eBOOK

How SaaS Cyber Resilience is Transforming State & Local Agencies

Driving cloud transformation and data security

Introduction

The cloud is transforming how we work. It has reshaped entire industries, helping organizations reimagine how they serve employees and customers. Cloud adoption may be the central driving force for today's state and local agencies looking to modernize their in-house technologies. It represents opportunities to breed new efficiencies, shed legacy tech debt, and rapidly innovate operations. While adopting cloud-based technologies has historically been arduous and painstaking, the Federal Risk and Authorization Management Program (FedRAMP), removes common hurdles associated with evaluating and consuming cloud-based solutions. Through FedRAMP, federal agencies can rapidly (and confidently) adopt cloud technologies to transform their operations—all while meeting staunch government mandates and security protocols.

These same compliance requirements, and assurances manifest themselves in State and Local governments due to Federal data regulatory requirements around health, privacy, law enforcement, and other types of data.

CLOUD ADOPTION FOR AGENCIES

Cloud adoption is a significant driver of federal, state, and local government as they look to transform and modernize their operations digitally. However, the promise of cloud adoption was diminished by the size and the nature of the government sector—which presented unique challenges in cloud service adoption:

Challenges with the cloud...

Constrained resources
The scarcity of technical talent and lack of clear business outcomes for cloud adoption dramatically slow modernization efforts.

Legacy spend
The US Government Accountability Office (GAO) estimates that 80% of IT and cyber-related investments are spent on maintaining and administering to existing IT and legacy systems—leaving bare bones budgets for new solutions.[1]

Siloed IT operations
Fragmentation of IT organizations which favors maintaining the status quo with the traditional and antiquated structures and solutions.

Malicious attack
Cybercrime is the primary concern of IT professionals, especially in government agencies, as the fear of cyberthreats accelerate and hinder new app adoption.

Commvault®

However, with the introduction of FedRAMP, agencies received a catalyst for change. Federal and local agencies gained a repeatable and effective framework for cloud solution evaluation and adoption through this government-wide program. By adhering to clearly documented security, authorization, and certification protocols, FedRAMP introduced a common and transparent method to vet and adopt government-wide cloud technologies.

FEDRAMP BENEFITS...

- **Accelerated processes**
  Federal, state, and local governments benefit from streamlined and uniform guidelines that shorten approvals, lighten the burden on IT, and streamline the acquisition processes.
- **Operational efficiencies**
  Significant reduction in time and costs due to removing duplication of efforts spent on assessing and evaluating suppliers and testing disparate products.
- **Cloud security awareness**
  Gained insight into cloud security solutions and controls, leading to higher confidence in offerings.
- **Compliance assurance**
  Peace of mind, knowing suppliers listed on the FedRAMP Marketplace adhere to FedRAMP compliance and security designations.

SAAS DATA PROTECTION FOR GOVERNMENT AGENCIES

Business models are evolving. Data security is top of mind for today's agencies, from the overnight shift in remote work to implementing new hybrid environments to the threat of emerging cyberattacks. And as these organizations modernize their workforce, infrastructure, and operations, data is sprawling into more places than ever. To stay resilient, today's agencies must reshuffle their data protection strategies to remove data silos while comprehensively safeguarding their data estate.

FedRAMP-certified backup and recovery solutions blend the best security with the best SaaS. Organizations get nimble, enterprise-grade protection without the infrastructure, maintenance costs, and IT burden. Agencies can deploy in minutes, remotely manage, and effortlessly scale while keeping data safe, recoverable, and compliant—wherever it may be.

Rapidly recover from deletion, corruption, or malicious attack	Meet federally mandated data security standards and requirements	Maintain compliance and meet regulatory SLAs	Optimize operations, with automated data backups and low-touch management	No hardware, maintenance, or upfront capital investments required

The federal agency IT budget for 2024 has allotted **$74B**[2] > including **$12.7B** for cybersecurity-related activities.[3]

Commvault

COMMVAULT CLOUD

Commvault Cloud for Government is currently the first and ONLY data protection solution to meet FedRAMP High standards. They are hosted on Azure Government Cloud, and meet the most stringent confidentiality, integrity, and availability standards set forth by the US government. From SaaS apps to endpoints to on-prem and cloud workloads, Commvault Cloud, powered by Metallic AI is industry-proven to keep your data secure, recoverable, and compliant from today's data loss threats. With enterprise-grade, multi-layered security built-in, Commvault Cloud includes additional access, identification, and incident response controls that can extend beyond federally mandated protocols and requirements.

COMMVAULT CLOUD FOR GOVERNMENT
hosted on Azure Government Cloud

FedRAMP High | CJIS Compliant | FIPS 140-2 Compliant

Microsoft 365 — For Exchange, Teams, SharePoint, OneDrive, Project, and more.

Microsoft Dynamics 365 — For CE applications + Power Platform.

Salesforce — For Salesforce Cloud data.

Endpoint — For laptops and desktops.

GCC High | Salesforce GovCloud

VM & Kubernetes — Microsoft Hyper-V, VMware, Azure VM, Kubernetes, Microsoft Azure, AWS, AVS, VMware Cloud.

Database — For Microsoft SQL, Azure PaaS, Oracle, Amazon AWS, SAP HANA.

File & object — For Windows Server, Azure Blob & Files, OCI Object Storage, Amazon S3, Linux/UNIX.

Cloud Storage — For Air-gapped cloud storage.

1. GAO, Information Technology: Agencies Need to Continue Addressing Critical Legacy Systems, May 2023.
2. Statista, Federal government information technology (IT) budget in the United States from FY 2015 to FY 2024, by department.
3. John Curran, MeriTalk, FY2024 Budget Request: $74B for Civilian IT, $12.7B for Cyber, March 2023.

To learn more, visit **commvault.com/platform/government-cloud**

Commvault

commvault.com | 888.746.3849