A Road Map Toward Operational Efficiency in the Federal Data Center

Federal agencies are under constant pressure to adapt to major technology trends while driving operational efficiencies. A road map is needed that supports both the agency’s short-term needs for legacy support and long-term goals for modernization.

Contents

Introduction………………………………………………………………. 2
Windows Server 2003: The end is actually the beginning………………… 2
Skyrocketing data growth………………………………………………… 4
Setting a successful mobility strategy……………………………………… 6
Navigating the software management Web…………………………….. 8
The next-generation data center…………………………………………. 9
The Insight data center migration road map……………………………. 11
The Insight difference…………………………………………………….. 12

The end of Windows Server 2003. Exponential data growth. An increasingly mobile federal workforce. Navigating a complex software procurement and management landscape. Individually, each of these trends and events places significant stress on current data center architectures and the teams that maintain them. Add in the pressure to continually increase operational efficiency, and it can be nothing short of overwhelming.

This whitepaper serves as an escape route of sorts, outlining practical solutions to help federal agencies:

1. Address the challenges above head-on.
2. Drive significant operating efficiencies and ROI in the process.
3. Ensure your data centers are ready to take advantage of next-generation architectures.
4. Focus more on modernization and less on maintenance of legacy systems.
Introduction

More than 70% of federal IT spending is devoted to maintenance of legacy systems, according to an August 2013 report from MeriTalk, a public-private partnership focused on improving the outcomes of government IT efforts.

That means most agency IT teams are stuck reacting to the daily upkeep of aging infrastructure when they'd rather be strategically focused on where the agency is going and what they need to do to get it there.

To compound the problem, the public sector has been grappling to support the same megatrends as the private sector — the end of Windows Server 2003, an increasingly mobile workforce and exponential growth in data — while also trying to juggle a growing number of federal IT-related mandates and guidelines and manage an increasingly complex on-premise and cloud-based software landscape.

As a result, federal IT teams are struggling to keep pace with the needs of their agencies, and that gap is only getting bigger. At the same time, chief information officers, chief technology officers and deputy chief experience officers face continuous pressure to reduce capital expenditures and operating expenses and increase overall efficiency.

Fortunately, a number of next-generation technologies and models are gaining traction as forward-thinking agency IT leaders and teams work to streamline their data centers. These models and approaches include:

- Hyperconvergence
- Software-defined data centers
- Open cloud solutions
- Active system management
- Enterprise software agreements

This whitepaper will break down four of the primary challenges that federal IT is facing today, and present potential solutions, mapping out an action plan to help your own data center:

- Address your primary obstacles to modernization
- Reduce complexity and increase IT agility
- Convert IT spend from ongoing maintenance to migration
- Simplify the software procurement, implementation and management process
- Cut expenses and drive operational efficiencies

Windows Server 2003: The end is actually the beginning.

On July 14, 2015, extended service for Windows Server 2003 will come to an end, closing out one of the most successful and widely adopted server operating systems to date.

Unfortunately, this success comes at a price: Many federal agencies that standardized their data centers on Windows Server 2003 years ago are now struggling to find a migration path that can lead them to Windows Server 2008, 2012, Windows Azure and other more secure, forward-looking options.

In the meantime, agencies face expensive, escalating custom support contracts through Microsoft that are unable to address a lack of compliance, lack of security, lack of support and more.
There are many reasons why federal agencies haven’t adopted a more aggressive migration plan away from Windows Server 2003, even when facing imminent end-of-support deadlines. These include:

1. **The end of 32-bit computing** – Windows Server 2003 was the last 32-bit operating system developed by Microsoft. Windows Server 2008 and 2012 are both 64-bit operating environments that offer no backward compatibility. This forces IT departments into an uncomfortable “all or nothing” posture rather than a tiered migration over time.

2. **“Version-locked” software applications** – The massive adoption of Windows Server 2003 encouraged many developers to write applications specific to that operating system. Although this delivered superior application uptime and performance at the time, it is counter to the more flexible “versionless” approach embraced by IT today.

3. **Proprietary applications** – Many federal agencies doubled down on their investment in Windows Server 2003 by creating proprietary software specific to that environment. These applications met specific needs for the agency that off-the-shelf solutions could not address, but they can be a decade or more old. The individuals and organizations responsible for their development and upkeep may no longer be readily available, leaving the IT teams stranded.

4. **Lack of resources** – Migrations take a great deal of time and money to execute properly, both of which are in short supply in the public sector, where reaction is the default mode of operation. Conducting readiness assessments and creating migration road maps are resource-intensive exercises that tax IT teams already stretched thin by competing technology events and trends.

**Inaction isn’t a strategy.**

The obstacles that prevent a migration away from Windows Server 2003 are significant, but the consequences federal IT agencies face by trying to delay the inevitable can be dire. They include:

1. **Security risks** – After July, Microsoft will cease to issue patches for Windows Server 2003, meaning any vulnerabilities discovered after the end of support will remain open indefinitely. With one security firm reporting that [34% of all malware ever created was coded in 2014](http://www.insight.com), chances are good that 2015 will be another banner year when it comes to potential security threats.

2. **Budget risks** – Paying for extended support from Microsoft is expected to cost thousands of dollars per server, and these fees are guaranteed to increase each year. With each passing month, an agency that remains on Windows Server 2003 will pay progressively more money for progressively less value.

Extended support is intended for organizations that are currently migrating to ensure they have the protection they need throughout the migration. The increased pricing model over time makes this an unattractive method of staying on Windows Server 2003 indefinitely.
The good news is, there is a way out for these teams and agencies like yours. In addition, the potential benefits you’ll receive from a successful migration can transform your data center, delivering:

- Increased efficiencies that result in strong return on investment for years to come, offsetting migration costs
- Reduced risk and improved compliance
- A more agile data center, ready to adapt to new architectures and technologies just coming to market

To find out how, turn to “The Insight Data Center Migration” toward the end of this whitepaper.

Skyrocketing data growth

The exponential rise in data in recent years has strained existing data architectures to the breaking point. According to industry analysts at IDC, the “digital universe” of data will grow from an estimated 4.4 zettabytes (equal to 1 billion 1TB hard drives) to 44 zettabytes in the next five years. This explosive and unrelenting growth exceeds the ability for many agencies and IT teams to store it, much less manage it, secure it and back it up. The result is unwanted complexity and cost in the data center, as IT teams reactively throw more hardware to scale quickly rather than proactively work to understand what data they have, where they have it and what has value.

A report from MeriTalk — a public-private partnership focused on improving the outcomes of government IT efforts — projects that by 2024, federal government agencies will spend as much as $16.5 billion storing nothing more than redundant copies of valueless, "nonproduction" data.

So it’s no wonder that despite the Federal Data Center Consolidation Initiative’s (FDCCI’s) goal of decreasing the number of data centers by a minimum of 800 from 2010 to 2015, the number of data centers has actually risen during that time.

Every problem creates solutions, however, and three storage trends — distributed architectures, federated deduplication and enterprise cloud storage — are gaining traction among federal agencies interested in managing explosive data growth and reducing complexity and cost at the same time.

Distributed backup architecture

Distributed backup moves the backup process from a traditional network architecture based on centralized servers and storage arrays to a decentralized system that allocates backup data across the entire network. In short, the network itself becomes the backup “device.”

With a distributed backup architecture, all computers within the network are leveraged as a collective virtual server. Based on peer-to-peer network technology, a distributed backup architecture splits the backed-up files from each computer (or node) and allocates that backup data across the network.

All computers within the network simultaneously function as clients and servers, copying their data to the network and providing access to the backed-up data of other computers. Physically, there is no central data storage — just the network nodes.
Powerful and cost-effective, a distributed backup architecture eliminates the need for capital-intensive backup hardware while automating a reliable backup process that can improve enterprise resiliency. If a node or even a data center goes down, the backup and restoration processes remain available.

**Federated deduplication**

Federated deduplication (“dedupe”) means data is saved once using a single technology, and then moved anywhere without ever having to be rehydrated or adding the duplicate data back in. Federated dedupe brings efficiencies that can lower both the storage overhead and Wide Area Network (WAN) bandwidth burdens.

However, although adding dedupe to a disk-based backup subsystem will save disk capacity, it will not reduce the amount of data that must be sent to the subsystem for storage. Conversely, deduplicating backup software may reduce the load on the network but increase the workload of the backup server.

Federated deduplication increases flexibility, enabling agencies to optimize backup processes, reduce network bandwidth costs and improve backup throughput.

**Cloud storage and Backup as a Service (BaaS)**

Cloud storage or remote backup services leverage the cloud for enterprise backup needs. Cloud BackUp and Restore (BUR) services assure agencies that what was backed up is recoverable whenever it is required. These services offer ubiquitous access to transfer data, and repositories that are always available and scalable by allocating storage on demand.

Cloud providers use strong security and encryption at rest and in-flight: Most remote backup services will use up to 448-bit encryption to send data over the Internet, meeting or exceeding the Advanced Encryption Standard (AES) established in 2001.

Cloud storage models can reduce backup times as the service adjusts compression rates dynamically. They also reduce management complexity by presenting a single interface to configure backup schedules, select retention periods, view job progress and alerts, and perform restores.

For agency data management, hybrid cloud backup models combine local backup — for fast backup and restore — with off-site backup for protection and scalability. Cloud backup models also present the possibility of unlimited data retention while reducing capital costs.

**Rein in “data sprawl.”**

The explosive growth of data has left many agency data centers struggling with a variety of disparate storage and backup architectures supporting a patchwork of protocols, standards and degrees of completion.

As a result, many IT teams have no centralized way to monitor or manage data storage consistently across their agencies — a concern exacerbated by increasing numbers of mobile and connected Internet of Things (IoT) devices crowding their networks.
The resulting data sprawl creates:

- IT inefficiencies and overlaps
- Wasted money on capacity
- Wasted IT administration time
- Added maintenance costs
- Slow backups
- Higher data center costs

Insight is ready to help you gain control over your storage infrastructure before it takes control of you. Insight brings together a veteran federal support team, third-party objectivity, deep technical integration expertise and strong relationships with more than a dozen best-in-class backup and storage vendors to ensure your solution is tailored to meet your agency’s needs.

Insight’s experts work with your team through in-depth workshops to surface the goals and challenges of your data architecture, allowing Insight to assemble a customized solution that:

- Meets your immediate backup and storage needs
- Migrates your data center seamlessly
- Dramatically reduces complexity and related costs
- Increases efficiency
- Allows you to scale smoothly and proactively as your data volumes grow

To find out more, turn to “The Insight Data Center Migration” toward the end of this whitepaper.

Setting a successful mobility strategy

Federal agencies have invested an estimated $1.6 billion in the mobile workforce since the government’s Digital Government Strategy was issued in 2012, according to a Mobile Work Exchange report released in June 2014.²

But despite the investment, just 56% of federal IT managers surveyed in the report felt they were taking “full advantage” of mobility in their agencies. What were the primary obstacles to their success? Security, funding, culture and procurement issues topped the list.

So while great strides have been made to give federal employees the ability to securely access files and data across a growing variety of mobile devices, most agencies still have a long way to go to reach full mobile enablement.

Bring Your Own Device (BYOD)

At the heart of the agency, mobility migration is the decision to embrace a BYOD or Choose Your Own Device (CYOD) strategy. Though they may seem similar on the surface, one offers significant advantages to federal agencies.

Telecommunications research firm Ovum believes that BYOD has a number of pros and cons associated with it, including:

- **Existing employee behavior, demands and requirements**: Ovum research indicates almost 68% of smartphone-owning employees will use that device for work, as will almost 70% of tablet-owning employees. BYOD allows that behavior to continue with organizational support.
Desire to cut costs: BYOD obviously passes the cost of the fast mobile refresh cycle on to employees, but the need to subsidize personal voice and data plans to account for increased work activity may offset or even eliminate these savings.

Mobility as a long-term strategic investment: BYOD allows employees to manage the procurement and upkeep of their mobile devices, letting the IT team focus on other strategic needs.

Heightened risk profile: It is significantly difficult to secure devices and data in a mobile ecosystem stocked with a variety of mobile device types, operating systems and methods of acquiring applications. This is the largest drawback for federal agencies and other high-profile industries and organizations.

Federal certifications and standards: For some federal agencies, BYOD simply isn’t an option. Within the U.S. Department of Defense (DOD) all eligible mobile device vendors must have “full operational capability” certification on devices that will access DOD systems and data, a certification that only BlackBerry has secured.

Choose Your Own Device (CYOD)
Instead of offering an unlimited number of device options like BYOD does, CYOD lets employees choose from a number of pre-approved devices to use at work and, often, personally as well.

CYOD strikes a balance between access and standards, allowing for more choice than standard agency-issued hardware but more control and security than BYOD. Let’s consider CYOD from the same pros and cons:

- Fits existing employee behavior, demands and requirements: Based on Ovum’s 2013 survey, nearly 60% of employees surveyed would welcome a CYOD strategy, while only 14% were strongly opposed to it. The biggest variable, of course, is the breadth of devices offered.

- Desire to cut costs: CYOD often leads to higher procurement costs than BYOD, because the agency bears the burden of device acquisition.

On the other hand, device monitoring, maintenance and support costs could potentially be lower, along with data plans negotiated on a much larger scale — a practice endorsed by the White House’s Office of Management and Budget.7

- Mobility as a long-term strategic investment: CYOD acknowledges the importance of employee mobility, and works to balance access and control for the long-term benefit of both agency and employee.

- Reduced risk profile: Perhaps the greatest benefit of CYOD — and thus, the reason federal agencies might favor it — is the improved security posture. CYOD ensures sensitive files and data are only accessed through a select number of pre-approved, government-owned devices. These devices can be remotely monitored, managed and wiped without concerns about potential usage outside the government’s data ecosystem.

- Federal certifications and standards: Here again, CYOD is the superior choice for federal agencies. By relying on the agency to create and maintain the list of approved devices, the IT team is able to ensure all devices offered meet all eligible standards and certifications.
The CYOD workshop begins with a previsit discovery to identify your strategic agency objectives. Then, during the on-site session, Insight will map your current IT initiatives, identifying gaps and sequencing issues, and compare your approach with mobility management best practices from the public and private sectors.

Contact Insight’s federal government team using the information at the end of this document to discuss Insight’s mobility capabilities with one of our federal government specialists.

Navigating the software management Web

As the number of devices assigned to employees multiplies and the cloud blurs the lines between individual licenses and Software-as-a-Service (SaaS) accounts, federal agencies are having a more difficult time monitoring and managing the software lifecycle from acquisition to disposition.

At best, this complexity is a distraction requiring already-limited resources to manage. At worst, it could:

- Expose the agency to significant liability due to unauthorized software usage.
- Make it difficult to capitalize on potential economies of scale during the acquisition process.
- Waste millions on software licenses that are no longer needed.

In May 2014, the General Accountability Office (GAO) addressed this growing issue by recommending that all federal agencies:

- Centralize management of software licenses.
- Create an inventory of existing licenses.
- Automate the inventory to ensure agencies are optimizing the licenses under their control.
- Use those metrics to guide future purchases.

These activities fall under what is broadly referred to as “enterprise agreements,” “enterprise software agreements” or “enterprisewide agreements.” Regardless of the terminology used, they can be a highly effective means of reducing complexity, management overhead and unnecessary costs.

For example, the Department of Homeland Security reported $181 million in cost avoidance from fiscal 2012, thanks to enterprisewide software license agreements executed with 10 software vendors, according to a May 2014 article in FCW magazine. ⁸

In addition, NASA, Veterans Affairs and the Department of State all reported savings in the millions, thanks to renegotiated license agreements with vendors.
Enterprise agreements aren’t just for enterprises.

For federal agencies looking to optimize their software procurement and management functions and reap the significant benefits that result, Insight offers Clear Advantage, the end-to-end solution for software management.

Insight applies its knowledge of the federal market — more than 100 years of collective federal government on the team — and its close relationships with more than 50 of the top software providers to craft the ideal solution for your agency’s needs.

This support takes place in three phases:

- **Software licensing** — Insight will assess your agency goals and needs, and develop a volume licensing strategy that helps you purchase efficiently and meet your objectives.

- **Implementation** — Insight offers unparalleled scale and support options, with remote and on-site operations in 22 countries. Insight representatives can get your team the support they need, no matter where they’re located.

- **Asset management** — Insight is able to provide valuable ongoing compliance support, as well as global on-demand reporting, dynamic tracking, audit support and accurate record management, all in one place.

To find out how Insight can help your agency streamline your software procurement and management needs and maximize your buying power, contact Insight’s dedicated federal government team using the information at the end of this whitepaper.

The next-generation data center

Thankfully, a number of emerging trends are able to address the challenges federal IT teams face: hyperconverged systems, Software-Defined Data Centers (SDDCs), open cloud solutions and active system management.

Individually, each trend offers promise for the next generation of data centers. Collectively, they present a compelling path forward for agencies looking to increase operating efficiency and agility while removing unnecessary size, complexity and cost in the process.

**Hyperconvergence**

Converged systems are an evolution from the traditional IT system and operational silos. They offer a relatively simple design that brings together best-in-class technologies based on reference architectures to greatly compress integration timetables compared to current architectures.

Hyperconverged systems are modular, designed to grow by simply adding modules. Framed around storage, hyperconverged solutions leverage improvements at the storage controller software layer to scale more efficiently. “Instead of scaling up by adding more drives, memory or CPUs, you scale out by adding more appliance modules,” says Keith Townsend, a technology management consultant for techrepublic.com.
Hyperconverged systems also take advantage of a simplified administration model and are often managed by a single screen. In other words, one team (or person) can manage the complete hyperconverged stack, which brings the advantages of simple designs, decreased administrative overhead and simplified vendor management to highly virtualized environments.

**Software-defined data center**

A SDDC is an IT infrastructure that extends virtualization concepts such as abstraction, pooling and automation to all of the data center’s resources and services to achieve IT as a Service (ITaaS). In an SDDC, every aspect of the infrastructure — storage, networking, computing and security — is virtualized and delivered as a service.

The idea behind an SDDC is that once hardware is virtualized into a pooled set of resources, software can automate processes and allocate pooled resources on demand as a service. Emily David at the Softchoice Advisor blog describes the SDDC approach as “kind of like a Netflix for business applications.”

Using her example, there’s no need for a DVD player (owned hardware) any longer: “You simply need access to Netflix’s pooled library of movies, and Netflix needs to deliver high-quality movies on demand, anytime,” she explains. The SDDC approach delivers business applications along a similar model.

**Open cloud solutions**

For federal agencies bogged down by legacy IT investments, moving to the cloud requires judicious steps that must increase value with each move. “The burden of legacy systems is just one challenge that adds to the complexity of cloud computing,” writes Ann Bednarz, assistant managing editor for CIO magazine and cio.com. “CIOs and cloud leaders wrestle with many other common challenges, including security, vendor lock-in and shadow IT.”

Vendor lock-in has always been an issue, precipitating a need for very open cloud solutions, while security represents an ever-evolving concern. Multiple tools and tactics are often needed to protect information. Cloud providers understand that legal and security issues are some of their biggest obstacles, so they’ve concentrated on addressing those issues by championing open solution sets.

“Shadow IT” refers to IT systems built or acquired without explicit organizational approval — essentially, technology solutions deployed without the agency’s IT department. As such, shadow IT solutions are not often in line with the agency’s requirements for security, maintenance, documentation or oversight.

Open cloud solutions, however, allow IT departments to resolve issues of vendor lock-in, security and shadow IT by encouraging a diverse cloud solution set while maintaining control of it for the agency.

**Active system management**

When managing a complex mix of platforms from a variety of vendors and multiple consoles, manual and disconnected IT processes can result in unpredictable service levels and users frustrated by IT deployment schedules.
An active system management approach, however, can help data centers more rapidly and efficiently deliver the IT services their users demand. Specifically, active system management can facilitate:

- **Accelerated IT service delivery** by automating and centralizing key functions, such as workload and infrastructure deployment
- **Deploying new resources with speed and confidence** with guided workflows and a wizard-driven graphical interface
- **Freeing up IT staff** by dramatically reducing manual tasks and touchpoints so IT can focus on strategically aligned projects
- **Using infrastructure more fully and efficiently** by pooling server, storage and network resources based on specific requirements
- **Standardizing workload delivery** to increase deployment accuracy and to scale IT workloads based on business demand
- **Managing infrastructure lifecycles** with comprehensive firmware updates, compliance and remediation across server, network and storage resources
- **Maximizing investments** with support for heterogeneous IT environments

**Charting a course for migration**

In a recent survey of 152 federal IT decision-makers, more than half — 50–65% depending on the data center function — have started to shift to software-defined solutions like those noted above.\(^9\)

The decision-makers also felt the migration would be a long one, with nearly one-third of respondents (31%) believing it would take four or more years to complete.

To begin taking advantage of these next-generation solutions more quickly and seamlessly, with less burden on your IT staff and for less money than you could procure the solutions yourself, look to Insight.

**The Insight data center migration road map**

Insight offers a dedicated, veteran federal support team and a proven, time-tested process devoted specifically to helping agencies like yours migrate to a next-generation data center environment smoothly and cost-effectively.

The road map consists of six steps:

1. **Creating a data center inventory**: Insight’s federal specialists begin by cataloging your data center architecture, using data augmentation tools to create a comprehensive snapshot that is more complete than what the IT teams themselves can provide.
2. **Categorizing the functionality:** Insight’s team applies a stoplight system to each function, noting whether it:

- Migrates easily (green) like file and print servers or storage area networks
- Requires some remediation (yellow) to migrate properly
- Poses significant problems (red) for functions that are well past end of life, proprietary, version-locked or require significant intervention in order to migrate

These instances may be rare, but they are the most time-consuming to address.

The deliverable for this first phase includes the following items based on your agency’s needs, budget, available resources and desired cutover time frame:

- Infrastructure inventory
- Migration plan and timeline based on the inventory
- Project plan to execute the migration plan
- Cost and resource estimate to fund the project plan

Once these details have been agreed upon, the second phase — the execution of the migration — can begin. While each integration differs greatly, most follow these steps:

3. **Hardware and software procurement:** Insight is a single-source provider of hardware from data center leaders HP, Cisco, Dell, Intel and more. Insight is able to specify the exact product for your needs, then procure it and pass its preferred provider savings on to you.

4. **Hardware integration:** Once the hardware and software are purchased, they are sent to Insight’s integration center, where your solution is integrated, tested, prepped and prestaged for your environment.

5. **Staged on-site:** Once the solution has been thoroughly tested and certified, the complete solution is shipped to your data center, where it is met by Insight engineers on location and readied for cutover.

6. **Cutover and ongoing support:** The new solution cutover is planned, practiced and executed according to the project timeline, with an expectation of zero downtime. Once the systems are successfully transitioned per the timeline, Insight provides additional on-site and remote support per your specifications.

**The Insight difference**

Although every migration has its own intricacies, agencies that rely on Insight to help plan and execute their successful migrations can expect a number of concrete benefits from the engagement.

These include:

1. **Reduced solution procurement costs** due to Insight’s relationships and sourcing power
2. **A focused agency IT team** by leveraging Insight’s scope, scale and federal government-specific resources
3. **A smooth cutover** by relying on Insight’s integration center to prepare the solution for your specific environment ahead of time
4. Reduced agency risk and increased compliance

5. Significant increases in operating efficiencies due to:

- Greater opportunities for virtualization, increasing server and storage use, eliminating downtime and increasing computing densities
- Greater data center agility and more dynamic resource allocation through virtualization and software-defined computing, storage, networking, security and management
- 64-bit operating environments that deliver higher performance than their 32-bit counterparts, for those data centers still relying on Windows Server 2003
- Lower power usage due to more modern components, greater computing densities and higher utilization rates
- Easier integration with private or hybrid cloud-based architectures
- Lower overhead and less downtime due to more modern, advanced hardware, monitoring and allocation systems