PURESTORAGE

FEDERAL GOVERNMENT DATA CENTER OPTIMIZATION STARTS WITH FLASH STORAGE

FEDERAL GOVERNMENT DATA CENTER OPTIMIZATION STARTS WITH FLASH STORAGE

It's a technology irony: The growth in mobile computing, cloud software and infrastructure, and server-reducing virtualization have caused organizations to renew their focus on the most traditional part of IT – the data center. Large organizations, including the federal government, have spent the last several years trying to reduce the population of data centers. That means the remaining ones have to be all the more modern and efficient.

Federal agencies have IT functionality and security requirements matching those of the largest companies. But public sector entities often have to accomplish their goals with relatively fewer resources. The big challenges:

- **Security**. Agencies must keep data safe while providing unfettered access for authorized users. They typically have thousands of users, often scattered internationally, accessing multiple data centers. That means their IT staffs, and those of their contractors, have to manage layered security systems.
- **Complexity**. Unlike the data centers of yesteryear, today's data centers are running virtualized workloads that are highly mobile among servers and locations. They share work with external cloud facilities. Data centers also support mobile users, physical and virtualized desktop users, remove users on virtual private networks, and guests such as visitors and contractors. And increasingly, they are the storage location for data stores not connected to any single application, but must be online as agencies fulfill the data-set availability goals of the Federal Digital Strategy.
- **Cost**. Agencies are under pressure to reduce infrastructure operations and maintenance spending so they can free up dollars for innovations such as improved digital services. Under the Federal Data Center Consolidation Initiative, they are to seek opportunities for savings by having fewer data centers and optimizing the remaining ones.

Beyond the specific federal issues, pretty much any vertical industry-specific IT challenge found anywhere, is also found in the federal government. These include the need to protect intellectual property, personally identifiable information and mission-specific data. And to meet ever-growing storage requirements in a cost effective way. As the policies of cyber threat information sharing take hold, they'll put more pressure of data center performance and security requirements.

One component in a simplified, lower cost, and more secure IT infrastructure consists of a basic but essential IT building block, namely the storage medium. A linchpin in any IT apparatus, storage represents a major cost element. Beyond the acquisition costs of disk arrays themselves, agencies are obligated to consider the lifecycle costs of storage, including maintenance, repair and power consumption.

In short, storage represents a major opportunity for performance improvement, cost streamlining, and improved security.

Now imagine a storage solution with these characteristics:

- Provides application acceleration so users and constituents experience better performance locally and across the WAN.
- Lowers costs by ridding the data center of traditional disk storage inefficiencies and complexity, and replacing it with storage that is five to ten times more efficient and entails lower power requirements.
- Is far simpler than other storage options to install, administer and maintain.
- Doesn't require added-on security with its added-on expense and complexity.

The Flash Arrays from Pure Storage fit the bill precisely. Read on to better understand their role in optimizing federal data centers.

High uptime thanks to FlashArray resiliency

The federal Digital Services Playbook provides federal agencies guidance for building the next generation of web applications deployed publicly. Implicit in this policy is high availability for citizen-facing apps. In fact, downtime during peak periods (such as health insurance exchange enrollment) can cause real and reputational program damage. Soon, citizens will have "feedback buttons" available on government websites to let agencies know when things are running right.

Product engineers at Pure Storage understand the need for continuous availability and operational resiliency. FlashArrays have proven five-nines availability. Because the arrays are built from flash memory, users practically never encounter the need to hot-swap failed units, as they regularly do with disks. Nevertheless, should a swap be required, it occurs without disruption to storage operations. That's also true for software Pure Storage upgrades.

Plus, unique to Pure Storage, FlashArrays are equipped with dual solid-state device (SSD) failure protection to compensate for the bit errors inherent in flash memory. The result: The IT staff can have confidence that rebuilds from failed drives will go online with zero data losses

FlashArray controllers also support the drive for availability beyond five nines. Pure Storage controllers are stateless. Should a controller fail, operations continue thanks to automatic failover to a second, redundant controller. The FlashArray itself is active from both controllers, even though it's using only one at a time

Because the clustered FlashArray controllers don't store any persistent information, they can also be upgraded with new firmware and features while running inline.

Better performance than disk, with cost parity

Federal agencies, under the cloud-first mandate, are discerning about the workloads they are willing to move to the cloud. When e-mail, software development and administrative workloads are moved to cloud providers, what remains are the mission critical applications and data.

Here, the application of Pure Storage solid-state arrays fulfills a variety of requirements. Chief among these is lightning speed, relative to disk. Solid- state arrays work nearly as fast as memory. Latencies typically run under 1 millisecond with up to 200,000 32K-wide input/output operations per second. All with extremely low error rates.

FlashArrays have proven five-nines availability. Nevertheless, should a swap be required, it occurs without disruption to storage operations.

Performance extends to availability. Because they have no moving parts, FlashArrays are inherently more reliable than disk drives. But should a malfunction occur, Pure Storage's purpose-built RAID-3D algorithm ensures that regardless of which drive in the array goes down, its data is served from a backup location while the OS re-builds and writes around the failed component. Users never experience any application performance hit, nor do they lose data.

Note, too, that because of Pure Storage's data deduplication algorithm built into each FlashArray, the effective cost of this lighting-fast storage is equal to, and in some cases lower than, lifecycle costs of disk storage.

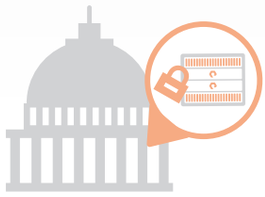
Security simplification

With traditional spinning disk arrays, federal tech shops must add in key encryption management systems. This entails management tasks of dealing with lost keys, revocation of keys from people who leave or otherwise lose authorization, or suspension of keys in a suspected breach. All this happens in an environment where oversight agencies and Congress are watching the cybersecurity scene closely.

With Pure Storage solid-state storage, you've got encryption upon power-up – no sys admin intervention required. Data written to Pure Storage FlashArrays is encrypted under the AES 256-bit standard. Pure Storage arrays use a combination of software and custom circuitry to provide the encryption-decryption muscle. Because FlashArrays operate at memory chip speed – they are made of flash memory, after all – virtually no performance degradation occurs from the encryption operation cycle.

The Pure Storage security schema works for both external and insider threats. To protect data internally, the Pure Storage FlashArray uses robust role-based access control (RBAC). No one can assign themselves access to files they aren't allowed to view. All RBAC accounts are tied to system administrators, so that only users with storage administration rights can give access to any application or host.

Imagine, unbreakable data-at-rest protection on an ultra fast drive operating at low cost. You can already measure the savings freed up for digital innovation.



Pure Storage: Encryption, Key Management Made Easy

Encrypting data is relatively easy, but keeping it safe takes both a robust key management solution and a way to protect the physical drives. The FlashArray solution accomplishes both.

The Pure Storage FlashArray requires no encryption external key management beyond initial setup. It incorporates a unique internal key management mechanism. No longer must the organization buy third-party key management programs, together with the training and administration they require. The Pure Storage solution generates keys automatically, so from a user's perspective, it's like having key management without the keys.

Should thieves take a drive physically, it won't do them much good, even if they plug it into another FlashArray enclosure. That's because of Pure Storage's two-factor approach. Data on FlashArray drives is AES-256 encrypted. The Purity operation system is designed so that a drive encrypted in one location defaults to staying encrypted when moved to otherwise identical hardware. Each drive has a unique, randomly-generated password that never leaves the Purity environment and is refreshed daily.

When users need to access FlashArray data, the OS polls all the drives to ensure their secret passwords are in place, and uses them to reconstruct the master system password. A stolen drive won't affect the remaining ones; the OS looks for a quorum of more than half of the drives in the system. But the removed drive is uncrackable.

Because there's a new password every day, even stealing an entire set of drives one at a time won't result in compromised data. The protective cycle starts automatically upon FlashArray installation.

Pure Storage, Inc.
Twitter: @purestorage

650 Castro Street, Suite #260
Mountain View, CA 94041

T: 800-379-7873
F: 650-625-9667

Sales: sales@purestorage.com
Support: support@purestorage.com
Media: pr@purestorage.com
General: info@purestorage.com