ATF Erases Technical Debt with Move to the Cloud

The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) is nearing the finish line of a campaign to shift away from antiquated on-premises IT systems toward a next-generation, all-cloud infrastructure. The process began six years ago when ATF and Mason McDaniel, ATF's chief technology officer, faced a hard reality: The bureau had been underinvesting in technology for years and was experiencing significant technological debt.

About 70 percent of ATF's applications were SPARC Solaris, which is obsolete and incapable of running well on most cloud environments. The agency also had an application written in Java 1.4, a language so old no manuals were available for it. On top of that, when ATF began looking at the application code, it discovered that most of it did not work.

"For years, users saw bugs in ATF systems, but they stopped even asking for fixes because they knew it wouldn't happen. If we were making even modest monthly updates, we were doing pretty well," McDaniel said.

The ATF team knew it could not do a simple lift and shift to the cloud; 70 percent of the enterprise portfolio would need to be rewritten and rebuilt on new technology stacks.

"Most of our systems were tightly inter-connected at the data level, not through nice, clean APIs. In the past we had tried to pull out individual systems and modernize them in isolation," McDaniel noted. "That hairball of data-level interconnections was largely what caused those efforts to fail."

ATF protects the public from crimes involving firearms, explosives, arson, and the diversion of alcohol and tobacco products; regulates lawful commerce in firearms and explosives; and provides worldwide support to law enforcement, public safety, and industry partners. ATF has about 5,500 employees, and its broader infrastructure supports about 7,000 people, including contractors, in approximately 200 offices.

Weather also played a role. The fear of having the roof collapse under the weight of snow prompted ATF to move its disaster recovery into the same floor space as its production systems. This did not bode well for critical systems that support the nation's gun investigations and laws. For that reason, ATF took a fairly unusual path to the cloud. It opted to build the enterprise infrastructure and then migrate all data to the cloud before moving any apps.

The AWS GovCloud (US) Selection

ATF chose Amazon Web Services (AWS) GovCloud (US) for its cloud migration in part because the company met its requirements for security and compliance with FedRAMP High authorization, and AWS was able to provide support with U.S. citizen staff. ATF was also confident that AWS would provide resilient, stable architecture with high availability to support the move of mission-critical applications to the cloud.

AWS GovCloud (US)'s mature platform also offers significantly more compliant, authorized third-party PaaS and SaaS solutions than other compliant cloud platforms. The platform enables ATF's IT team to try new applications within the AWS ecosystem for a quick, no-obligation proof of concept. The move also provides access to AWS's highly rated Platform-as-a-Service offering a variety of AWS native services.

> "If you do cloud right, there is no government data center that can be as secure as a good cloud environment. We prefer to have our applications and data in the cloud and well-locked down there … because of the ease with which we can update things and avoid configuration creep. When you are patching the same systems over and over, it's very difficult to accurately track every one of those configuration changes to be sure you're not making mistakes … which can introduce security vulnerabilities."
>
> **– Mason McDaniel**

By converting and migrating the data from all systems first, the data-level interdependencies were no longer major hurdles as ATF started working through the process of migrating individual applications.

"ATF's approach to AWS is more than just migration into cloud services. Kudos to the leadership at ATF, who recognized the value of cloud and the efficient way in which cloud resources provide better resiliency, security, and scalability," said Jack Lan, a senior account executive with AWS. "With an application-by-application approach, customers typically spend more time and budget in reaching the goal of transforming their technology landscape and the benefits. ATF received more for its investment by putting its data in the cloud first in order to accelerate time to mission."

The Benefits of Bold Choices

ATF leaders consider the agency's six-year cloud odyssey a major success because it enabled IT and business units to work together on technical challenges that had been neglected. It also transformed ATF's IT governance and compliance framework for the cloud and shifted the IT mindset from "keeping the lights on" to continuous improvement.

Cloud capabilities have transformed IT operations at ATF. With modern architecture and automation in place, IT staff can make production deployments mid-day with zero downtime. In the six months after going live, they made production deployments on 91 percent of all workdays, averaging eight features per day – without disruptions to users.

In addition, ATF's system can now handle 4,500 simultaneous users, an increase of more than 4,000 percent. ATF's pace of processing paper forms has increased more than 400 percent.

AWS high-performance computing capabilities have enabled data scientists at ATF's Fire Research Laboratory to run simulations to analyze the spread of fire or gas leaks. Future plans include migrating the National Integrated Ballistic Information Network, which automates ballistics evaluations and helps law enforcement officers nationwide to quickly match cartridge casing evidence to more effectively close cases involving firearms.

ATF's success in the cloud brought about a dramatic shift in agency business leaders' trust and engagement with IT – in ATF and in other Department of Justice agencies, observed Nicci Neal, who leads AWS GovCloud (US) business development.

"Previously, they were hesitant about doing any kind of modernization, because they simply did not believe any timeline," Neal said. "But then they saw what ATF has done over the last six years, and that has garnered a lot of trust among business owners."

Lessons Learned

Based on its cloud migration experience, ATF had a few takeaways.

1) **Challenge the notion of "we've always done it this way."**
When the ATF embarked on its cloud migration, the status quo was a production data center that had a failover just one aisle away and structural integrity concerns due to a snow storm. Unfortunately, this predicament resonates with other government agencies. This is why it is essential to have cloud and a thorough analysis of the agency IT environment. Discovery services are almost always offered at no cost to the end government customer and provide valuable insights into planning.

2) **The ability to engage with the mission or business is crucial for program/project success.**
With any significant modernization, there will be hiccups. An open and honest dialogue between the government administrator and the office of the chief information officer is essential. Ongoing engagement with end-user subject matter experts, from the beginning to the end of a project, is also critical.

3) **Success depends on IT governance updates throughout the lifecycle of the modernization program.**
Otherwise, the modernization journey may stop before it begins due to outdated compliance checks that ensure safety but need massive updating for cloud innovation. ATF continuously updated its IT governance to avoid being bogged down by additional compliance cycles. Leveraging inherited compliance controls from the underlying AWS GovCloud (US) infrastructure and imbedding automation and compliance-as-code practices were other essential steps for streamlining and accelerating governance practices.

Amazon solutions in use at ATF include:

Analytics
- Amazon OpenSearch Service for Elasticsearch

Compute
- Amazon EC2
- AWS ParallelCluster (HPC)
- AWS CloudShell

Containers
- Red Hat OpenShift Service running on EC2

Databases
- Amazon DynamoDB
- Amazon RDS

Governance
- AWS Organizations

Migration
- AWS Database Migration Service

Networking and Content Delivery
- AWS Direct Connect
- AWS Transit Gateway
- AWS Site-to-Site VPN
- Amazon Route 53
- Elastic Load Balancers
- AWS PrivateLink

Security
- AWS Identity and Access Management
- AWS Key Management Service

Storage
- Amazon Simple Storage Service (S3)
- Amazon FSx for NetApp ONTAP