

DHS Private Cloud: Key Enabler for Data Center Consolidation, Agile Development, and Information Sharing



The *25 Point Plan to reform Federal Information Technology Management* focuses on improving information technology practices across the federal government “to deliver more value to the American taxpayer.” Within the twenty-five points, two of the primary themes are data center consolidation and reducing development cycles to deliver “manageable chunks” of functionality. In alignment with the *25 Point Plan*, the Department of Homeland Security (DHS) acted quickly to plan, architect and deliver an internal private cloud to support more efficient development and delivery of enterprise application services and ultimately support its goal of consolidating its data centers.

DHS Business Case

Recently, the Department launched a data center consolidation initiative to reduce the number of DHS data centers, aimed at decreasing costs, improving integration of systems, and enhancing the Department's overall security posture. However, DHS recognized that consolidating systems to the enterprise data centers could not be achieved efficiently by simply migrating legacy physical infrastructure components. In addition, standup of new infrastructure was costly, often plagued by long acquisition cycles, and required a significant Certification and Accreditation effort to ensure adequate security compliance.

In order to truly achieve efficient migration and integration of these systems, DHS needed to implement a model that would enable DHS to more quickly provision secure computing environments to support the agile development, testing and deployment of new applications and capabilities. By implementing an internal private cloud at the enterprise level, DHS helped remove barriers to entry by significantly reducing consolidation costs and improving the overall efficiency of migrating and standing up systems.

Initial Solution

After sponsoring in-depth studies and publishing findings on how cloud-based technologies could meet the DHS information assurance and security standards, the Department set out to prove it. To truly achieve the benefits of the cloud, DHS recognized that it needed to implement a solution that supported the streamlined provisioning of development platforms commonly used by IT and business units across DHS. These platforms could be quickly stood up by development organizations and customized for their particular business requirements. In addition, they could be further integrated with legacy or new services to support improved information sharing.

It was also critical that DHS offered a solution with security included as a service. DHS historically invested significant resources into certifying and accrediting individual systems, often resulting in programmatic delays and cost overruns. By offering pre-certified application platforms that could quickly be provisioned to support development and integration efforts, security processes were significantly streamlined to support more agile development and deployment of services.

Initial Results and Go-Forward Strategy

Leveraging cloud computing technologies and capabilities DHS has pioneered new ways to deliver IT services within the federal government by:

- Significantly reducing the time and level of effort required to certify and accredit (C&A) a system
- Drastically reducing both acquisition and development cycles

Moving forward, Blackstone believes the cloud will become the enablement platform that will mature to serve as a platform within DHS and other Federal agencies to enable Information Sharing. The challenge that DHS faces with cloud computing is developing a reliable system of information sharing while depending on an infrastructure historically designed to protect information and institutional silos. The key questions that must be considered include:

- How we share just the “correct” information?
- How do we ensure Data Sovereignty?
- How do we ensure the information is disseminated in a timely fashion?
- How do we ensure it is secure?

In order to answer these questions we must mature the current technologies that are utilized to secure our information. Steps have been taken in this area with the implementation of HSPD12 and other supporting authentication solutions such as the Identity Assurance solution implemented as part of the DHS E-Verify Self Check online service. These technologies and others such as Behavior Analytics and Semantic Technology will need to be added to the cloud in order for the platform to reach its full potential.

At Blackstone, we believe that the use of Behavioral Analytics, which can be defined as the ability to utilize real time business intelligence capabilities on how individuals are using the system, should be implemented to secure information within the cloud. Key attributes such as tracking behavior and anomalies of behavior need to be delivered.

Semantic Technology is the ability for a computer to understand meaning and relations of data information, allowing Cloud providers to ensure that we deliver the correct information to the correct individuals at the correct time. This is a key component for the ability of the Cloud to Secure the Homeland, as the delivery of too much information to an individual can have the same effect as not enough information.

The Cloud can be the platform that enables DHS and other Federal agencies to achieve more efficient and effective information sharing. As agencies move more services to the public cloud, additional solutions will be required to ensure only the right information is efficiently made available to the appropriate parties.

For more information, please visit our website at www.bstonetech.com.

Key Blackstone Contributors:

Jason Cohen, Sr. Consultant

Giles Kesteloot, Manager

Greg Adams, Director

Sam Ceccola, Sr. Director



BLACKSTONE
technology group