five service integrations designed to simplify and expand how customers capture, analyze, and take action on their data. Together we announced that the AWS Canada (Central) Region will be the first new AWS Region supported in Salesforce's planned international infrastructure expansion on AWS. Salesforce customers will be able to use the company's core service—including Sales Cloud, Service Cloud, Community Cloud, Analytics Cloud, and more—delivered on AWS Cloud infrastructure in Canada, with general availability expected in mid-2017.

> "We're thrilled to extend our great partnership with AWS. Integrating AWS' industry-leading infrastructure services and technologies with Salesforce will bring even more exceptional solutions to our customers."
>
> -- Marc Benioff, Chairman and CEO, Salesforce

5.2 AWS Marketplace

AWS Marketplace allows you to directly deploy business applications to your AWS environment, simplifying licensing and deployment. AWS Marketplace is an online store that helps you find, buy, and immediately start using the software and services you need to build products and run your businesses. AWS Marketplace offers 35 product categories and more than 3,800 software listings from more than 1,170 ISVs.

6.0 Security and Compliance

As cloud computing customers are building systems on top of cloud infrastructure, the security and compliance responsibilities are shared between the CSP and cloud customers. In an Infrastructure as a Service (IaaS) model, you control how you architect and secure your applications and data put on the infrastructure, while the CSP is responsible for providing services on a highly secure and controlled platform, and providing a wide array of additional security features. The level of CSP and customer responsibilities in this shared responsibility model depends on the cloud deployment model (see the NIST Definition of Cloud Computing models). AWS' shared responsibility model is depicted in **Figure 7** below.

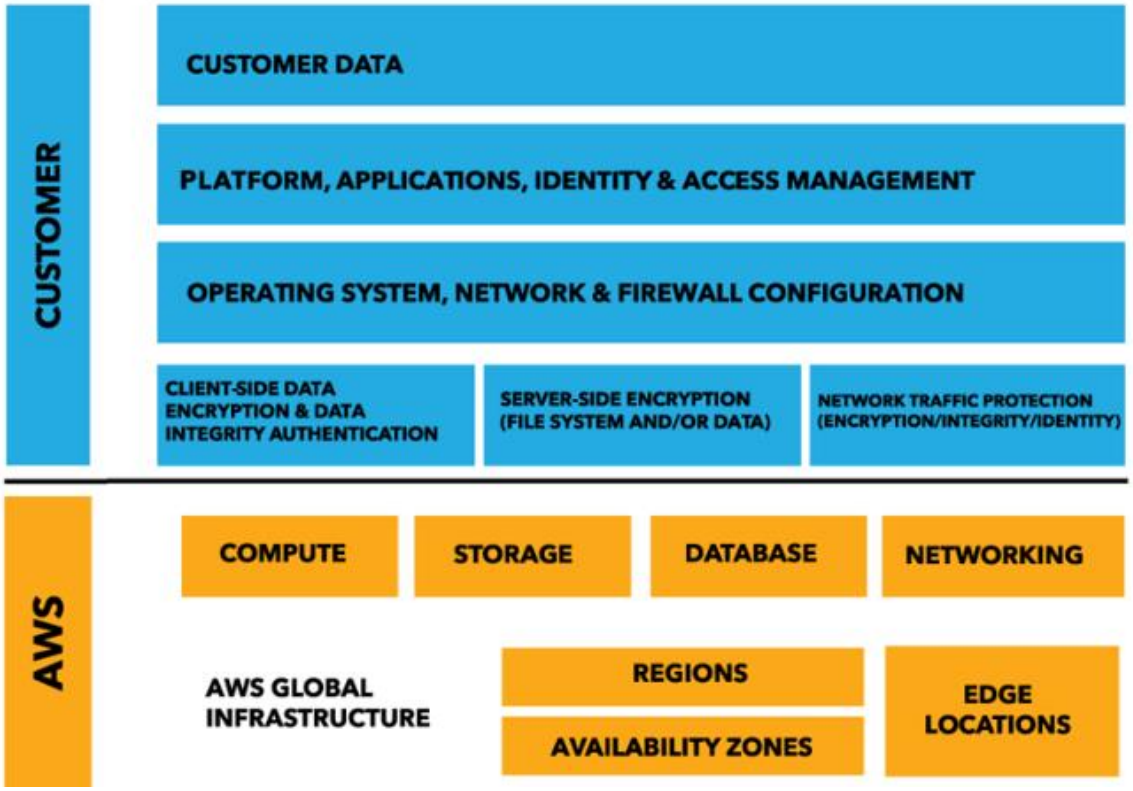

CUSTOMER
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 7 – AWS Shared Responsibility Model

- **AWS Responsibility –** AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.
- **Customer/Partner Responsibility –** Customers/partners assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, configuration of the AWS-provided security group firewalls, and other security, change management, and logging features.

AWS' shared responsibility model is further explained on the AWS Compliance webpage at http://aws.amazon.com/compliance/shared-responsibility-model/.

6.1 Data Privacy

AWS does not access customer data, and you are given the choice as to how you store, manage, and protect your data. There are four important basics regarding data ownership and management in the shared responsibility model:

1) Customers continue to own their data.
2) Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
3) Customers can download or delete their data whenever they like.

4) Customers should consider the sensitivity of their data and decide if and how to encrypt the data while it is in transit and at rest.

AWS gives customers ownership and control over their customer content by design through simple but powerful tools that allow customers to determine where their customer content will be stored, secure their customer content in transit or at rest, and manage access to AWS services and resources for their users. We also implement responsible and sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer content.

Maintaining customer trust is an ongoing commitment, and we strive to inform customers of the privacy and data security policies, practices, and technologies we've put in place. These commitments include:

- **Access:** Customers manage access to their customer content and AWS services and resources. We provide an advanced set of access, encryption, and logging features (such as AWS CloudTrail) to help you do this effectively. We do not access or use customer content for any purpose other than as legally required for maintaining the AWS services and providing them to our customers and their end users.

- **Storage:** Customers choose the Region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer's chosen Region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users.

- **Security:** Customers choose how their customer content is secured. We offer our customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys.

- **Security Assurance:** We have developed a security assurance program using global privacy and data protection best practices in order to help customers establish, operate, and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation. Our highly secure data centres use state-of-the-art electronic surveillance and multi-factor access control systems and maintain strict, least-privileged-based access authorizations. Our environmental systems are designed to minimize the impact of disruptions to operations, and our multiple geographic Regions and AZs allow customers to remain resilient in the face of most failure modes, including natural disasters or system failures. AWS manages over 1,800 security controls to provide an optimally secure environment for all of our customers.

In addition, network traffic between AZs and individual data centres travels over private network segments by default. These private network segments are fully isolated from the public Internet and not routable externally. AWS resources can be configured to reside only on isolated AWS network segments and to avoid utilizing any public IP addresses or routing over the public Internet. Note that communication between AWS Regions is across the public Internet. Therefore, you should use the appropriate encryption methods to protect your data. AWS security engineers and solutions architects have developed whitepapers and operational checklists to help you select the best options for your needs and to recommend security best practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

6.2 Compliance

Cloud accreditation certifications and evaluations provide customers with assurance that cloud providers have effective physical and logical security controls in place.

CJIS
Department of Defense
PCI Security Standards Council
PARTICIPATING ORGANIZATION
FedRAMP
Department of Education
FIPS 140-2 CRYPTOGRAPHY
AICPA SOC
NIST
FISMA
PCI DSS LEVEL 1 SERVICE PROVIDER
HIPAA
U.S. Securities and Exchange Commission
ITAR Compliant International Traffic in Arms Regulations
ISO
CSA cloud security alliance
irap
ISAE 3402 TYPE 2
GOV.UK
DISA
NERC
MOTION PICTURE ASSOCIATION OF AMERICA
TÜV TRUST IT
TÜV AUSTRIA Group

Figure 8 – AWS Certifications and Accreditations

When public sector entities leverage these reports, they avoid subjecting themselves to overly burdensome processes or approval workflows that may not be required for a cloud environment. Using such accreditations also enables you to build a quicker, more efficient compliance process. The AWS Cloud infrastructure has been designed and is managed in alignment with regulations, standards, and best practices, including:

- International Organization for Standardization (ISO) 27001
- ISO 27017
- ISO 27018
- ISO 9001
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)

- SOC 2
- SOC 3
- Cloud Security Alliance (CSA)
- Payment Card Industry Data Security Standard (PCI DSS) version 3.2
- Cloud Computing Compliance Controls Catalog (C5) (Germany)
- Cloud Infrastructure Services Providers in Europe (CISPE)
- Data Processing Addendum (DPA) Authorisation (Spain)
- Esquema Nacional de Seguridad (ENS) (Spain)
- EU Data Protection Directive (Directive 95/46/EC) Model Clauses
- Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS)
- Federal Information Processing Standard (FIPS) 140-2
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)
- Information Security Registered Assessors Program (IRAP) (Australia)
- International Computer Room Experts Association (ICREA)
- International Traffic in Arms Regulations (ITAR)
- IT Grundschutz (Germany)
- National Institute of Standards and Technology (NIST) 800-171
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Singapore Multi-Tier Cloud Security (MTCS) Level 3
- UK Cyber Essentials Plus
- UK Data Protection Act 1998
- UK National Cyber Security Centre (NCSC) Cloud Security Principles
- US Health Insurance Portability and Accountability Act (HIPAA)

For information on all of the security regulations and standards with which AWS complies, visit the AWS Compliance page.

6.3 Compliance in Canada

6.3.1 Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian federal law that applies to the collection, use, and disclosure of personal information in the course of commercial activities in all Canadian provinces as supplemented by substantially similar provincial privacy laws in Alberta, British Columbia and Québec. PIPEDA also applies to international and interprovincial transfers of personal information. As AWS does not have visibility into or knowledge of what customers are uploading onto its network, including whether or not that data is deemed subject to PIPEDA regulations, customers are responsible for their own PIPEDA compliance.

AWS customers have granular control over their data they store in the AWS Cloud. AWS can assist customers directly with teams of Solutions Architects, Account

Managers, Consultants, Trainers and other staff in Canada who are expertly trained on cloud security and compliance to assist AWS customers in achieving high levels of security and compliance, including those customers subject to the PIPEDA regulations.

6.3.2 CACP Information and Communication Technology Sub-Committee

The whitepaper *AWS Response to CACP Information and Communication Technology Sub-Committee* provides information that Canadian police agencies can use to help determine how AWS services support their requirements, and how to integrate AWS into the existing control framework that supports their IT environment. The "CACP Requirements" tables in this whitepaper address the requirements listed in the *Canadian Association of Chiefs of Police (CACP) Information and Communication Technology Sub-Committee's Offsite Data Storage and Processing Best Practices*.

6.3.3 Automating Security Best Practices

Automating security best practices is one of the key security enablers that the cloud brings to public sector customers. Software-based security mechanisms improve the ability to securely scale more rapidly and cost effectively. Customers can create and save a custom baseline image of a virtual server and then use that image automatically on each new server that is launched, creating an entire infrastructure that is defined and managed in a template.

When customers build in automation to their cloud architecture, along with management features such as AWS Service Catalog (which provides a permission controlled self-service capability for using AWS services), they can securely and repeatedly allow end users access to the resources they need, in a fraction of the time it takes to do so using a cloud platform that does not have deployment tools such as AWS CloudFormation. Additional information can be found in the below whitepapers:

- *Introduction to AWS Security by Design*
- *Automating Governance on AWS*

6.4 Built-in Security Features

Not only are applications and data protected by highly secure facilities and infrastructure, they are also protected by extensive network and security monitoring systems. AWS and our partners offer hundreds of tools and features to help you meet your security objectives concerning visibility, auditability, controllability, and agility. These tools and features provide basic but important security measures such as Distributed Denial of Service (DDoS) protection and password brute-force detection on AWS accounts. AWS-provided security features include:

- **Secure Access** – Customer access points, also called API endpoints, allow secure HTTP access (HTTPS) so that you can establish secure communication sessions with your AWS Cloud services using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

- **Built-in Firewalls** – You can control how accessible your instances are by configuring built-in firewall rules—from totally public to completely private or somewhere in between. And when instances reside within an Amazon Virtual Private Cloud (VPC) subnet, you can control egress as well as ingress.
- **Unique Users** – AWS Identity and Access Management (IAM) allows you to control the level of access your own users have to AWS infrastructure services. With AWS IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.
- **Multi-Factor Authentication (MFA)** – AWS provides built-in support for MFA for use with AWS accounts as well as individual IAM user accounts.
- **Private Subnets** – Amazon VPC allows you to add another layer of network security to instances by creating private subnets and even adding an Internet Protocol Security (IPsec) Virtual Private Network (VPN) tunnel between a home network and Amazon VPC.
- **Encrypted Data Storage** – You can have the data and objects you store in Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon Redshift, and Amazon Relational Database Service (Amazon RDS) on Oracle and SQL Server encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
- **Dedicated Connection Option** – AWS Direct Connect allows you to establish a dedicated network connection from your premises to AWS. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable access to both public and private IP environments within the AWS Cloud.
- **Dedicated, Hardware-Based Crypto Key Storage Option** – For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.
- **Centralized Key Management** – For customers who use encryption extensively and require strict control of their keys, AWS Key Management Service (KMS) provides a convenient management option for creating and administering the keys used to encrypt data at rest.
- **Perfect Forward Secrecy** – For even greater communication privacy, several AWS Cloud services such as Elastic Load Balancing and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use perfect forward secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.
- **DDoS Protection** – AWS Shield is a managed DDoS protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

Several of AWS' built-in cloud security features focus on providing visibility into data, performance, and resource usage. The tools listed below can help you gain more insight into your cloud operations, giving you the means to better control your security and providing information for data-driven decisions.

- **AWS Personal Health Dashboard** – AWS Personal Health Dashboard provides a personalized view into the performance and availability of the AWS services you are using, as well as alerts that are automatically triggered by changes in the health of those services. In addition to event-based alerts, Personal Health Dashboard provides proactive notifications of scheduled activities, such as any changes to the infrastructure powering your resources, enabling you to better plan for events that may affect you.
- **AWS Trusted Advisor** – AWS Trusted Advisor is a convenient way for you to see where you could use a little more security. It monitors AWS resources and alerts customers to security configuration gaps such as overly permissive access to certain Amazon Elastic Compute Cloud (Amazon EC2) instance ports and Amazon S3 storage buckets, minimal use of role segregation using IAM, and weak password policies.
- **Amazon CloudWatch** – Amazon CloudWatch enables you to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS database instances, as well as custom metrics generated by your applications and services and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly.
- **AWS CloudTrail** – AWS CloudTrail provides logs of all user activity within an AWS account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS Cloud service. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.
- **AWS Config** – With the AWS Config service, you can immediately discover all of your AWS resources and view the configuration of each. You can receive notifications each time a configuration changes, as well as dig into the configuration history to perform incident analysis.
- **Amazon Inspector** – Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.
- **AWS Organizations** – AWS Organizations allows you to create groups of AWS accounts that you can use to more easily manage security and automation settings. With Organizations, you can centrally manage multiple accounts to help

you scale. You can control which AWS services are available to individual accounts, automate new account creation, and simplify billing.

- **AWS Managed Services** – AWS Managed Services provides ongoing management of your AWS infrastructure so you can focus on your applications. AWS Managed Services automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support your infrastructure. Our rigour and controls help to enforce your corporate and security infrastructure policies, and enable you to develop solutions and applications using your preferred development approach.

6.5 Third-Party Security Tools

AWS also offers access to additional third-party security tools to complement and enhance our customers' operations in the AWS Cloud. APN partners offer hundreds of familiar and industry-leading products that are equivalent to, identical to, or integrate with existing controls in a customer's on-premises environments. Customers can browse and purchase APN partner products on the AWS Marketplace. These products complement existing AWS Cloud services to enable customers to deploy a comprehensive security architecture and provide a more seamless experience across their cloud and on-premises environments. The APN partner security products cover multiple areas of security, including application security, policy management, identity management, security monitoring, vulnerability management, and endpoint protection. **Figure 9** is a snapshot of the APN partners and categories of products available under the security category in the AWS Marketplace.

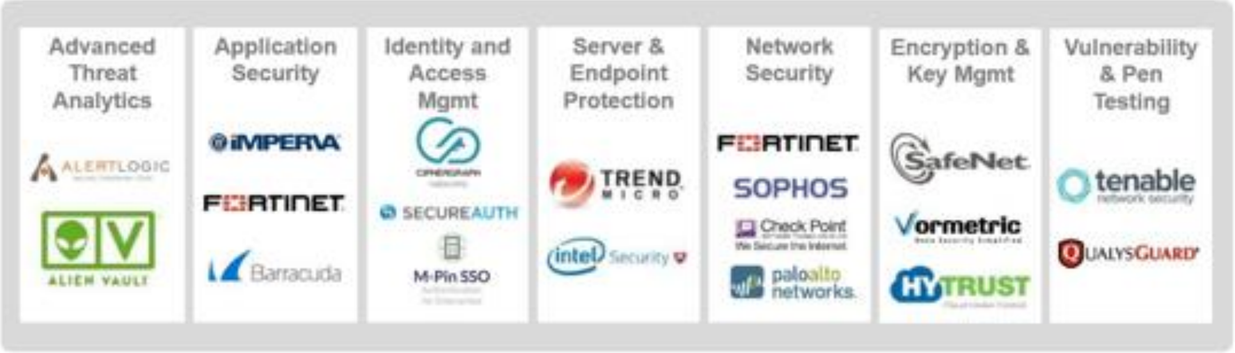


Figure 9 – AWS Marketplace provides access to many familiar and trusted security vendors.

6.6 Managing Security in the Cloud versus On-Premises

Managing security in the cloud is much like managing security in on-premises data centres, only without customers having to deal with the costs and complexities of protecting facilities and hardware. Lower cost and higher efficiency are two of the most obvious benefits of using the cloud, as opposed to building and running a physical data centre. You can also obtain greater security in the cloud than is available in traditional data centres, with benefits that include:

- **Free Security Tools** – Many of our security features and services are free, like individual firewalls (security groups) for Amazon EC2 instances, security logging with AWS CloudTrail, private subnets with Amazon VPC, user access control with IAM, and automatic encryption of archived data in Amazon Glacier.
- **Independent Regions Provide Data Privacy Compliance** – With our data centres located in so many geographical Regions across the world, you can choose the area that meets your data privacy requirements. AWS never moves your data out of the Region you specify.
- **Significant DDoS Protection** – Along with AWS Shield, AWS' size and scale can help you be DDoS-resilient. AWS infrastructure is equipped to handle extremely large amounts of traffic. In addition, when you use AWS Cloud services like Elastic Load Balancing, Auto Scaling, Amazon CloudWatch, and Amazon CloudFront, you can architect a highly available system that can help you weather DDoS attacks.
- **Security Economies of Scale** – The smallest AWS customers reap the same security benefits as the largest customers when they operate in our cloud. AWS has a large, dedicated security team and a variety of systems and tools that continuously monitor and protect the underlying cloud infrastructure.
- **No More Duplicate Data Centres for Disaster Recovery** – When you use AWS features like Auto Scaling and Elastic Load Balancing, you can ensure that your production systems remain online and that traffic is always routed to healthy instances. You can continuously replicate your data and have it ready to bring online if your primary nodes fail, only paying for the nodes when you actually use them.
- **Continuous Hardware Replacement and Upgrade** – We are always improving our infrastructure. We replace end-of-life hardware with the latest processors that not only improve performance and speed but also include the latest secure platform technology, like the Intel Advanced Encryption Standard New Instructions (AES-NI) encryption instruction set, which significantly speeds up the execution of the AES algorithm.
- **Part of the Compliance Work Is Done** – Because AWS has already received many certifications for our infrastructure, part of your compliance work has already been done. You only have to certify the applications and architectures you create on AWS.

6.7 New Governance Models

With cloud computing you get the chance to build the IT environment you want, not simply manage the one you have. The cloud enables customers to: (1) start with a full inventory of all IT assets; (2) manage all of these assets centrally; and (3) create alerts regarding usage/billing/security/etc. All of these vital benefits of the cloud ensure that customers have an optimized—and to the fullest extent, automated—architecture, with no need to continually procure and install new hardware. This is done by the CSP, allowing customers to shift focus from undifferentiated infrastructure management to the mission-critical operational level.

The AWS Cloud provides almost incomparable capabilities for asset tracking, inventory management, change management, log management and analysis, and overall visibility and governance. The AWS Management Console provides a single view of an entire infrastructure, with additional third-party management and monitoring products available on AWS Marketplace. With Amazon CloudWatch, customers can monitor AWS Cloud resources and the applications that run on AWS. With AWS Config customers get full visibility to the state of AWS resources, monitoring changes over time and viewing the full history of configuration changes for a resource. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing. Even when it comes to billing, customers can tag each AWS resource to track usage and spend. Additionally, services such as AWS Trusted Advisor augment AWS and third-party monitoring and optimization products to provide best practices (or checks) in areas including cost optimization, security, fault tolerance, and performance improvement.

One helpful way to view AWS is that it is effectively a very large API. Whether you are launching a new server or changing a security setting, you are just making API calls. Every change to the environment is logged and recorded (the who, what, where, and when of each change is recorded). This provides governance, control, and visibility that is only possible in a cloud environment like the AWS Cloud. It also provides the hooks for DevSecOps to continuously track changes and enable deep security automation.

7.0 Moving to the Cloud

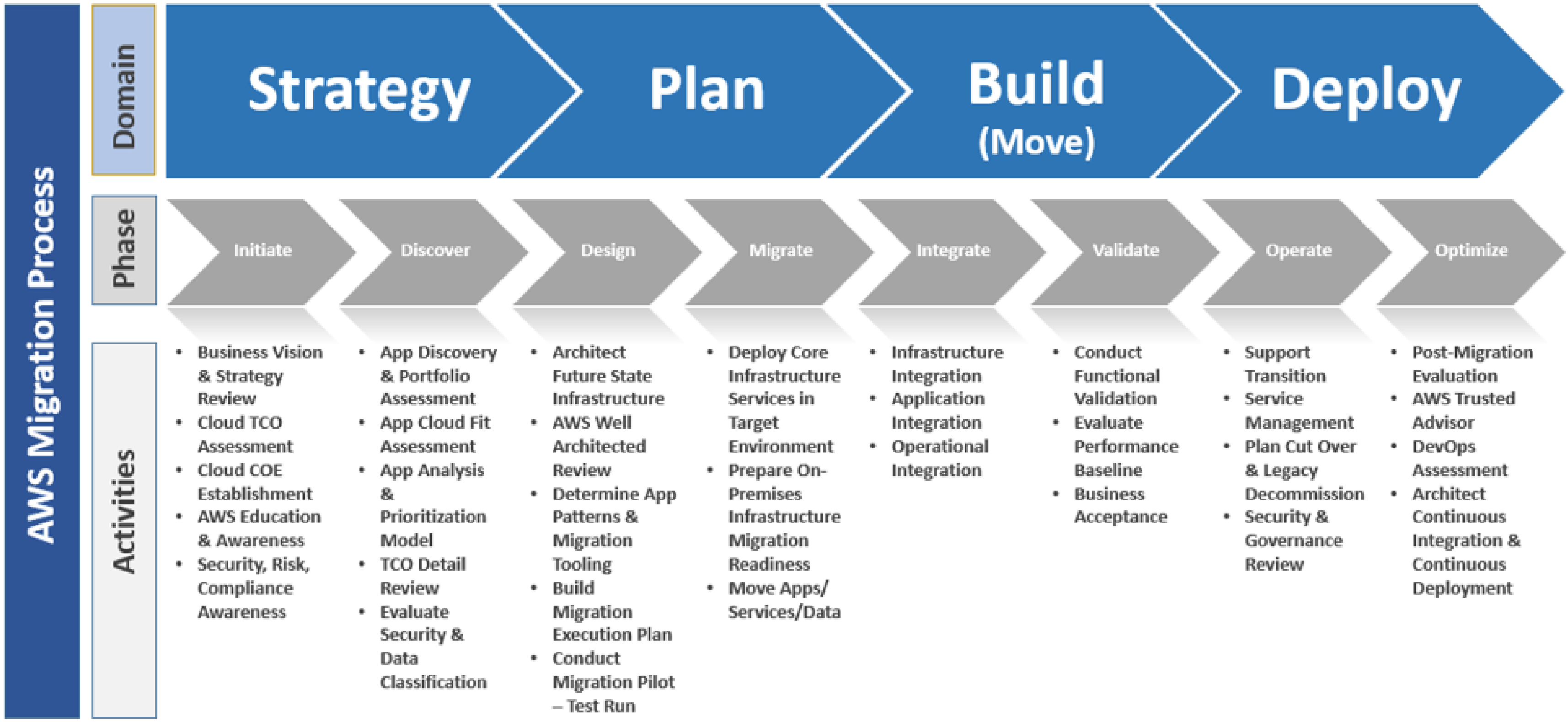
All cloud journeys are unique, but many share commonalities. There are common patterns, approaches, and best practices that can be implemented to streamline the process. Recognizing this, we do not provide a prescriptive cloud migration methodology with a sequential process. Instead, we provide guidance and best practices that you can use to build a cloud migration strategy that best meets your unique needs. AWS has helped countless customers achieve their cloud migration goals. AWS Professional Services can engage with customers and partners in the discovery, architecture, governance, migration, and knowledge transfer stages of a customer’s journey to the AWS Cloud.

The AWS Cloud Adoption Framework (CAF) identifies a set of general design principles to facilitate good design in the cloud. Documents describing the AWS CAF are available on the AWS website (see links below), and consultants from our AWS Professional Services Team would be happy to discuss migration best practices with customers.

- AWS CAF Perspectives
- *A Practical Guide to Cloud Migration: Migrating Services to AWS*
- *Architecting for the AWS Cloud: Best Practices*
- *AWS Well-Architected Framework*
- *Cost Optimization with AWS: Architecture, Tools, and Best Practices*

The AWS Partner Competency Program has validated which partners have demonstrated that they can help enterprise customers migrate applications and legacy infrastructure to AWS: https://aws.amazon.com/migration/partner-solutions/.

To illustrate commonalities in a cloud migration, **Figure 10** below displays an application migration methodology. The methodology outlined provides a standardized general process of migration. It also contains the work products in each phase commonly performed as part of application migrations. They are not intended to operate in sequence, but can be multi-threaded, with some activities being performed concurrently.



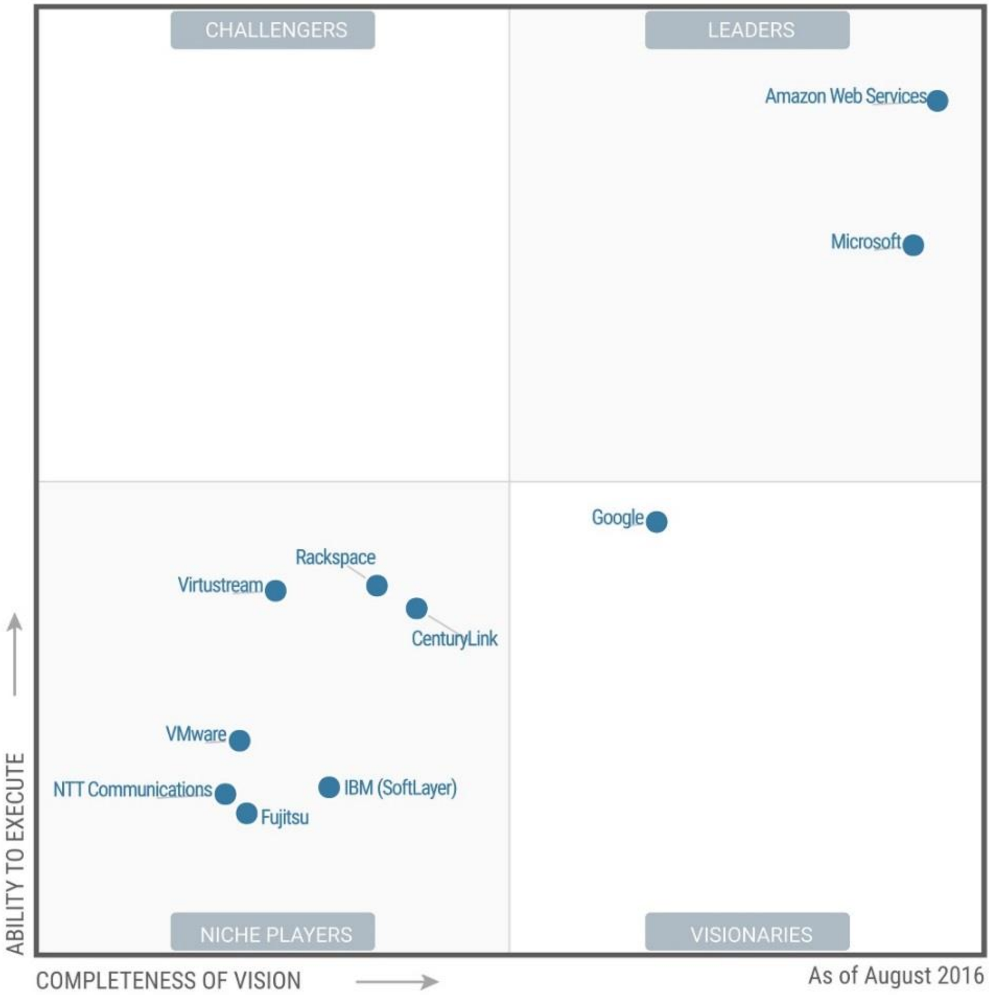
AWS Migration Process								
Domain	Strategy		Plan		Build (Move)		Deploy	
Phase	Initiate	Discover	Design	Migrate	Integrate	Validate	Operate	Optimize
Activities	• Business Vision & Strategy Review • Cloud TCO Assessment • Cloud COE Establishment • AWS Education & Awareness • Security, Risk, Compliance Awareness	• App Discovery & Portfolio Assessment • App Cloud Fit Assessment • App Analysis & Prioritization Model • TCO Detail Review • Evaluate Security & Data Classification	• Architect Future State Infrastructure • AWS Well Architected Review • Determine App Patterns & Migration Tooling • Build Migration Execution Plan • Conduct Migration Pilot – Test Run	• Deploy Core Infrastructure Services in Target Environment • Prepare On-Premises Infrastructure Migration Readiness • Move Apps/ Services/Data	• Infrastructure Integration • Application Integration • Operational Integration	• Conduct Functional Validation • Evaluate Performance Baseline • Business Acceptance	• Support Transition • Service Management • Plan Cut Over & Legacy Decommission • Security & Governance Review	• Post-Migration Evaluation • AWS Trusted Advisor • DevOps Assessment • Architect Continuous Integration & Continuous Deployment

Figure 10 – AWS Application Migration Methodology

Some of AWS' native features and services for cloud migration such as AWS Database Migration Service, AWS Server Migration Service, and AWS Snowball are described in the whitepaper *An Overview of AWS Cloud Data Migration Services*.

8.0 Industry Analyst Reports

Gartner, Inc., a leading information technology research company, released its 2016 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide[1] [2] report, where AWS is positioned highest in execution and furthest in vision within the Leaders Quadrant.



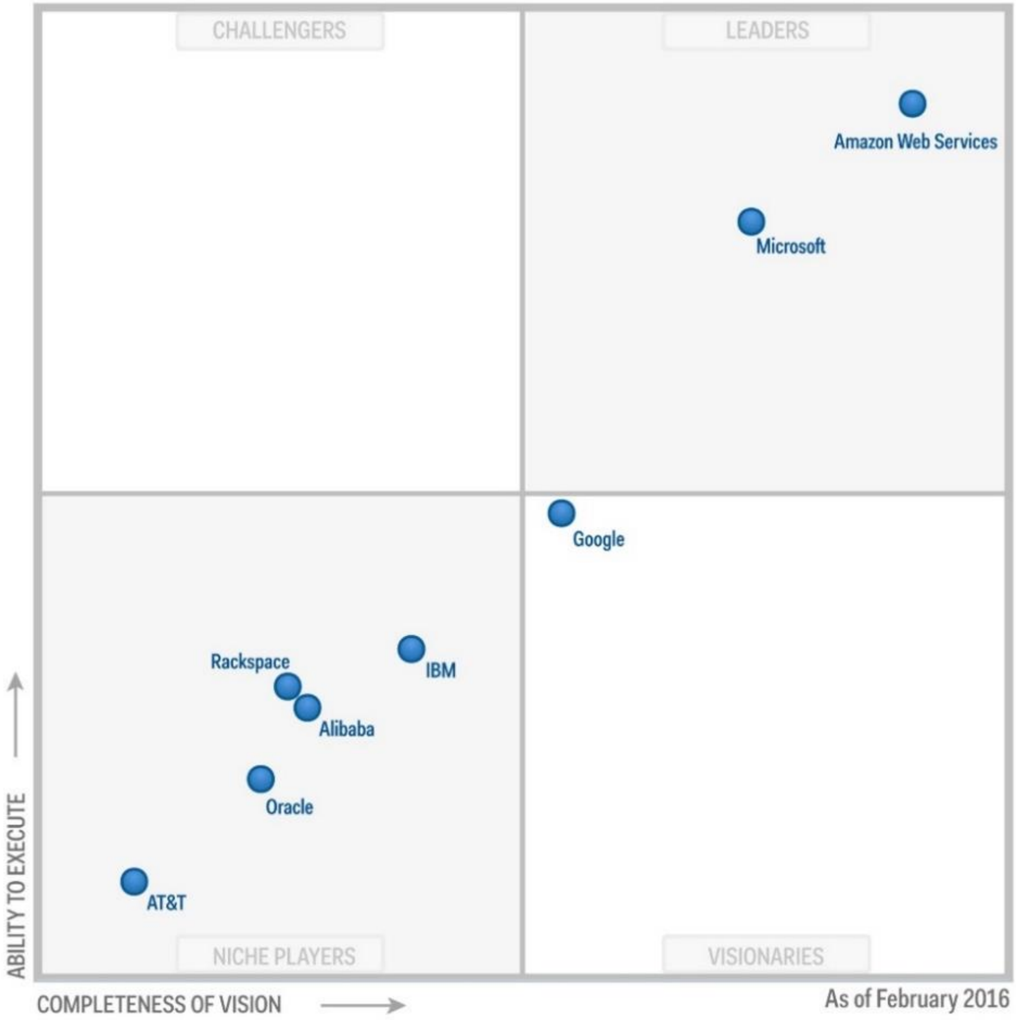
Source: Gartner (August 2016)

Figure 11 – Gartner 2016 Magic Quadrant for Cloud IaaS, Worldwide

[1] Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Leong, Lydia, Petri, Gregor, Gill, Bob, Dorosh, Mike, August 3, 2016. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from AWS: http://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb. Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[2] All statements in this report attributable to Gartner represent AWS’s interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this proposal). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

AWS is also positioned highest in execution and furthest in vision within the Leaders Quadrant of Gartner, Inc.'s 2016 Magic Quadrant for Public Cloud Storage Services, Worldwide report.[3] [4]



Source: Gartner (July 2016)

Figure 12 – Gartner 2016 Magic Quadrant for Public Cloud Storage Services, Worldwide

Gartner defines Leaders as organizations that "execute well against their current vision and are well positioned for tomorrow."

[3] Gartner, Magic Quadrant for Public Cloud Storage Services, Worldwide, Bala, Raj, Chandrasekran, 26 July 2016. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from AWS: http://www.gartner.com/doc/reprints?id=1-2IH2LGI&ct=150626&st=sb. Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[4] All statements in this report attributable to Gartner represent AWS's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this proposal). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

The Forrester Wave: Public Cloud Platform Service Providers' Security, Q4 2014 report (**Figure 13**) evaluated four of the leading public clouds along 15 key security criteria and detailed the findings about how well each vendor fulfills criteria and where they stand in relation to each other, to help S&R professionals select the right public cloud partner with the best options for security controls and overall security capabilities. AWS leads the pack and demonstrated not only a broad set of security capabilities in data centre security, certifications, and network security, but also excelled in customer satisfaction, security services partnerships, and a large installed base.

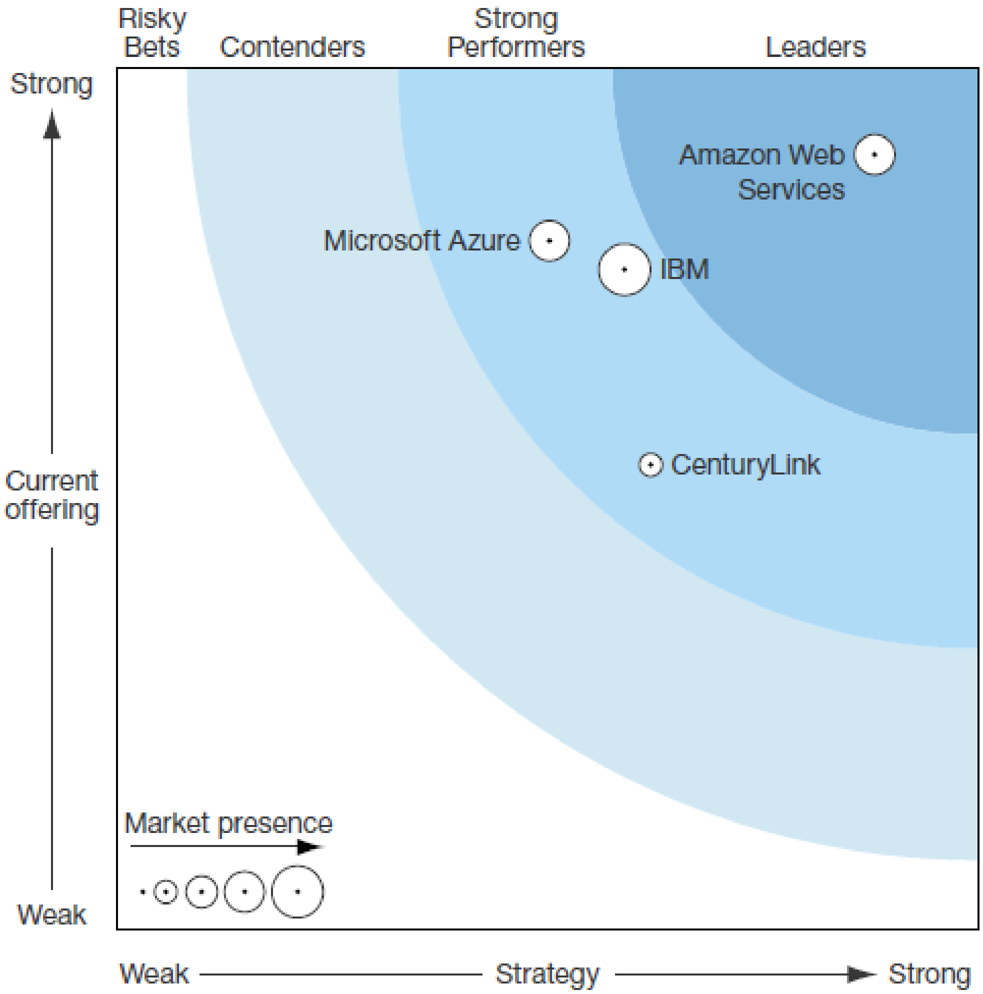


Figure 13 – Forrester Wave™: Public Cloud Service Providers' Security, Q4 '14

More analyst reports can be found at http://aws.amazon.com/resources/analyst-reports/.

9.0 Service Level Agreements (SLAs)

AWS currently provides SLAs for several services. Due to the rapidly evolving nature of AWS' product offerings, SLAs are best reviewed directly on our website via the links below:

- Amazon EC2 SLA: http://aws.amazon.com/ec2-sla/
- Amazon S3 SLA: http://aws.amazon.com/s3-sla
- Amazon CloudFront SLA: http://aws.amazon.com/cloudfront/sla/
- Amazon Route 53 SLA: http://aws.amazon.com/route53/sla/
- Amazon RDS SLA: http://aws.amazon.com/rds-sla/
- AWS Shield Advanced SLA: https://aws.amazon.com/shield/sla/

Instead of recycling existing SLAs, we encourage public sector organizations to shift focus to building well-architected and optimized solutions that use capabilities that are unique to the cloud, such as AWS' multiple AZs or Regions, which can ease the burden of achieving SLA standards.

Many public sector organizations are already drafting cloud-centric SLAs that focus on workloads and outcomes, instead of on SLAs specifying certain storage capacity or throughput requirements. For example, an SLA may require that a system complete 100,000 benefits applications with 99.99% accuracy within a certain timeframe. This transition to outcomes, not specifications, is a fundamental shift in contracting terminology.

Specifically relating to cloud procurements, organizations often establish government-unique specifications, rather than rely on existing, commercial performance specifications and SLAs. Organizations dictate methods, infrastructure, or hardware that they require to achieve their specific performance requirements, rather than focus on application-level, performance-based requirements. In the cloud model, the CSP owns and maintains the network-connected hardware required for their cloud services. With this infrastructure burden removed from customers/agencies, organizations do not need to, and should not, include prescriptive requirements that specify what the underlying infrastructure stack should consist of.

For example, a 2016 U.S. Request for Proposal (RFP) included the following requirement: *"The CSP must have at least 2 data centres that are within 100km (60 miles) of each other to support synchronous replication."* (The same procurement required addresses of CSPs' data centres and data centre site visits, which are incongruent with cloud security models). It should be sufficient to require that CSPs be able to support synchronous replication; there is no reason an agency should tell CSPs how to perform that replication. Organizations should leverage a CSP's established best practices for data centre operations and should avoid developing (without the depth of expertise and experience that established CSPs have) specifications for equipment, operations, and procedures (e.g., racks, server types, distances between data centres, etc.).

Leveraging CSP SLAs, organizations can further seek their own unique SLAs that focus on outcomes, workloads, and results—through accepting commercial CSP SLAs and architecting their cloud usage to satisfy additional, specific requirements. The National Aeronautics and Space Administration (NASA) successfully captured this approach in the following cloud requirement:

“NASA will maintain awareness of CSP SLAs and deploy important workloads and applications in such a way that they continue to operate in the event an SLA is not met. NASA will be responsible for maintaining appropriate SLAs associated with any NASA owned equipment or NASA operated services used with the CSP.”

NASA Cloud Service Office Solutions for Enterprise-Wide Procurement (SEWP) Statement of Work for Agency Cloud Computing Services, page 2 of Attachment D**.**

Appendix - Useful Links

AWS Overview

- What is Cloud Computing: https://aws.amazon.com/what-is-cloud-computing/
- Types of Cloud Computing: https://aws.amazon.com/types-of-cloud-computing/
- Choosing a Cloud Platform: https://aws.amazon.com/choosing-a-cloud-platform/
- About AWS: https://aws.amazon.com/about-aws/
- AWS Global Infrastructure: https://aws.amazon.com/about-aws/global-infrastructure/

AWS Solutions

- Websites and Web Hosting: https://aws.amazon.com/websites/
- Development and Test: https://aws.amazon.com/dev-test/
- Backup and Recovery: https://aws.amazon.com/backup-recovery/
- Data Archive: https://aws.amazon.com/archive/
- Disaster Recovery: https://aws.amazon.com/disaster-recovery/
- Big Data: https://aws.amazon.com/big-data/
- High Performance Computing: https://aws.amazon.com/hpc/
- Internet of Things: https://aws.amazon.com/iot/
- Financial Services: https://aws.amazon.com/financial-services/
- Health https://aws.amazon.com/health/
- Life Sciences: https://aws.amazon.com/health/life-sciences/
- Genomics: https://aws.amazon.com/health/genomics/
- Business Applications: https://aws.amazon.com/business-applications/
- DevOps: https://aws.amazon.com/devops/

AWS Products and Services

- List of all AWS cloud services: https://aws.amazon.com/products/
- AWS Marketplace: https://aws.amazon.com/marketplace/
- AWS service documentation: http://aws.amazon.com/documentation/

AWS in the Public Sector

- AWS Public Sector Homepage: https://aws.amazon.com/government-education/
- Public Sector Resources: https://aws.amazon.com/government-education/resources/
- State and Local Government: https://aws.amazon.com/stateandlocal/
- Defense and Aerospace: https://aws.amazon.com/government-education/defense/
- Education: https://aws.amazon.com/education/
- AWS Educate: https://aws.amazon.com/education/awseducate/
- Nonprofit Organizations https://aws.amazon.com/government-education/nonprofits/
- AWS GovCloud (US) Region: http://aws.amazon.com/govcloud-us/
- AWS Government Partners: https://aws.amazon.com/partners/government/
- AWS Public Sector Blog: https://aws.amazon.com/blogs/publicsector

AWS Partner Ecosystem

- AWS Partner Network: https://aws.amazon.com/partners/
- AWS Partner Directory: http://www.aws-partner-directory.com/
- AWS Partner Programs: https://aws.amazon.com/partners/programs
- AWS Public Sector Partner Program: https://aws.amazon.com/partners/public-sector/

AWS Professional Services

- AWS Professional Services: https://aws.amazon.com/professional-services/
- AWS Cloud Adoption Framework: https://aws.amazon.com/professional-services/CAF/
- AWS Enterprise Accelerators: https://aws.amazon.com/professional-services/enterprise-accelerators/

AWS Pricing

- AWS Pricing Overview: http://aws.amazon.com/pricing/
- Pricing for each service: https://aws.amazon.com/pricing/services/
- AWS Economics Center: https://aws.amazon.com/economics/
- Cost Optimization: https://aws.amazon.com/pricing/cost-optimization/
- AWS Simple Monthly Calendar: http://calculator.s3.amazonaws.com/index.html

- AWS TCO Calculator: http://aws.amazon.com/tco-calculator/

AWS Billing

- AWS Billing and Cost Management: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html
- Consolidated Billing: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html
- Cost Explorer: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-explorer-what-is.html
- AWS Budgets and Forecasts: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

AWS Security and Compliance

- AWS Security Center: http://aws.amazon.com/security/
- AWS Shared Responsibility Model: http://aws.amazon.com/security/sharing-the-security-responsibility/
- AWS Security Features: http://aws.amazon.com/security/aws-security-features/
- AWS Compliance: http://aws.amazon.com/compliance/
- AWS Compliance FAQs: http://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
- AWS Data Privacy: http://aws.amazon.com/compliance/data-privacy-faq/
- Access Control: http://aws.amazon.com/iam/
- AWS Security Blog: https://blogs.aws.amazon.com/security/

AWS Support

- AWS Support Tiers: https://aws.amazon.com/premiumsupport/
- Support Knowledge Center: https://aws.amazon.com/premiumsupport/knowledge-center/
- AWS Trusted Advisor: https://aws.amazon.com/premiumsupport/trustedadvisor/

AWS Training and Best Practices

- AWS Training and Certification: http://aws.amazon.com/training/
- AWS Architecture Center: http://aws.amazon.com/architecture/
- AWS Test Drive: http://aws.amazon.com/testdrive/

Industry Analysis

- Analyst Reports: http://aws.amazon.com/resources/analyst-reports/
- Gartner Magic Quadrant for Cloud Infrastructure as a Service (August 2016): https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb
- Gartner Magic Quadrant for Public Cloud Storage Services (July 2016): https://www.gartner.com/doc/reprints?id=1-2IH2LGI&ct=150626&st=sb
- Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014: http://www.forrester.com/pimages/rws/reprints/document/113065/oid/1-SBOUWE
- IDC Report: Quantifying the Business Value of Amazon Web Services: http://d0.awsstatic.com/analyst-reports/IDC_Business_Value_of_AWS_May_2015.pdf

AWS Case Studies

- AWS Case Studies: https://aws.amazon.com/solutions/case-studies/
- Public Sector Case Studies: http://aws.amazon.com/solutions/case-studies/government-education/

Procurement

- AWS Public Sector Contract Center: http://aws.amazon.com/contract-center/
- 10 Considerations for a Cloud Procurement Whitepaper: http://d0.awsstatic.com/whitepapers/10-considerations-for-a-cloud-procurement.pdf
- How to Buy Cloud Computing Services for your Agency (Webinar): https://aws.amazon.com/webinars/buying-cloud-computing-services/

AWS Legal

- AWS Customer Agreement: http://aws.amazon.com/agreement/
- AWS Service Terms: https://aws.amazon.com/service-terms/
- AWS Acceptable Use Policy: http://aws.amazon.com/aup/
- AWS Trademark Guidelines: http://aws.amazon.com/trademark-guidelines/
- AWS Site Terms: http://aws.amazon.com/terms/
- AWS Privacy Policy: https://aws.amazon.com/privacy/
- AWS Tax Help: http://aws.amazon.com/tax-help/

Additional Resources

- AWS Blog: https://aws.amazon.com/blogs/aws/

- AWS Discussion Forums: https://forums.aws.amazon.com/index.jspa
- What's New from AWS: http://aws.amazon.com/new/
- AWS YouTube Channel: https://www.youtube.com/user/AmazonWebServices
- AWS Twitter Feed: https://twitter.com/awscloud
- AWS on SlideShare: http://www.slideshare.net/AmazonWebServices
- Events and Webinars https://aws.amazon.com/about-aws/events/
- An E-Book of Cloud Best Practices: https://medium.com/aws-enterprise-collection/an-e-book-of-cloud-best-practices-for-your-enterprise-4a211840c55b#.corzpjf3m

AWS Whitepapers

- AWS Whitepapers: http://aws.amazon.com/whitepapers/
- Overview of AWS Whitepaper: http://d0.awsstatic.com/whitepapers/aws-overview.pdf
- Security Resources and Whitepapers: http://aws.amazon.com/security/security-resources/
- Introduction to AWS Security Processes: https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf
- AWS Compliance whitepapers: http://aws.amazon.com/compliance/aws-whitepapers/
- AWS Risk and Compliance Whitepaper: https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- AWS Storage Services Overview: https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf
- Backup and Recovery Approaches Using AWS: https://d0.awsstatic.com/whitepapers/Storage/Backup_and_Recovery_Approaches_Using_AWS.pdf