The Government Digital Workspace for Dummies
A Wiley Brand

Learn to:

- Lead the digital transformation to drive efficiency and modernization in your agency
- Improve data security, service delivery, and continuity of operations with a digital workspace
- Enable secure, real-time access to data and applications across any device or location

Brought to you by

vmware

Samantha Reid
About VMware

VMware is a global leader in cloud infrastructure and business mobility. Built on VMware’s industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant, and more secure. Customers can innovate faster by rapidly developing, automatically delivering, and more safely consuming any application. With 2015 revenues of $6.6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.
The Government Digital Workspace
VMware Special Edition
The Government Digital Workspace

by Samantha Reid
Table of Contents

Introduction .................................................................1

  About This Book ..........................................................2
  Foolish Assumptions ......................................................2
  Icons Used in This Book .................................................3
  Beyond the Book ..........................................................4

Chapter 1: The State of the Union: An IT Perspective ... 5

  The Evolution of Digital Government ................................5
  Code Red: Cybersecurity in Government ............................7
  The Digital Workspace for Government ...............................8

Chapter 2: Inaugurating a New Approach: The Digital Workspace .......... 9

  Understanding the Role of IT ............................................9
  Improving Agency Outcomes ............................................10
  Meeting Diverse Needs ..................................................11
  Key Drivers of the Digital Workspace ................................11
  Advancing Missions ......................................................13

Chapter 3: Becoming a Change Agent: Planning the Digital Workspace ...... 15

  Developing Your Strategy ................................................15
    Establishing your goals and objectives ............................16
    Identifying issues .......................................................17
  Developing Your Framework .............................................19
    Starting with people: Users ...........................................19
    Recognizing that work style determines applications ...........22
    Letting work styles determine form factors .......................24
    Being the change you want to see ..................................25

Chapter 4: A More Perfect Union: Architecting the Digital Workspace for Government .... 27

  Many Powers in One Platform: Virtualized Desktops .......... 27
  Application Delivery ......................................................30
  Mobility Management ....................................................31
  Identity Management ......................................................33
Chapter 5: Checks and Balances: Managing the Digital Workspace ................. 37
  Assessing the Real Cost of Desktop Management ..................... 37
  Simplifying Desktop Management .......................................... 38
  Improving Application Delivery and Management .................... 40
    Managing by policy ........................................................ 41
    Managing identity ....................................................... 43
    Managing content ....................................................... 43
    Managing disaster recovery .......................................... 43
  Choosing a Mobile Device Management Solution ................... 44
  Planning for an Enterprise Mobility Management Solution ........ 46

  Identifying Digital Workspace Security Essentials .................. 47
  Securing the Network ................................................... 50
  Deploying a Digital Workspace Purpose-Built for Government ....... 51
    Security from Endpoint to Endpoint ................................ 51

Chapter 7: The Briefing Room: Deploying the Digital Workspace ............... 53
  The Digital Workspace in Action ........................................ 54
    Operationalizing the digital workspace ............................. 54
    Leveraging resources ............................................... 54
    Piloting and testing ................................................ 55
    Establishing guidelines ............................................ 55
    Training IT staff ................................................... 55
  Rights and Responsibilities: Bringing It All Together ............. 56

Chapter 8: Nine Key Areas to Address When Making a Business Case for the Digital Workspace ................................. 61
Introduction

Today’s government agencies are experiencing a seismic shift in computing capabilities, core processes, and personnel workstyles. Blame the consumerization of mobile devices and around-the-clock advances in end-user computing technology for creating entirely new IT and operational models.

There is no doubt that mobility can advance mission success, and there are mobile pioneers across all levels of government who have invested in new technologies to transform service delivery and operational efficiency. The key driver behind their success is workforce mobility — empowering personnel with remote access to government resources — which can only be attained by modernizing IT infrastructure and operations. But modernization is a complex and arduous undertaking for any IT department, let alone a department managing the world’s most sensitive data. To truly embrace the benefits of a mobile workforce, what is needed is a modern approach to managing data, applications, and identities across devices.

We call this approach the digital workspace, which, in layman’s terms, is the digital manifestation of the applications, workflows, and operations typically found in a physical workplace. Whereas a traditional workspace relies on the client-server computing model (with applications, workloads, and users tightly intertwined with physical hardware), the digital workspace relies on the cloud and other mobile technologies to enable secure remote access to government resources across devices and locations. This modern approach to computing not only addresses mobility’s influence in the workplace, but also embraces IT modernization to improve service delivery, mission outcomes, and internal operations.

The digital workspace takes on different forms and meanings across agencies. For some, an agency-wide desktop and application refresh is the first order of operations to enable widespread mobile access to resources; for others, already comfortable using mobile devices in the field, deploying an advanced identity and enterprise mobility management initiative is the obvious next step in their digital workspace journey.
Working backward from deployment, the digital workspace requires a substantial amount of planning, architecting, and validating. For those ready to embrace this brave new era of mobile cloud computing, this book serves as a digital workspace for government primer.

About This Book

This book provides an excellent starting point for any line-of-business leader, technology decision maker, or IT administrator looking for advice, best practices, and tips on how to securely enable a mobile workforce. By the end of this book, agencies should have a good understanding of the operational and technical requirements needed to empower a mobile workforce.

For the sake of context and continuity, we define a few terms used throughout this book as follows:

- **Digital government**: The use of digital technologies to support agency operations.
- **Mobility**: The functionality that enables users to access information remotely.
- **End-user computing (EUC)**: A computing approach focused on the experience of the end user in the computing environment.
- **Workspace**: The attributes that make up a user’s work environment, including physical location, applications, and devices.

Finally, as if there aren’t enough three-letter acronyms in technology, because practically every government agency has its own three-letter acronym for just about everything — and they don’t always mean the same thing across different agencies — we spell out any acronyms used throughout this book.

Foolish Assumptions

It’s been said that most assumptions have outlived their uselessness, but we’ll assume a few things nonetheless:
✓ You have a strong working knowledge of government IT, including desktop and application management.

✓ You’re part of an agency that relies on field-based personnel to conduct critical functions, or an agency that can benefit from mobile access to work resources.

✓ You’re a chief information officer (CIO), chief technology officer (CTO), chief information security officer (CISO), chief security officer (CSO), department head, IT manager, information architect, engineer, or other senior leader evaluating strategies and solutions that empower personnel and improve constituent services.

If any of these assumptions describes you, then this book is for you. If none of these assumptions describes you, keep reading anyway. It’s a great book, and when you finish reading it, you’ll know a few things about designing a secure digital workspace fit for a government agency!

**Icons Used in This Book**

Throughout this book, we occasionally use special icons to call attention to important information. Here’s what to expect:

![Remember Icon]

This icon points out information that should be etched in marble on the steps of the Lincoln Memorial. Well, maybe not, but you should at least etch this information into your own gray matter!

![Technical Stuff Icon]

You won’t find the secret to cold fusion here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff legends — well, nerds — are made of!

![Tip Icon]

These tips aren’t the “tip of the spear,” but they do point out helpful suggestions and useful nuggets of information.

![Warning Icon]

Although not as serious as a surgeon general’s warning, you should nonetheless take heed of this icon and the information it points out. You might just save yourself some time and frustration!
Beyond the Book

There’s only so much we can cover in 72 short pages, so if you find yourself at the end of this book, thinking, “Gosh, this is an amazing book — where can I learn more?,” just go to www.vmware.com/products/digital-workspace, and if you find yourself itching to test drive the digital workspace, visit https://portal.vmwdemo.com/session/new.
In This Chapter
▶ Tracing the evolution of digital government
▶ Highlighting the importance of cybersecurity in government
▶ Acknowledging the need for the digital workspace in government

IT departments across every market sector are responding to a new era of computing: the mobile era. Innovations in end-user computing (EUC) technologies have made the possibility of a mobile government workforce more secure, affordable, and achievable than ever before. According to information technology research and advisory company Gartner, government chief information officers (CIOs) estimate that 80 percent of business processes will be impacted by digital within five years. What is your agency doing to embrace this second coming of government IT?

In this chapter, we explore the evolution of digital government, the importance of cybersecurity, and the opportunities the digital workspace presents.

The Evolution of Digital Government

Digital is not new to government. In 1969, the Advanced Research Projects Agency Network (ARPANET), a precursor to the Internet, was the first network to implement TCP/IP — a standardized protocol for transporting data packets over a
network developed under contract by the U.S. Department of Defense. Since then, the move to digital has been slow but steady.

Agencies transitioned from mainframes to PCs and laptops, eventually standardizing on Microsoft desktop software. E-government initiatives resulted in providing citizens with online access to government resources and services and, in 2002, the E-Government Act took Internet-enabled information sharing one step further by advising U.S. federal agencies to develop mobile-responsive websites.

Then came the BlackBerry, offering mobile email access and catapulting many agencies into the world of personnel mobility. For a time, managing mobility equated to managing the workforce’s BlackBerry devices, which offered a glimpse into the benefits of a more modern end-user computing environment.

Looking back, the early years of digital government focused on network and device security. Today, with the amalgamation of users, applications, operating systems, and devices within the workforce, the digital landscape is much more complex and difficult to manage.

Microsoft applications and desktop PCs no longer dominate the government workplace. Cloud-native, web, and Software-as-a-Service (SaaS) applications are able to accomplish the same levels of productivity as legacy applications. BlackBerry adoption rates continue to decline because Apple iOS and Android devices are better suited for complex, application-heavy mobile workloads.

It’s not just IT responding to change; users are also looking for ways to improve their workflows. Field-based service workers are asking to transition from traditional desktop environments — which impede productivity and drain resources — to government-furnished mobile solutions (and apps) that deliver the same consumer-grade experience they get from their personal devices. Last but not least, even citizens are beginning to expect government to adopt mobile technologies to improve service delivery, agility, and response.

Although many agencies still operate on legacy applications and desktop infrastructure that are expensive to maintain, complex to manage, and difficult to secure — making them
more vulnerable to increasingly complex cyberattacks — IT foundations are evolving. Federal leaders have attempted to address untenable legacy computing environments. The Executive Office established a Digital Government Strategy, as well as mandates such as the Telework Enhancement Act of 2010, the Federal Data Center Consolidation Act of 2013, and the CloudFirst Policy to address personnel mobility and cloud computing. Through end-user computing technologies, agencies can comply with any digital mandate and position themselves for future mobile cloud policies.

**Code Red: Cybersecurity in Government**

Understandably, mobility is trickier for government. The sensitive nature of internal operations and the enormous amount of data on file pose very serious breach risks to national security, citizen privacy, and critical infrastructure and services. For this reason, integrating mobility into user workflows adds stress and uncertainty for IT leaders.

To further complicate matters, the mechanics behind successfully delivering mobility initiatives involve new EUC technologies to purchase, and expertise to deploy. Couple that with a risk-averse culture, a reliance on traditional desktop management, and flat budgets, and you have a recipe for infrastructure complacency.

Security and risk management continue to remain a top priority among government CIOs at the local, state, and federal levels. Although agencies remain vigilant about outside threats, the primary driver of government data leakage is internal negligence. Data security, powered by EUC technologies, is a critical issue that the digital workspace addresses.

When it comes to mobility in government, the old adage, “You’re damned if you do and damned if you don’t” applies quite well. If you do embrace mobility, you’re expected to address cultural change, security risks, and procurement headaches while giving personnel what they want, when they need it. If you don’t, you’re the outdated agency still too reliant on PCs, where no one wants to work — or at least where no millennials want to work.
The Digital Workspace for Government

Agencies recognize the confluence of legacy systems, traditional desktop management, shadow IT, and user workarounds that are challenging data security, efficiency, and mission outcomes. They understand the shifting dynamics of work — defined less by where someone goes each day and more by how he or she gets work done — and are intrigued by the possibilities of a new IT model to shift core processes, empower mobile workflows, and deepen service delivery engagements. This IT model is the secure digital workspace.

Powered by the software-defined data center (SDDC), the secure digital workspace integrates virtualization with desktop, application, and enterprise mobility management to deliver complete workforce mobility. This combination of virtualization and end-user computing technologies truly addresses mobility from all angles, resulting in a workspace available any time, across any device.

If you think your agency is behind when it comes to adopting a mobile-friendly work environment, it isn’t — at least, not yet. If you think that mobility won’t have that much of an impact on your agency, keep reading. If you want to become a change agent within your agency and believe the IT department has an important role to play in agency outcomes, definitely keep reading and think about the following questions to kick-start the digital workspace conversation:

- How much closer would your agency be to achieving mission goals and improving service delivery if your personnel had anywhere, anytime access to information?
- How much more efficient would your IT team be if it could centrally manage and secure desktops and applications across the entire workforce?
- What if you could considerably strengthen data security across any network, application, or device?
- What if you could guarantee zero downtime in the event of a disaster?
- What if you were an instrumental force in reconstructing your agency’s IT infrastructure and employee workflows to transform mission accomplishment?
Chapter 2

Inaugurating a New Approach: The Digital Workspace

In This Chapter

▶ Becoming a digital workspace change agent
▶ Getting results for your agency
▶ Addressing different constituent needs
▶ Recognizing key drivers of the digital workspace
▶ Improving mission outcomes

In this chapter, we examine the role of IT as a digital workspace change agent and explore various digital workspace outcomes, needs, drivers, and missions.

Understanding the Role of IT

IT has more influence over agency operations, investments, and outcomes than most people may realize. Think about it: As an IT leader, you have a direct impact on cybersecurity, workforce mobility, and computing infrastructure.

Data security, employee mobility, and legacy expenditures rest on the IT department’s shoulders. A complacent approach to IT modernization means employees will not likely adopt mobile workflows in the field (or will do so in spite of IT). A risk-averse approach to mobility means that the agency will continue to believe current desktop infrastructure can
withstand evolving cyber threats. Both approaches affect the agency’s talent pool, resistance to cyberattack or breach, and operations. With that said, IT has the power to merge agency priorities with today’s end-user computing (EUC) technologies to achieve dramatic security, operational, and efficiency gains.

You are the digital workspace change agent (yes, you). Becoming the digital workspace champion means putting the agency’s needs first — and potentially advancing your career along the way.

A lot goes into deploying the digital workspace. Your digital workspace journey requires re-architecting the way you deliver applications and information to the workforce. It requires new technologies, many of which you may not have experience in deploying. It requires cultural change and internal buy-in. The benefits of the digital workspace, however, far outweigh any perceived barriers.

## Improving Agency Outcomes

Along their digital workspace journey, many agencies have documented the following outcomes from their IT modernization efforts:

- Improved service delivery and mission advancement
- Lower workforce attrition
- Increased productivity and efficiencies among all types of end users (including IT)
Increased cybersecurity and compliance

Reduced capital and operational expenditures

Achievement of continuity of operations (COOP) and disaster recovery (DR) goals

Meeting Diverse Needs

The digital workspace is a platform that supports many needs:

- For the end user, the digital workspace is a consumer-simple work platform that provides freedom to access the apps and data needed to complete work from any device or location.

- For IT, the digital workspace is an end-user computing (EUC) platform that modernizes desktop management and application delivery to allow for secure workforce mobility.

- For business leaders, the digital workspace is an IT-managed mobile-computing platform built to improve agency operations, outcomes, and service delivery.

- For citizens, the digital workspace is the mark of a new era of government service delivery and response.

Key Drivers of the Digital Workspace

Although desired outcomes from the digital workspace differ across agencies, the following drivers are some of the most common starting points for agencies interested in implementing a digital workspace:

- Strengthen data security: As cyberattacks, ransomware, and insider threats continue to multiply across the computing landscape, traditional desktop and application management cannot detect, remediate, and protect against data breaches fast enough.
Modernize IT infrastructure: Many government agencies operate on inflexible legacy infrastructure that can’t keep up with a mobile cloud ecosystem composed of multiple device types, platforms, users, and applications. Siloed access to data, combined with traditional, cumbersome IT management, impede innovation and increase total cost of ownership (TCO).

Enable mobile access to government resources: With a diverse workforce ranging from active-duty military personnel to health and human services caseworkers to first responders and law enforcement, government agencies (and in turn, citizens) stand to benefit the most from mobile access to resources. As a result of a securely mobilized workforce, agencies are able to transform operations, citizen service delivery, and employee morale. Yet many agencies today struggle with the idea of managing secure workforce mobility across disparate applications, devices, and user types.

Maintain COOP: Neither mission-critical nor operational departments within local, state, and federal agencies can cease operations because of inclement weather, cyberattacks, or events that cause an office closure or shutdown. Citizens depend on government for medical treatment, protection, aid, and national security, and agencies must look to new solutions that ensure high availability and secure remote access to critical resources across devices and locations.

Keeping calm and carrying on

In 2016, when winter storm Jonas left as much as 30 inches of snow across the Washington, D.C., region and forced the closure of government offices, nearly 95 percent of the U.S. General Service Administration’s (GSA) 3,800 employees were able to work remotely for two days thanks to the agency’s robust teleworking solution, which enables employees to access full virtual desktops from home. No longer limited to just DR strategies, today’s COOP plans must incorporate digital workspaces into the overall design and architecture.
Advancing Missions

Government agencies, from local to federal, ultimately have three missions:

- To maintain democracy and justice
- To ensure national security and protection
- To provide for the general welfare of citizens

With a digital workspace, the prospect of greatly improving citizen service delivery and mission outcomes through a secure mobile workforce is within reach for any agency, from local law enforcement to the Department of Defense. In Chapter 3, you learn how to begin designing your agency’s digital workspace.
Chapter 3

Becoming a Change Agent: Planning the Digital Workspace

In This Chapter
▶ Creating a digital workspace strategy
▶ Building a framework
▶ Embodying your role as a change agent

Although it might be nice, a comprehensive and validated digital workspace blueprint for government agencies does not exist. The person (or team) responsible for digital transformation can use organizational goals as a guide, but planning and securing funding for a digital workspace is unique for each agency and calls for a change agent to champion the initiative and break through government’s cycle of continued investments in legacy systems.

In this chapter, you learn how to develop a digital workspace strategy for your agency, implement a framework that encompasses users, applications, and devices, and leverage all available resources to become a change agent for digital transformation.

Developing Your Strategy

Change agents drive transformation by focusing on organizational effectiveness, improvement, and development. More so than ever before, IT is the modern-day change agent for
many organizations. Because information technology affects so many aspects of today’s workplace operations, IT has the opportunity to become a center of innovation and an essential enabler in improving workforce productivity and efficiency. Developing a strategy for change is necessary, although IT must take a new approach when planning the digital workspace.

Many agencies struggle to develop a strategy for the digital workspace because of the following:

✓ Perceived risk to data security, service reliability, or loss of IT control
✓ Lack of C-level and cross-organizational support
✓ Cultural resistance or fear of change
✓ Organizational silos
✓ Ineffective governance
✓ Inadequate budget or resource allocation
✓ Lack of IT readiness or expertise

The key to developing a strategy for change is to adopt a planning approach that supports the end users’ needs, while delivering near-, mid- and long-term value to the agency. The result is an end-user computing (EUC) strategy that contributes to agency value, while addressing fears and removing barriers to the digital workspace.

Without a plan, many agencies will wait until an inflection point is reached and address the need for a digital workspace in a piecemeal fashion. However, deploying technology solutions incrementally, by pain point or urgency, is ineffective. The problem with such an approach is that without a comprehensive strategy, IT cannot transcend sporadic digital initiatives to accurately prioritize and forecast long-term digital workspace projects.

**Establishing your goals and objectives**

Strategically planning for the digital workspace is a collaborative effort among leaders, stakeholders, and end users.
An effective strategy is a “design in progress” that is always changing to reflect new business drivers, operational changes, technological advances, and, most important, end-user dynamics.

Plans must be flexible enough to continually evolve as priorities shift and new technologies are introduced.

When planning a digital workspace strategy, aligning with the agency’s goals and objectives (as well as cross-departmental goals and objectives) is crucial. Not only does this approach take the goals of the entire agency into account, but it also serves as the basis for performance measurement. Organizational and IT leaders must work together to develop the strategy with both groups determining digital priorities, measures of success, and key performance indicators (KPIs). Consistently reviewing performance against plan and refining the strategy accordingly is a must.

Examples of quantifiable digital workspace KPIs include reductions in

- Monthly data center costs
- Personnel attrition
- Service (or help) desk incidents (or issues)
- Desktop or application deployment or refresh times

**Identifying issues**

Prior to developing a framework, interview and survey anyone in the agency who will be impacted by a digital workspace, including executives, end users, and department heads. Discuss current challenges and the operational and societal benefits of a digital workspace, as well as the consequences of maintaining the same infrastructure and processes despite the changing IT landscape.

During this discovery phase, it’s also critical to identify all the foreseeable mobility needs of the organization and to prioritize cycles relative to budget, agency goals, and feasibility. For some agencies, the first digital workspace project may involve a desktop refresh; for others, the need to address a particular use case within a unit or department — such as
enabling caseworkers in the field to access applications from secure mobile devices — will take precedence. Your digital workspace strategy should account for individual projects and user groups through a multiphase approach delineated by time frames.

Here are some common starter projects for the digital workspace:

- Windows operating system (OS) and application migration
- BlackBerry Enterprise Server (BES) and other legacy mobility migrations
- Meeting continuity of operations (COOP) and disaster recovery (DR) goals
- Providing field workers with secure mobile access to data and apps
- Managing mobile devices across the organization
- Enabling secure content collaboration and file sharing on mobile devices
- Strengthening data security across users, applications, and devices
- Improving desktop and application management

A detailed understanding of a user group’s work style and the applications they use to power that work style is also a core component of your digital workspace strategy. Without this level of granularity about the different applications, devices, and requirements for specific user types, an agency’s digital workspace strategy will inevitably become a one-size-fits-all solution fraught with restrictive policies, low adoption rates, and overprovisioning.

When planning a mobility solution for a user group, consider the following questions:

- What percentage of the team is mobile?
- What devices do they use?
- What does their day-to-day work life entail?
- What are their core job responsibilities, and how are they measured against them?
✓ What applications do they rely on?
✓ What applications have they requested access to?

You don’t have to “rip and replace” all your infrastructure to deploy the digital workspace; the ability to leverage existing technology investments, including legacy applications, is a key attribute of the digital workspace.

Developing Your Framework

The digital workspace blends the boundary between work style and workspace to deliver unified and consistent access to work programs and applications across device types and locations. The three key ingredients that make up the digital workspace are users, applications, and devices.

Starting with people: Users

Users are at the top of the list. At the end of the day, the digital workspace is all about people; it’s about how they work (work style) and where they work (workspace). Government inarguably employs the most diverse workforce in the world, which means that government IT is tasked with managing a wide range of user types across job functions, security clearances, locations, and form factors, each with its own unique application, device, and mission requirements. Technically, hundreds of unique user types could exist within an agency, but managing hundreds of different user personas is not the point of the digital workspace. Instead, the digital workspace focuses on managing personnel by core user groups, further broken down by work style. From there, IT can set up a multitenant management structure to apply specific access controls and applications to users within the common work style groups.

The following user groups (and work styles) are among the most common within government:

✓ **Office workers:** The office worker’s responsibilities range by job function, but this type of worker’s use case is fairly standard: He or she requires access to a broad set of
applications — from productivity to 3D graphics — to get work done, and primarily works from a single office location on a desktop PC. This worker doesn’t necessarily require mobile access to government data and resources, but that isn’t to say that a digital workspace isn’t important to this work style. From an IT management and PC performance perspective, managing office workers through a digital workspace frees up IT resources, budget, and, in the event of an office closure, supports COOP with access to a full suite of applications remotely. Examples of office workers include office administrators, IT service desk and administrators, human resources (HR), and finance.

- **Field-based personnel:** Extremely common in local and regional municipalities, the field-based worker spends all or part of the workday in multiple locations outside of the office. This type of work style is best suited for mobility. A large category of field-based personnel includes emergency and first responders who have a direct impact on citizen health and safety, and mobile access to resources beyond traditional vehicle-mounted computer-aided dispatch (CAD) applications is transformative. Nonemergency field-based workers also experience substantial gains in productivity through mobile data capture, reporting, and collaboration. Laptops and tough books have been the primary devices for this type of worker, but tablets and large-screen smartphones are gaining traction.

- **Mobile executives:** The mobile executive often manages sensitive or classified data and requires access from any device or location. The mobile executive relies heavily on productivity applications, including the full suite of Microsoft Office applications, with email ranking as one of the most important applications for communication, collaboration, and operations. Because this worker often travels, tablets and laptops are the most commonly used devices. Examples of the mobile executive include heads of state, agency executives, chief information officers (CIOs), chief technology officers (CTOs), and controllers, department heads, and other senior managers.

- **Shift workers:** This type of worker uses a limited set of applications in a very systematic fashion within a single office location. Usually deskbound, this type of worker
often shares devices with other shift workers. Examples of shift workers include call center personnel, emergency dispatchers, census workers, and government contractors.

✓ **Intelligence and defense personnel:** Reserved for the highest echelons of physical and cyber security, this type of worker is either on the ground or in an office supporting the front line. Maintaining data security and COOP at all times is imperative to this type of worker, as a data breach or disruption to a network or application can delay life-saving and time-sensitive, mission-critical information. Devices in the field are usually rugged, while office-based defense and intelligence personnel primarily access Microsoft Office applications and email on desktops or laptops.

---

### The impact of mobility on government field workers

There is no shortage of mobile use cases in government. Here are just a few ways that agencies have deployed mobility in the field to improve mission outcomes and service delivery:

 ✓ **Law enforcement, firefighters, and emergency medical services personnel** can leverage reliable, real-time mobile access to critical applications and dispatch information from the field to substantially improve response times and service delivery.

 ✓ **Warfighters** can gain real-time access to a city’s geographic information system (GIS) to improve situational awareness and mission outcomes.

 ✓ **Field-based social services caseworkers** can remotely update and report from a tablet in their parked vehicles, eliminating extra drive time to and from the office to complete routine paperwork, while increasing the number of client visits per day.

 ✓ **A county parks and recreation department** can integrate its existing back-end financial system with a mobile point-of-sale (POS) system that accepts electronic payment for park services.

 ✓ **County food services personnel** can quickly and easily log inspection reports with secure mobile access to back-end reporting systems.
Recognizing that work style determines applications

It’s no surprise that different work styles require different sets of applications. Office workers may use a combination of Windows, web, and legacy applications, while law enforcement may require access to internal and criminal justice information service (CJIS) supported applications. The list of applications per work style is not exhaustive, but it becomes the baseline for digital workspace delivery and architecture per user group.

If an IT department can’t deliver all the applications needed to complete a job, the digital workspace falls short of the end user’s expectations.

Unlike some industries that primarily rely on web, cloud, or mobile applications to complete work, government relies on vertical-specific software (VSS) for many job functions and user types. Examples of VSS include

- Records management
- Case management
- Computer-aided dispatch (CAD)
- Video surveillance
- CJIS
- Project management
- Geographic information systems (GIS)

To better align with digital initiatives, agencies will need to consider deploying VSS from the cloud not only to provide mobile access to mission-critical applications, but also to improve application performance.

For agencies that mostly deal with classified or extremely sensitive data, moving VSS to the cloud may not be an option or may be met with extreme skepticism. To overcome this barrier, some agencies will host applications within their own private clouds while others will utilize public clouds operated by vendors that have achieved the authority to operate cloud services for highly secure environments, per Federal Risk and Authorization Program (FedRAMP) standards.
Although commercial cloud applications are gaining traction within government, on-premises legacy applications are still very much the norm. In fact, the majority of an agency’s IT budget goes toward maintaining legacy infrastructure. A report by the U.S. Government Accountability Office (GAO) found

### The cloud debate

When President Obama called for government to adopt a cloud-first computing model in 2010, the plan was to overhaul an aging, fragmented, and expensive agency IT environment. Years later, cloud hosting remains a hotly debated end-user computing topic, especially within federal government. The most common reasons against cloud hosting include

- Perceived risk of data loss and cost of moving legacy applications to the cloud
- An “If it’s not broke, don’t fix it” attitude
- Specific government-built applications that can’t be configured for cloud
- Lack of internal cloud knowledge and expertise

These concerns have largely been mitigated across cloud-based digital workspace solutions, and public cloud vendors continue to innovate offerings to align to strict federal standards. Many of the reasons agencies provide for not hosting in the cloud are actually the same reasons that other agencies give for adopting a public or hybrid cloud, including

- **Security:** Centralized management, automated application updates and patches, and the ability to store data in the data center versus on the physical device are security features that legacy host systems cannot offer.
- **Cost:** Through centralized management, workload elasticity, and gains in IT efficiency, cloud computing reduces energy, hardware, and operational costs.
- **COOP:** Cloud-based backup and DR solutions help agencies maintain business continuity through any type of system failure.
- **Mobility:** With the cloud, agencies can meet telework and field mobility goals and allow personnel to seamlessly work from anywhere.

The hybrid cloud model continues to be an attractive option for agencies looking to improve performance, management, and cost savings. Through a hybrid approach, mission-critical or sensitive applications can remain on-premises or in a private cloud while productivity applications can be hosted in the public cloud.
that of the total technology budget of more than $78 billion earmarked for fiscal year 2015, 26 federal agencies spent a total of $60 billion on legacy investments. Not only are these systems cumbersome and costly to maintain, but they were never intended to be used in a mobile-cloud work environment and, therefore, lack next-generation security features. A huge benefit of the digital workspace is preserving legacy investments while deploying modern applications, which often means hosting legacy applications in the cloud.

**Letting work styles determine form factors**

As mobility transforms mission outcomes and mobile devices become more affordable and useful within the work environment, more agencies will invest in laptops, tablets, and smartphones as part of their digital workspace strategy (in addition to adopting thin and zero clients for physical PC users).

As you can probably guess, work style and applications also drive form factors, because certain applications or job functions are not conducive to specific device types. For example, Microsoft Office applications are not generally regarded as user-friendly on tablets and smartphones.

---

**How a retiring workforce impacts the digital workspace**

There is no doubt that in the years to come, agencies will experience a dramatic shift in the makeup of their workforce. As droves of baby boomers begin to retire, decades of valuable knowledge and history will leave with them. Because mobility will continue to push its way into government workplaces, it’s critical to put forth resources now to recruit the right talent to manage and lead the digital workspace for future decades. Recruiting efforts should focus on hiring personnel with knowledge and experience in cybersecurity, cloud hosting, and mobile device management, as these skills will become future job requirements at most agencies.
Bring your own device (BYOD) in government

Government workforce studies confirm that users access internal resources on personal devices irrespective of agency policy. Labeled shadow BYOD, this trend in workforce mobility is often the result of weak internal BYOD governance or guidance. Organizations across industries are adopting BYOD initiatives to improve productivity and reduce hardware costs, but most government agencies avoid BYOD programs out of fear of compromising data security or individual privacy. A digital workspace solution can support secure government BYOD programs through a containerized approach that separates the management of agency and personal data while enforcing specific data loss prevention controls.

Customizing device types to work styles maximizes investment in the digital workspace and, when appropriate, investing in multiple form factors per user type will pay off in productivity and efficiency gains. For example, provisioning both a traditional desktop PC and a tablet for the office worker addresses both in the office and work at home situations.

Being the change you want to see

In the change agent role, you have the opportunity to guide your agency in deploying transformational end-user technologies to solve specific challenges related to data security, user mobility, desktop performance, and IT management. As you become a subject matter expert in the digital workspace for government, don’t try to reinvent the wheel. Consult with trusted advisors — from platform vendors and government contractors to professional services teams and best-of-breed product experts — to ensure proper planning across your agency’s entire digital landscape. The best advisors will be those that understand how to integrate end-user computing (EUC) solutions to solve your agency’s digital workspace goals now and into the future.
Chapter 4

A More Perfect Union: Architecting the Digital Workspace for Government

In This Chapter
▶ Virtualizing the desktop
▶ Deploying virtualized applications
▶ Managing mobile devices
▶ Improving security and user experience with identity management

The mention of workforce mobility typically conjures up images of personnel working remotely with smartphones and tablets in hand, but the digital workspace also addresses the elephant in the room: the physical desktop. Desktop management is just as important to the digital workspace (and end-user mobility) as mobile devices.

In this chapter, you learn how to achieve security, operational, and mobility goals, with a digital workspace framework that addresses the desktop architecture, application delivery, mobile device management, and user identity components of a digital workspace strategy.

Many Powers in One Platform: Virtualized Desktops

Because the desktop PC remains the de facto form factor in government, the opportunity to improve the manageability
and security of the desktop environment becomes yet another compelling reason to adopt the digital workspace; as such, deploying a virtual desktop infrastructure (VDI) is often the logical first step in any IT modernization initiative.

VDI relies on the foundation of the software-defined data center (SDDC) to integrate compute, network, and storage into a virtual desktop platform that can be centrally deployed and managed. This is in stark contrast to the traditional desktop management model that groups the physical device, operating system (OS), and applications into a bundled architecture requiring considerable IT involvement. When it comes to IT innovation, a legacy desktop environment steers investments away from more efficient end-user computing (EUC) and mobile technologies that can do a much better job of securing data and managing users across devices.

The desktop isn’t going away any time soon, so IT leaders interested in shifting to a more agile, mobile-ready infrastructure should treat the physical desktop as an endpoint device that is capable of delivering secure access to information across operating systems and locations. This is only possible with VDI. VDI replicates the physical desktop environment by running applications in the data center, and allows multiple user desktops to run as separate virtual machines sharing physical hardware resources such as compute, memory, networking, and storage.

VDI inherently strengthens data security because data resides in the data center rather than on the endpoint device. Storing data in the data center also allows IT to maintain central control of data and applications while improving departmental efficiency and reducing costs. For many agencies, the upfront cost of VDI may be steep, but unlike traditional desktop architecture, agencies can quickly begin to realize a lower total cost of ownership (TCO) through decreased operational expenses, which will continue to pay dividends year over year.

Although VDI reduces capital costs by requiring less hardware and storage expenditures over time, the real cost savings are in operational expenditures due to more efficient desktop management and maintenance.
The cost-saving benefits of VDI are buoyed with other attractive features, including improved data security and continuity of operations (COOP) with built-in backup. VDI is an ideal digital workspace solution for deskbound personnel who need fast, reliable access to agency resources, and for mobile workers who need secure, unified access to agency applications across a variety of devices.

VDI doesn’t exist in a vacuum; to achieve the best results, the following software-defined technologies are required to support VDI within the digital workspace:

- **Virtual compute**: Virtualizing x86 server resources controls infrastructure sprawl and enables agile allocation and management of applications and workloads. With server virtualization, the physical server is partitioned into smaller virtual servers, otherwise known as virtual machines (VMs) — reducing hardware and maintenance costs while improving data center efficiency and desktop performance.

- **Virtual storage**: Virtual storage area network (SAN) technologies complement virtual machines (VMs). Unlike legacy storage solutions, virtual SANs streamline and automate VM storage tasks, delivering better performance, maximizing storage space, and reducing costs. A typical storage configuration for the government digital workspace is segregated into two clusters: management and VDI.

- **Virtual networking**: Virtualizing the network has similar cost savings and operational benefits as compute and storage virtualization. Virtualized networks eliminate manual network configuration changes, maximize network capacity, strengthen data security, and support COOP.

The digital workspace for government requires separate virtual compute and desktop management components. For federal and Department of Defense (DoD) environments, the server architecture must also include integrated Common Access Card (CAC) and Host-Based Security System (HBSS) components (see Figure 4-1).

Chapter 5 provides more information on managing the digital workspace.
Intelligent networking

In an increasingly software-defined world, agencies must implement a cybersecurity strategy that extends beyond the perimeter firewall. Network micro-segmentation is a direct response to the evolving security threats that are beginning to take aim within the data center. Available as a VDI add-on, micro-segmentation segregates traffic from desktops or applications to specific workloads in the data center — substantially reducing attack vectors for malware and exploits that could do significant harm to the organization.

![Image of network diagram]

**Figure 4-1:** The secure mobile desktop for government (logical topology).

Application Delivery

Today’s computing landscape is a complex mixture of legacy, web, cloud, and mobile apps across multiple operating systems and form factors. The number of applications — both commercial and government — has grown into the hundreds or thousands for many agencies, and the cost of supporting, securing, and maintaining these applications has led to gaps in security, exorbitant management costs, and poor user experience.
IT departments are turning to application virtualization to speed deployment, increase efficiency, and reduce TCO. Just as VDI decouples desktop performance from the underlying hardware, application virtualization removes an application’s dependency on the operating system to

- Simplify OS migrations
- Eliminate application version conflicts
- Support browser and plugin virtualization
- Streamline application management
- Reduce IT support and help desk costs
- Strengthen endpoint security
- Increase workforce mobility

Application virtualization encapsulates application files and registries into a single package that can be deployed, managed, and updated independently from the underlying OS — executing across different configurations for compatibility, consistent end-user experience, and ease of management. Other benefits of application virtualization include the ability to instantaneously deploy, patch, and upgrade applications across the agency’s entire computing environment, as well as license and provision applications on an as-needed basis.

The digital workspace accounts for the most commonly used productivity apps, including email, calendar, content management, and chat. Through specific access controls, IT can granularly manage, monitor, and protect the organization from data leakage while enabling seamless, consumerlike mobile productivity.

**Mobility Management**

Device and application heterogeneity is part of the digital workspace, which means that agencies interested in enabling remote access to resources across mobile devices (including laptops) must deploy a mobile device management platform in conjunction with a VDI environment.
If you’re planning to enable remote access to applications and content on mobile devices, an enterprise mobility management (EMM) platform is necessary to secure data across endpoints. With an EMM platform, you’re able to manage every mobile aspect of the digital workspace, including

- **Devices**: Smartphones, tablets, laptops, mobile kiosks, rugged devices, printers, and peripherals
- **Operating systems**: Android, Apple iOS, BlackBerry, Chromebook, Mac OS X, and Windows
- **Applications**: Native, web, remote, and legacy
- **Email systems**: Exchange, Outlook, Gmail, Yahoo!, and iCloud
- **Content**: Internal content repositories and file-sharing applications
- **Browsers**: Native, containerized, and intranet
- **Telecom usage**: Voice, text, and data
- **Ownership models**: Government-furnished, shared, and bring your own device (BYOD)

A best-in-class EMM platform architecture is designed to meet government’s deployment complexities, security requirements, and work styles. The platform should offer both cloud and on-premises deployment options and facilitate seamless integration with all existing enterprise systems, including Active Directory and Lightweight Directory Access Protocol (AD/LDAP), Certificate Authorities (CAs), content repositories, and email infrastructures.

Additional best-in-class EMM architecture includes

- **Security** extending to users, devices, applications, content, data, email, and networks
- **Scalability** that supports an unlimited number of devices without sacrificing security or management capabilities
- **Multitenant management** capabilities across all internal subgroupings, whether by geographies, units, divisions, or other segmentations aligned with your organizational structure
Freedom of choice: Instituting a BYOD program

Although agencies operating on classified networks or managing highly sensitive data restrict personnel from using personal devices to access work resources, many others have been able to achieve the cost savings, productivity, and user satisfaction benefits that BYOD programs provide.

BYOD programs can span the range from basic email access to provisioning mission-specific enterprise applications on personal devices. The digital workspace is able to manage and secure applications and data across devices and operating systems, making it an ideal solution for government BYOD programs.

Through adaptive user enrollment, users can choose the level of access, security, and management that makes sense for their work style, providing friction-free adoption of BYOD programs. Meanwhile, IT can protect agency data within the data center, while managing enterprise data access and compliance — and ensuring end-user privacy.

If your agency is considering the use of employee-owned devices to access internal data, it’s important to create and document privacy and usage policies as part of your BYOD program to alleviate individual privacy concerns.

- **Role-based access** and authentication capabilities that allow your organization to delegate access based on user identity
- **Automated compliance monitoring** of the entire mobile environment
- **High availability and disaster recovery (DR)** with active-active configurations for high availability and redundancy with all components made to failover with minimal downtime

Identity Management

To add another layer of data security and improve user experience, consider integrating an identity management solution to monitor and manage user accounts across Software-as-a-Service (SaaS), web, and native mobile applications.
An identity provider (IDP) removes the traditional barriers to mobility — like complex passwords, configuration steps, traditional virtual private networks (VPNs), and tokens — by uniquely optimizing authentication for each device type and eliminating the need for users to remember multiple user-names and/or passwords. Combined with EMM, a mobile identity management solution establishes conditional access between the user, his or her device, and the data center, enhancing both security and user experience.

Best-of-breed identity management solutions for government agencies offer the following:

- **Managed access** with the ability to apply conditional access policies by user security group, network, and authentication strength across Windows, web, virtual, and natively installed applications

- **Multifactor authentication**, which establishes a second layer of trust, such as third-party biometrics, tap-and-go systems, and a range of adaptive authentication techniques
✓ **Directory integration and federation** that supports multiple Active Directory (AD) domains, forests, and trust configurations, and offers extreme flexibility for integrating with existing environments

✓ **Hybrid deployment models** that allow for deployment from the cloud or on-premises

✓ **Central management console** to manage identity and entitlement from one central user interface (UI)
Chapter 5

Checks and Balances: Managing the Digital Workspace

In This Chapter
▶ Getting started with the digital workspace
▶ Reducing costs with a virtual desktop infrastructure (VDI)
▶ Driving operational efficiencies with virtual application delivery
▶ Managing users, apps, and data across mobile devices

In this chapter, you learn how the digital workspace streamlines desktop, application, and mobile device management to achieve operational efficiencies and fiscal benefits.

Assessing the Real Cost of Desktop Management

The upfront cost of overhauling traditional desktop infrastructure and application management for a VDI environment may seem overwhelming, but the substantial cost savings as a result of more efficient IT management is well worth the initial investment for most agencies. In addition to operational cost avoidance, agencies that deploy VDI also significantly reduce the risk of security breaches — which often result in both monetary losses and qualitative costs such as a tarnished reputation or lack of trust among citizens.
Ultimately, VDI enables IT departments to reallocate the hours spent on repetitive management tasks and “fire drills” with new value-added projects that transform agency operations.

Take a moment to consider the answers to the following IT management questions, in order to help you gain a better understanding of the amount of time that your agency could gain back with the digital workspace:

- How long does it take your IT organization to onboard a new user?
- How many hours does it take a desktop administrator to deploy a new (or refresh) desktop?
- How many master images do you maintain?
- How long does it take IT to develop, test, and deploy an image?
- How many applications do you support?
- How long does it take to update or patch an application across devices?
- What is your average time for packaging an application?

The answers to these questions provide a glimpse into the resources — time, money, and people — that go into maintaining traditional desktop infrastructure. Through its mobile cloud architecture, the digital workspace centralizes core services, simplifies management, and enables IT to comprehensively address every endpoint, OS, user, and application within the workplace like never before.

Workspace management has a symbiotic relationship to data security, meaning that better management of data across all endpoints leads to improved data security and loss prevention.

**Simplifying Desktop Management**

From a budget perspective, the hardware, software, and labor costs associated with maintaining a traditional desktop
environment are exorbitant. Repetitive management and administration tasks such as application packaging, testing and deployment, desktop imaging, hardware configuration, and help desk support are some of the most time-consuming drains on IT resources. Across the board, the highest levels of return on investment (ROI) as a result of the digital workspace are in desktop management.

Any virtual desktop infrastructure (VDI) deployment should include an integrated environment management solution that proactively monitors the desktop environment. Intelligent real-time data regarding all desktop-related events also enables IT administrators to provide the right amount of intervention and guidance when system performance falls below expected ranges of behavior or compliance.

With VDI, the process of copying a virtual image and assigning it to a user is much faster and more foolproof than setting up a physical desktop. VDI also allows IT to repurpose legacy hardware to access the virtual desktop image, extending the useful life of the hardware.

There’s never a dull moment in IT administration and management. The most common end-user issues include

- Faulty hardware
- Application failure
- Network connectivity issues
- Malware infections
- Sluggish performance

## Supporting remote users

The geographically distributed nature of the desktop environment at some agencies adds yet another layer of complexity to desktop administration, which can make desktop troubleshooting more difficult and costly. By centrally managing desktops in the data center, administrators are able to service branch and remote locations without using a remote management tool or traveling to different locations.
Improving Application Delivery and Management

No IT organization enjoys the laborious cycle of packaging, testing, and provisioning applications. As new versions of applications and desktop operating systems are released in quicker intervals, IT needs a more efficient way to update desktop environments while minimizing downtime and data loss.

Traditional application management doesn’t account for individual work styles, which means IT typically creates a common image to support all job roles, resulting in users having access to more applications than they need. With the digital workspace, applications and user personas are decoupled from the operating system (OS) and managed from the software-defined data center (SDDC), resulting in faster application packaging and deployment across endpoints. IT administrators are able to manage configurations based on individual work styles, which consider device information and user attributes, and update automatically as those change.

Real-time application delivery and management through the digital workspace enables IT to

- Easily package applications to avoid compatibility issues
- Instantly provision applications at scale
- Dynamically attach applications to users, groups, or devices
- Provision, deliver, update, and retire applications in real time
- Ensure a more seamless end-user experience

The digital workspace also revolutionizes patch management, enabling IT to apply patches to a single parent virtual machine (VM) across the entire desktop environment between user logins. In doing so, the digital workspace benefits from the latest OS and application updates, while users never experience disruptive patch maintenance windows. With the digital workspace, IT is able to deliver and manage any application, including the following:
✓ The latest mobile cloud applications
✓ Legacy enterprise applications
✓ RDS-hosted apps

When it comes to RDS-hosted apps and desktops, the digital workspace must account for a number of features, including support for printing, USB flash drive, imaging devices and scanners, HTML access, multimedia redirection, file association, and 3D graphics support.

✓ Internal web or mobile apps
✓ Software-as-a-Service (SaaS) applications
✓ Native public mobile apps
✓ Modern Windows applications
✓ Legacy Windows applications

Download a free copy of *Applications For Dummies* at [www.vmware.com/go/appsfordummies](http://www.vmware.com/go/appsfordummies) to learn how to develop a successful application strategy that will work now and into the future.

**Managing by policy**

Policies are the gatekeeper of any organization, and IT relies on the effectiveness of policies to enforce access rules. The more granularity in your access policies, the more you can be assured that the right information is getting to the right people and, more important, that none of your organization’s sensitive data is falling into the wrong hands.

A basic policy management system should include the ability to set policies based on

✓ Session length
✓ Device type
✓ Geographic location
✓ Application type
✓ Authentication type
✓ User-group membership
Managing your Microsoft investment in the cloud

Microsoft is doing its part to push customers into the mobile-cloud era with Windows 10, the first operating system (OS) truly designed for the mobile end user. Designed to work seamlessly across physical desktops, mobile devices, networks, and ownership models, Windows 10 takes a page out of the digital workspace playbook and leverages end-user computing technologies to manage desktops, applications, and mobile devices from the cloud. The result is unified application management across devices, an extensive app ecosystem, out-of-the-box enrollment, and advanced data security.

More robust policy management systems can streamline the management of multiple identity sources like Active Directory and LDAP to efficiently manage end-user identity and access across devices.

Efficiency is the name of the game with the digital workspace. Through advanced automation of desktop images, mobile deployments, and security updates, as well as real-time analytics and performance dashboards, IT can continue to deliver high-value services while containing costs (see Figure 5-1).

Figure 5-1: Digital workspace cost comparison per user per month.
Managing identity

Optimized for the mobile cloud era, the digital workspace can also establish conditional access between the user, his or her device, and hybrid cloud infrastructure, improving security and end-user experience. Through an Identity-as-a-Service (IDaaS) offering, IT can address complex enterprise directory structures with a modular, standards-based architecture permitting nearly any type of authentication, from third-party biometrics to adaptive authentication. (Read Chapter 6 to learn more about identity and the digital workspace.)

Managing content

Seamless access to content across devices and locations is a critical function of the digital workspace, and content hosted on internal repositories should not impede mobile access. Look for content management solutions that enable IT to securely deliver files directly across a range of internal repositories and external cloud storage providers — including SharePoint, Network File Shares, OneDrive, Office 365, Google Drive, and Box — while maintaining access, editing, and sharing controls.

Managing disaster recovery

If an agency is hit by a disaster that causes its servers to fail-over to a disaster recovery (DR) location, end users need access to the applications running on those servers. In addition, users need to connect to centralized data stored at the
Managing the user environment

When it comes to desktop virtualization, many organizations have had to choose between deploying persistent desktops (desktops that are tied to a specific user) or deploying non-persistent desktops (generic desktops that get destroyed every time a user logs off). Although persistent desktops provide end users with a personalized desktop experience, they also come at a higher cost. Conversely, although nonpersistent desktops help drive down costs for IT, they do nothing to support end users with a customized experience.

Thankfully, user environment management (UEM) systems have evolved, enabling IT to install UEM clients on RDS or VDI hosts and devices such as desktops and laptops. Clients are enabled and configured through central group policy objects (GPOs) in Active Directory, allowing IT to deliver a consistent and personalized workspace experience to end users across devices and locations while driving down the operational costs of persona management.

*Remember:* Any virtual environment requires an integrated management platform that delivers comprehensive visibility and analytics across desktop and application environments, with insight into the health, performance, and capacity management of IT services across hybrid cloud environments.

recovery location. A DR plan must connect end users (and their devices) to the recovery infrastructure so that they can continue being productive. With the digital workspace, VDI, coupled with a site recovery manager add-on, allows agencies to maintain continuity of operations (COOP) throughout any contingency.

Choosing a Mobile Device Management Solution

Because mobile access to information is part of the digital workspace “DNA,” the need to secure data across devices, locations, and networks is critical. Agencies vary in their approaches to mobile device management (MDM); some only require basic device management while others require an
enterprise mobility management (EMM) solution to secure and manage complex deployments, enterprise applications, and content repositories. For most agencies, a basic MDM solution simply cannot manage and secure the proliferation of data, applications, users, and devices in the mobile work environment. Therefore, an EMM approach is becoming necessary to manage a mobile workforce. To gain the most value and security out of an EMM solution, look for the following management capabilities in a vendor:

✓ A simple enrollment process with automatic user restrictions, policies, apps, and content pushed down to devices
✓ The ability to configure and update device settings over-the-air without hindering the user experience
✓ The ability to manage entire workspace deployment from a single, web-based console
✓ The ability to enable granular “app” distribution by ownership type, device platform, or user group
✓ The ability to manage all device types, including rugged and peripherals
✓ The ability to integrate with existing infrastructure, such as directory services, certificate authorities, public key infrastructure (PKI) services, email, and content repositories
✓ System monitoring that includes detailed app and device analytics with the ability to view logs directly in the console

Preserving legacy investments

The best EMM platforms integrate with existing infrastructure through extensible APIs and a robust independent software vendor (ISV) ecosystem composed of leading device manufacturers, network access control (NAC), certificate authorities, content repositories, directory services, email infrastructures, security vendors, and more — ultimately helping your organization gain the most value out of current investments while seamlessly extending those systems to mobile devices.
When evaluating MDM vendors, make sure the provider offers a truly multitenant management platform. Multitenancy enables IT to granularly manage devices through role-based access controls (RBACs) across geographies, departments, job functions, and other custom segmentations.

Windows 10 and EMM

Windows 10 is not only revolutionizing desktop management but also leveraging core EMM principles to secure and manage mobile environments. With Windows 10, IT teams can integrate a comprehensive EMM solution to manage their Windows environment across laptops and mobile devices via a single platform.

Planning for an Enterprise Mobility Management Solution

The following questions should be answered prior to designing an EMM framework. By taking the time to evaluate these questions, you can begin to design according to your use cases and develop a solid EMM strategy:

- What is your mobility initiative?
- Which device types and operating systems do you want to manage?
- Which existing IT infrastructure are you integrating with?
- What does your organizational structure look like?
- How will you set your policies and enable your end users?
- What are all the use cases that you need to cover?
- Which resources do your employees need access to?
- Which device ownership models will be supported?
- How will users get access to applications on their devices?
- Which statutory and regulatory standards need to be met?
Chapter 6

Safeguarding Your Borders: Securing the Digital Workspace

In This Chapter
- Addressing data security in the digital workspace
- Protecting the network with micro-segmentation
- Ensuring compliance with a purpose-built digital workspace

In this chapter, you examine essential security requirements for the digital workspace, including data security, network security, and regulatory compliance.

Identifying Digital Workspace Security Essentials

Whether it’s a lost or stolen tablet, a sophisticated cyber-attack, or a user copying files to a USB flash drive in violation of agency policy, there is no shortage of accidental or malicious ways that sensitive or classified data can be compromised. Managing access to information across users, locations, and devices is an arduous task for IT, and with so many applications, files, users, and devices to manage, the likelihood of a security incident is very high.
One of the most important outcomes of the digital workspace is data security. A virtual desktop infrastructure (VDI) alone inherently strengthens data security by centrally managing users, data, and applications from the data center. Combining application and network virtualization with identity access management (IAM) and enterprise mobility management (EMM) further protects against data loss.

Because users, devices, and data increasingly operate beyond the physical walls of the workplace, designing a digital workspace that enables the following mobile security features is imperative:

- **Conditional access**: Through conditional access, IT can combine policy enforcement with IAM and EMM to restrict user access to data, applications, or devices. The same technologies can also be used to apply conditional access to mobile apps and ensure that only compliant applications can access internal systems.
✓ **Multifactor authentication**: Multifactor authentication is a requirement for many agencies; therefore, a digital workspace needs to be able to enforce multifactor authentication across devices and applications, as well as support third-party authentication services.

✓ **Smart card support**: Common Access Card (CAC) and Personal Identity Verification (PIV) cards are still standard authentication methods among defense computer networks and systems and should be supported across devices.

✓ **Automated compliance**: An automated compliance function aligned to agency policy is critical to the digital workspace. Through automated compliance monitoring, agencies can enforce access to data, based on a range of conditions, from strength of authentication to network or location, and remediate policy violations through customizable warnings or remote device wipe. The ability to “set and forget” granular compliance controls around rooted or jailbroken devices, whitelisted and blacklisted apps, open-in app restrictions, cut/copy/paste restrictions, geo-fencing, or network configuration, for example, removes the complexity of manually monitoring compliance across devices.

✓ **Data loss prevention**: For ultimate application security, administrators should be able to set compliance policies per application and prevent data loss across content with email attachment controls, copy/paste restrictions, dynamic watermarking, and more.

✓ **Basic device management**: Basic mobile device management (MDM) functionality (see Chapter 5) should include, at a minimum, the ability to remotely lock or wipe a device if it’s lost or stolen, locate a missing device, and obtain real-time device information such as operating system (OS) version, last update, location, and more.

✓ **Single sign-on (SSO)**: Made possible by a Secure Application Token System (SATS) and an identity management solution, one-touch mobile SSO allows users to access desktop, mobile, and cloud applications without passwords or complex PIN challenges.
Securing the Network

These days, bulletproofing data security means strengthening current processes and tightening controls inside the data center. With micro-segmentation, fine-grained network controls enable unit-level trust, and flexible security policies can be applied all the way down to a network interface. In a physical network, this would require deploying a physical firewall for every workload in the data center, so up until now, micro-segmentation has been cost-prohibitive and operationally unfeasible. However, with network virtualization technology, micro-segmentation is now a reality. Through data center micro-segmentation, agencies are able to

- Build an environment of zero trust within the data center, isolate servers from endpoints with known configuration vulnerabilities, and limit hosts from accessing assets they never need to access, thereby reducing the threat landscape.

- Simplify network security by enabling each virtual machine (VM) to be its own self-defending perimeter.

- Align policies with logical groups (for example, office staff, field workers, and others) to prevent threats from spreading to other assets.

- Create a matrix of policies on centralized, choke-point firewalls to attain the correct security posture.

What about derived credentials?

Because mobile device smart card readers are expensive to procure and clunky to manage, derived credentials is a mobile authentication method gaining traction within government. With derived credentials authentication, a cryptographic credential is stored securely on a mobile device in compliance with smart card regulations, which means no additional physical smart card reader hardware is needed to securely access sensitive agency applications, data, and services. The use of derived credentials within government is still in its infancy, although agencies are working in tandem with security and EMM providers to develop policy and best practices regarding the use of soft tokens in mobile identity management.
Deploying a Digital Workspace
Purpose-Built for Government

Many agencies, particularly within intelligence and defense, must adhere to specific security standards and mandates set forth by various overseeing federal organizations, although agencies with less stringent security requirements still benefit from architecting a digital workspace that aligns with federal requirements.

Your digital workspace should support the following purpose-built security standards, policies, and features:

- 256-bit, FIPS 140-2 encryption
- Smart card support
- Common Criteria/NIAP certification
- Criminal Justice Information Services (CJIS) compliance
- IPv6
- National Institute of Standards and Technology (NIST) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- Public Key Infrastructure (PKI)
- Third-party antimalware software
- Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate

Security from Endpoint to Endpoint

An integrated EMM solution addresses the same security vulnerabilities present in any agency computing environment and should deliver the same set of security features in the
Digital Workspace Security Essentials checklist mentioned earlier in this chapter. For peace of mind, ensure that your mobile deployment includes the following:

- Device security with end-to-end encryption and device restrictions
- User security through identity management, conditional access, and multifactor authentication
- Application security through app containerization
- Data security with compliance monitoring and advanced data loss prevention policies

For more information on the mobile security and management features to look for in an EMM vendor, turn to Chapter 5.
Chapter 7

The Briefing Room: Deploying the Digital Workspace

In This Chapter

▶ Exploring best practices for deploying the digital workspace
▶ Following a common approach for best results
▶ Reviewing the underpinnings of the digital workspace

By now, you should know what the digital workspace is, how it’s transforming government, and why you (together with your IT organization) are uniquely qualified to lead your agency’s transition to workforce mobility.

As you consider your first mobile project, keep this advice from Chuck Riddle, CIO of the U.S. Government Printing Office, in mind: “You only get one shot at a first impression. If you blow that, your users are not going to be as inclined to use the solution. You want to get users engaged enough to use it because otherwise your cost becomes a lot more expensive.”

In this chapter, you review best practices for deploying the digital workspace in government; examine a few common use cases across local, regional, and federal agencies; and review the structural, organizational, and technological essentials of the digital workspace to help ensure your first impression leads to a successful outcome.
The Digital Workspace in Action

Although your agency’s goals will determine your initial digital workspace projects, it never hurts to get a clear view of how other agencies have implemented the digital workspace to improve data security, IT management, and end-user mobility.

Operationalizing the digital workspace

The most effective change agents use a combination of knowledge, technology, and expertise to ensure project success. Digital workspace projects that have consistently shown the best results have followed a common approach that includes the components described in the following sections.

Leveraging resources

Possible resources to leverage for your digital workspace project include the following:

✔️ Third-party advisors: Government IT systems are complex, which means that even on a small scale, mobility initiatives can be challenging. Because the concept of a digital workspace, and the technology that supports it — specifically VDI, EMM, and even the cloud — are quite novel within government, it’s best to seek out trusted advisors who can strategize, architect, and help deploy the digital workspace for your agency. Suffice it to say, the third parties or technology vendors that you choose to assist in any stage of your digital journey should be experts in government IT, VDI, and EMM.

✔️ Other agencies: Test the strength of your professional network and talk with other agencies about their digital workspace experience and lessons learned. Many agencies are deploying desktop virtualization and EMM solutions to solve needs similar to yours. As we’ve said throughout this book, the primary drivers of the digital workspace across agencies are data security, management of the computing environment, and user mobility.
✓ **Colleagues:** Successful planning, review, and governance of the digital workspace requires input from leaders, decision makers, managers, and end users at all levels and departments within the agency. Develop a steering committee that represents executive, managerial, operational, and technological roles, as well as end users. A diverse group of voices, knowledge, and experience from operational, user, and technology perspectives will help guide digital workspace requirements.

### Piloting and testing

Before any widespread digital workspace deployment, it’s best practice (and just plain common sense) to select a pilot project with a small group of users. Establish clear goals for the pilot within a specific time frame, as well as specific roles and responsibilities. Continuously document user experience and outcomes, and adjust processes and technologies based on feedback. Continue methodically until the pilot is ready for full-scale deployment.

### Establishing guidelines

Although successfully running your digital workspace project as quickly as possible is often the goal, be sure to invest the same amount of time upfront, and together with advisors and the steering committee, to specify and establish the management of the structures, policies, guidelines, and processes that will govern IT decision rights, accountability for operating decisions, investments, standards, and management.

### Training IT staff

Outside teams — contractors, professional services, and the like — can accelerate deployment cycles, but it’s imperative that your internal IT team be able to maintain and sustain workforce mobility technologies. If not, the cost and complexity of the new solution is certain to rise quickly. Making the investment to bring in highly experienced staff, or train existing staff, will help mitigate deployment risks.
Rights and Responsibilities: Bringing It All Together

The chapters in this book are written to correspond to the structural, organizational, and technological underpinnings of the digital workspace. To recap, the process of deploying a digital workspace requires the following:

✔ **Agent of change (Chapter 2):** A change agent delivers the vision of the digital workspace to various internal constituents, including executives, department heads and other senior leadership, and end users. The change agent has a thorough understanding of the agency’s digital workspace readiness, and can articulate the value of the digital workspace across departments and job functions, addressing its benefits from all angles, including service delivery, efficiency, user satisfaction, security, and cost avoidance.

✔ **Strategy (Chapter 3):** A flexible, well-researched digital workspace strategy that aligns to agency goals, both near- and long-term, is essential to the program’s success. The strategy should include the rationale behind the project road map, the impact on various stakeholders, and the unique technological requirements across user types and work styles. Keep in mind that your strategy will constantly evolve as goals are reprioritized, new leadership comes onboard, and end-user computing (EUC) technologies evolve and mature.

✔ **Framework (Chapter 4):** Implementing a digital workspace requires re-architecting desktop infrastructure and operational processes. Your strategy will guide the order of projects, and your framework will detail the technologies required for deployment. For most agencies, a digital workspace program will include some combination of desktop virtualization, virtual application delivery, EMM, identity access management (IAM), content management, and the cloud — each with varying technical, platform, and vendor requirements.

✔ **Management and security (Chapters 5 and 6):** EUC technologies that support the digital workspace dramatically improve user, application, and device management and security. The data security and IT efficiencies gained from a digital workspace alone are enough for many
agencies to consider modernizing their desktop infrastructure and their approach to application and device management. Employing VDI, EMM, and cloud experts to deploy and manage the agency’s digital workspace is critical because an investment in the digital workspace is only as good as its ongoing management. Invest in resources that can successfully oversee the digital workspace, taking advantage of the numerous management and security features the digital workspace provides, while implementing new end-user technologies to meet goals.

✓ **Governance (Chapter 7):** At the point of deployment, you’ve clearly received support and buy-in from those responsible for the budget. Long-term success, however, requires ongoing governance across senior leaders, departments, and end users. An internal team, made up of various stakeholders that consistently review and refine the digital workspace, can help mitigate issues before they become critical barriers to projected outcomes. Working with this team (and including human resources) to foster an internal culture that embraces mobility is also critical to future success. Be sure to account for those in your agency that will be responsible for governance over the digital workspace — both near- and long-term.

Crafting your pitch

A digital workspace offers more benefits for your agency than first meets the eye. As a change agent, it’s critical to be able to pitch the digital workspace to anyone with decision-making authority, purchasing power, end-user influence, and anyone else who stands to benefit from a more efficient work style.

To start, develop a list of critical areas for improvement across your agency’s computing and operational environments, and use the following table to begin outlining specific outcomes and KPIs related to your initiatives.

The following table lists common digital workspace drivers among government agencies. Your agency’s needs will vary, but the drivers listed here align to the core use cases driving the digital workspace in government, including strengthening data security, enabling employee mobility, achieving COOP, and modernizing IT infrastructure and operations. (continued)
<table>
<thead>
<tr>
<th>Key Digital Workspace Drivers</th>
<th>Traditional IT Challenges</th>
<th>Digital Workspace Benefits</th>
<th>Success Metrics and Key Performance Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve data security</td>
<td>Traditional desktop and application infrastructure cannot adequately secure the proliferation of data among disparate users, applications, and devices in an increasingly complex mobile-cloud computing ecosystem.</td>
<td>Centralized desktop and application management</td>
<td>Reduced number of annual security incidents</td>
</tr>
<tr>
<td></td>
<td>Data stored in the data center versus endpoint device</td>
<td>Data stored in the data center versus endpoint device</td>
<td>Reduced cost of security incident resolution</td>
</tr>
<tr>
<td></td>
<td>Contextual, policy-driven access to data and applications across devices</td>
<td>Contextual, policy-driven access to data and applications across devices</td>
<td>Reduced window of time between desktop patch/update release and deployment</td>
</tr>
<tr>
<td></td>
<td>Streamlined security patches and updates</td>
<td>Streamlined security patches and updates</td>
<td>Achievement of regulatory compliance standards</td>
</tr>
<tr>
<td></td>
<td>Advanced data loss prevention tools</td>
<td>Advanced data loss prevention tools</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Desktop or application traffic segmented into specific workloads inside the data center</td>
<td>Desktop or application traffic segmented into specific workloads inside the data center</td>
<td></td>
</tr>
<tr>
<td>Enable workforce mobility</td>
<td>Traditional government IT infrastructure cannot simultaneously support mobile mission objectives while ensuring data security, leaving many agencies in a holding pattern that stalls mobile service delivery innovation.</td>
<td>Streamlined access to applications and content across any mobile device</td>
<td>Reduced workforce attrition</td>
</tr>
<tr>
<td></td>
<td>Containerized access for BYOD and shared device models</td>
<td>Containerized access for BYOD and shared device models</td>
<td>Improved personnel satisfaction</td>
</tr>
<tr>
<td></td>
<td>Centralized, multitenant management from a single console</td>
<td>Centralized, multitenant management from a single console</td>
<td>Gains in workforce productivity and efficiency</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Improved service delivery, response times, and citizen satisfaction</td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Key Digital Workspace Drivers</th>
<th>Traditional IT Challenges</th>
<th>Digital Workspace Benefits</th>
<th>Success Metrics and Key Performance Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieve COOP goals</td>
<td>Traditional desktop and application architecture cannot ensure high availability or uptime following an attack, shutdown, or power outage, compromising both mission-critical operations and noncritical workloads.</td>
<td>Operate desktops and applications from the data center to enable on-demand remote access to resources, even in the case of a disaster. Access information across any device type or operating system — anytime, anywhere.</td>
<td>Reduced downtime (both planned and unplanned)</td>
</tr>
<tr>
<td>Modernize IT infrastructure to reduce costs and increase efficiencies</td>
<td>Traditional desktop management, legacy applications, and siloed computing environments lead to inefficient use of IT resources, higher maintenance costs, and security vulnerabilities.</td>
<td>Deliver virtual or published desktops and applications through a single platform to streamline management across devices and locations. Transform application management with real-time delivery, provisioning, and updates.</td>
<td>Reduced hardware costs with virtual compute, storage, networking, security, and desktops</td>
</tr>
<tr>
<td></td>
<td>Reduced IT administration and incident support</td>
<td>Reduced operational expenses through centralized desktop, application, and identity management.</td>
<td>Reduced power, cooling, physical rack space, and office workspace requirements.</td>
</tr>
</tbody>
</table>
Chapter 8

Nine Key Areas to Address When Making a Business Case for the Digital Workspace

In This Chapter
▶ Determining project scope
▶ Calculating hardware, desktop, and application management costs
▶ Quantifying the benefits of workforce mobility
▶ Addressing security and disaster recovery (DR)
▶ Understanding the total cost of incident management
▶ Identifying gaps in project management and governance

Building a business case for the digital workspace is just as important as mapping out its technical requirements. Getting buy-in for the digital workspace takes more than just listing the benefits of implementing end-user computing technologies into everyday operations. Attracting support, approval, and funding for the digital workspace requires thoughtful, well-researched commentary and quantitative proof that your agency is facing a losing battle against your current IT infrastructure, and significantly bleeding money, resources, talent, and reputation (to name a few) as a result. The following questions can help in your quest to present a detailed, informative digital workspace pitch based on common operational pain points and IT expenses associated with traditional desktop and application management.
Each section alludes to the complex mix of operational, cultural, and technological barriers facing government IT today, and your answers will provide the operational insight and quantitative analysis needed to frame the digital workspace as the necessary end-user computing initiative to dramatically improve and change the course of agency operations and citizen service delivery now and well into the future.

**Digital workspace business drivers and project scope:**

- What is the total number of users (personnel) in the agency, including contractors?
- How many locations does your agency operate in?
- How many client-device operating systems do you support (Windows XP, Windows 7, Windows 8, Windows 10, Android, Mac OS X, iOS, Linux based, and so on)?
- What is the total number of government-furnished desktop and mobile devices in the agency, broken down by form factor (desktop PC, thin client, laptop, smartphones, tablets, and so on)?
- What is the size of the agency’s total IT organization?
- What is the agency’s average IT labor rate?
- What is the agency’s average non-IT labor rate (from entry-level employees to executives)?
- What is the total number of IT resources that directly and indirectly support end-user systems?
- Rank the following IT business drivers according to priority: strengthen data security, reduce total cost of ownership (TCO), increase return on investment (ROI), enable mobile access to resources, achieve COOP/DR goals, increase workforce productivity and efficiency, optimize/lower IT operational expenditures, improve citizen service delivery.

**Hardware cost and maintenance:**

- What is your agency’s desktop PC acquisition cost?
- What is your agency’s mobile device acquisition cost?
- How often does your agency refresh desktop PCs?
- How often does your agency refresh mobile devices?
Desktop management:

- What is the total time required to deploy (or refresh) a desktop PC?
- How many desktops/endpoints can an administrator deploy simultaneously?
- What is the total time required to reimage a desktop PC?
- What is the average number of desktop workloads per administrator?
- How long does it take to onboard a new user?
- How many hours does it take IT to develop, test, and deploy an image? How often are images refreshed?
- What are the average operational expenses per end user per year?
- Are workloads regularly evaluated to identify areas for virtualization?

Application management:

- How do you deploy applications today?
- How many applications do you support?
- What is the average application deployment effort/time?
- How do you control access to Software-as-a-Service (SaaS) applications?
- What is the total average time required to test a single application?
- How many operating system (OS) or application patches are deployed annually?
- What is the total time required for a desktop administrator to test and deploy a patch?
- What percentage of applications are packaged?
- What is the average IT time required for packaging an application?
- Are applications actively monitored, supported, and managed to ensure they meet performance requirements?
• What is your agency’s application management strategy?

**Mobility management:**

• What percentage of the agency (or department) work remotely or are mobile workers?

• How are mobile devices used within the various agency departments?

• Which types of workflows could be improved or redesigned through field mobility?

• What quantifiable impact would better field efficiency, productivity, and connectivity have on the department?

• Which applications are critical to the field?

• How are field workers currently accessing data and files remotely? Do you expect the percentage of mobile workers to increase in the next 12 months?

• Do you plan on instituting a bring your own device (BYOD) program?

**Data security:**

• What is the annual cost of your agency’s current data protection solution?

• What is the average total number of security incidents or events, such as malware infections, data losses, denials of service (whether due to cyber-attack or unplanned downtime), and system compromises or breaches, that occur in your agency annually?

• On average, what is the total time required for IT to respond to and resolve an incident or event?

• How does your agency currently ensure that your systems and processes are in compliance with all applicable standards and regulations?

• How does your agency currently ensure that data is protected against breach or loss across all users, devices, and applications?
• How does your agency currently monitor desktops, mobile devices, apps, and data usage?

• What is the total time required annually to achieve, maintain, and audit compliance following a security update or new mandate?

✓ Continuity of operations (COOP):

• What percentage of endpoints does your agency back up?

• What is the annual cost of your agency’s data backup solution?

• What is the average cost of operational downtime per hour (known as single loss expectancy, or SLE)?

• What is the average number of operational downtime events (in total hours) that occur annually (known as the annualized rate of occurrence, or ARO)?

• What is the total annual cost of operational downtime (annualized loss expectancy, or ALE = SLE × ARO)?

• What is your agency’s process for restoring critical services in the event of an outage?

• Does your agency have a documented disaster recovery plan and process that has been communicated across the organization?

✓ Incident management and help desk support:

• How many user incidents does your agency’s IT department resolve annually?

• What percentage of user incidents are hardware related?

• What is the average resolution time per hardware-related incident?

• What percentage of user incidents are software related (for example, conflict, incompatibility, or upgrade issues)?

• What is the average resolution time per software-related incident?
• What is the average time required to resolve user ID, password, and login issues?

• What is the average lost productivity time (and average labor rate) for agency personnel due to user ID, password, and login issues? How are incidents prioritized according to urgency and impact?

 Governance

• What is the current process for identifying, categorizing, evaluating, and selecting IT projects and initiatives across departments and teams?

• How are resources and investments managed throughout the project life cycle?

• How are IT systems and solutions evaluated to determine if targeted benefits have been realized?

• How are emerging information technologies evaluated to determine applicability to operational processes?

• Does your agency have documented procedures for PC life cycles?

• Are IT goals and objectives aligned to the agency’s goals and objectives across key stakeholders, departments, and business units?

• How is end-user experience evaluated across the workforce?
A new generation of mobility is helping our business REIMAGINE what’s possible.

One CLOUD. Any APPLICATION. Any DEVICE.™

VMware’s mobility solutions — including AirWatch — are transforming businesses across a wide range of industries. By empowering employees, engaging customers, and enabling new business models, VMware is turning the potential of business mobility into a reality. It’s the brave new mobile cloud architecture built for innovation.

vmware airwatch

vmware.com/mobility
Access government resources anytime, anywhere, on any device with the digital workspace

Today’s government agencies are undergoing a seismic shift in computing capabilities, core processes, and personnel work styles. The digital workspace is a direct response to this new era of computing, transforming traditional workstations into secure, unified digital workspaces available across desktop and mobile environments.

- **Plan your digital workspace strategy** — align with agency goals and objectives, define measures of success and key performance indicators, and identify key initiatives

- **Develop a framework** — understand and plan for different user work styles, and match applications and form factors to workflow requirements

- **Architect the digital workspace** — bridge end-user computing technologies with legacy investments to transform desktop management, application delivery, and operational efficiency

- **Deploy a digital workspace** — get advice and best practices on implementing a digital workspace fit for your agency

**Samantha Reid** drives global government adoption of end-user computing solutions and evangelizes the power of the digital workspace within VMware’s Public Sector practice. In her spare time, she avoids discussing politics.

Go to Dummies.com for more!
WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.