

Don't Get Left Behind in the Digital Race



Why Government Agencies Need to Move to the Cloud Today



Cloud momentum continues to accelerate all across industries, but the uptick in adoption by government agencies has been slow. Organizations that run their own IT have to deal with hardware, software, patches, data security, networking updates, disaster recovery, and IT staffing which are all resource intensive. Cloud vendors like Microsoft efficiently and economically handle those activities.

There are a few instances in which government agencies have recognized the advantages of adopting cloud and are moving in that direction. The Defense Information Systems Agency (DISA) announced their decision to call for **proposals for MilCloud2.0**, a private commercial cloud that can offer cutting-edge commercial services to defense customers.

There is also the case of the **Federal Data Center Consolidation Initiative (FDCCI)** to use green IT and reduce the cost of data center infrastructure and increase overall IT security. **Gartner has even predicted that by 2020**, a corporate 'no-cloud' policy will be as rare as a "no-internet" policy is today.

Why Cloud is Here to Stay

Cloud addresses all the needs of an organization, changing how we work, where we work, and the ways we do business.

1. Reduces infrastructure costs and overall TCO

The cloud eliminates physical servers and storage space, real estate, power, and personnel to a large extent. Organizations don't have to worry about high costs of hardware and software upgrades and obsolete security and networking devices.

While it may seem like the costs of an on-premise solution are lesser, most organizations forget that most of these costs are hidden and recurring. The subscription fees of a cloud solution might be high, but the ongoing costs are minimal thus providing long-term benefits to government agencies often riddled with low budgets and lack of resources.

An average five-year on-premise licensing cost is 9% of the total cost while subscription costs for a cloud solution can be as high as 80%. But that is just the tip of the iceberg for an on-premise solution. There are so many hidden costs that the actual 5 year TCO is at least **two to three times** higher than a cloud solution for the same time frame.

ON-PREMISE – KNOW THE COSTS

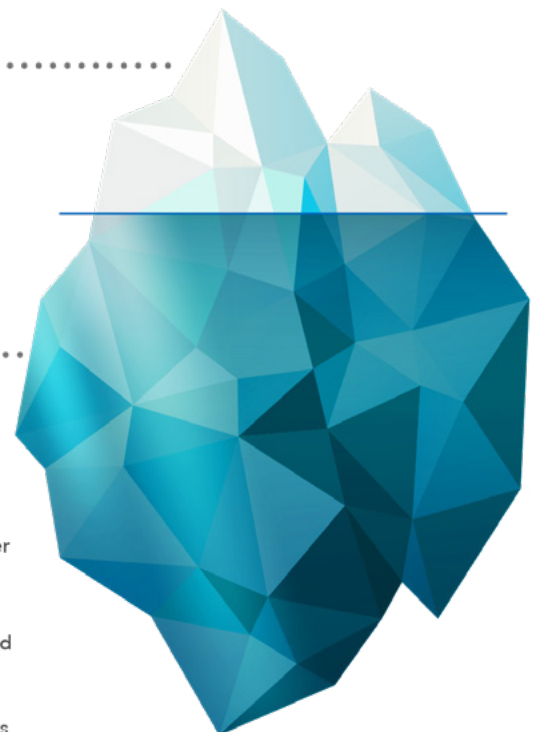
How a cloud solution makes more business sense in the long term

20%
Upfront

- Hardware
- Software
- Training, People, and Maintenance Costs

80%
Hidden

- License and Support Costs
- Upgrade
- Server and Application Server
- Database
- Implementation
- Customization and Integration Costs
- Internal Support and Training Costs



2. Scalability

Instead of using all the space all the time, cloud solutions can scale during peak times and ramp down at other non-peak times due to low usage.

3. Business continuity and automatic updates

There are many solutions today that promise great up-times, for example, Microsoft Azure guarantees 99.9% uptime. Disaster recovery solutions are also available, thus making business continuity a no-problem area. Regular software updates are provided automatically thus eliminating precious time of government agency personnel.

4. Security

Contrary to popular belief, cloud gives greater protection if implemented right. Even if personal machines get hacked, the data on the cloud is secure.

5. Increased collaboration

A cloud solution makes it possible to share documents amongst colleagues thus making collaboration easier and increasing productivity.



These benefits are evident for everyone to see. The other advantage of using a cloud platform that is not so evident is the innovation it offers. Many cloud platforms can enable organizations to push the boundaries of testing new apps, simplifying processes to free up resources, and making data driven decisions. Data analytics becomes easier and simpler in cloud as it allows a connected ecosystem of users, customers, and developers. New offerings like machine learning, server development, and advanced security services are also available today for maximum return on investments.

Even with all the Cloud advantages, public sector agencies have been slow to adopt cloud for many reasons. They have the challenge of trying to achieve all of the above advantages cloud provides while adhering to the highest level of security such as perimeter, building and, computer room controls. Additional challenges include compliance requirements such as the IRS 1075, FedRAMP, DISA, and ECSB, and government oversight regulations, not to mention compliance obligations for the Criminal Justice Information Services Division (CJIS) and the Health Insurance Portability and Accountability Act or HIPAA.

Public Sector entities exist under a microscope of expectations and demands. One eye faces towards connecting all the pieces within and across agencies most seamlessly, while the other looks towards future innovations, both in technology and the creation of ideas. To make both visions come together requires robust management tools that create a simplified IT experience. But that's strictly at the IT level. At the resource level, these agencies need the agility to respond to almost any situation. At the economic level, they need to maximize their investments in ways that address constricted budgets. Finally, they need to evolve their security levels to minimize risk continually.

According to a [recent survey by Penn Schoen Berland](#), 693 US Government customers were asked to rank their top 20 most important needs from a cloud services provider. In addition to security and privacy, compliance and data residency were in the top five most important needs.

Top 5 Most Important Needs from a Cloud Service Provider



So the question today is not whether the public sector should adopt cloud or not, but how fast and how far can the public sector go to the cloud? The benefits of cloud far outweigh the problems, and clear strategies can be set to overcome adoption inhibitors. Government agencies can rely on their IT partners who have experience in multiple cloud migrations and trust them to help migrate to the cloud.

Why We Recommend Microsoft Azure Government Cloud

Approximately 5.2 million people use Microsoft Cloud for Government, which includes Azure Government, Office 365 Government, and Dynamics CRM Online Government, according to Curt Kolcun, vice president of the U.S. Sector for Microsoft.

In 2013, Sagitec made a business decision to expand our partnership with Microsoft by adopting their Azure government cloud platform for achieving optimal performance and value. Currently, we have an “Azure First” approach to all new business proposals and encourage all potential clients to move from on-premise solutions toward a cloud infrastructure. This recommendation is based on industry trends, best practices, scalability, flexibility, and overall lower total cost of ownership. **We are a certified Microsoft Azure Government Cloud Managed Service Provider and reseller.**

For you, and other state and local government organizations, we strongly recommend the Azure Government Cloud as your best choice for adhering to foundational principles of security, privacy, control, compliance, and transparency.

Microsoft Azure is a government-community cloud that extends world-class security and control for dedicated U.S. Public Sector workloads and provides a full commitment to government compliance standards.



Provides a physical and network-isolated instance of Microsoft Azure.



Offers continuous commitment to rigorous compliance demands (i.e. FedRAMP, CIIS, and HIPAA) of a government-community cloud.



Provides screened U.S. citizens and policies to help protect customer data and applications.



Provides rich infrastructure, storage, and identity management capabilities delivered through cloud, on-premises, and hybrid solutions.



Stores data within the United States.



Delivers integrated, familiar experiences with Office 365 for Government in the cloud.

Operated by screened U.S. persons, Azure Government supports multiple hybrid scenarios for building and deploying solutions on-premises or in the cloud. Through us, you can also take advantage of the instant scalability and guaranteed uptime of a hyper-scale cloud service.

We standardized our approach to hosting over several Azure Government implementations. First, we set up an Azure Government subscription which is a dedicated environment for each client. Within the subscription, we create a highly available network with remote access (i.e., site-to-site). Next, we provide for redundant storage and Virtual Machines, which run the application, to be deployed and hardened.

By utilizing Azure Government, we can quickly scale and deploy VMs as demand requires. The client benefit to this capability is that clients will only be paying for needed performance.

Security

Security is a significant concern for any data center. Security includes both physical and virtual security. Sagitec’s proposed Azure Government Data Centers contain security features built into all aspects of the physical and virtual features of their platform offering. In addition to the “virtual” security offered through encryption and other software security measures, these Data Centers include industry standard and best practices for physical security measures. These include, but not limited to, biometrics access controls of physical assets, servers, buildings, and overall data centers.

Microsoft Azure Government has implemented its robust security, privacy, and compliance controls framework plus additional stringent controls to meet the higher level requirements found in the CIIS Security Policy, HIPAA, Fed-RAMP, IRS-1075, and others.

Reliability and Up Time

Overall reliability is a significant concern with any production system. Azure Data Centers are built and run at the highest infrastructure capability levels that few organizations can match. Server uptime is one of the biggest concerns for any data center. Most cloud services within Microsoft Azure come with a 99.95% SLA guarantee, which is much higher than most on-premises data centers.

To address the inevitable hardware failures, there are some features built into Microsoft Azure.

- Three redundant copies of data at all times, with the option of geographically redundant copy stored in a separate data center.
- Automatic failover to the backup server to minimize downtime.
- Hosting applications on a minimum of two server instances to minimize downtime when a hardware failure occurs.

The Only Cloud: Enterprise Level, Hyper-Scale, and True Hybrid

Microsoft is the only Cloud provider that combines a Hyper-Scale cloud offering, a truly hybrid platform, and an Enterprise Level Support for cloud workloads with Enterprise level SLAs. Enterprises need global reach and massive scale. Only Microsoft operates global-scale cloud services AND provides on-premises tools designed for the largest scale mission-critical requirements.

Microsoft delivers Microsoft Azure, Office 365, Outlook.com, Skype, Bing, and Xbox Live – some of the world’s most extensive cloud services. Microsoft Azure has 42 regions, more than any other cloud provider. In the cloud or on-premises, Microsoft delivers the hyper-scale that can be used to instantly scale up and scale down solutions with confidence, virtually anywhere in the world.

A True Hybrid Platform

Microsoft provides a truly hybrid cloud platform with a standard set of technologies and capabilities across on-premises, Cloud, and Service Provider clouds with a consistent experience across each (e.g., Unified search for SharePoint and SharePoint online, AD, Cloud Backup, Azure Media Services, and SharePoint on-premises).

Leader in 6 Gartner’s Cloud Magic Quadrants

Microsoft is considered by Gartner (Sept 2016) as a leader in seven of the nine Cloud related Magic Quadrants: Cloud IaaS, Disaster Recovery as a Service, Enterprise Application Platform as a Service, Identity and Access Management as a Service, Public Cloud Storage Services, and

x86 Server Virtualization. Amazon Web Services (AWS) is a leader in just two of them, Salesforce.com in one, and Google in none.

Industry-leading with Security, Privacy, and Compliance (e.g., ISO/IEC 27018)

All of Microsoft’s services are independently verified to meet legal and compliance requirements, are financially backed and offer transparent information on their availability. Microsoft was the first cloud provider that adhered to ISO 27018. This assures enterprise clients that privacy will be protected in several distinct ways:

- Clients are in control of their data.
- Clients know what’s happening with their data.
- There is strong security protection provided for clients’ data.
- Data won’t be used for advertising.
- Microsoft informs clients about government access to data. Microsoft shares its development and operational practices, publishes Law Enforcement Requests Reports, and invests in Transparency Centers whereby government clients can review source code and confirm that there are no back-doors.
- And more importantly for Microsoft’s clients, independent auditors have verified that Microsoft Azure, Office 365, Dynamics CRM Online, and Microsoft Intune follow the standard’s code of practice for the protection of personal information.



Sagitec’s partnership with Microsoft as a certified Azure Government Managed Services Provider (MSP) and Microsoft Gold Partner enables us to deliver a proven and flexible solution for the public sector that minimizes datacenter investments and meets requirements for security, compliance, and oversight. Azure Government is the flexible solution required for an infrastructure that will grow and change over time.



Do not get left behind in the digital race. Contact us to know how your agency can transform digitally with Sagitec and Microsoft Azure Government Cloud. Learn more at www.sagitec.com/services/microsoft-azure-services-sagitec