Federal CIO Guide to Modern Data Protection

Growing uncertainty and accelerating threats require advanced backup and recovery solutions

A Frost & Sullivan White Paper

Powering clients to a future shaped by growth

FROST & SULLIVAN

CONTENTS

Data have become major strategic assets for federal agencies and departments to utilize and protect. The government's digital transformation of operations and services increases its reliance on information and analytics, which creates mounting pressure on federal agency IT teams to continuously secure, modernize, and innovate systems and processes, often within strict budget and resource limitations.

The last few years have seen a rapid acceleration of digital transformation, mainly stemming from the sudden pivot to remote work and citizen services. The core challenges of securely accessing and transferring information, compounding growth in the amount of data generated and expanding cybersecurity threats (partly because of geopolitical uncertainty), will continue and possibly intensify. These challenges underscore the critical nature data protection plays for the nation's security and prosperity.

Never Trust, Always Verify: Realizing a Constant State of Breach Approach

Federal agencies need a zero-trust security posture that assumes a constant state of attacks and breaches. But security and data protection controls often fall short of this mark. According to a 2022 survey of public sector IT leaders, nearly 90% of respondents said they had a gap between how much data the mission could afford to lose versus how often mission data received protection.[1] In the same survey, 76% of organizations said they had a ransomware attack that year, and in 94% of those attacks, the ransomware tried to delete backup data. This research shows a need for data security tightening and prioritizing.

> *On Zero Trust:* "If you want a secure IT environment, you cannot assume good firewalls and perimeter defenses are enough. Assume a state of constant breach; assume an adversary has already penetrated. Mission-critical data and backup data need to be safe even if a threat actor has been active for weeks or months and gained admin credentials. Zero Trust architecture moves static, exterior defenses to a focus on users, assets, and resources. Move from 'trust, but verify' to 'don't trust AND verify'"
>
> —Jeff Reichard, *VP public sector and compliance strategy, Veeam*

Data backup and recovery are integral parts of a robust security program but can take a back seat to front-door initiatives such as securing networks and endpoints. This unintentional oversight can have grave consequences: On average, more than one-third of data subject to ransomware attacks is unrecoverable. Government agencies strive to make systems impenetrable but struggle with funding and the lack of in-house skill sets to ensure all the right boxes have been checked. These challenges make it crucial for data recovery, backup, and management to command a government's strategic cybersecurity and data management strategy. Such a strategy can require partnering with an advanced solution provider who can ensure that backup mechanisms are ultra-resilient, that data stores are immutable, and that at least one unchangeable and air-gapped copy is maintained offline. Government agencies may feel their stores are sufficient, but the numbers suggest otherwise: Data security is the primary concern for government IT teams, as 41% of government respondents noted in a 2021 Frost & Sullivan report—a higher proportion than any other vertical industry.[2] In addition, 91% of public sector IT professionals saw an availability gap between service level agreement expectations and how quickly IT can return to productivity.[3]

Keeping Ahead of Adversaries

Advanced data backup and recovery is a fast and effective way for federal agencies and departments to improve data and system security significantly. Agencies need simple, intuitive, and comprehensive tools covering workloads, applications, and unstructured data. Protecting data with a minimal number of tools can reduce the attack surface across applications and interfaces. Using an advanced, cloud-enabled platform has many benefits:

- Comprehensive and flexible protection
- Intuitive tools to streamline IT activities
- Use-scaling fee structures
- Cloud infrastructure to reduce agency hardware modernization and maintenance costs and lessen the need for future hardware investment

Holistic, flexible security enables government agencies to own and manage their data while providing comprehensive protection. Advanced solutions should work across cloud, multi-cloud, and hybrid cloud environments; provide complete coverage on-premises, including physical workload backup; encompass Kubernetes and container implementation as well as Software-as-a-Service solutions, such as Microsoft 365 or Salesforce.

Comprehensive tools can save costs by streamlining an in-house IT team's workload. For example, advanced solutions with disaster recovery orchestration can quickly and automatically run audits and reports needed to satisfy regulatory requirements. Leveraging the cloud for disaster recovery allows an agency to simplify equipment modernization and maintenance, lessening solution costs. From the agency's perspective, streamlining backup and recovery management, auditing, and hardware maintenance frees internal IT resources from either rote or administrative tasks or those beyond their competency level to focus more on core agency work.

> Comprehensive tools can save costs by streamlining an in-house IT team's workload.

Another quality of an advanced data backup, recovery, and management solution is its ability to recover from ransomware or other malware attacks. Malware threat actors often lurk undetected on a network for weeks or months, escalating their privileges, gaining credentials, and moving laterally. Completing backups during this time with older or less sophisticated solutions may retain malware and reintroduce it during recovery. To combat this, Veeam Software, for example, has multiple avenues for protecting its customers: Veeam's solutions allow agencies to scan and thoroughly expunge malware from data on restoration, allowing them to restore safely without reintroducing malware into the environment. Because adversaries frequently try to destroy backup data as part of their attack, Veeam's solutions protect backups from deletion. In addition, restoring sensitive or questionable data into an isolated environment can occur without network connectivity to ensure the data and the system remain protected.

Next Steps: Building a Data Backup and Recovery Fortress

Other factors to consider are the solution provider's ability to implement role-based access control and multi-factor identification across its portfolio. This must include the option for immutable, air-gapped backup that no admin can delete, arguably a necessity for today's federal agencies. A vendor must support numerous infrastructure types—with an agnostic platform to integrate advanced security and compliance features—enabling government organizations to focus on their core activities, reduce risks, and prepare for new and unforeseen challenges. Advanced technologies, such as artificial intelligence and machine learning, can drive automation-based tools to eliminate protection gaps, such as autonomous backup and recovery systems and consistent monitoring, analytics, and disaster recovery.

Highly secure mission-critical data protection cannot be left to aging technologies, nor can the responsibility rest solely with in-house teams that may lack the time, resources, or skill sets needed to stay ahead of a constantly evolving threat landscape. As government data generation increases and we enter a new era of intensifying cybersecurity assaults, working with the right partner can secure essential data, protect systems across the organization, and lay the foundation for modern and efficient agencies, departments, and societies.

About Veeam

Veeam Government Solutions, Inc. (VGS) is the leading backup solutions provider delivering Modern Data Protection for cloud, virtual, SaaS, Kubernetes, and physical environments to the U.S. federal government. With 1,200+ government customers, VGS provides simple, reliable, flexible and secure solutions agencies trust to protect, manage, and safeguard data, workloads, and mission-critical applications no matter where they reside. Headquartered in Washington, D.C., VGS is U.S.-owned, managed and supported.

To learn more, visit www.veeamgov.com

Endnotes

1. *2022 Top Trends in Data Protection*, Veeam, February 2021.
2. *Security Priorities in the COVID Era—An IT Decision Maker's Perspective, 2020–2021*. Frost & Sullivan, February 2022.
3. 2022 *Data Protection Trends in Public Sector.* Veeam, 2022. https://go.veeam.com/data-protection-trends-executive-brief-public-sector

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion