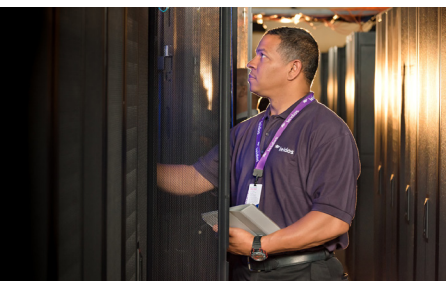


CAMEO: Optimized Secure Cloud for Application Hosting



BACKGROUND

In May 2014, the General Services Administration (GSA), with the assistance of the Federal Systems Integration and Management Center (FEDSIM), contracted the Business Services Platform (BSP) team of Leidos to work on a large cloud project. The GSA project — CIO Application Maintenance, Enhancement, and Operations (CAMEO) — entailed plans to modernize and onboard GSA applications across multiple data centers and other, less secure cloud platforms onto this cloud, and move these processes into the BSP. The BSP team also had to provide backend maintenance and security. The primary reason for onboarding GSA apps onto the cloud was to take advantage of cost savings and to modernize aging systems.



The BSP team worked together with GSA tenants and their application teams to deliver unified processes and procedures to support a unified BSP concept of operations (ConOps). This close collaboration was critical in the success of the project, as there were multiple apps across multiple data centers or clouds, many of which were built in-house and outdated.

"We were looking at apps that were 20 or 25 years old. The architecture of those apps may not allow them to take advantage of the cloud," said the BSP Program Manager. A comprehensive and streamlined onboarding process was a priority.

Tenants also faced having to invest large amounts of time and money in order to comply with up to 296 security controls of the current version of their System Security Plan (SSP). These security controls are carried out once during the initial Authorization to Operate (ATO) process and are also updated and maintained throughout the life of the system.



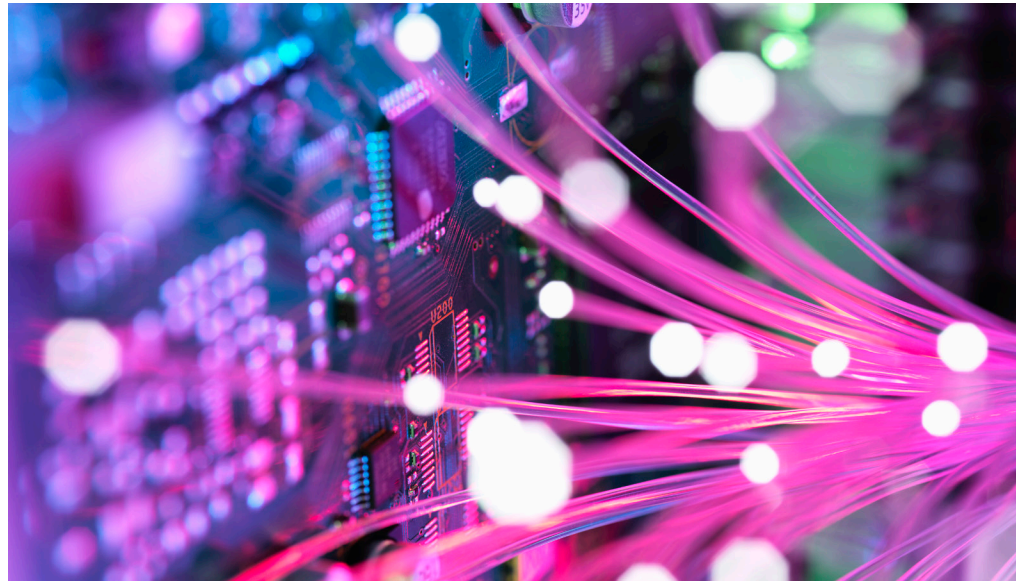
With aging systems and the need for tighter security controls, the GSA recognized the need to make the switch to the cloud. The GSA was further motivated to make the switch by the prospect of saving developer time and reducing cost because of the advantages of using a cloud-based solution.

SOLUTION

With an extensive cloud infrastructure, BSP offers a turn-key onboarding solution, with deployment times as short as 10 minutes. After the BSP team has defined the goals of their tenants through a discovery phase, the process is simplified. Artifactory first stages the data and pre-configures the deployment, then the tenants receive a set of jobs and tools via Jenkins, a deployment service. This allows tenants to manage their application stacks and use click-button deployment. The code is managed by BSP so that the tenants' app team only has to worry about application, resulting in time and money saved in deployment activities.

BSP's benefits include security-driven architecture networking for multiple tenants, separation of data and multi-tenant setup within the BSP structure. This means that the cost to the tenants is calculated based on their particular resources utilization. The ability to only charge tenants for the amount of resources they use is a huge plus, considering that many data centers charge for the highest level of resource utilization, irrespective of what the tenant actually needs.

"Calculation of the cost makes BSP a more cost-effective solution compared to a data center with the highest level of resource utilization," said the Onboarding Lead for BSP.



BSP also offered GSA significant flexibility. In the case of aging apps, it allowed onboarding of apps to be done incrementally.

"With some apps, you can just move them onto the cloud without making a lot of changes. With others, we have to refactor the code," said Rick Piper, Deputy Program Manager of CAMEO for Leidos.

The BSP team also worked closely with Security Operations, GSA Security and BSP Security on the Leidos team throughout the implementation to maintain a secure environment for tenants.

RESULTS

The biggest impact of CAMEO is just how much time BSP saves tenants and their application teams.

"Calculation of the cost makes BSP a more cost-effective solution compared to a data center with the highest level of resource utilization."

— Onboarding Lead for BSP

BSP streamlines onboarding through a comprehensive process that reduces time to onboard applications and unifies how applications are onboarded. In concrete terms, automatic onboarding reduced touch labor by GSA application teams from 32 hours to 5 minutes.

BSP also dramatically reduced the amount of touch labor required to operate the platform, resulting in a reduction in Amazon Web Services (AWS) hardware costs. It does this by automating certain tasks that tenants would otherwise have to manually perform, such as

automated patching via virtual servers. BSP employed AWS lambda functions to shut down non-ops environments during off-peak hours for significant cost savings for GSA, and built an automated patching capability, which can patch the platform and resources in 30 minutes.

By implementing its ServiceNow ticketing process, BSP was able to deliver exceptional support to tenants by improving ticket response time and accountability. More than 2,100 tickets have been closed since Aug. 2016, with 85 percent of the services exceeding targets.

The BSP team further supported tenants by converging two adjacent work streams of service providers that were operating in less capable cloud environments onto the BSP. With tenants now operating from one common ATO-accredited platform, there's uniformity in operations for the government. The BSP team also onboarded 10 production applications, including high-profile initiatives such as beta.sam.gov, Acquisition Gateway, and FAR Data Collection — and provided extensive troubleshooting and tenant support on an ongoing basis.

The BSP team developed and delivered features and services to improve the user experience and security, and to enhance existing services. This was achieved by developing and delivering the S3 Portal as a web application based on the serverless architecture of AWS. Another important feature that the BSP team worked on was the ability to monitor security vulnerabilities across the platform. The BSP did this by automating Amazon Machine Image (AMI) management and building processes, developing and delivering Nessus agent deployment solution for all work streams, and finally, by increasing Stack offerings from 5 at ATO to 11 to meet application team requirements.

Security compliances tend to be complex, and BSP takes some of this complexity away from the tenants by implementing multi-factor authentication, delivering Security Assertion Markup Language (SAML) as a Service and successfully completing a Federal Information Security Management Act (FISMA) audit. A concrete example of how this benefits BSP tenants is that they no longer have to be responsible for all 296 security controls; instead they are only responsible for 30 for FISMA low systems and 77 for FISMA Moderate. This results in big time savings for tenants and their application teams.

In essence, the BSP Team offers tenants the ability to streamline and optimize their processes. According to the BSP Program Manager, BSP is a force multiplier — it has the capability to converge hundreds of applications onto one single platform. This results in innumerable hours of development saved and the ability to transform traditional on-premise data center operations into an efficient cloud-based solution.