

Data Protection Issue Brief

With the increased telework capability comes an increased attack surface for our adversary. They're already taking advantage of the situation and the environment that we have on hand.

– Principal Deputy and DoD CIO, Essye Miller, during a virtual town hall meeting, March 16.

The Federal Data Deluge Requires Real Data Protection

Eighty percent of Federal leaders say that their organization's data is growing rampantly. At the same time, government data is under an increasing threat. Federal agencies must support more teleworking employees than ever before, many of whom are using personal, non-government issued devices.

In April 2020, the Cybersecurity and Infrastructure Security Agency released temporary guidance for safely connecting remote users to agency networks through cloud service providers. While systems are typically designed with scale and growth in mind, many traditional environments are not equipped to expand to support agency-wide teleworking.

Cyber concerns rise as agencies are forced to expand their network bandwidth, and Virtual Private Networks are unable to scale to secure an entirely mobile workforce. And, as more users connect remotely, the attack surface continues to grow, potentially exposing sensitive Federal data. Because Federal agencies possess more data than any private

company, such an environment poses an immediate need for a comprehensive data protection and disaster recovery solution.

As agencies determine current and future data management plans, they need to consider their challenges, priorities, and the technology solutions that will enable them to leverage their data, and to do so at the speed required by an always-on, increasingly digital Federal government. To minimize disruption and mitigate risk of data loss and downtime, agencies need reliable, scalable, and more automated solutions for protecting applications and data regardless of the platform (physical, virtual, containers, cloud-native, software-as-a-service) or of the environments that workloads are deployed into (edge, core, multi-cloud).

Agencies should consider the following best practices for real data protection in an increasingly digital Federal environment.

Backup and Restore Across the Entire Environment

Ensure data protection extends from on-premises environments to multiple clouds, so it provides the same level of protection regardless of where the data resides. Look for unified data

protection for the enterprise that centralizes, automates, and accelerates backup and recovery across the entire IT environment.

Cyber Capabilities

Review cyber infrastructure and potential gaps given expanded telework. As the scope of Federal telework is likely to continue, the attack surface of the Federal enterprise has exploded. Now more than ever, it's critical that agencies employ solutions that can protect and isolate critical data, identify suspicious activity, and accelerate recovery.

Native Application Integration

Look for native application integration with data protection solutions, so data owners can perform backup and recovery operations directly from native applications, while IT maintains central oversight and governance to ensure compliance.

Backup at Flash Speed

Leverage flash storage to facilitate fast backups and fast restore, minimizing user downtime. While flash remains cost-prohibitive for every use case, it's



well-suited for continuous backups of highly transactional data and backing up heavily used databases.

Scalability

Ensure data protection solution can scale to accommodate the explosion in data growth as driven by new applications of the Internet of Things and artificial intelligence, regardless of platform or workload environment.

Deduplication Guarantee

To help control capital costs, look for a guarantee that the data protection solution will provide an agreed-upon data deduplication ratio, or the vendor will provide compensation – assuming the agency has followed best practices.

Dell Technologies and ThunderCat Can Help

Dell Technologies, the market leader in purpose-built backup appliances, offers cost-effective data management and protection solutions, no matter where data resides. Its multi-cloud data protection solutions, cyber recovery management and automation software, data protection as a service, and tight integration with VMware help agencies meet the challenges of the constantly evolving IT landscape.

ThunderCat Technology, in partnership with Dell Technologies, offers Federal organizations a comprehensive portfolio of solutions to help them meet their goals, whether they concern digital transformation, infrastructure consolidation and optimization, cloud migration, or data management and analytics.

For more information, visit <https://www.thundercattech.com/partners/delltechnologies/>