IDC MarketScape

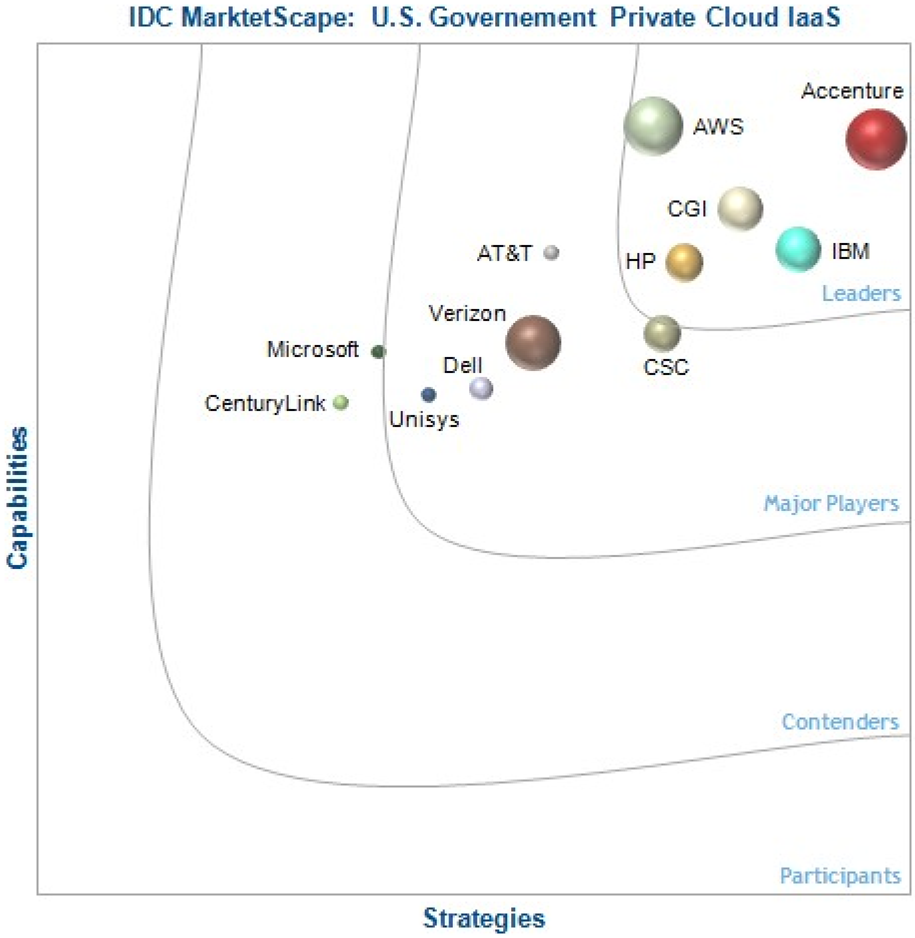
IDC MarketScape: U.S. Government Private Cloud IaaS 2014 Vendor Assessment

Adelaide O'Brien

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape U.S. Government Private Cloud IaaS Vendor Assessment



Source: IDC, 2014

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

This IDC MarketScape represents a vendor assessment of 12 vendors that provide private cloud IaaS to the U.S. federal government. This research is a quantitative and qualitative assessment of the characteristics that explain a vendor's success in the marketplace and help anticipate the vendor's ascendancy. This evaluation is based on a comprehensive framework and set of parameters expected to be most conducive to success in providing cloud IaaS for both the short term as a platform for platform as a service (PaaS) and software as a service (SaaS) and the long term for the transformation of IT services. IDC believes that:

- Government agencies are facing the combined struggle of exponential data growth and tight or diminishing budgets and are viewing cloud as the way to transfer more workloads to lower-cost infrastructure platforms, such as IaaS, often without acquiring significant resources. Therefore, massive investments in technologies, facilities, operational personnel, tools, and best practices are the table stakes for vendors participating in this market.
- Making these investments is only the start. Government cloud buyers want vendors' portfolios to offer a full range of integrated physical and virtual infrastructure systems with pre-integrated, modular units of compute, storage, and networking that allow IT to add blocks of physical resources in a repeatable, scalable fashion. Government is also looking for vendors that can use their domain knowledge, technology expertise, and intellectual property (IP) to reduce cost and increase efficiency from day one.
- Security is also paramount when considering cloud, and the U.S. federal government will continue to spend more on private cloud systems than on public over the next five years. The U.S. Government Federal Risk and Authorization Management Program (FedRAMP) and other secure certifications are easing this concern, and in addition to the 19 commercial vendors that have certification, another 34 vendors are lined up and working to get their FedRAMP certifications.
- Government decision makers should review their strategic plans and select vendors for their IaaS based on best fit. This IDC MarketScape is intended as a guide.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendors included in this IDC MarketScape meet the following four criteria:

- Initially, the U.S. Government Federal Risk and Authorization Management Program certification was required to participate in this IDC MarketScape. This process requires vendors to adhere to more than 290 security controls, document their security processes, and comply with audits. Vendors have indicated that it can take more than six months and an investment of over $200,000 to receive the FedRAMP certification. Therefore, IDC has included in this IDC MarketScape vendor status in undergoing FedRAMP certification as well as a table listing the vendors' additional security certifications.
- Vendors achieved at least $1 billion of revenue in calendar 2013 in the global IT services (consulting, systems integration, implementation and support, outsourcing, and cloud) market

- Vendors have a direct sales market presence in the IT services market for the U.S. federal government sector (many participants also have supplemental partner distribution).
- Vendors have at least two customers and provide at least two government reference customers that have implemented or are implementing cloud IaaS (compute or storage) services in either managed private cloud or virtual private cloud (VPC) in the U.S. federal government. Reference interviews from each participating vendor gauge the customers' experience working with the vendor and the customers' overall satisfaction with the IaaS project. Customer reference interviews are without attribution, built around a standard set of questions, and used to rate the importance of different elements of the capabilities section of the IDC MarketScape.

Ultimately, 12 vendors were invited to participate in this study:

- Accenture
- AT&T
- Amazon Web Services (AWS)
- CenturyLink
- CGI
- CSC
- Dell
- HP
- IBM
- Microsoft
- Unisys
- Verizon

ESSENTIAL BUYER GUIDANCE

Government agencies are facing the combined struggle of exponential data growth and tight or diminishing budgets and are viewing cloud as the way to transfer more workloads to lower-cost hosting platforms, often without acquiring significant resources. For decision making, government must rely on seamless access to trusted information and access to analytics tools. While sharing information through cloud computing can liberate data and greatly enhance situational awareness leading to better-informed decisions at all levels of government, the use of cloud in government raises concerns such as privacy, data veracity, and ownership.

However, government is espousing and trusting data standards such as the National Information Exchange Model (NIEM), Federal Information Security Management Act (FISMA), and the Federal Risk and Authorization Management Program. IDC advises our government clients to use the FedRAMP process and security requirements as a baseline for authorizing cloud services and require potential cloud vendors to comply with FedRAMP security requirements. This IDC MarketScape includes vendor compliance with FedRAMP as well as other security standards.

IDC advises that government pay attention to the extent to which a vendor's current portfolio offers a full range of integrated physical and virtual infrastructure systems with pre-integrated, modular units of compute, storage, and networking that allow IT to add blocks of physical resources in a repeatable, scalable fashion.

Additional requirements that U.S. federal government agencies should require from their IaaS vendors and are used as the basis for evaluation in this IDC MarketScape include:

- **Scalability.** Is the offering able to scale when needed through autoscaling? Does the vendor provide load balancing to manage and handle an increasing number of servers across heterogeneous resources, including multiple servers, hypervisors, and operating systems?
- **Compute services.** Does the vendor offer database services such as SQL (MySQL, Oracle Database, or other) as well as distributed processing compute services such as NoSQL database open source options that allow government to prepare for Big Data analytics by using such databases as Hadoop and MongoDB for processing unstructured data?
- **Pricing.** Is pricing aligned with the government market direction on the range of licensing options, such as subscription pricing, enterprise licensing agreements, and allowing concurrent users?
- **Flexible contract conditions as standard.** Such conditions include no minimum contract period, no minimum number of users, no up-front fixed fees, and compensation for breach of SLAs. A key question to ask vendors is "How does the vendor enter into and terminate the data contract?"
- **Value-added services.** The vendor offers value-added services including assessments and road map development; free trials; and/or implementation of pilot programs, proof of concepts and testing, and application migration.
- **Single point of accountability.** The ability to leverage partnerships and mix direct and indirect channels and still provide a single point of accountability for government clients.

The bottom line is if government decision makers do not have confidence in a prospective vendor's ability to securely meet projected capacity requirements in a timely fashion, with the capability (often through partners and alliances) to meet future needs through deployment of proven best practices, then IDC advises government to look elsewhere.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in this IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's portfolio, strengths, and challenges and IDC's viewpoint.

Accenture

Accenture provides flexible deployment for IaaS cloud options including managed private cloud on agency sites through Accenture Cloud Platform (ACP). Through ACP, Accenture provides dedicated, virtual private, hybrid, community, and public cloud via partners such as AWS, Verizon-Terremark, NTTA, Microsoft Azure, Layered Tech, and Carpathia. ACP for the federal government integrates to FISMA-compliant public cloud providers as well as FedRAMP-certified community clouds such as AWS and Microsoft Azure. ACP provides a technical platform for cloud service integration, enabling consistent end-to-end service management and governance across a federal agency's IT ecosystem. ACP 3.0 has been updated to include a new discovery engine and an exposed application programming interface that allows users to access services either through the ACP portal, through applications directly, or through the native cloud provider console. This provides flexible integration options and greater resiliency, enabling organizations to stay on top of and leverage new service introductions and innovations from cloud service providers immediately, helping improve productivity. The platform also provides a centralized view of usage patterns and unified billing with access to in-depth analytics for visibility of overall cloud spend, providing full budgetary control and an audit trail of user actions.

Through an online service catalog, ACP centralizes service request management and provisioning. It provides an audit trail of user actions and aggregates key functions including policy management, orchestration of automated workflows, service monitoring, metering, and chargebacks. Once integrated into the service catalog, services are auto-provisioned for on-demand delivery. Accenture provides IaaS managed services as a core component of the ACP Service Catalog.

Accenture's cloud management platform provides self-service requesting, provisioning, and deployment of virtual infrastructure. This includes virtual servers, virtual networks, and storage from the cloud as well as an integrated 24 x 7 service desk for support. Government users are able to build, deploy, and manage their own virtual infrastructure and cloud solutions. ACP provides a fully managed on-demand service for cloud infrastructure with integration to Accenture's pre-integrated cloud service providers, such as AWS.

Strengths

Accenture initiates its cloud readiness and assessment with a cloud strategy methodology, aligning cloud opportunities with agency business imperatives. Accenture also provides an assessment tool that identifies cloud opportunities and business value and a cloud-enabled IT operating model that details functions, processes, governance practices, roles, and organizational models in a cloud environment.

Accenture's security certifications are based on the certifications of the company's IaaS partners listed in Table 3, and through its partners, Accenture offers a full set of cloud management capabilities listed in Table 4. Accenture supports SQL and NoSQL databases as well as various hypervisors. Accenture offers all the value-added services listed in Table 5. Accenture deploys PaaS offerings such as Big Data as a service, one-click ERP, testing as a service, and development tools in the cloud as well as SaaS. Accenture offers cloud disaster recovery/backup as well as the capability for government to leverage Big Data in the cloud through its Big Data services with pre-integrated tools.

Accenture is investing heavily in cloud, having recently announced a $400 million investment in professional services capabilities – including training, building new and existing offerings, and developing assets across the cloud stack of infrastructure, platform, and software. Accenture is also providing government with proven, pre-integrated, cloud-based solutions, such as Federal ERP in the Cloud, with demonstrated benefits of lowering the cost, reducing the risk, and increasing the speed of implementation.

Accenture has a strong two-pronged approach to this market. First, provide a cloud platform for government based on recognized industry infrastructures, platforms, and services. Accenture will add to its ecosystem of providers as other CSPs complete their FedRAMP certification processes. Accenture is driving growth through market development for new cloud services, with an emphasis on expanding partnerships and the breadth of current offerings, including large-scale transformational professional services. Examples include building additional tools/assets, creating an application migration to the AWS offering, and building additional capability on the Accenture Cloud Platform to automate and improve provisioning and management of Microsoft Azure. Second, business services are still Accenture's major focus. Accenture plans to expand cloud management offerings with the ACP, capitalize on its industry capabilities, and bundle cloud with industry business services as well as newer transformational services such as mobility, Big Data and analytics, and social business.

Challenges

Challenges that Accenture faces as a broker of pre-certified and compliant solutions are to stay on top of the cloud vendor ecosystem, continue to focus on key alliances including emerging technology vendors, and assemble solution components that are pre-certified and compliant for government use, all while strengthening and building teaming relationships with existing cloud providers whose solutions are developing rapidly.

IDC Viewpoint

Using a "brokered services" approach, Accenture provides government organizations the ability to build out cloud from legacy IT infrastructure systems and integrate with pre-approved, pre-certified public and private cloud providers and provision with multiple deployment options based on recognized industry infrastructures, platforms, and services. IDC believes that Accenture's cloud-enabled IT operating model, which details functions, processes, governance practices, roles, and organizational models in a cloud environment, is illustrative of the steps that are so critical for addressing the key changes that must occur in people, process, and technology.

Accenture's focus on cloud management offerings is evident by the following: Accenture allowing government clients to BYOC when using ACP as well as Accenture's investment in capabilities to support ecosystem partners. For example, the Accenture Center for IBM Technologies (ACIT) provides Accenture access to sales and delivery support, asset development, best practices, and methods and tools for IBM cloud products such as IBM Bluemix.

A key capability that Accenture offers is cloud labs for pilot testing, or testing as a service. Lab testing enables government to test its cloud solutions, with full scalability and an entire system environment such as ERP, without risk. Because of this ability to quickly demonstrate system capability and operational results to government clients, coupled with Accenture's deep industry knowledge, ecosystem relationships, and experience-as-a-service integration to create differentiated solutions that address governments' unique issues, IDC has assessed Accenture as a Leader in this IDC MarketScape.

AT&T

AT&T offers managed private cloud on government sites, dedicated private cloud on AT&T sites, and a private cloud solution that can be deployed within AT&T datacenters or on a customer's premise, virtual private cloud, hybrid cloud, and public cloud. AT&T is working to build a government-only computing community cloud based on a partnership with CSC. Today, AT&T offers a government cloud storage solution, AT&T Synaptic Storage as a Service (STaaS) for Government. This is a multitenant storage infrastructure that operates within AT&T's Internet datacenters exclusively for government. AT&T STaaS stores government data in a protected environment while making it available to authorized personnel and is accessible online via an API.

The AT&T STaaS platform utilizes EMC Atmos technology and AT&T networking components to create a separate cloud for federal government clients where an agency's physical data and metadata are separated from commercial clients' data and access is gained via a separate, fully qualified domain name. Protection of and access to agency data objects are accomplished using policy-based data storage. STaaS service administration is through a Web-based portal, enabling easy management of cloud-based storage resources. Access to the STaaS Web portal is secured through two-factor authentication.

AT&T Synaptic Compute as a Service (CaaS) with VMware vCloud Datacenter Service is a pay-as-you-go, on-demand public cloud service that provides and manages the virtualized infrastructure including network, servers, and storage. This solution allows users to create and control their network and storage resources. AT&T Synaptic CaaS can be accessed over the Internet or via AT&T's private networking options.

AT&T also offers the AT&T Government Cloud, powered by CSC, a compute-as-a-service offer delivering AT&T networking capabilities and CSC integration backed by the hardened and layered network security and AT&T's Internet datacenter. This offering provides self-management tools for customers to create manage and monitor their own virtual datacenter environment. Optionally, clients may choose to implement a fully managed service environment monitored and operated by AT&T.

As part of AT&T Consulting Services, AT&T provides a portfolio of professional services support for cloud and datacenters. The AT&T Cloud and Data Center Transformation includes architecture, integration, optimization, and transition services for cloud and datacenter including network, datacenter fabrics, server, storage, virtualization, and security. AT&T professional services assists clients in optimizing the application delivery infrastructure, provides an analysis of legacy applications for migration to virtualization and cloud services, and provides required readiness activities including security, capacity, performance and orchestration, and provisioning management. AT&T also assists clients in developing a phased deployment road map for datacenter and cloud optimization and provides an evaluation of the physical plant for support of private cloud services and long-term datacenter growth requirements. Additional professional services capabilities include IT service management (ITSM), contact center, unified communications, project management, IT transformation, and security.

AT&T Synaptic Storage as a Service is FedRAMP complaint, and AT&T is pursuing a JAB Provisional Authorization for the AT&T Government Cloud, powered by CSC, as a government-only IaaS community cloud. AT&T is complaint with additional cloud security standards as listed in Table 3.

AT&T offers a full set of cloud management capabilities as seen in Table 4. AT&T does not support SQL or NoSQL databases but does support hypervisors. AT&T offers all the value-added services listed in Table 5 as well as PaaS, SaaS, and cloud disaster recovery/backup. Future plans may include cloud brokering/aggregation/marketplace and capability for government to leverage Big Data in the cloud.

Strengths

AT&T is focused on growing its IaaS revenue in the federal government segment, sells through a direct sales force, and works through partners to provide services to the federal government. Some of AT&T's channel partners include Lockheed Martin, SAIC, HP, Northrop Grumman, and CSC.

AT&T's technology partners include CSC and VCE with community cloud; VMware for CaaS; EMC for cloud storage; and Amazon, Microsoft, and IBM for NetBond. AT&T NetBond connects AT&T Multiprotocol Label Switching (MPLS) VPN to a growing list of leading cloud solution providers in addition to AWS, IBM, and Microsoft; AT&T's technology partners, SoftLayer, Equinix, HP, CSC, Salesforce, Box, and VMware, are also named as strategic NetBond partners. AT&T NetBond's proprietary technology leverages network orchestration, allowing customers to "bond" their AT&T Multiprotocol Label Switching VPN to the cloud for the delivery of mission-critical applications. The benefits of NetBond include the ability to extend network security to cloud solutions without additional equipment or access lines for existing AT&T MPLS VPN customers. AT&T NetBond provides coordinated, on-demand scaling of networking and computing resources and built-in network burstability to align with workload demands.

Challenges

AT&T's core strength remains the company's ability to offer a secure, integrated network and leverage the company's datacenter capacity. AT&T needs to continue to deepen its expertise in the government cloud segment to keep pace with its rivals in the SI and cloud-centric provider segments and not only deliver automated IaaS offerings but also develop platform-based service delivery and create network-dependent communications, collaboration, and business applications to keep pace with solutions for the government market.

IDC Viewpoint

As one of the first FedRAMP cloud storage providers, AT&T is now leveraging its STaaS as a government community storage cloud by providing logically separated government data and separate physical storage towers. This solution functions as an expandable pool of stored data and, through the API, is especially suited for user files that need to be archived or shared for all applications other than those demanding tier 1 storage performance. AT&T is currently extending its FedRAMP offerings to include a community cloud computing platform that is dedicated to government customers. IDC has assessed AT&T as a Major Player in this IDC MarketScape. AT&T is leveraging its strength as a secure network provider; NetBond efficiently extends and directly connects not just the network component to the datacenter but all endpoints through secure tunnels with VPN to lower costs, speed up traffic, and provide higher performance and network availability for users, thus securely enabling mobile users' access to stored information.

AWS

Amazon Web Services offers hosted dedicated private cloud, virtual private cloud, public cloud, hybrid cloud, and community cloud. AWS, however, does not offer managed private cloud on the client site. U.S. government community cloud offerings are supported by AWS GovCloud (US), an isolated AWS region of datacenters for U.S. government customers. While GovCloud caters specifically to U.S. government customers, and provides some unique capabilities, many of those customers have chosen to deploy their workloads — including a number of mission-critical and sensitive data workloads — into the standard U.S. commercial regions of AWS.

AWS GovCloud (US) provides the following capabilities:

- Amazon EC2 delivers scalable, pay-as-you-go compute capacity in the cloud. Amazon Virtual Private Cloud (Amazon VPC) provisions a logically isolated section of the AWS cloud. AWS resources are launched in a virtual network defined by the agency. Agencies control their virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways. Agencies can also create a virtual private network (VPN) connection using the IPSec family of protocols between agency datacenters and the VPC (leveraging the AWS cloud as an extension of the agency datacenter.) A VPC can be created quickly using the AWS Management Console or AWS Command Line Interface tools or APIs. When using the AWS Management Console, one of the common network setups that best match agency needs can be selected, and through a virtual private cloud wizard, subnets, IP ranges, route tables, and security groups are automatically created.
- Storage is offered through Amazon S3, a fully redundant data storage infrastructure for storing and retrieving data using RESTful interfaces over the HTTPS protocol. Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance block storage collections that persist independently from EC2 instances, with potentially separate life cycles and life spans. AWS Import/Export accelerates moving large amounts of data into and out of the AWS cloud using portable storage devices for transport.
- Amazon has offered the Amazon Virtual Private Cloud since 2009. The Amazon VPC allows users to create a virtual network of logically isolated EC2 instances and an optional VPN connection to the Amazon datacenter. Additional features include multiple IP addresses, multiple network interfaces, dedicated instances, and statically routed VPN connections. For the past 18 months or so, Amazon has provided EC2 with the VPC automatically provisioned by default (the "set it and forget it" strategy, with VPC already provisioned for more user control and security). Amazon VPC is designed to be compatible with existing shell scripts, AWS CloudFormation templates, AWS Elastic Beanstalk applications, and Auto Scaling configurations.

Strengths

AWS has made strategic investments in complying with U.S. government cloud security requirements, as evidenced by its two "firsts" certifications. AWS was the first vendor to receive an Agency Authorization to Operate (ATO) from the U.S. Department of Health and Human Services (HHS) utilizing a FedRAMP-accredited Third Party Assessment Organization (3PAO) for the following services: Amazon EC2, S3, EBS, VPC, and IAM. The FedRAMP Agency ATO was granted for both AWS GovCloud (US) as well as the U.S.-East-1, U.S.-West-1, and U.S.-West-2 commercial regions.

AWS is also compliant with multiple cloud security standards, as listed in Table 3. Moreover, AWS has opened significant U.S. government market opportunity by also being the first company with the ability to take any and all of DoD's unclassified data to the cloud. AWS previously attained DoD CSM levels 1-2, allowing DoD entities to store, process, and maintain a diverse array of DoD data within the AWS cloud. As of August 2014, AWS GovCloud has been issued a provisional authorization to allow DoD agencies to deploy pilot applications handling their most sensitive unclassified data, levels 3-5.

AWS offers a full set of cloud management capabilities as shown in Table 4, as well as cloud readiness, proof of concept, implementation, migration, and integration with legacy infrastructure. Through its partners, AWS supports a variety of SQL databases such as Microsoft SQL Server, Oracle, and MySQL and NoSQL databases such as Apache Cassandra, Apache HBase, and MongoDB. AWS supports Hyper-V and vSphere EXSi for services such as VM Import/Export, and relies on Xen for EC2. AWS offers all the value-added services listed in Table 5, as well as PaaS, SaaS, cloud disaster recovery/backup, and the capability for government to leverage Big Data in the cloud. AWS customers pay only for what they use, with no minimum fees. Reserved Instances give customers the option to make a one-time payment for each instance for one or three years and, in turn, receive a significant discount on hourly charges, as well as a capacity reservation so that they can always launch an instance corresponding to the Reserved Instance.

AWS also has a rapidly growing partner program that includes systems integrators (SIs) such as Booz Allen Hamilton, Deloitte, Capgemini, Accenture, and CSC, as well as Cloudexa, Smartronix, DLT Solutions, InfoReliance and Aquilent. AWS works with Oracle, Red Hat, IBM, SAP, Salesforce, Infor, Lawson, SAGE, Novell, and Dassault Systèmes to provide applications. U.S. government IaaS technology partners for AWS include Acquia, Adobe, Digital Reasoning, Esri, Pega Systems, Digital Globw, MapLarge, and Recorded Future.

Challenges

AWS' strategy is to innovate and deliver features at a very fast clip. AWS does not conduct R&D in a typical fashion following a long-term product development road map. Rather than fund large R&D teams for long-term projects, each AWS service team conducts its own R&D utilizing agile methodologies. An agile software development model first identifies customers' key business needs, creates "stories" around satisfying those needs in small chunks, and then conducts "development sprints" to introduce new features, expanding the list of AWS services available in AWS GovCloud. However, AWS will increasingly compete with systems integrators (many of which are partners) that have strategically developed their product road map as well as best practices in professional services. As the U.S. government market matures, and cloud supports critical government business processes, AWS may need to rely more on partners whose "asset light " nature may place the company in a more profitable position to support government business needs with innovative professional services approaches, strategic product planning, and broad application developer ecosystems.

IDC Viewpoint

AWS (AWS GovCloud [US]) is a Leader in this IDC MarketScape. AWS has an excellent chance to gain U.S. government business in the IaaS solution space and continue to leverage its behemoth datacenter assets. As the first company with the ability to take any and all of DoD's most sensitive unclassified data to the cloud, AWS has opened a significant opportunity for not only itself but its partners as well. Although AWS is known for its forward-looking pricing and multiple price reductions as well as "try and fail fast" for "pennies a day" marketing messages, IDC observes that AWS' strategy is to look beyond being a low-cost cloud provider and to focus on innovation spanning the promise of quickly adding infrastructure from additional servers to deploying a 1PB data warehouse to launching significant services and features. Similar to other U.S. cloud providers, AWS has renamed its government cloud offering to AWS GovCloud (US), allowing for branding and clarification of features and services available on government-certified solutions.

CenturyLink

CenturyLink currently provides virtual private cloud, public cloud, and private cloud capabilities (through its acquisition of Tier 3). In the third quarter of 2014, CenturyLink announced the availability of managed private cloud within its datacenters, but it does not offer managed private cloud on an agency site. CenturyLink also announced the availability of community cloud for the U.S. federal government in the third quarter of 2014. CenturyLink's cloud platform uses VMware vSphere 5 and includes custom engineering for automation and orchestration functions. CenturyLink provides storage area network (SAN)-based designed block storage, object storage, flash, and SATA. CenturyLink is undergoing testing for FedRAMP Moderate for its public cloud offering and is compliant with additional cloud security standards as listed in Table 3.

CenturyLink offers a full set of cloud management capabilities as seen in Table 4 and supports SQL databases such as MS SQL Server and MySQL. CenturyLink is also compatible with NoSQL databases such as Couch, Cassandra, and Hadoop. CenturyLink supports VMware hypervisors. CenturyLink offers the value-added services listed in Table 5, as well as PaaS, cloud disaster recovery, and the capability for government to leverage Big Data in the cloud. CenturyLink is currently providing cloud training for CenturyLink and CenturyLink Technology Solutions (formerly Savvis) direct sales personnel. CenturyLink is also focused on growing indirect revenue via white-label capabilities with resellers and jointly promoting cloud services with its partners such as Intel. U.S. government technology partners include VMware, Dell, Intel, NetApp, and Pivotal. U.S. government channel partners include Accenture, Layered Technologies/New World Apps, CSC, SRA, and Deloitte.

Strengths

CenturyLink is one of four U.S. telco vendors that provide carrier-class cloud services as a vendor-managed Trusted Internet Connection (TIC). CenturyLink's road map is focused on bringing "agile infrastructure" services into a single, unified platform – making it easy for customers to provision and manage different types of infrastructure for enterprise workloads. Through its recent acquisitions of Savvis and Tier 3, CenturyLink is in the process of integrating different types of infrastructure, managed services, and network capabilities into a single platform and increasing indirect revenue via channel partners.

Challenges

The challenges that CenturyLink faces include moving beyond its telco revenue base and leveraging its acquisitions as well as positioning itself as a trusted network provider to compete with the likes of large infrastructure providers with significant presence in the U.S. federal government market. CenturyLink's alliances with SIs such as Accenture, CSC, and Deloitte will assist in positioning the company's cloud offerings.

IDC Viewpoint

IDC has assessed CenturyLink as a Contender in this IDC MarketScape. In its quest to transition form a telco provider to a provider of cloud services for the U.S. government, CenturyLink is leveraging its deep IT infrastructure experience and robust network with its recent acquisitions of Savvis (managed hosting and datacenter outsourcing) and Tier 3 (a provider of both IaaS and PaaS) to become a more credible player in this space. Tier 3 also brings the capabilities of an automated cloud management and orchestration platform and a multi-framework/multiservice application deployment and runtime environment based on Cloud Foundry and Iron Foundry. These acquisitions will help CenturyLink move beyond its traditional target buyers in the IT department to developers and line-of-business decision makers who will play increasingly important roles in cloud implementation and service provider selection.

CGI

CGI provides managed private cloud on the client site, hosted dedicated private cloud, virtual private cloud, and dedicated community cloud for the U.S. public sector. Future plans include multicloud management to include private, community, and/or public cloud workloads. CGI's cloud strategy is to focus on services that enable the IT mission through a high-touch service model that provides:

- Business-centric analysis and transition planning including datacenter consolidation and cloud readiness assessments and adoption (CGI deploys tools such as Cirba to help government optimize its infrastructure portfolio and migrate from physical or virtual environments to the cloud. CGI has developed proprietary assessment methodologies to assess the readiness for cloud migration.)
- Automated cloud service management via CGI's secure cloud portal that enables such features as provisioning and deprovisioning services and powering up and down virtual machines (VMs) and Web servers, order management, and workflow-based approvals for security and network changes (i.e., firewall rules changes) (CGI provides a service catalog of products and services.)

CGI is one of the first large cloud services providers and systems integrators to receive FedRAMP P-ATO. In addition to FedRAMP, CGI is complaint with additional cloud security standards as listed in Table 3.

CGI offers a full set of cloud management capabilities, except for burst across private and public cloud as seen in Table 4, and supports databases such as Microsoft SQL Server, Oracle, and MySQL. CGI also supports Hadoop. CGI supports VMware and Hyper-V hypervisors. CGI offers the value-added services listed in Table 5, as well as PaaS, SaaS, and cloud disaster recovery. Future offers will include the capability for government to leverage Big Data in the cloud and cloud brokering for the U.S. federal government that will allow access to various SaaS offerings (such as Microsoft Office 365 and salesforce.com), platform as a service, and bursting capabilities to public IaaS providers such as AWS and Microsoft Azure.

CGI goes to market with a combination of a client proximity model (around strategic accounts with dedicated sales and delivery leads) as well as industry verticals (practices). CGI also has a partner program to jointly sell CGI IP and solutions and partner technology. U.S. government technology partners include BMC, Cisco, Hitachi, Microsoft, and VMware. U.S. government channel partners include Cisco, Hitachi, and Microsoft.

Strengths

Government represents a major share of CGI's business, which has driven the company to develop very in-depth expertise in a variety of areas (for instance, growing its focus on cybersecurity). CGI also has deep experience in legacy systems, strong consulting and integration capabilities, and a history of IT outsourcing and business process outsourcing. Its practice includes planning for successful transition and operations in cloud. CGI is also leveraging its IT investments through three global governance bodies, a global technology council, an IP management framework, and an internal VC program. These governance bodies monitor key trends and govern investments such as United States-based government-specific IaaS solutions, additional maintenance solutions, and seed monies for innovations.

Challenges

The U.S. government has more IaaS cloud vendor options than ever before. CGI will need to continue to build out its IaaS offerings as well as key partnerships to support this market's requirements. CGI has a sense of urgency to evolve its cloud capabilities; the challenge for CGI, though, will be to reach beyond its traditional clientele and differentiate itself based on its service practice.

IDC Viewpoint

IDC has assessed CGI as a Leader in this IDC MarketScape. IDC believes that CGI has the potential to drive new cloud revenue growth in its federal government business via its enterprisewide horizontal cross-industry practice that facilitates "industry cross-pollination" for cloud computing. CGI is also investing in the creation of thought leadership in the areas of cloud brokerage, cloud security, and cloud readiness and expanding its technology partnerships and including these solutions into its private cloud offerings. Although CGI's solid IP and end-to-end service delivery capabilities will act to the advantage of the company, CGI has a way to go in proving that it has differentiating offerings here. As it grows, CGI needs to plan for consulting offers that drive revenue beyond agencies' application portfolio rationalization, cloud readiness, and cloud migration planning.

CSC

CSC's IaaS private cloud portfolio consists of CSC BizCloud, which provides managed private cloud on U.S. government sites, as well as a dedicated private cloud for a single tenant in a CSC datacenter. CSC private IaaS clouds provide dedicated compute capacity with blade segregation, dedicated VPN, and point-to-point connections as well as public Internet connectivity. CSC also provides multiple logically segregated cloud storage options but does not offer object-based storage. Through its partnership with AWS and AT&T, CSC provides virtual private cloud and community cloud. Through its partnerships with Microsoft Azure and AWS, CSC leverages these public clouds with its BizCloud for a hybrid cloud offering. AT&T, AWS, and Microsoft cloud solutions are covered in their respective sections in this study.

CSC's FutureEdge for Modernization provides modernization and application portfolio management services that leverage transformative technologies such as cloud. CSC provides many choices through a modular set of services, such as application remediation to extend functionality and unlock data from legacy applications for better access and usability, as well as re-architecting of processes such as moving legacy data structures to relational databases and building a cloud-based infrastructure to host critical business applications. Options include moving from mainframe to AIX or cloud, COBOL to Java or .NET, legacy data structures to relational databases or refactoring custom applications. CSC offers management of cloud after migration, including management, integration, and brokering of IaaS, PaaS, and SaaS. CSC also offers building application stores. CSC provides the ServiceMesh Agility Platform, an enterprise cloud management platform that automates and provides a single, policy-driven, integrated control point for governance; compliance; and security for IaaS, PaaS, and SaaS across private, public, and hybrid cloud environments. The ServiceMesh Agility Platform provides fully governed, self-service access to applications, platforms, and services.

CSC has an agency ATO for its private cloud and is seeking FedRAMP compliance for the CSC BizCloud for dedicated private cloud on a vendor site and FedRAMP compliance for hybrid and community cloud. CSC partners with AWS for virtual private cloud. CSC's public cloud partners such as AT&T's STaaS (storage as a platform) and Microsoft's Global Foundation Services (GFS) have FedRAMP certification. CSC also has the additional security certifications listed in Table 3. CSC does not offer the capability to burst across private and public cloud but offers the other capabilities shown in Table 4.

CSC supports SQL through Microsoft SQL Server, Oracle, MySQL, PostgreSQL, and AWS RDS. CSC supports NoSQL databases such as DynamoDB, Cassandra, MongoDB, and Hadoop. Hypervisors supported by CSC include VMware, Hyper-V, KVM, and XEN. CSC offers all the value-added services listed in Table 5 except for integration with legacy infrastructure, which is in the planning stage.CSC offers PaaS, SaaS (through partners) cloud brokering/aggregation/marketplace, cloud disaster recovery/backup, and the capability for government to leverage Big Data in the cloud.

Strengths

Cloud services is one of five core areas of focus for CSC (the other four core areas are Big Data, mobility, cybersecurity, and apps services), and CSC is putting investments behind a plan to become number 1 or 2 globally in cloud. CSC's approach is to provide a breadth of consulting services through FutureEdge to assist government in migrating to IaaS either through the CSC BizCloud or through the

IaaS offerings provided by partners such as AWS, Microsoft Azure, and AT&T. For these cloud services, CSC is the first-level triage for its customers, and CSC staff is licensed to support these partners. CSC provides managed services in addition to tier 1 support such as providing software patches and antivirus software.

CSC recently changed its R&D funding process for cloud initiatives. An investment review board pulls requirements and resources globally looking for commonality versus each region or business segment funding separate cloud initiatives. The result is efficient solutions, eliminating overlap and duplication, with a single team focused on a standard way of doing business.

In August 2014 CSC announced plans to establish a new IBM Center of Excellence to offer clients SoftLayer cloud services and the IBM Bluemix cloud development platform. Also, IBM and CSC will enable CSC's ServiceMesh Agility Platform to deploy to the IBM Bluemix and SoftLayer cloud environments. Both IBM and CSC will collaborate on consulting, apps modernization tools, Big Data and analytics, cloud and mobile capabilities, and security to create a single, consumable services framework.

Challenges

Beyond "no vendor lock-in," CSC will need to distinguish itself from its partners and competitors in a crowded field of government cloud vendors and show how it is well suited to support agency long-term strategies and road maps. CSC clearly understands its aggregator role, and this allows CSC to pursue transformational work rather than pure infrastructure delivery. CSC needs to stay focused on the application set of services and not let its migration strength become a weakness that prevents CSC from developing deep expertise in supporting government line-of-business managers (in addition to its loyal IT customers) in deploying transforming technologies such as Big Data and mobility.

IDC Viewpoint

CSC brings vast experience in legacy IT support and is positioned to leverage its existing and long-standing base of government customers that have outsourced IT infrastructure and applications to CSC. In its role as a cloud aggregator/broker, CSC is continuing its traditional vendor-agnostic technology approach. Migrating many larger and older government legacy systems, known for having a host of obscure languages and technologies, to cloud may be challenging. However, CSC may be in a well-placed position to assist government in its infrastructure modernizing to cloud and can leverage this expertise as an enabling stepping stone toward digital transformation. CSC is taking an important step away from infrastructure ownership through alliances with AWS, AT&T, and Microsoft Azure. This is part of CEO Mike Lawrie's strategy to make CSC an asset-light company in order to focus on areas where it has market-leading expertise and can extract the highest margins – its application and business services to support government increasingly moving workloads to the cloud. IDC has assessed CSC as a Major Player in this IDC MarketScape. Through its alliance partners, CSC now provides its government client base with additional options when assessing service providers that can migrate their existing infrastructure and put together complex solutions that tie network, cloud platform, and applications together.

Dell

Dell offers two options for the U.S. federal government. A government private cloud solution with complete physical separation of the infrastructure aims to support production applications and databases with specific performance, data privacy, and/or compliance requirements. In 2013, Dell launched a multitenant government community cloud aimed at supporting less sensitive workloads, such as office and productivity suites and Web-based platforms that require more flexible and affordable delivery.

The Dell private cloud solution is based on cloud technology System Center 2012 with the Dell Integration Suite and Microsoft Windows Server Hyper-V; it can be deployed as a converged solution in the customer datacenter or delivered as a dedicated private cloud from a Dell datacenter. The Dell multitenant cloud is also based on the Dell-Microsoft converged stack and is delivered from Dell datacenters. Dell's converged infrastructure solutions are usually packaged with Microsoft software; however, Dell's cloud solutions fully support VMware, and Dell recently announced collaboration with Red Hat to further enterprise adoption of OpenStack. Dell supports multiple SQL databases and hypervisors and plans to make investments in non-SQL databases in the next 12 months.

Beyond converged infrastructure hardware and software, the Dell cloud portfolio includes IT services for datacenter transformation such as virtualization performance health check for cloud readiness assessment for government customers that want to implement a dedicated private cloud solution on their premises. And Dell includes management services for the ongoing support of its cloud solutions.

Dell is undergoing provisional FedRAMP certification for its IaaS community cloud and also has the additional certification listed in Table 3. Dell offers all the cloud management capabilities shown in Table 4. Dell offers all the value-added services listed in Table 5, except for proof of concept/piloting/testing. Dell does not currently offer PaaS and delivers Dell Boomi's management and development interfaces as SaaS. Dell Cloud Manager has a SaaS edition, as does Foglight. For its IaaS, Dell offers cloud disaster recovery/backup and the capability for governments to leverage Big Data in the cloud. Dell is entering into a public beta for Dell Cloud Marketplace in late 2014. The Dell Cloud Marketplace is designed to bring IT managers, developers, and vendors together to create a new ecosystem and exchange and simplify how Dell's customers compare, purchase, use, and manage cloud solutions from a variety of leading public cloud vendors and cloud-based application providers. While not specifically designed to support the government market, this is part of the greater Dell cloud offering. As a cloud broker, Dell combines its cloud partner ecosystem of public cloud providers with analytics, expert service and support from Dell Services, Dell Cloud Manager, and additional third-party cloud-based applications.

Strengths

Dell's growth strategy is focused on infrastructure transformation and migration of a customer's technology portfolios to appropriate environments, including cloud and mobile computing. The strategy aims to provide converged infrastructure solutions for building cloud environments including appliances, validated reference architectures, and optimized components for compute, storage, and networking — all with platform-agnostic operations software (OpenManage). Dell's strategy is to achieve unified management in hybrid cloud provisioning via cloud management and brokerage models. Dell has developed a vast array of infrastructure solution partnerships, such as VMware and

Red Hat, as well as cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, CenturyLink, and Google Cloud Platform. Dell is entering into public beta for Cloud Marketplace. Dell provides a wide-ranging product and service offering, including mobile computing capabilities that are becoming a key driver of cloud adoption.

Challenges

Historically, Dell has been adept at selling point products such as PCs and servers into the market. The company needs to become more competent at putting hardware, software, and services offerings together in order to meet unique customer challenges and deliver business solutions. This will necessitate engaging with a different set of influencers and decision makers.

IDC Viewpoint

IDC has assessed Dell as a Major Player in this IDC MarketScape. Although Dell has announced several partnerships with SIs, it is also entering into intense competition with SIs that have long focused on enterprise solutions and will need major commitments and investments in resources to provision superior, end-to-end enterprise solutions for virtualization and cloud.

HP

HP's U.S. government IaaS deployment models include managed private cloud on the agency site, hosted dedicated private cloud, virtual private cloud, public cloud, hybrid cloud, and community cloud. HP Helion Managed Private Cloud for Public Sector is a dedicated single-tenant managed private cloud offering of compute and storage delivered on-premise or off-premise and sold on either a capex or an opex basis. HP owns, manages, and hosts all server hardware. HP provides the option of managing the cloud operating system with HP-Managed Server, or government clients can manage their own through HP Customer-Managed Server.

The HP Helion Managed Virtual Private Cloud for Public Sector uses one of HP's datacenters, with a secured multitenant environment for U.S. persons only. For both the HP Helion Managed Private Cloud for Public Sector and HP Helion Managed Virtual Private Cloud for Public Sector, HP offers self-service portals, capacity management, service catalogs, network security services with policy compliance management, vulnerability scanning, and ID/access management. The HP Helion portfolio includes products, software, and services that span HP. The portfolio includes the next-generation HP CloudSystem; HP Cloud Service Automation (HP CSA) software for managing hybrid IT environments; HP Public Cloud; HP Managed Enterprise Services (including VPC, private cloud, and managed cloud application services); HP Helion OpenStack — an open standards-based scale-out and extensible cloud platform that delivers a common architecture across private, public, and hybrid clouds; and OpenStack technology-based professional and support services.

HP has FedRAMP certification for its virtual private cloud for the U.S. government as well as the additional security certifications listed in Table 3. HP offers a full set of cloud management capabilities as seen in Table 4 and supports databases through Microsoft SQL Server, Oracle, and MySQL. HP plans to support NoSQL databases through Vertica. Hypervisors supported by HP include VMware, Hyper-V, and KVM. HP offers all the value-added services listed in Table 5 as well as PaaS, SaaS, and cloud disaster recovery/backup. HP has plans to offer cloud brokering/aggregation/marketplace and the capability for government to leverage Big Data in the cloud.

Strengths

HP has united its cloud products and services under the Helion moniker, a move that assures that all new products and services are tightly integrated and aligned. One of the drivers for this is to assist federal government customers in making it easier to build, integrate, manage, and consume workloads in a hybrid IT environment. HP plans to invest more than $1 billion over the next two years on cloud-related product and engineering initiatives, professional services, and expanding HP Helion's global reach. HP is also extending its commitment to OpenStack technology and hybrid IT delivery — spanning traditional IT, public, private, and managed clouds. HP is one of the primary proponents of the OpenStack project, promotes open source innovation, and enables customers to combine public, private, and hybrid clouds models along with traditional IT solutions. HP provides indemnification and professional services with HP Helion OpenStack.

Challenges

While HP's approach focuses appropriately on mission as the starting point and provides a traditional comprehensive HP solution marketplace support to government in a new cloud venue, HP may not be agile enough to compete with other systems integrators that are leveraging each other's strengths or with cloud brokers in this market. As strong as HP's approach to the government market is (focusing on mission outcomes) and as robust as the company's life-cycle services approach is, there are a few questions regarding HP's cloud strategy. Is HP positioning its cloud infrastructure at the expense of avoiding vendor lock-in? Can HP maintain its track record in being an "enabler" and "arming" service provider partners with hardware and OpenStack technology while at the same time becoming a large and successful provider of OpenStack-based cloud services (especially in the virtual private cloud market), essentially based on the same technology stack it is providing its partners with?

IDC Viewpoint

IDC has assessed HP as a Leader in this IDC MarketScape. It's apparent that HP no longer sees the product — hardware or software — as the goal. The goal is now the business outcome, enabled by the product. HP's approach to providing government cloud services is unique in two ways. The positioning of HP's cloud solutions begins with the agency mission outcomes as the first of seven steps in delivering services across interconnected practices (the steps are mobility and workplace, analytics and data management, applications, security services, and business process services). Having HP executives dedicated to specific agencies or agencies with common business needs, understanding the requisite outcomes as the driver of the solution, and then leveraging the vast HP Helion solution portfolio should give HP an advantage in providing a solution that can provide desired outcomes. HP also takes a traditional service management approach to supporting its federal customers for design, build, operate, evolve, and extend for managed private clouds and a similar offering beginning with operate for managed virtual private cloud, leveraging its EDS history of life-cycle services management.

Uniting its cloud offering under the Helion brand enables a consistent overall product and services strategy and messaging and represents a significant effort to simplify the customer experience and make it much easier for governments to purchase unified hybrid cloud hardware, software, and services solutions from HP. With its support for OpenStack, HP has made a very strong commitment to an open and heterogeneous approach to hybrid cloud management and support for third-party hardware, even though some of the features of HP Helion OpenStack are only available for HP technology. By providing a hardened distribution of the open source-based OpenStack framework, HP may make it easier for government customers to take advantage of this hybrid cloud management framework and mediate some of the risk involved in deploying open source technology.

After HP's split into two separate public companies, Hewlett-Packard Enterprise focusing on technology infrastructure, software, and services (where the Helion platform will reside) and HP Inc. focusing on personal systems and printing company, HP should assist in the focus, operational alignment, and leverage of resources within each company.

IBM

IBM offers managed private cloud on the client site, hosted dedicated private cloud, virtual private cloud, public cloud, hybrid cloud, and shared community private cloud referred to as IBM SmartCloud for Government. IBM continues to expand its cloud infrastructure offerings for the U.S. federal government through its acquisitions, such as SoftLayer. The SoftLayer platform provides single-tenant and multitenant cloud servers and storage. SoftLayer provides bare-metal servers (i.e., single-tenant servers) (government can choose from entry-level single processor servers to quad-core processors, hexa-core, and GPU-powered workhorses.) Bare-metal servers can be customized with RAM, SSD hard drives, and network uplinks. IBM SoftLayer also provides flexible virtual servers. SoftLayer virtual servers can be deployed with primary storage based on local disk or storage area network and with portable storage volumes as secondary storage. SoftLayer provides a common management interface across a unified architecture that allows for a single control panel, API, portal, or mobile application management of mix-and-match bare-metal servers, virtual servers, and turnkey private clouds. This feature allows government clients access, control, and visibility for their cloud infrastructure, allowing agencies to not only build cloud environments to their specific compliance and security needs but also to manage deployments across public, private, or hybrid clouds on one platform.

IBM SmartCloud for Government has FedRAMP certification as a certified managed hosting environment hosted within two secure IBM datacenter sites in the United States. In addition to FedRAMP, IBM is complaint with additional cloud security standards as listed in Table 3.

IBM offers a full set of cloud management capabilities as seen in Table 4 and plans to support SQL (Microsoft SQL Server) and NoSQL, MySQL, Cloudera, Hadoop, MongoDB, and Cloudant within the next 12-18 months. IBM IaaS supports VMware. IBM plans to additionally offer ESX and ESXi, Citrix XenServer, Citrix CloudPlatform, Parallels Virtuozzo, and Microsoft Hyper-V hypervisors within the next 12-18 months. IBM offers all the value-added services listed in Table 5 as well as PaaS, and SaaS, and cloud disaster recovery/backup (providing backup and restoration of data, including configuration of the backup storage [scheduling, encryption] as well as management of sequential media and coordination of offsite storage). IBM provides multiserver deployments for Big Data and NoSQL solutions through collaboration with Cloudera (purchased by IBM), MongoDB and Basho.

Strengths

IBM's strategy is to deliver end-to-end solutions, offering customers a step-by-step deployment road map to transition from traditional IT environments to private, public, or hybrid clouds. IBM consultants use a cloud adoption framework and the IBM Cloud Workload Analysis Tool to analyze an existing environment and determine the cloud computing model best suited for the business model. IBM has also developed ROI tools and solution accelerators like the Cloud Migration Rapid Assessment that provides a cost-effective, low-risk plan for the migration of workloads to a new platform so that organizations can quickly realize the benefits of a cloud environment. IBM is growing its portfolio to match this strategy and investing heavily in the cloud — more than $7 billion, including investments of more than $4.5 billion in more than a dozen acquisitions since 2007, such as start-up Cloudant and, most recently, SoftLayer, to extend IBM's cloud capability. SoftLayer provides an IaaS foundation upon which IBM continues to innovate by bringing software capabilities into the cloud environment. IBM has a deep portfolio of SaaS capabilities, delivering over 120 individual offerings to the market including Watson Analytics services.

Challenges

Through its acquisitions and investments, IBM is now managing lots of moving parts. The challenge for IBM will be how fast the U.S. government market can move for IBM to receive a return on its major investments.

IDC Viewpoint

IDC believes that the SoftLayer acquisition provides IBM a strategic advantage in providing one of the most advanced automation layers in the IaaS market. SoftLayer bare-metal servers (dedicated single-tenant servers) provide added control and enhanced performance predictability ideal for government workloads focused on high-performance computing and advanced analytics. SoftLayer allows self-service and rapid provisioning of a wide variety of IaaS configurations. This sets IBM SoftLayer up to play a leading role in serving the "hybrid/mixed" cloud requirements of government entities, which, to date, have shied away from leveraging public cloud–only offerings. IBM's IaaS technology (highly scalable, self-service optimized, and low cost) is also easier for government to deploy because of consumption-oriented billing and no long-term contracts.

IBM is on a path to provide services and solutions to all layers of the cloud stack, and that coupled with its deep industry knowledge positions it to deliver innovation for new cloud workloads. IDC believes that this IBM capability, coupled with IBM's strong Bluemix open standards–based PaaS environment, which simplifies application development in the cloud, is a game changer. Bluemix allows line-of-business users and application developers to quickly deliver new applications. IBM's Bluemix Garage and the IBM Cloud Marketplace continue to extend the IBM cloud ecosystem and support large-scale enterprise adoption of cloud computing. IDC has assessed IBM as a Leader in this IDC MarketScape.

Microsoft

Microsoft is currently launching Azure Government, and this solution is in the preview stage for U.S. federal government clients. Microsoft Azure Government solutions include managed private cloud and community cloud with data, applications, and hardware hosted in Microsoft datacenters located in continental United States. Microsoft Azure Government provides scalable storage, backup, and recovery. Azure Backup provides incremental backups to conserve storage and reduce bandwidth consumption, with point-in-time recovery of multiple versions. This feature is designed to protect applications by coordinating the replication and recovery of private clouds across sites, with options of using a second disaster recovery site, including the option of Azure Government.

Key elements include two specially constructed datacenters that are more than 500 miles apart with logical, physical, and network isolation from Azure Public Cloud and data that will reside on servers that only contain data from other U.S. federal, state, and local government customers.

Microsoft offers public cloud and virtual private cloud through Microsoft's Global Foundation Services cloud infrastructure. Microsoft Azure IaaS also offers virtual private cloud instances, where customers have options for greater security and control over their own logically isolated data. Microsoft is expanding its preview of Microsoft Azure Government and has announced plans to broaden its government cloud portfolio with a new Microsoft Dynamics CRM Online U.S. Government cloud offering.

Microsoft Azure Government is in the process to receive FedRAMP certification. This offering will be a separate instance for government customers in compliance with FedRAMP and operated by U.S. citizens. The service, which will be available in late 2014/early 2015, will allow customers to leverage their existing Microsoft investment on-premises and in the cloud through hybrid cloud capabilities including integration with the Azure and Office 365 Government clouds. Microsoft holds FedRAMP approval for IaaS and PaaS with Azure and SaaS for Office 365 Government. Additional certifications are listed in Table 3. Microsoft Azure Government offers a full set of cloud management capabilities as shown in Table 4 and supports SQL Server, Oracle, and MySQL, and many OSS options are supported through virtual machines. Microsoft Azure Government also offers NoSQL databases such as Hadoop, Azure Tables, Queues, and many OSS options supported through virtual machines. Microsoft supports Hyper-V. Microsoft Azure Government offers the value-added services listed in Table 5, and Microsoft offers PaaS, SaaS (Office365), a cloud brokering/aggregation/marketplace through Azure Store, and cloud disaster recovery/backup through Azure StorSimple and Azure Site Recovery.

Strengths

Microsoft's vision is to be set apart from cloud infrastructure providers through finished services such as Azure Active Directory, data, mobility, and productivity alignment. Microsoft continues to invest in increased network and datacenter capacity. Microsoft also has a strong market presence and partnership network. Microsoft has stepped up its investment by offering Azure Government cloud, operated by screened personnel, with a physically isolated datacenter and network.

Challenges

Microsoft started with PaaS solutions and has moved into first public and now private IaaS for its U.S. government clients. Microsoft will be challenged to scale its IaaS business for the U.S. government and compete with the SIs that have supported this market starting with datacenter consolidation and outsourced services. Microsoft will need to build the capability to migrate government customers to the cloud, and the Microsoft stack may limit agility for customers that need to integrate with other software platforms.

IDC Viewpoint

There are currently varying levels of cloud and mobile maturity across the U.S. federal government, and many IT departments have made significant investments in both on-premise infrastructure and systems management software. Therefore, Microsoft will need to clearly articulate how it intends to further innovate, integrate, and/or replace its more traditional, yet well-established and profitable, on-premises offerings with its new cloud-based solutions. In addition, Microsoft and its channel partners will need to make continual investments in providing a full spectrum of IT services related to cloud in order to compete to win. IDC has assessed Microsoft as a Contender in this IDC MarketScape. However, the launch of Microsoft Azure Government cloud is positioning Microsoft as a significant private cloud provider for the U.S. federal government.

Unisys

Unisys offers managed private cloud on government sites, dedicated private cloud at Unisys datacenters, virtual private cloud, hybrid cloud, and public cloud through its partnership with AWS, Google, Microsoft, and Virtustream. Unisys' private cloud services provide a flexible computing environment consisting of both virtual and physical servers in either a shared or a non-shared (private) cloud for customers that require server capacity on a subscription basis.

Unisys is provisioning and managing all its services by standardizing on a common IT service management platform that can provide for consistency of service and more cost-effective delivery. This ITSM is also available via cloud/SaaS under the *Edge* brand name for customer-operated environments. Generally combined with Edge, Unisys also offers *VantagePoint* and *Choreographer.* VantagePoint combines enterprise service catalog with user experience analytics, and Choreographer provides a cloud management platform that automates life-cycle management of datacenter and public infrastructure resources from a single Web-based pane of glass. Combined, this capability supports the service delivery and monitoring needed for hybrid applications, leveraging public and private virtual resources to provide efficiency and maximize the agility of the infrastructure that hosts development, test, and production workloads in an elastic, scalable, highly secure manner.

Unisys' FedRAMP certification is in midstream, pursued in parallel for IaaS/Secure Private Cloud for Government (PaaS and SaaS) and SaaS/Edge, with approval anticipated in early 2015. Unisys has the security certifications listed in Table 3. Unisys has announced the availability to achieve FISMA High compliance with *Stealth* on AWS and is working with other CSPs to achieve the FISMA High certification. Unisys offers a full set of cloud management capabilities as shown in Table 4 and supports SQL and NoSQL databases. Hypervisors supported include VMware, Hyper-V, and XEN. Unisys offers all the value-added services listed in Table 5 as well as PaaS, SaaS, a multitenant cloud brokering/aggregation marketplace, and cloud disaster recovery/backup.

Strengths

Unisys, a self-described cloud enabler, broker, and cloud service provider serves government decision makers and executives focused on ITSM to provide a comprehensive cloud architecture to deliver customers the cloud on "their terms." This integrated ITSM capability is core to Unisys' point of view on enabling and managing hybrid cloud environments on behalf of the company's customers. Unisys is enhancing its cloud offering through investments including the following:

- Unisys Edge. Unisys rebranded ITSM as Unisys Edge, an Azure platform product that allows customers to deploy an ITIL-based ITSM service management platform. Edge for Government is the U.S. federal government implementation. Edge also includes the Unisys VantagePoint services.
- Unisys VantagePoint. VantagePoint includes a user-driven knowledge management dashboard that provides visibility into service delivery and workflow. Common job functions within client organizations can be tailored into "personas," delivering highly efficient services. Executive dashboards and service portals that manage and track a full range of service requests are provided.
- Unisys Choreographer. This capability provides a vendor-independent brokerage service that reaches across the Unisys-managed Secure Virtual Private Cloud to simplify hybrid cloud management of public cloud offerings like Azure and AWS. Choreographer integrates brokered cloud offerings with consistent service offerings defined by the client; for instance, the creation of a mission-critical virtual server also triggers the creation of disaster recovery services for that server and full integration into the ITSM platform to associate incidents with appropriate severity.
- Unisys Stealth. The Unisys Stealth technology protects "data in motion" across public or private networks through encrypted key management that conceals communication endpoints, making them undetectable to all unauthorized parties inside and outside the enterprise. Stealth is able to securely virtualize the network, integrating public/private resources into a secure hybrid cloud and promoting compliance with government regulations such as PCI.

Challenges

The breadth and depth of Unisys' capabilities is good and is expanding toward managed cloud and orchestration services that will enable clients to successfully deploy cloud while maintaining operational compatibility. Although Unisys' strong customer service focus is supported by the company's federal clients, a question remains — Are Unisys' strong foundational tools and services support enough to differentiate the company in a crowded market and provide long-term value to the U.S. federal government by transforming its existing infrastructure for the delivery of an agile IT-as-a-service model?

IDC Viewpoint

IDC views Unisys' services strategy as centered across the spectrum of IT, both through vendor choices and multiple cloud infrastructure deployment models, with a lens on offering customers the ability to help transform their IT environments to new service delivery models through the cloud. Unisys has a strong understanding of government requirements as well as unique agency mission requirements. Unisys also has a focus on operational excellence through the use of standards (ITSM), continuous improvement (CSIIP), and robust security capabilities. IDC has assessed Unisys as a Major Player in this IDC MarketScape.

Verizon

Verizon provides dedicated private cloud on its site or at the customer premise, virtual private cloud, community cloud, and hybrid and public cloud solutions. Although private IaaS is part of Verizon's product road map, the company does not manage private IaaS on an agency site at this time.

Cloud professional services are offered for a smooth and secure transition to the cloud and include the following engagements:

- **Application Performance Analysis and Augmentation** — with performance and load testing
- **Business Continuity Planning** — includes business impact analysis
- **IT Infrastructure Strategy and Consolidation** — with datacenter strategy, enterprise architecture review, IT infrastructure design and build, and service catalog design and implementation
- **Cloud Migration Services** — with fine-tuning of virtualization technologies
- **Cloud Strategy and Consulting** — includes application rationalization and infrastructure and application and data discovery
- **Project Management** — with implementation and integration
- **Staff Augmentation** — includes operations and life-cycle support

Beyond these services, Verizon Cloud Onboarding Services provide customers with VM import/export/migration support and workload architecture planning and design through the following offerings:

- Cloud architecture best practices
- High availability design and planning
- Environmental sizing and optimization
- Data backup and storage strategy and best practices engagement
- Proof-of-concept guidance and deployment assistance engagement
- Connectivity and security governance best practices

Verizon currently offers two types of cloud services, base and guided. Base service is recommended as a "DIY" approach and provides agencies with fundamental management and configuration tools supporting users who are well suited to manage most aspects of their cloud space deployment on their own. Clients have access to information through Verizon community forums and online chat assistance. The underlying cloud infrastructure, configuration tools, and unified customer interface are managed by Verizon. In addition, features and tools such as snapshots, backups, self-service monitoring, and advanced performance aspects can be unlocked for incremental monthly fees. Guided service provides additional support expertise and designated response-time commitments beyond what is included in the base service, including 24 x 7 phone access to the Verizon Global Support Operations Service Center manned by technical support personnel. Verizon's Standard and Premium service tiers, where clients have increasing levels of support from named engineers, service managers, and dedicated support teams, are scheduled for deployment in 1Q15.

The Verizon Cloud Console is on the road map to be offered to federal customers and will bring together all cloud spaces under a single user experience, allowing users to provision one cloud space or as many as needed to support varying computing demands and access to additional public and virtual private clouds as well as the new Verizon Cloud Marketplace.

Verizon has recently achieved a community cloud Agency Authorization for FedRAMP through the Department of Health and Human Services. Verizon is also compliant with the additional security certifications listed in Table 3. Verizon offers all cloud management capabilities as shown in Table 4, except for autoscaling, and has plans to provide those to the U.S. federal government. Verizon supports SQL through Microsoft and Oracle but does not currently support NoSQL databases (plans are in the works). Hypervisors supported include VMware and Open XEN. Verizon offers all the value-added services listed in Table 5.

Verizon does not offer PaaS, SaaS, nor cloud brokering, although it is planning to add these offers. Verizon does offer cloud disaster recovery/backup, but for now, it must use Verizon's DBR facility directly until access to disaster recovery/backup options are provided via the use of Verizon Cloud Console by federal customers at a future date. Verizon Cloud does support a capability for government to leverage Big Data in the cloud.

Verizon has a 10-year-plus history of partnering in the federal sector to provide infrastructure services with large, midsize, and small systems integrators (such as Booz Allen Hamilton, CSC, Lockheed Martin, Accenture, Northrop Grumman, and SAIC), independent software vendors, and technology partners (such as VMware, NetApp, EMC, Cisco, and Citrix); Verizon often partners with other technology providers on certain deals and will act as the prime contractor or subcontractor depending on what the solution requires and the contract vehicles that must be used. Verizon is building up an indirect channel to increase distribution and launched a channel program earlier this year.

Verizon has also signed an agreement to go to market with Unisys to offer Verizon enterprise-class cloud computing solutions through Unisys' Public Cloud Hosting contract with the Western States Contracting Alliance-National Association of State Procurement Officers (WSCA-NASPO) cooperative purchasing organization. Although this agreement does not impact the U.S. federal government, it is noteworthy as it signals a partnership of these two government cloud providers.

Strengths

Verizon is leveraging its position as one of four telco vendors that provide Managed Trusted Internet Protocol Services (MTIPS), solutions that are fully compliant with the U.S. federal government Trusted Internet Connection (TIC) initiative. Verizon positions its solution as a simple, secure, and effective way for agencies to expand their private networking functions (such as Multiprotocol Label Switching and VPN) by terminating their private network directly into Verizon Cloud. Verizon positions this to agencies, allowing them to run cloud-ready seasonal or fast-growing apps as if they were running in the government's own datacenter.

Verizon acquired Terremark almost four years ago and has rationalized its portfolio into a unified cloud set of services. Verizon is in the process of adding capability to its U.S. government cloud offering, from enhanced service tiers to additional value-added services such as monitoring, patching, and additional backup options. Verizon is also planning to expand the product portfolio beyond IaaS to include PaaS, SaaS, network, mobility, and machine-to-machine (M2M) services.

Challenges

Verizon's strength may also be its Achilles' heel. Profitably moving mindshare beyond its core network, becoming a cloud solution provider with well-established professional services, and attracting a robust network of app developers are major tasks. Verizon is going all in on cloud to establish its commitment. So far, telcos have largely sold cloud services to the existing base of network service customers. Time will tell if Verizon will become only the vendor of choice for network connections or will compete with already established cloud providers in this market.

IDC Viewpoint

Verizon continues to invest and improve its key enabling assets and is strategically leveraging its position as a TIC in the federal government market. The acquisition of Terremark provided a capable IaaS platform that was able to scale and accelerated Verizon's efforts to expand the company's cloud market presence. Verizon is engaged in significant efforts to develop and expand partners, and it needs a robust partner ecosystem to compete in this market. IDC has assessed Verizon as a Major Player in this IDC MarketScape.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

This IDC MarketScape focuses on private and community IaaS. IDC includes in this definition the following:

- Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units) (It may be owned, managed, and operated by the organization or a third party – or some combination of them, and it may exist on-premise or off-premise.)

- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations) (It may be owned, managed, and operated by one or more of the organizations in the community or a third party – or some combination of them, and it may exist on-premise or off-premise.)

IDC also defines virtual private, public, and hybrid cloud as follows:

- **Virtual private cloud.** The cloud infrastructure includes services consisting of a hosted hardware environment (pooled resources) with a virtualization layer, allowing customers to directly create, provision, and manage multiple dedicated virtual server and storage instances within a shared physical infrastructure. This capability is either licensed for a specific quantity/capability or accessed as "burst" capacity as part of a standing services contract for users of customer premise–based private cloud appliances. Virtual private cloud services share physical resources among multiple unrelated customers and provide tiered options for greater privacy/security and customer control (e.g., VPN or private network access, firewall and IPS/IDS between guest VMs and the Internet, and root access to guest VMs). Physical resources are not dedicated to a single customer.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization – or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of a review board of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

This IDC MarketScape focuses on vendors that provide private IaaS cloud to the U.S. federal government. For further definition of private IaaS cloud, see *Business Strategy: Sourcing to the Cloud – Key Requirements for Government Vendors* (IDC Government Insights #GI251471, September 2014). Massive investments in technologies, facilities, operational personnel, tools, and best practices are the table stakes for vendors participating in this market. Although there are a multitude of vendors participating in other cloud markets such as PaaS and SaaS, the IaaS investments required are limiting this market to just dozens of vendors that can profitably provide the scale required for government. Indeed, even vendors covered in this IDC MarketScape are leveraging each other's infrastructure assets in support of stated strategies of being "asset light."

In addition, this IDC MarketScape focuses on private IaaS services because of the U.S. federal government's preference for the security of private cloud. Vendors are rated on their FedRAMP certification, which requires investment in resources for months (if not a year) and can cost vendors upward of $200,000.

Vendors in this IDC MarketScape tend to fall into the three categories discussed in the sections that follow.

Systems Integrators

These vendors offer a full range of cloud technologies, including hardware and software as well as migration services for IaaS. Many of these SIs have long-standing relationships with U.S. federal government clients at the decision-making level. Indeed, as government plans and funds strategic plans to consolidate datacenters and move to the cloud, some of the vendors providing IaaS were brought into the contract by SIs managing the transition. Many of the SIs included in this IDC MarketScape (Accenture, CGI, CSC, Dell, HP, IBM, and Unisys) are investing millions and billions of dollars in acquisitions, such as IBM's $2 billion acquisition of SoftLayer, investing in personnel, training, and professional services. In addition, many of the SIs are investing in partnering and leveraging each other's strengths. Examples include the Accenture Center for IBM Technologies providing Accenture access to IBM cloud products like IBM Bluemix and CSC's plans to establish a new IBM Center of Excellence to offer clients SoftLayer and IBM Bluemix. Many of the systems integrators in this IDC MarketScape have experienced the intricacies of large-scale systems integration and have invested in services to assist government clients in moving to the cloud. Because of their strong foundation in IaaS, SIs are in an excellent position to provide hybrid cloud to government, providing the capability to run applications in a public cloud while maintaining data in their private cloud and/or the ability to run Web front-end applications and data in a public cloud and back-end transactions in private clouds, as well as the ability to burst from public/private cloud.

Cloud-Centric Providers

Cloud-centric firms are vendors with infrastructure services offerings centered on IaaS. IDC included AWS and Microsoft in this IDC MarketScape category. Both Microsoft and AWS are providing cloud as an extension of their traditional business and leveraging massive investment in datacenter assets to package and deliver services. AWS has leveraged the internal infrastructure provided by Amazon, isolating datacenters for government-only use. Microsoft has expanded its development platform by launching Azure in 2010. Both providers are building extensive VAR and channel relationships.

Telco-Based Providers

Telcos offer the full scope of infrastructure services, including hosting, networking, and managed application services. Some telcos have yet to build out their portfolio to include extensive software or professional service options. Instead, the telcos are focused on providing infrastructure-based services to federal government clients; leveraging their position as a Trusted Internet Connection require that CSPs route their traffic through a TIC. A key differentiator for telco-based vendors is their ability to offer approved network and Internet components embedded in their cloud services, which results in seamless, high-availability IaaS services. Many of the telcos in this IDC MarketScape, including AT&T, CenturyLink, and Verizon, are partnering with SIs. As an example, AT&T is partnering with CSC, Accenture, and IBM, and Verizon and CenturyLink are both partnering with Accenture and CSC. IDC projects that telcos will extend their offers into end-to-end value propositions.

Strategies and Capabilities Criteria

Table 1 provides the strategies criteria and market-specific definitions as well as the weights applied to each subcriteria in this IDC MarketScape. Table 2 provides similar information for the capabilities criteria.

TABLE 1

Key Strategy Criteria for Success: Government Private Cloud IaaS

Strategies Criteria	Subcriteria	Market-Specific Subcriteria Definitions	Subcriteria Weighting
Offering strategy	Functionality or offering road map	The vendor provides strategy for increasing the highly elastic and granular scalability and scope of computing services and storage and provides road maps of extended capabilities, either organically or through acquisitions or partnerships.	3.00
	Delivery model	The vendor clearly articulates plans to expand the breadth of models deployed and enhance the ability to burst from one instance to another and continuously improve value-added services.	2.00
	Portfolio strategy	Portfolio strategy includes plans for providing additional solutions such as hybrid cloud, PaaS, SaaS, and cloud brokering/aggregation/marketplace.	2.00
	Security strategy	The vendor has U.S. government security certifications including FedRAMP, FISMA, and others.	3.00
	Subtotal		10.00
Go-to-market strategy	Pricing model	The vendor's pricing is flexible and offers a range of options such as traditional licensing and subscriptions.	1.50
	Sales/distribution strategy	The vendor's sales strategies are well defined, combining direct presence with indirect channels (VARs, network service providers, SIs, etc.). Beyond simply expanding market reach, the vendor seeks partners that provide solution innovation.	3.50
	Marketing strategy	The vendor's messaging is fine-tuned to the needs of government and is well integrated across the vendor's GMS activities with partners. The vendor provides prospective customers with a venue to gain more familiarity with the product by publishing thought leadership white papers, staging customer events, or establishing innovation centers.	3.50

TABLE 1

Key Strategy Criteria for Success: Government Private Cloud IaaS

Strategies Criteria	Subcriteria	Market-Specific Subcriteria Definitions	Subcriteria Weighting
	Customer service strategy	Based on vendor/customer interviews, the vendor is able to obtain high levels of customer satisfaction and retention. Customer satisfaction is a key goal. Have a good ratio of customer service, support, professional services, and training staff available either via the vendor's own staff or through a professional services partner. Have the vendor's ecosystem of partners well integrated and trained to ensure consistent customer experience and assure customers that they can get full value out of the portfolio.	1.50
	Subtotal		10.00
Business strategy	Growth strategy	The vendor has solid market momentum and growth as measured by ongoing acquisition of new clients and expansion of existing relationships.	3.00
	Innovation/R&D pace and productivity	The vendor shows evidence of ongoing investment and continued maturation of the portfolio through R&D and/or acquisition. The vendor participates in standards bodies.	3.50
	Financial/funding model	The cloud business unit has financial autonomy.	3.00
	Employee strategy	The vendor has stringent security requirements for employees to minimize government concerns. The vendor's employees obtain high marks from customers in perceived employee retention rates and overall competency.	0.50
	Subtotal		10.00

Source: IDC, 2014

TABLE 2

Key Capabilities Criteria for Success: Government Private Cloud IaaS

Capabilities Criteria	Subcriteria	Market-Specific Subcriteria Definitions	Subcriteria Weighting
Offering capabilities	Functionality/ offering delivered	The vendor's offerings are able to scale when needed through autoscaling, provide load balancing to manage and handle an increasing number of servers across heterogeneous resources (including multiple servers, hypervisors, and operating systems), offer SQL and NoSQL database services and distributed processing compute services for processing unstructured data, and support virtual private cloud.	4.00
	Delivery model appropriateness and execution	The vendor has the capabilities to deliver via multiple deployment models — managed private cloud on agency site, dedicated private cloud on vendor site, and virtual private cloud — and the capability to migrate government to hybrid cloud.	2.00

TABLE 2

Key Capabilities Criteria for Success: Government Private Cloud IaaS

Capabilities Criteria	Subcriteria	Market-Specific Subcriteria Definitions	Subcriteria Weighting
	Cost competitiveness	The vendor has plans to improve the flexibility and transparency of costs and provides compensation for breaching SLAs.	2.00
	Portfolio benefits delivered	The vendor offers value-added services including assessments and road map development, pilot programs, proof of concepts and testing, and application migration.	2.00
	Subtotal		10.00
Go-to-market capabilities	Pricing model options and alignment	Based on government client interviews, the vendor's pricing is flexible and offers a range of options such as traditional licensing, subscriptions, pay as you go, and unit pricing for all components. The vendor provides integration of IaaS into the customer's IT environment (whether cloud related or non-cloud related).	2.50
	Sales/distribution-structure capabilities	The vendor's sales capabilities are well diversified, combining direct presence with indirect channels (VARs, network service providers, SIs, etc.). The vendor maintains a dedicated government sales and support team.	2.50
	Marketing	The vendor's messaging is fine-tuned to the needs of government and is well integrated across the vendor's GMS activities with partners. The vendor provides prospective customers with a venue to gain more familiarity with the product by publishing thought leadership white papers, staging customer events, or establishing innovation centers.	2.50
	Customer service	Based on government client interviews, the vendor provides high levels of customer satisfaction and has a high level of customer retention. The vendor demonstrates market responsiveness and is able to utilize the user feedback loop in order to deliver compelling service.	2.50
	Subtotal		10.00
Business capabilities	Growth strategy execution	The vendor has solid market momentum and growth as measured by ongoing acquisition of new clients and expansion of existing relationships.	3.50
	Innovation/R&D pace and productivity	The vendor shows evidence of ongoing investment in and continued maturation of the portfolio through R&D and/or acquisition. The vendor is able to bring new services and features to market in a timely fashion.	3.50
	Financial/funding management	Financial strength is determined by the financial autonomy of the cloud business unit and the vendor's commitment to IaaS for the U.S. government market.	2.00
	Employee management	The vendor has put into place stringent requirements for its employees to minimize concerns of its government sector customers.	1.00
	Subtotal		10.00

Source: IDC, 2014

LEARN MORE

Related Research

- *Perspective: The Multifaceted Aspects of U.S. Government Cloud* (IDC Government Insights #GI251719, October 2014)
- *Business Strategy: Sourcing to the Cloud – Key Requirements for Government Vendors* (IDC Government Insights #GI251471, September 2014)
- *Business Strategy: IDC MaturityScape – Cloud in Government* (IDC Government Insights #GI248989, June 2014)
- *Business Strategy: Cloud – Six Steps to Performance Improvement* (IDC Government Insights #GI248367, May 2014)
- *U.S. Government 2014 Top 10 Predictions* (IDC Government Insights #GI244696, December 2013)

Appendix

Table 3 presents vendors' compliance with security standards for private cloud.

Table 4 presents vendors' cloud management capabilities.

Table 5 presents the value-added services offered by vendors.

TABLE 3

Compliance with Security Standards for Private Cloud

	Accenture	AT&T	AWS	CenturyLink	CGI	CSC	Dell	HP	IBM	Microsoft	Unisys	Verizon
FedRAMP	X	X	X	NA	X	X	NA	X	X	NA	NA	X
ISO 2007	X	X	X	X	X	X	X	X	NA	X	X	X
Cloud Controls Matrix	X	Partial	X	NA	NA	X	NA	X	NA	X	NA	NA
FISMA	Moderate	Moderate	Moderate	NA	Moderate	DHS FlexPod high; AWS and Azure moderate	Moderate	Moderate	Moderate; datacenter high	Moderate	Moderate	Moderate and low
NIST SP 800-53	X	Moderate	Moderate	NA	Moderate	Moderate	Moderate	Moderate	Moderate — Data-center high	NA	Moderate	X
DoD Cloud Security	Levels 1–2	In progress	Levels 1–5	NA	NA	X	NA	Levels 1–2	NA	NA	NA	NA
Other	NA	NA	HIPAA, ITAR, SOC1/SSAE16/ISAE 3402, SOC2-3, PCI DSS 1, FIPS 140-2, CSA	NA	NA	AWS ITAR	NA	FIPS 140-2 encryption, CIS Level 1, HIPAA, HITECH, ITAR, FERPA, and PCI-DSS. DIACAP/DIARMF (with uplift)	NA	SOC 1 Type 2, SOC 2 Type 2, PCI DSS, and HIPAA/HITECH	NA	NA

Notes:

Accenture's compliance with security standards is through partners.

CSC's compliance with security standards is through the AWS and Azure partnerships.

Source: IDC Government Insights, 2014

TABLE 4

Cloud Management Capabilities

	Accenture	AT&T	AWS	CenturyLink	CGI	CSC	Dell	HP	IBM	Microsoft	Unisys	Verizon
Autoscaling	X	X	X	X	X	X	X	X	X	X	X	NA
Load balancing	X	X	X	X	X	X	X	X	X	X	X	X
Burst across private and public cloud	X	X	X	X	NA	NA	X	X	X	X	X	X
Dedicated VPN/VLAN connection and network optimization technologies	X	X	X	X	X	X	X	X	X	X	X	X
Storage optimization technologies	X	X	X	X	X	X	X	X	X	X	X	X

Source: IDC Government Insights, 2014

TABLE 5

Value-Added Services Offered

	Accenture	AT&T	AWS	CenturyLink	CGI	CSC	Dell	HP	IBM	Microsoft	Unisys	Verizon
Cloud readiness/ assessment and road map development	X	X	X	X	X	X	X	X	X	X	X	X
Proof of concept/ piloting/testing	X	X	X	X	X	X	NA	X	X	X	X	X
Implementation	X	X	X	X	X	X	X	X	X	X	X	X
Migration	X	X	X	X	X	X	X	X	X	X	X	X
Integration with legacy infrastructure	X	X	X	X	X		X	X	X	X	X	X

Source: IDC Government Insights, 2014

Synopsis

This IDC study uses the IDC MarketScape model to present a vendor assessment of 12 vendors that provide private IaaS to the U.S. federal government. This research is a quantitative and qualitative assessment of the characteristics that explain a vendor's success in the marketplace and help anticipate the vendor's ascendancy.

"Government decision makers should review their strategic plans and select vendors for their IaaS based on best fit," says Adelaide O'Brien, research director, IDC Government Insights. "This IDC MarketScape is intended as a guide," she adds. This evaluation is based on a comprehensive framework and set of parameters expected to be most conducive to success in providing cloud IaaS for both the short term as a platform for PaaS and SaaS and the long term for the transformation of IT services.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com