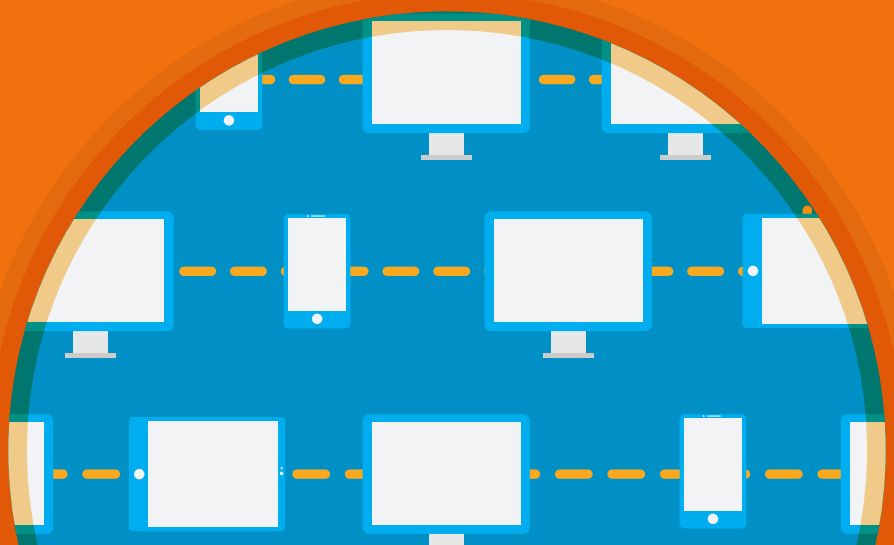
STRATEGIES FOR GOVERNMENT TO NAVIGATE THE DIGITAL FUTURE

INDUSTRY PERSPECTIVE

CITRIX®

Public Sector



EXECUTIVE SUMMARY

The digital transformation of government has begun. The major driving forces in this transformation are cloud, mobility, big data analytics, the Internet of Things – and respective security concerns. At the same time, these technologies shape the business of government. It's no longer the norm to stand in line at a government facility, waiting for a face-to-face interaction to complete a paper form before receiving a particular service. Today, citizens, contractors and employees can access and serve government from anywhere, anytime. Mobile apps and text messaging, web sites and automated email enable such access while ensuring private information is protected.

While agencies move some of their digital workloads to the cloud, they must also sustain some legacy systems and applications in government data centers. This new digital workspace offers dramatic improvements in productivity and mobility, but also presents challenges for IT and security professionals. Standardizing how applications are delivered to an increasingly mobile workforce simplifies the challenges presented when app suites can include legacy, client-server, Software-as-a-Service (SaaS) and mobile apps. In addition to app suite standardization, next generation networks are needed to assure both the availability and security of apps and data.

GovLoop sat down with Tom Simmons, Vice President for U.S. Public Sector at Citrix, an industry leader that securely delivers apps and data to an increasingly mobile workforce, to address how government should navigate the new digital landscape and leverage strategies including: Workspace-as-a-Service; virtual client computing; Virtual Desktop Infrastructure (VDI); Enterprise Mobility Management (EMM); Enterprise File Synch and Sharing (EFSS); and next generation networks both in the cloud and traditional data centers.

In this industry perspective, you'll learn what comprises government's digital transformation, the benefits of digital workspaces and next generation networks and how agencies can secure data and apps through cloud solutions.

THE DIGITAL IMPERATIVE

The explosion of information in the digital age presents a challenge to government to collect, analyze and disseminate content. Citizens have come to expect real-time access via the web to online applications and services on virtually everything including travel advisories, weather and national and local disasters.

Secure network access to these online resources is an important element of next generation networks that will assure government's role in today's digital world.

"Digital transformation will have the same dramatic impact on productivity and efficiency in government that it does in the private sector," Simmons said, "with an increased emphasis on security."

Government's access to the applications and data necessary to serve citizens presents a whole new set of challenges. The new digital workplace must address the proliferation of mobile and SaaS apps, new desktop operating systems and a continued reliance on legacy systems and applications developed by and for government. Securing the access and use of this wide variety of apps and data has led to unique paths and authentication methods for specific devices, locations and user types. The resulting complexity can be unmanageable as new devices and new work-flow processes are introduced.

That's why standardizing on an application delivery infrastructure and file synch and sharing can dramatically reduce that complexity. This will also help reduce costs while enhancing security.

Mobility continues to be a significant and growing requirement for digital government. Securing devices, data and user identity while allowing for personalization is a must for many organizations as they look to leverage a BYO (bring your own) device strategy.

Authenticating users internally is another major focus in the digital future. Government needs to provide employees access to the apps and data necessary to complete job functions while accommodating personal items like pictures, music, games and applications. The resulting positive impact of employee satisfaction and retention also reduces government's costs and increases flexibility without sacrificing security.

To fuel digital transformation, government should prioritize the following three strategies:

1. Adopt software-first next gen networks to ensure network agility in a software-first world.

2. Adopt digital workspaces as a new method of deploying end user computing resources.

3. Explore Enterprise Mobility Management and BYO adoption to help employees be more productive by focusing on secure access and productivity, in addition to device management.

ADOPTING SOFTWARE-FIRST NEXT GENERATION NETWORKS

In many government data centers today, hardware appliances perform a single function and are long overdue for updates. Software-defined networks offer the government cost savings, flexibility and agility as well as enhanced security capabilities. This is because network solutions are based on a "software-first" approach. Such approaches offer the benefits of hardware appliances as well as the flexibility to migrate the same functions across platforms both in the data center and in the cloud.

"We anticipate changes to standards and capabilities in platforms, form factors, and hypervisors, as well as increased reliance on cloud, orchestration and enterprise architectures. Such solutions are portable and provide the government the benefit of moving, re-purposing and re-using their investment in these network capabilities," Simmons said.

Security in next generation networks continues to be a driving factor. Government agencies can better protect their web infrastructure against cyberattacks like Distributed Denial of Services (DDoS), obtain network analytics for all mobile, web and desktop traffic and save costs by consolidating multiple remote access solutions. They can also better address insider threats with monitoring and alerting capabilities when network traffic or abnormal user activity is present.

Data center consolidation and the move to cloud services also increases the demand on networks to ensure a reliable and agile connection from branch offices to core applications and services. Agencies are beginning to apply Software Defined Networks (SDN) to provide measurable value in the Wide Area Network (WAN). WAN is a computer network that extends over a large geographical distance and is often established with leased telecommunication circuits. As part of WAN, the next gen of networking promotes the use of software-defined networking (SDN). SDN has been influencing new network architectures by providing greater transparency and simplified management.

With a software-defined WAN (SD-WAN), agencies can reduce deployment costs by reducing bandwidth costs. SD-WAN allows the use of multiple WAN connections from one network to a variety of internet links such as DSL, fiber, cable, satellite and 4G/5G connections. In other words, SD-WAN allows for increased remote access to a network while also decreasing general WAN costs.

Some other tangible benefits of SD-WAN as part of next gen networks include:

- Maintain high performance for mission critical apps to prevent disruption and seamlessly deliver applications, video, secure connectivity and virtualized desktop services.
- Simplify network management and configuration to reduce time to add new services and minimize troubleshooting.
- Prioritize mission-critical applications to avoid costly network capacity growth, especially during peak periods.

By adopting software-first next gen networks to secure delivery of apps and data, government agencies can modernize IT infrastructure providing easier management, increased security and increased agility.

THE DIGITAL WORK-PLACE

The concept of work is undergoing a major shift from a physical workplace to an aggregated workspace, where experience, flexibility, identity and security are central. The workplace of the digital future allows workers to be more productive when they have easy access and a seamless user experience across all devices and platforms. That's why securing the world's data requires a new holistic approach that safely delivers and manages all apps, data, devices and networks from a single integrated platform.

Employees need to access government's critical IT resources remotely, for traveling, remote and teleworking. The traditional approaches of issuing every employee and contractor a computer, locking down the image and configuration, encrypting everything and limiting remote access to a few are no longer viable options.

As part of the digital transformation, everyone will want to move to a digital workspace. Components of a digital workspace include:

APP VIRTUALIZATION AND VIRTUAL DESKTOP INFRASTRUCTURE (VDI): VDI provides employees with access to their familiar operating systems, like Windows, from any device. With app virtualization and VDI, government can give employees the freedom to work from home or anywhere, increase productivity and mobility, all while cutting IT costs.

> **"The workplace of the future is a dynamic digital environment in which a user can access the applications and data necessary to be productive by clicking on a button."**
>
> *Tom Simmons, Vice President for U.S. Public Sector at Citrix*

ENTERPRISE MOBILITY MANAGEMENT (EMM): EMM is an all-encompassing approach to securing and enabling employee use of devices like smartphones and tablets. EMM enables governments to increase productivity and security. Additionally, agencies can safely implement BYO by providing end-to-end enterprise-grade mobile device security for smartphones, tablets, laptops and desktops.

ENTERPRISE FILE SYNC AND SHARING (EFSS): EFSS facilitates access, sync and file-sharing from any location and any device to ease collaboration and improve productivity. With EFSS, agencies can also determine how sensitive data is stored, accessed and shared, with security features and policies that meet their enterprise compliance requirements.

"The workplace of the future is a dynamic digital environment in which a user can access the applications and data necessary to be productive by clicking on a button," Simmons said. "And that button looks and acts the same regardless of the user's device or location. IT has complete visibility into what that user is doing with the government's applications and data."

By securing at the edge, government can use strong authentication that includes Common Access Cards (CAC) or Personal Identity Verification (PIV). Such measures ensure that only authorized users have access to a menu of applications and data resources either in the government data center or in their cloud infrastructure.

By focusing on data and applications, government can re-architect their approaches to employee mobility while ensuring security. Users are presented with an app store interface as well as a set of applications that the government administrator establishes based on role, location and/or access scenario. The store front also aggregates applications that include virtualized legacy apps, client server apps, SaaS and web apps and offers IT the visibility and control over who is accessing what from a single centralized environment.

Multiple versions of desktops can be afforded based on user needs and application compatibilities. If some legacy applications are not compatible with the newest desktop operating system, government can use other types of devices or BYO strategies. With next generation endpoint security, government employees can still use a single interface to access their workplaces, regardless of device, be it Kiosks, smartphones, tablets, or home computers. This eliminates the need for unique paths, authentication and access and the associated complexity and cost of each.

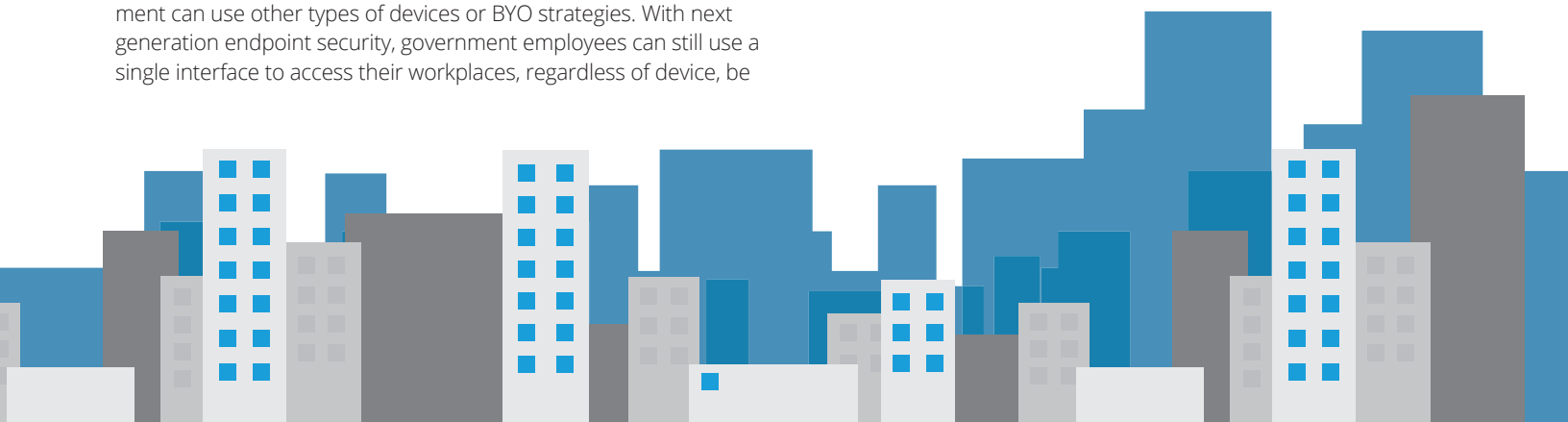
Critical to the digital workplace is also the ability to access and sync files. Enterprise file synch and sharing solutions provide users the ability to access and share documents and data files, databases and multimedia across all of their devices. This capability leverages files in government data stores in data centers, the cloud and on the end-points.

"Mobility is no longer just secure email on a portable device. Government enterprise mobility must address devices, applications (email being only one of those) and data," Simmons said. "Certifying specific devices and restricting users to a subset of the solutions is expensive, limiting and certainly not necessary with today's technology."

Using new cloud technology, agencies can deploy and deliver digital workspace components using a Workspace-as-a-Service (WaaS) model. WaaS can help government dramatically simplify infrastructure management by empowering IT staff to:

- Configure and deliver workspaces to uniquely meet the needs of given functions or roles
- Integrate apps and data across any cloud, platform or device
- Set and monitor access, security and data across an entire infrastructure
- Monitor and manage all corporate apps, data and networks through a unified control console

The digital government workplace of the future will be a cloud-delivered conduit to individual productivity.



CASE STUDY: ALCOHOL AND TOBACCO TAX AND TRADE BUREAU

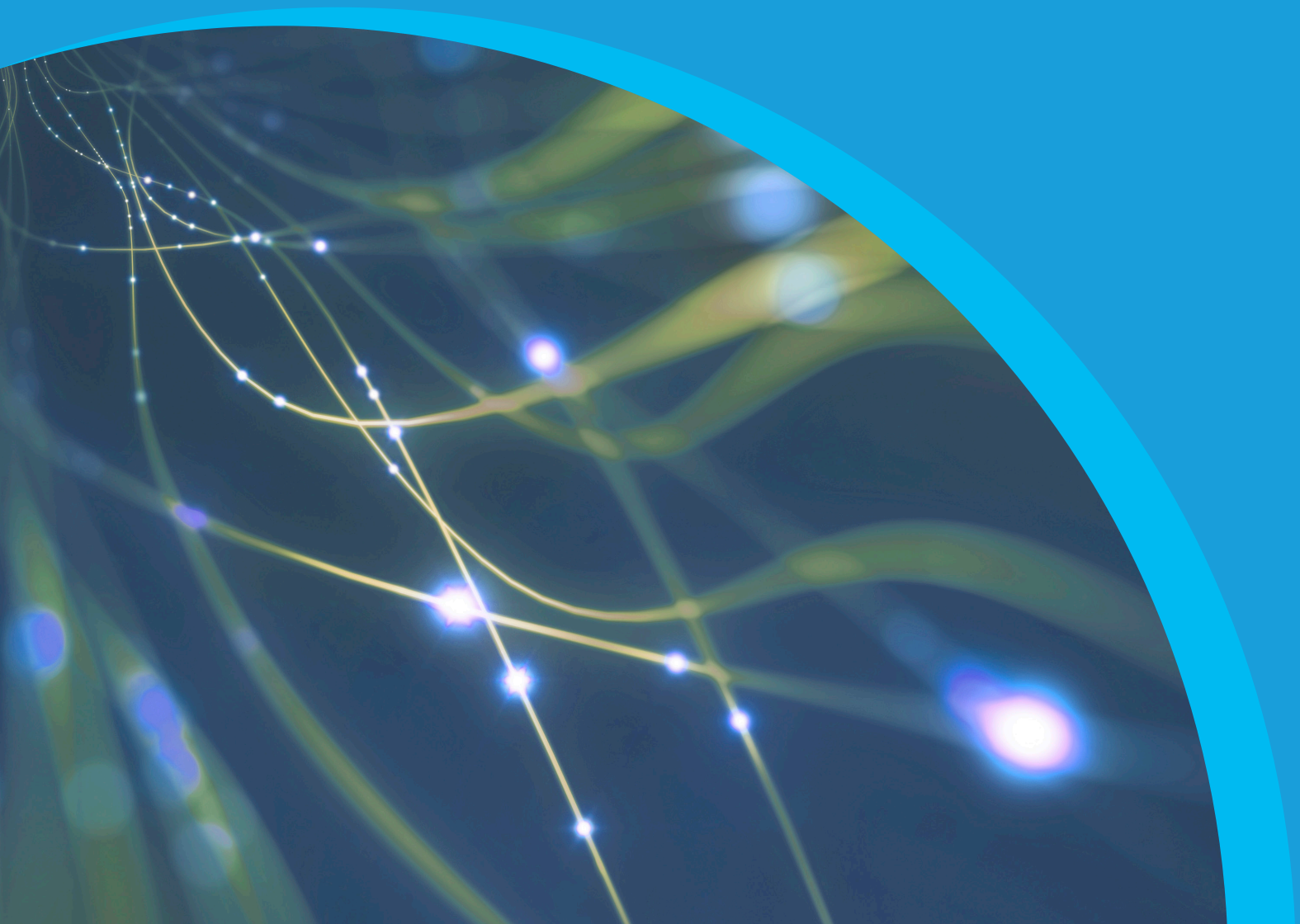
Agencies stand to gain a number of benefits from the digital transformation by leveraging the digital workplace and BYO. In addition to enhanced mobility and flexibility, agencies can also save on costs by avoiding having to purchase extra equipment and hardware as well as on-premise storage for data.

In 2013, the Alcohol and Tobacco Tax and Trade Bureau (TTB) developed an initiative to slash the expense, time and effort required to refresh its desktop and laptop computers. TTB has a dispersed workforce, with 80 percent of its staff regularly teleworking. The desktop and laptop refresh cost about $2 million every few years and disrupted work for general employees and those in the IT department for months on end.

Over time, the bureau opted to centralize all client computing power and applications, user data and user settings and allow access to TTB resources via thin-client computing devices (lightweight computers that are built for remote access to a server). In light of limited funding for virtual desktop implementation, TTB examined its existing hardware, software and technical expertise to determine the path that would help meet its objectives of providing central access to all IT resources while realizing cost savings.

With approximately 80 percent of its Windows servers and 20 percent of its Sun Solaris servers virtualized, the bureau was confident that a virtual desktop infrastructure could be built without physical servers. Due to TTB's extensive telework program, its priority was to support remote workers with a robust remote access capability. TTB used Citrix to create thin-client devices from almost any device and power its BYO computing initiatives.

The bureau was able to save $1.2 million by applying a virtual desktop approach. Today, about 70 percent of TTB's users access its resources through thin devices provided by the bureau as well as employees' own personal devices. Now, any user configuration that works is allowed, giving staff enhanced productivity and unprecedented freedom to work from anywhere.



CONCLUSION

Government agencies are implementing next generation networks to support digital workplaces and enhanced online services as part of the digital transformation. Citrix is helping agencies transform with solutions that enable employees and contractors to be more productive, and give them more flexibility, while providing IT with the visibility and tools to manage. Ultimately, the government digital transformation is about providing an outstanding user experience and protection against potential cyberthreats.

ABOUT CITRIX

Citrix (NASDAQ:CTXS) aims to power a world where people, organizations and things are securely connected and accessible to make the extraordinary possible. Its technology makes the world's apps and data secure and easy to access, empowering people to work anywhere and at any time. Citrix provides a complete and integrated portfolio of Workspace-as-a-Service, application delivery, virtualization, mobility, network delivery and file sharing solutions that enables IT to ensure critical systems are securely available to users via the cloud or on-premise and across any device or platform. With annual revenue in 2015 of $3.28 billion, Citrix solutions are in use by more than 400,000 organizations and over 100 million users globally. Learn more at www.citrix.com/government.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

CITRIX®

Public Sector

govloop

1152 15th St. NW, Suite 800
Washington, DC 20005
P: (202) 407-7421 | F: (202) 407-7501
www.govloop.com | @govloop