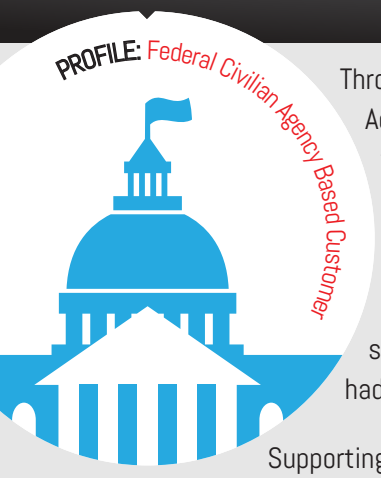
CASE STUDY: Addressing the Security Challenges of a Federal Agency Partner



Through an extensive network of field offices and partnerships with public and private organizations, this CFO Act, U.S. Federal Agency supports over 5000 users across the United States and U.S. territories, Puerto Rico, the U. S. Virgin Islands and Guam.

Similar to other federal agencies, our customer's mission requires a widespread inventory of platforms and technologies to support it. Compounded by a geographically dispersed and sometimes remote and offline workforce, this Agency has struggled to deploy a common compute solution for end users, much less a standard Operating System and software configuration across end point devices. In addition, our customer had difficulties automating the assessment of its level of compliance enterprise-wide.

Supporting over 90 field offices across 174 IPv4 subnets, this Agency's ISCM process proved complex, expensive, and time-consuming, and ultimately was not successful in achieving the Administration's Cybersecurity Cross Agency Priority (CAP) Goal. With the amount of known software vulnerabilities increasing daily, the Agency realized the task of manually searching, classifying, and patching software vulnerabilities on their own was too great. The Agency's FY2013 FISMA Audit concluded that Configuration Management was a recurring weakness, and that there were challenges remediating vulnerabilities and implementing baseline configurations. The audit also revealed that the Agency had a tedious and time consuming patching process. It would take the Agency an entire month to deploy the Microsoft Patches that were released monthly on "Patch Tuesday."

CUSTOMER CHALLENGES	1901 Group's SOLUTION
High cost and high complexity for IT security compliance system hardware, software, operations and maintenance.	Lower cost and lower complexity of 'cloud service' models for IT security compliance as-a-service.
Lack of visibility across all assets within an organization.	Asset tracking and automated compliance reporting, as well as, software use analysis across the enterprise.
Lack of configuration management and control across enterprise assets.	Automated vulnerability management for multiple operating systems and applications across all endpoints regardless of location or connection type.
Lack of a centralized and automated means to enforce vulnerability compliance.	Establishment of a Configuration Management Data Base (CMDB) with automated discovery scans for all Configuration Items (CI).

ACTIONS TAKEN: Key Factors that Led to the Agency's Success

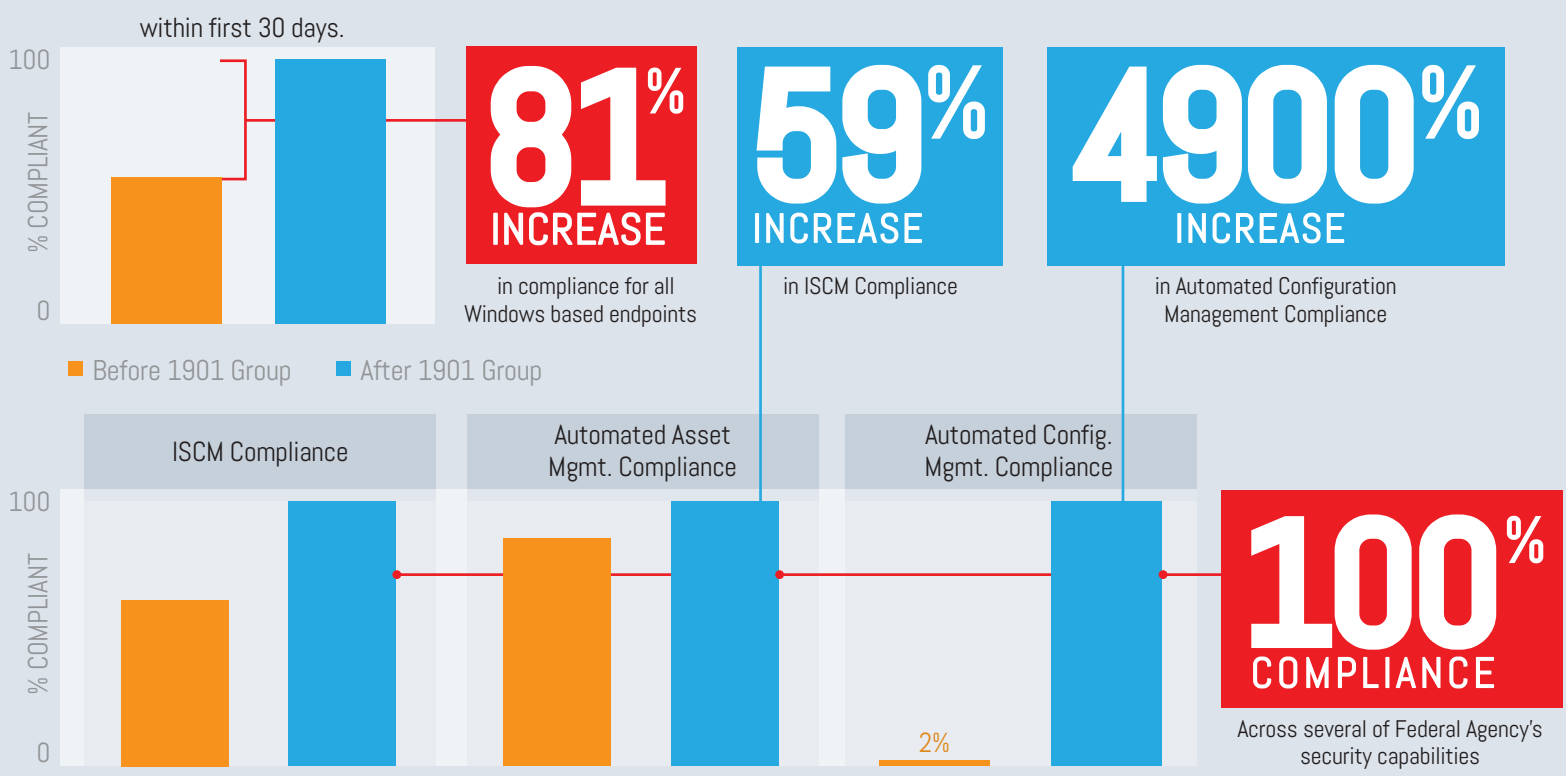
Consumption-based RFP on GSA Schedule 70. "Pay for what you use".

"**Cloud service**" included hardware, software, and labor to design, test, implement, and operate.

FedRAMP Approved Cloud Service Provider (CSP) expedited progress.

Increased compliance by 81% for all Windows-based endpoints within 1st 30 days from award.

RESULTS: Real World Examples of Substantial Improvement



Our customers are able to:

Decrease vulnerabilities by having a complete, accurate, and timely software and hardware inventory.

Improve security by establishing effective controls and security configuration baselines.

Increase usage of cloud computing solutions.