VDC Research
Insights for the Connected World

2016 | Enterprise Mobility & Connected Devices

VDC | Case Study

Getting Government IT up to Mission Speed

Aging Systems are too Costly to Maintain and Lack in Functionality

Exclusive License to Distribute:

vmware

By Eric Klein, Director, VDC Research

VDC Research

Table of Contents

Table of Contents
Introduction
Legacy Applications Can't Keep up with Agency Needs
Reliant on Mobility
Government Service Expansion Opportunity
Exhibit 1: Service Expansion Opportunities in Government
Exhibit 2: Desired Capabilities to Reduce the Cost Structure and Complexity of Managing Mobile Deployment
CUSTOMER PROFILES:
U.S. Central Command (CENTCOM)
Mecklenburg County, North Carolina
Conclusion
About VMware
VDC Research
About the Author
About VDC Research

Introduction

Citizens are increasingly demanding greater responsiveness, efficiency, and accountability from their governments. The ubiquity of Internet access, proliferation of mobile devices, and the popularity of applications have made it critical for governments across the globe to improve their citizen services via mobile channels. In this vein, governments at all levels (federal, state, and local) must implement the appropriate technologies and infrastructure that will allow for the expansion of mobile capabilities. However, these organizations are simultaneously challenged to increase information security, comply with regulatory mandates, transition retiring workers and cut IT costs—while also increasing operational efficiency.

This case study will highlight the opportunity for mobile and cloud technologies in the Public Sector–specifically for state, local and federal government agencies where secure mobile application access can offer key productivity gains. The deployment scenarios for mobile solutions in the government sector are diverse, as many government organizations have extensive field workforces, particularly in agencies where logistics, delivery and field service operations are business and/or mission-critical. Not leveraging advances in mobile computing technologies to drive operational efficiencies for this critical segment of our nation's workforce will be unthinkable, going forward.

Legacy Applications Can't Keep up with Agency Needs

Several years have passed since the U.S. Government announced its "Cloud First" policy, but government agencies are still grappling with which type of cloud configuration to use and which data center technologies will help to simplify application delivery while offering robust security. Government agencies have begun to shift their strategies towards creating greater value from and enhancing their mobile applications. This means a fundamental shift towards more dynamic applications through greater contextual awareness and environmental sensing and measurement capabilities. To accomplish this, internal development teams are experimenting with new platforms and tools to gain efficiencies as they create new backend services, connect to existing services, and create custom front ends for services. Ultimately, government entities will be tasked with identifying the appropriate mobile use cases, as they tackle migration and integration with various backend systems and systems of records.

The U.S. Government formally established the role for a Federal CIO in 2003, with the passage of the E-Government Act of 2002. The current Federal CIO is charged with establishing a government-wide enterprise architecture that ensures system interoperability, information-sharing, and effective information security and privacy controls across the Federal Government. The job is as massive as it is critical, as the need to modernize legacy systems has been a perennial problem. Since 2010, the amount of spending on the operation and maintenance of our federal government's legacy systems has increased by about $5 billion (approximately 6% of the $80B IT budget), while the amount slotted for investing in developing new systems has declined by more than

$7 billion; to make matters worse, many state, local and federal agencies have yet to formalize a strategy to modernize their infrastructure and applications. Modernizing and transforming these systems will require more than updating core infrastructure components—leveraging the cloud to streamline and revolutionize service delivery will be the way forward, and will only be possible through a shift in culture.

This is not a public sector problem alone; VDC's data shows that CIOs across industries found that legacy applications and networks are key areas of concern, with the potential to impede new technology adoption. As agency IT needs become more complex due to an influx of devices and data, agencies must get a handle on legacy systems and maintenance costs.

Reliance on Mobility

The impact consumerization has had in government has been just as visible as in the private sector. Government agencies, like businesses, are leveraging the convergence of cloud, mobile and social technologies to increase efficiencies and improve service delivery. Increased mobile device usage will make responding to the transformative forces of mobile, social, cloud, and big data critical moving forward—but it won't necessarily be easy. Without the appropriate security controls and established policies, government employee use of personal devices can have unintended consequences. Recently, visible and high profile cases have emerged, such as former Secretary of State Hillary Clinton using her personal phone and email server for government business; scenarios such as this highlight the prevalence of employees accessing government resources on unmanaged personal devices, as well as the problems inherent in doing so when federal data is involved.

> *"Any of the sort of back office things that are common to many different agencies, I think that's where industry can take itself to build capabilities that frankly I don't want to have to build. I want our guys to focus on tactical mission stuff, not HR or financial stuff."*
> *Kevin Tunks*
> *Mobile Strategy Lead*
> *Federal Bureau of Investigations*

Directives from government agencies to leverage mobile technologies to promote and support communication, collaboration and social connections to improve service delivery to constituents continue to increase—these programs support a variety of applications from mobile payments, to incident documentation and informational services. Government agencies are looking to leverage mobile services to not only appear more progressive, but to significantly increase the effectiveness in their communication and interactions with the public. Mobile opportunities in the government sector are diverse. Large U.S. Government agencies such as the Federal Emergency Management Agency (FEMA), the Environmental Protection Agency (EPA) and the Department of Transportation (DOT) rely heavily on mobile solutions to improve service delivery, workplace safety and field operations efficiency.

The ability to quickly access and respond to information is critical to effectively running any government agency—mobile technologies have become crucial, as many of the workflows require the ability to access and act

on real-time data. Securing and supporting these workflows and applications is challenging amid the rapid pace of change and innovation and considering the myriad mobile form factor, OS, and I/O options available. For these reasons, VDC urges government CIOs and IT executives to explore and experiment with solutions that have been purpose built to enable government agencies to take advantage of the heterogeneous computing platforms that their workforce typically carries.

To date, the lion's share of mobile IT infrastructure investments have been in enterprise mobility management (EMM) suites; however, there are other end-user computing innovations which can reduce IT support needs—via virtual desktops and hosted applications—extending the life of aging desktop deployments, while also offering new service delivery opportunities and maintaining Continuity of Operations (COOP). Providing anytime, anywhere access to desktops and applications directly to key personnel in the field presents a massive opportunity—not only for the workforce productivity and multiplier opportunities, but also for the ability to provide the applicable segments of the remote workforce with key mobile transactional capabilities, such as: scan-based delivery confirmation, mobile point-of-sale, signature capture, and the ability to time stamp transactions with an audit trail. Most importantly, the risk of data leakage can be greatly reduced because information is stored in the data center or cloud, rather than locally on the employee's mobile device.

Government Service Expansion Opportunity

Business software and applications are becoming increasingly distributed within government, and the number of users needing to access information from outside organizational boundaries is expanding. For this reason, implementing security with mobile and cloud-based access in mind will be a requirement for any deployment; role-based single sign-on technology can extend across all in-house and external applications and platforms and enable granular security and compliance policies.

Technological innovation has cemented mobile's crucial role in government deployment environments, thus further complicating the job of IT professionals attempting to manage endpoints, which continue to increase in both quantity and complexity. Given these parameters, government IT departments have quickly found they are working with a moving target which requires a broad range of measures, including identity management, application distribution, device management, and data security. These requirements impact the agency's IT organization and deployment architecture(s). Due to the multilayered nature of mobile platforms, security, compliance or management cannot be achieved by finding one ideal hardware configuration or relying on one type of communications network or vendor. In a dynamic market, operating systems, applications, devices, and networks have all been impacting the endpoint management landscape. Delivering critical IT services across heterogeneous devices to internal end users has become more complicated over the last few years—smart vendors have evolved to enhance their value play from a technology perspective by investing heavily in R&D, and by embracing open standards so they can leverage the investment of a whole industry.

Those governments embracing mobility are moving past basic mobile device management (MDM) and beginning to integrate content management systems and custom applications for employee collaboration and service innovation. The availability of mobile solutions has caused work styles to change as well: employees want or need to work at any time or any location, with data that's accessible from the company network, the Web, or the cloud. The "customers" of a government can be divided into four main categories: citizens, businesses, government (employees) and other government agencies/organizations. For government agencies, this impact is broad, as providing improved services are requisite going forward. Exhibit 1 details the scenarios and efficiency gains that are available through service modernization.

Given the portable nature of mobile devices, government agencies must have the ability to remotely lock down and wipe devices. VDC's research shows that lost or stolen devices easily rank as the No. 1 key threat to mobile IT security. However, the risks inherent in enterprise mobility extend well beyond device loss. Educating employees is critical to minimizing threats to an IT infrastructure; typical users have neither the necessary understanding of the available security mechanisms nor the ability to properly utilize the appropriate protection mechanisms to their (and their agency's) full benefit. Unfortunately, the continued proliferation of smartphones and tablet computers will continue to expose networks and information to unprecedented risk—this makes expediting efforts to harden their mobile security posture and infrastructure a key priority for government deployment environments.

Exhibit 1: Service Expansion Opportunities in Government

Technology Brings Government Services Expansion Opportunity			
G2C	**G2B**	**G2E**	**G2G**
• Convenience • Ease of access to information • Increased efficiency • Improved customer service / service delivery • Cost reduction • Reduced bureaucracy	• Convenience • Ease of access to information • Increased efficiency • Cost reduction • Reduced bureaucracy	• Improved bureaucracy • Increased efficiency • Reduced administrative costs	• Convenient access to employment related information/services • Integrated human resources • Reduced administrative costs • Shared services
• Improved democracy • Improved perceptions of government	• Improved manpower efficiency • Improved transparency / accountability • Reduced corruption	• Improved employee satisfaction / morale • Improved employee retention	

The mobile enablement opportunity in Government to Citizen (G2C) remains centered around field mobility. An essential element of all successful field mobility solutions is to support real-time decision making in the field in a scalable fashion. Bottom line, next-generation mobility solutions have evolved beyond just task optimization and integrating more advanced capabilities that provide an agency with the ability to drive new revenue and to evolve the service operation from a cost center to a profit center—agencies that are equipping their workers with real-time access to mission-critical applications and data are going to be best positioned to mobilize quickly, improve first response and advance the agency mission.

Government to Employee (G2E) technology deployments are a prime modernization candidate. Mobility and desktop transformation can improve productivity, streamline IT management and enhance work/life balance via teleworking. Telework is a cornerstone and critical response strategy of continuity plans for many government agencies; unfortunately, current IT infrastructures are not capable of supporting large-scale teleworking. New innovations in IT service delivery bring the flexibility to successfully deploy applications and content at scale for all use cases, while balancing security, privacy and usability. These types of capabilities are significant, as they will help to streamline and speed up deployments, while reducing the amount of training time required for new users to become productive. Solutions that feature virtual desktop infrastructure technology that tightly integrates network access control and sophisticated enterprise mobility management functions that extend security to modern mobile platforms are a logical path forward for many deployment scenarios in the government sector. Technology vendors such as VMware have optimized their government solutions to meet stringent security standards while minimizing the risk of data leakage through granular compliance policies that cover the variance in security postures based on employees roles.

The opportunity for enhanced collaboration in Government to Government (G2G) scenarios is also notable. Many state and local governments are forging ahead with initiatives to consolidate IT assets and adopt shared services in order to reduce complex operating environments, cut costs and streamline services. Many government CIOs will need assistance in making the cultural adjustments that will be necessary, not just with managing services, but also with transitioning their agencies to the new services model and evolving their internal IT organizations into a more strategic role within government. By improving IT service delivery and addressing outdated technology issues agencies have an opportunity to:

Improve Delivery of Services: Define standardized configurations for provisioning infrastructure resources to enable repeatable and reusable IT services in private cloud and data center automation. Self-service capabilities will also reduce operating costs for time-consuming tasks such as password resets, account unlocks, and resource provisioning while reducing IT service desk queues.

Enhance Information Sharing: Eliminate internal barriers to accessing cross-agency information, by reducing technical complexity and improving data sharing between agencies and offices to meet business missions.

Encourage Greater Efficiency: Streamline operations and provide a better return on investment on technology expenditures, to support cost savings across the agency and to funnel cost savings into new IT programs and offerings.

Mission Critical Security

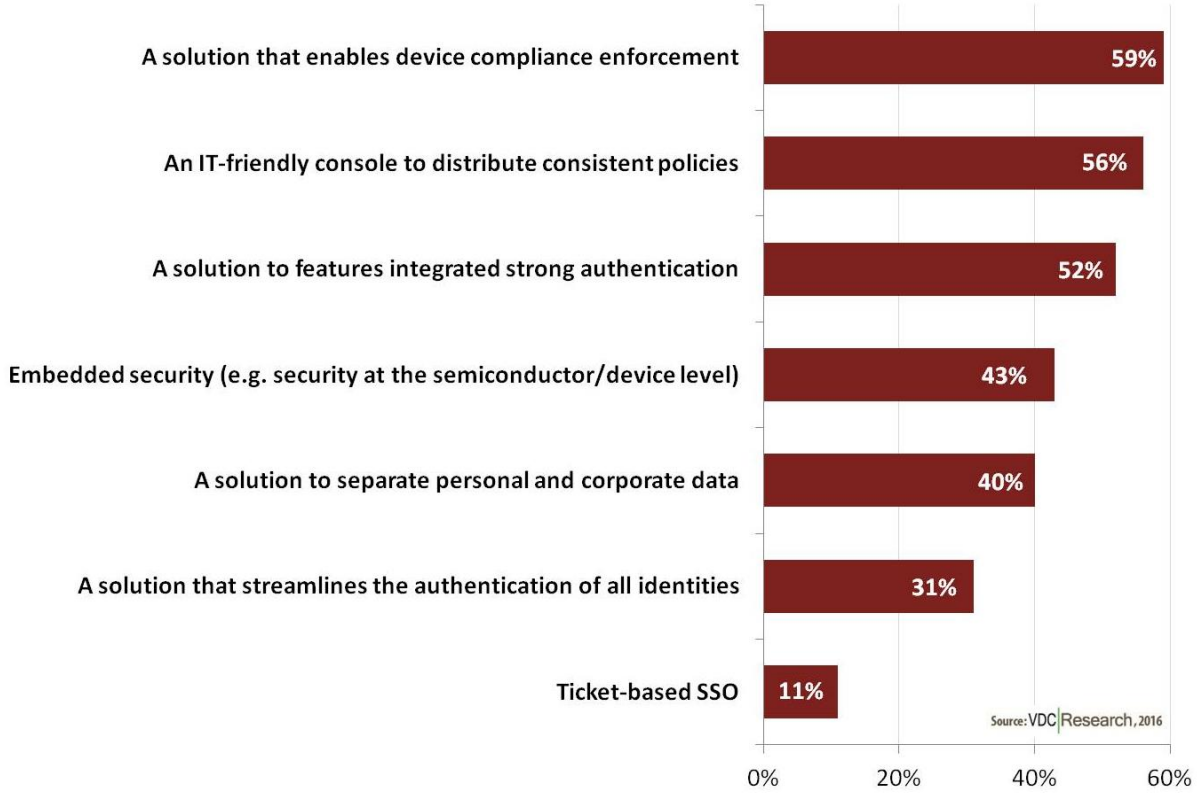
The security landscape is in a state of constant change. Government CIOs must constantly assess the best ways to secure and manage a multitude of mobile devices on diverse platforms. Changing work styles increase employees' desire or need to work at any time, from any location, with data that is accessible from the agency

network, the Web, or the cloud. Mobility initiatives require a broad range of protective measures, depending on the agency's security posture. Due to the multilayered security dynamics of mobile platforms, neither an ideal hardware configuration nor one type of communications network can reliably catch all threats and assure security. Operating systems, applications, devices, and networks all affect security in a dynamic market. Investing in IT staff with mobile-first expertise that is specific to security is important, as is implementing the appropriate infrastructure to enable secure remote access to pre-existing data stores and application platforms.

Context-aware detection and data loss prevention capabilities are also increasingly important. Organizations find that they require secure access and authentication to a wider range of back-end services from multiple mobile applications/platforms. Exhibit 2 shows the most desired capabilities government organizations are evaluating to reduce the cost structure of their mobile deployment(s).

Exhibit 2:

Desired Capabilities to Reduce the Costs and Complexities of Managing Mobile Deployments



Highly regulated industries must ensure that their pre-existing identity and access management solutions are able to transition into the mobile domain. However, even the largest organizations in these vertical markets lack the infrastructure for implementing mobile initiatives in a secure manner. Specifically, VDC's research found that only about half (52%) of companies have application controls as a part of their BYOD (bring your own device) program. These firms, often burdened by disjointed combinations of legacy software, struggle to incorporate

mobile applications in a constantly evolving mobile landscape that remains heavily fragmented. For this reason, understanding how to manage the mobile application lifecycle is crucial to achieving functional enterprise applications. To best prepare for the ongoing mobile shift, organizations should leverage the traditional software development lifecycle (SDLC) capabilities they have in place.

CUSTOMER SUCCESS PROFILE: US Central Command (CENTCOM)

FAST FACTS:

U.S. Central Command is one of ten unified combatant commands in the US military, with responsibility in the Middle East, North Africa, and Central Asia (including Afghanistan and Iraq)

CHALLENGES:

- Replace existing desktop environment with secure, virtualized solution
- Decrease time and labor required to implement new desktop images
- Replace desktop and server hardware, which was reaching end-of-life

SOLUTION:

- Upgrade desktop virtualization platform to VMware's Horizon solution
- Upgrade desktop hardware with EVGA PCoIP Zero Clients
- Upgrade servers to Dell PowerEdge M610 Blades
- Implement EMC Symmetrix DMX-4 systems for storage
- Upgrade desktop operating system from Windows XP to Windows 7
- Use VMware's Professional Services Organization (PSO) to automate user logins and support more effective load-balancing within VMware Horizon
- Work with EVGA to add functionality to its zero client hardware

CENTCOM's deployment of VMware's Horizon desktop virtualization solution was successfully adopted and the organization continues to roll out new desktops, having deployed more than 10,000 over time. The new environment makes more efficient use of resources by requiring less Storage Area Network (SAN) space, saving as much as $160 million in hardware costs. The VMware solution also allowed CENTCOM to standardize desktop deployments for about 60 percent of its users, which makes it easier for IT to manage the environment and improves security.

In addition, the new environment allows new desktop images to be deployed in just 8 hours compared to the old system's one week per network. This improved efficiency enables CENTCOM to reallocate IT technicians to areas that need more support. It has also made it possible for users to request new applications and have the new software within minutes, instead of 3-5 weeks as on the old platform.

Another improvement to the user experience is that users can log in and view their desktops in 30-45 seconds. This increase in availability combined with the integrated virtual 3D graphics card allows users to respond in real-time to military situations. VMware's Horizon solution is robust enough to deliver 100 percent uptime which CENTCOM requires for its mission.

CUSTOMER SUCCESS PROFILE: Mecklenburg County, North Carolina

FAST FACTS:

Most populous county in North Carolina with more than one million citizens who live in and around the city of Charlotte

CHALLENGES:

- Improve the reach and availability of services throughout the county
- Improve protection of citizen data that county employees collect
- Increase security of county employees working in the field
- Meet compliance requirements for Health Insurance Portability and Accountability Act (HIPAA), Personal Health Information (PHI), and Personally Identifiable Information (PII)
- Enable county employees to access data and applications from anywhere on tablets and mobile devices
- Achieve “One Person, One Device” initiative goals and reduce computer replacement equipment purchases (CREP)

SOLUTION:

- VMware Horizon desktop virtualization
- Implement VMware Horizon on Cisco Blade Servers for server virtualization beginning with 100-user pilot
- Use non-persistent Dell Latitude desktops with Horizon Persona Management for user profiles
- Support mobile deployment with AirWatch Enterprise Mobility Management (EMM) platform
- Simplify user profile migration to different devices
- Use VMware ThinApp for application virtualization

The Mecklenburg technical services team deployed more than 3,000 AirWatch-managed devices to the county workforce, which have allowed employees to stay securely connected to information while on the job. Employee email is integrated into AirWatch, and the devices are tracked and inventoried through AirWatch as well.

Youth and Family Services (YFS) social workers have experienced especially large improvements in productivity. The mobile devices allow social workers to eliminate paper files along with the necessity of constantly returning to the office to print material. YFS social workers can now access and create files from anywhere, as well as video chat with supervisors and fax documents in the field. The lack of bulky paper files has also improved security, making the employees less of a target in bad areas of town. The devices are estimated to save YFS social workers about two hours per day. The Parks and Recreation department has also benefitted from the new investment, using mobile point-of-sale systems for on-site sales and AirWatch Content Locker for event planning.

The success of the “One Person, One Device” initiative has resulted in cost avoidance of more than $3.2 million for the county. Productivity improvements account for $1.2 million, and reductions in CREP saves the county approximately $1,000 per user, per year. Devices can be configured in less than 5 minutes and deliver the same experience for the county’s nearly 6,000 employees. Mecklenburg County received the 2013 Digital Government Achievement for the initiative and plans to expand its deployment.

Conclusion

Our research shows that the average company spends the majority of its IT budget maintaining legacy applications that fail to meet the changing competitive needs of the business. Government organizations are no different. However, slowly but surely, agencies are beginning to realize that maintaining their applications and associated infrastructure elements in a legacy environment consumes a disproportionate percentage of their IT budget. As the opportunity to benefit from consumer-oriented mobile devices from a business context becomes more pronounced in government deployments, it will be important to reconsider how to optimize the delivery of IT services as new mobile-first work patterns continue to emerge. While the pace of mobile enablement has frustrated some government workers, progressive agencies that leverage modern solutions will be able to offer the quality of service and user experience that citizens and end users expect.

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.

About the Author

Eric Klein is a market research and consulting professional specializing in the design, analysis, and delivery of project-based research. Over the past 15 years, Eric has worked with a wide array of firms across a number of industries, leading quantitative and qualitative research in areas such as innovation in enterprise software, supply chain risk management, manufacturing operations/automation, and IT spending research. Eric has worked in a variety of market research and management roles, providing market data and competitive intelligence to Fortune 500 firms. His previous employers include: AMR Research, The Yankee Group, and Affiliated Computer Services (ACS). Eric holds a Bachelor of Science in Finance from Boston University.

About VDC Research

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.

For more information, contact us at info@vdcresearch.com.