A GCOM White Paper

Supporting Remote Workers

gcom
EXPERIENCE.INNOVATION.

vmware®

VMware
Master Services
Competency
DIGITAL WORKSPACE

Achievement of advanced technical certifications, proof of high-level service capability and expertise validated by customers.

Table of Contents

Introduction: The Growing Need to Support Remote Workers

The COVID-19 pandemic has accelerated a trend that was already in motion: Empowering employees with the flexibility to work remotely, including from home. This trend is expected to continue long after the pandemic is extinguished, driven by a number of factors including: Environmental benefits of reducing commutes; Increased productivity and personal satisfaction employees gain working from home; and Affordability of living away from major urban centers.

Change is in the air. Consider:

- "As COVID-19 forces government organizations to embrace virtual work, leaders must reimagine how they engage and collaborate with their colleagues. … Since the world is unlikely to ever return completely to its pre-pandemic ways, the public sector should seek to rapidly change how it works, including improving its agility and productivity, in lasting ways." - McKinsey & Company
- "Local governments and municipalities across the U.S. are facing an unprecedented need to shift employees to remote work due to the spread of COVID-19. … This is uncharted territory for most entities across the country, and many are now looking for the best solutions and practices on how to continue business as usual as offices transition to remote work for employees." - American City and County Magazine
- Headline: "Who Needs Cities When We All Work from Home?" - The Wall Street Journal
- Headline: "What if You Don't Want to Go Back to the Office?" - The New York Times

Governments, along with private sector business, prior to the pandemic were already facing the need to accommodate a growing generation of tech-savvy employees—who expect to remain fully connected when away from the office, either traveling or working in the field. Similarly, the citizens they serve increasingly expect to see the ease of access—including from mobile devices—that they already make use of when interacting with employers, banking and online shopping.

Soaring Demands for Remote Support

> **"Government IT organizations must move beyond just supporting remote workers. They must create a digital workspace"**

Demands instantly ratcheted up with the advent of the pandemic. Within a matter of weeks, supporting remote workers became an emergency priority. Few expect this movement toward remote work to lessen. As pandemic pressures ease, many expect environmental, cost-of-living and professional personal preference forces to continue adding momentum to the move toward remote working. American City and County Magazine notes: "Countless cities across the country are doing everything possible to ensure public meetings are limited and allow employees to work remotely." Gallup recently released a report titled U.S. "Workers Discovering Affinity for Remote Work" about their poll finding that more than 60% of American adults working from home would prefer to continue doing so "as much as possible" after the pandemic.

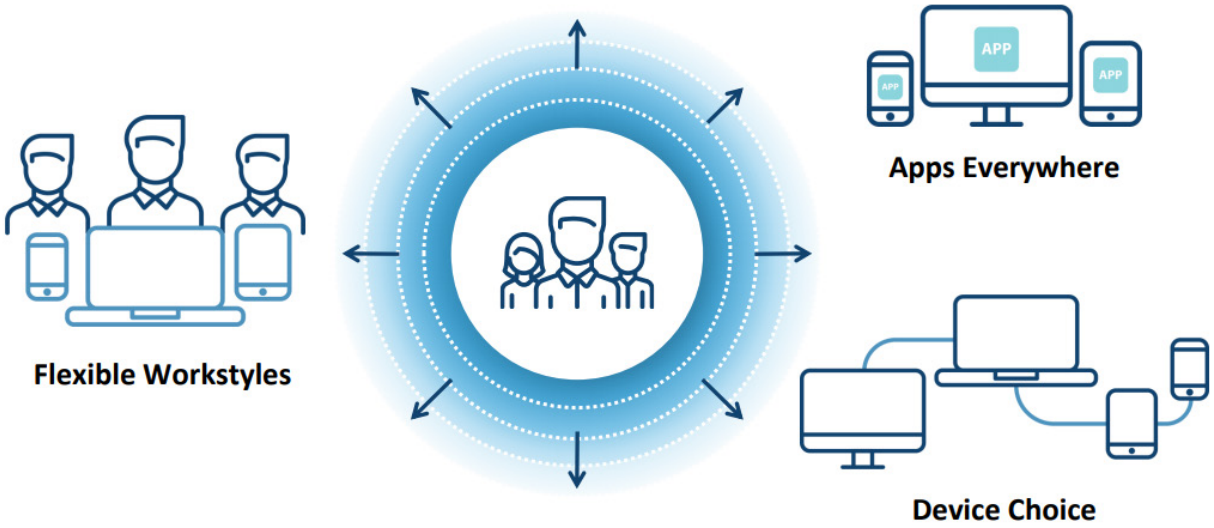
All of this poses great challenges to government IT organizations, as supporting remote workers requires providing highly secure access to backend applications and databases—while providing a user-friendly front end that can be accessed across not just desktops and laptops, but all forms of mobile devices.

Needed: A Digital Workspace

Government IT organizations must move beyond just supporting remote workers. They must create a digital workspace. They must enable seamless integration with backend systems—while satisfying the need for tighter project timelines.

And the digital workspace once created, must be maintained and continually updated and secured. After project completion, the real work has just begun. Ongoing administrative and security demands require extreme expertise and dedication of 24x7 expertise, which can often be best supplied by a U.S.-based managed services provider.

This white paper explores the challenges that must be met to support remote workers, and the expertise, processes, and technologies that GCOM incorporates to help government organizations succeed.



EMPLOYEE PRODUCTIVITY DEMANDS HAVE DISSOLVED THE PERIMETER

Remote worker productivity requires seamless integration beyond the traditional IT perimeters.

The Challenge of Creating a Seamless & Secure Digital Workspace

The technology exists to create robust and secure digital workspaces, but knowledge gaps can prove to be time-consuming, project-delaying barriers. Government agencies typically have highly skilled IT personnel, but they may lack knowledge in some of the key areas required for digital workplace integration and deployment.

Successful remote worker digital workspace projects require the right combination of knowledge, talent, tools and project management. The challenge goes far beyond simply supporting remote workers. Success depends upon creating a comprehensive, purpose-built solution with a human-centered design.

The challenge includes assembling expertise in areas such as application virtualization, cloud, identity, application integration, security and mobility. It can be time-consuming to find such talent, and expensive to hire. Yet these resources are required, whether for departmental or large agency-wide adoptions.

Additionally, once deployed, these same areas of special expertise are required on an on-going basis to maintain, secure, troubleshoot and evolve the solution. The lack on industry-leading security and compliance knowledge and practices increases risk of project failure, and the potential for exposed attack vectors. This is an area that requires ongoing strategy and performance management with continual skill updates.

While internal IT talent can—given the time and training—develop expertise in creating, securing, and maintaining digital workspaces, the research and training involved can lead to project delays. And the learning curve can distract IT workers from core functions and responsibilities.

The Four Key Competencies Required for Success

Government agencies around the world have been hurled into the task of equipping their workers with the ability to securely and efficiently work from home. Creating these solutions require a number of key competencies, including these foundational ones:

- **Identity & Access Management Expertise**
- **Application Virtualization Expertise**
- **Desktop Expertise**
- **Mobility Expertise**

> **Headline: "The Coronavirus Outbreak Has Become the World's Largest Work-From-Home Experiment"**
>
> **- Time Magazine**

Identity & Access Management Expertise

Ensuring identity needs to be at the top of the list for any remote working solution. In an article titled "Amid Disruption, Identity Access Takes Center Stage," RSA recently noted: "The rapid shift to remote work is also an opportunity for security leaders to examine a challenge that has been evolving since long before the current disruption became a headline: managing the risk of a dynamic workforce. … A growing base of users, applications, devices and data all over the world gives attackers more vulnerabilities to exploit."

While traditional solutions like VPNs and firewalls support the existing network/device centric security model, when it comes to remote working the paradigm change for IT is the need to adopt an identity-based security model. An identity-based security model is required so remote workers can access cloud-based software-as-a-service applications and services in addition to enterprise resources such as databases and line of business applications sitting behind agency firewalls.

Device-based identity and access management doesn't work in a remote worker scenario, as workers may log in from home on personally owned devices not centrally managed and controlled. Solutions can include multi-factor authentication and "zero trust" approaches of using multiple pillars of security and identity in granting least-privilege access to specific applications or databases—so a breach from one zone can't be used to access other areas of the network.

Agencies also need to address other areas including VPNs, encryption, virus protection, operating systems and application patching and updates. Agencies need to balance the need for granting access to essential line of business applications and data stores, while tightly administering granular role-based access.

In short, identity & access management, as well as security have long been areas for concern. The essential—yet rapid—move toward remote workers has intensified the challenge. Cybersecurity is based upon reducing and defending points of attack. Deep technical expertise is required to provisioning remote workers without expanding the cyber threatscape.

Application Virtualization Expertise

Government agencies that have supported remote workers in the field or while travelling, now face massive scalability issues. Application virtualization expertise is required in order to select the right architecture for a workload and how to balance end-user experience with infrastructure cost optimization. Application virtualization expertise helps guide creation of flexible deployment options that enhance nimbleness and user satisfaction. Supporting remote workers means applications will likely no longer be delivered based on specific desktop images. Instead, remote workers can be working on a spectrum of personal devices ranging from Android to Apple, to Windows, with a wide array of operating system versions for all. This all places a premium on strong yet flexible support for virtualized applications—including managing integration of directories and identity management to enable secure role-based data access, while strengthening security.

Desktop Expertise

The desktop should serve as the friendly secure virtual workplace. This is where the work gets done. This is a touch point of familiarity. The office is gone, but the screen is where the work has always been done.

The challenge is to make the desktop from home work just as seamlessly and intuitively and completely (and securely) as what workers had in the office. As noted above, this requires tight integration with backend resources, including with cloud-based resources and third-party data sources and applications. And there is also the question of whether desktops will be on the devices or virtual.

> "The challenge is to make the desktop from home work just as seamlessly and intuitively and completely (and securely) as what workers had in the office."

Desktop expertise is required to achieve all of this. Desktops, while simple to look at can be complex and extremely varied, even when working from what began as standardized images. Workers change settings to suit their working styles, they add applications to meet their work needs and the use of home devices can introduce complexities of OS and application versions and patches, networking issues, as well as hardware problems.

Careful analysis and planning are required to build out the support system needed to handle what will likely be an increase in not just volume but in complexity of problems.

Mobility Expertise

Mobility has been eagerly embraced by government workers—and the citizens they support. Even before the pandemic, agencies were working to meet the needs and expectations of a population that increasingly does on a smartphone what used to be done on a laptop or desktop computer.

Mobility expertise is required in crafting mobile solutions—whether line of business or public facing—that provide all of the functionality of conventional desktops, in a highly secure manner. Expertise is required in:

> "Mobility expertise is required in crafting mobile solutions—whether line of business or public facing—that provide all of the functionality of conventional desktops, in a highly secure manner."

- Designing mobile applications
- Integrating mobile devices with backend and third-party resources and services
- Enabling user-friendly interactions between citizens and agency services across mobile devices—including payments, and form submissions, where applicable
- Implementing profile-based unified endpoint management
- Authenticating identity and providing granular, role-based access to resources
- Offline continuity
- Securing all communication and resources against hackers who seek to use mobile endpoints as attack surfaces

All of this must be done for a wide range of mobile devices, including across multiple OS versions for Apple, Android and perhaps, embedded devices. Even if your agency has IT support for unified endpoint management for mobile devices, additional expertise is required for providing the same profiled-based management for remote desktops.

For all of the above, additional consideration may include licensing and capacity. Do you need to increase seats when moving from supporting road warriors to full agency staff? Will the VPN you've used in the past for road warriors have be able to support an entire workforce at home? Do you need to increase cloud provisioning, SaaS capacity or any other elements that could see increased usage from your expanded remote workforce?

Decisions made today can set a course that can be difficult to later alter, so it is essential to carefully consider options and make the best choices for today and into the future.

How GCOM Helps You Succeed

GCOM isn't your typical government IT provider. We combine the experience and resources of a large systems integrator with the agility and accessibility of a smaller firm. Much of the GCOM leadership team has been on the inside, so we understand how you work and the obstacles you may be facing. We stand out for our deep experience and innovative approach. When GCOM responds to an RFP, it's because we have a vision for what success looks like for you and we know how to help you achieve it.

We have built our reputation on delivering innovative, tailored technology solutions to state and local governments nationwide, with a focus on modernizing legacy IT systems in the public health, social services, public safety, licensing and permitting and cybersecurity markets. GCOM is the industry partner of choice in helping clients enhance operational performance by leveraging cutting-edge, scalable technology to facilitate systems integration while mitigating risk. GCOM's diverse team of experts brings the know-how to deliver both tactical and strategic solutions to the public sector's most critical challenges.

Part of our value proposition includes:

- **Experience.** Our team collectively brings decades of successful government experience to the table, so we're fluent in the language of state and local government. We're deeply familiar with state and local structures, so we can help clients answer their most pertinent questions — from securing employee buy-in for new technology, to navigating internal politics, to addressing nitty-gritty questions of procurement and funding. Simply put: We know you because we were you.
- **Domain Expertise.** Our wealth of domain expertise across HHS, Justice and Public Safety, Licensing and Regulations and more enables us to offer state and local governments a tailored approach to digital transformation. By recognizing the nuances of different agencies' technology challenges, we help bridge the gap between legacy systems and next-generation solutions.

- **Innovation.** GCOM is tech-forward and always ahead of the curve. We are building on our excellent track record to innovate leading-edge solutions for state and local governments.
- **Deep Partnerships.** We work extensively with third parties to create best-of-breed solutions for governments. Our deep partnership with VMware uniquely positions us to help empower remote workforces with a digital workspace experience that delivers access to any app on any device without compromising security.
- **In the Trenches.** We're not merely consultants who advise from the outside in — we're willing to get into the trenches with our clients. Our C-Suite executives sit in on client meetings to help them solve their challenges. That's why customers trust and keep coming back to us.
- **Future-Proofing Government.** We make systems built to last. We're not only solving the problems agencies have today — we're setting up a system built for an unknown future, with the countless unknown challenges that may arise. Too often, when agencies discover a problem, they've already lost critical time and resources. We're not in the business of playing catch-up — we provide future-proofing solutions for both today and tomorrow.

Proven Assessment Process: Our Digital Journey Framework

We know that it's not enough to simply understand state and local government in the abstract—every jurisdiction is unique. We know—through years of experience—that though agencies face similar challenges, no two challenges are ever the same.

This is why our engagement process begins by listening—sitting with you and your team exploring your unique needs. We call this assessment process our Digital Journey Framework and we use it to Identify exactly what your organization needs to succeed.

> "We call this assessment process our Digital Journey Framework, and we use it to Identify exactly what your organization needs to succeed."

During the Digital Journey Framework, we help assess where you currently are in regards to the four competencies of Identity, Application & Backend, Desktop, and Mobility. As part of the process we identify the gaps and then outline the next steps you need to take. At the same time, we draw on the breadth and depth of our expertise working on similar issues facing agencies nationwide. We learn from every new product development and implementation, and draw upon these lessons to constantly hone our products and services for you.

Included in the process is ensuring the solution is envisioned with your constituents in mind. As constituents increasingly come to expect the same quality of service from their state and local government agencies as they do from top private sector companies, we're here to make sure agencies aren't caught in the lurch. That's why we look at every IT challenge from a constituent's perspective, asking: How do we help our government agency clients optimize the constituent experience?

The result is a road map we create together, prioritizing project elements, and then working together to create a solution that will solve your problems of today and help your organization build into the future.

Full Lifecycle Support

The GCOM team of experts is there for you throughout the full project lifecycle, from initial proof of concept to full production. For virtual workspaces, our comprehensive approach ensures an efficient and low risk implementation with services covering:

- User Profiling
- Test Plans
- Network Setup
- Provisioning
- User Acceptance Testing
- Network Readiness
- Cloud Tenant Creation
- Domain Setup (AD, DHCP, DNS)
- Virtual Desktop/Application Prep
- Peripheral Setup
- Managed Services

Managed Services for Digital Workspaces

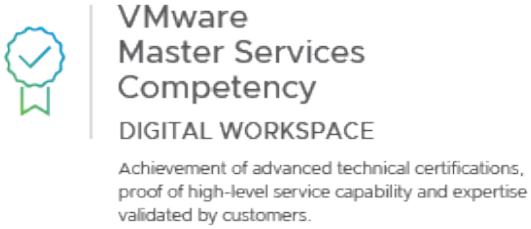
Government organizations can continue to benefit from our expertise by taking advantage of our managed services in which our 100% U.S.-based 24x7network operations center keeps operating systems and managed applications current with latest releases and security updates, and continually protects your infrastructure and endpoints from cyber attacks.

About GCOM

GCOM is led by government innovators who recognized a need in the market for a new way of doing things. During their time both in government service and serving government, they were often frustrated by a state and local tech market characterized by fragmented small companies and a few industry behemoths. For years, being forced to choose between the higher risk smaller players and the low risk but high cost of big system integrators. GCOM's innovative leadership saw an opportunity for change and were determined to provide tech savvy government leaders a third option.

GCOM is headquartered in Albany, NY and has offices around the country including Columbia, MD; Tallahassee, FL; Kansas City, MO and New York City. GCOM LLC is backed by Sagewind Capital, a middle-market private equity firm and Bagnols Family Office Investment Partners. For more information about GCOM products and services,

please visit us at: www.gcomsoft.com



References

When Governments Go Remote, McKinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/when-governments-go-remote#

Case Study, American City and County Magazine. https://www.americancityandcounty.com/2020/04/24/the-pandemic-and-the-future-of-remote-work-for-local-government/

Who Needs Cities When We All Work From Home? The Wall Street Journal. https://www.wsj.com/articles/who-needs-cities-when-we-all-work-from-home-11591394516

What if You Don't Want to Go Back to the Office? The New York Times. https://www.nytimes.com/2020/05/05/business/pandemic-work-from-home-coronavirus.html

Case Study, American City and County Magazine. https://www.americancityandcounty.com/2020/04/24/the-pandemic-and-the-future-of-remote-work-for-local-government/

U.S. Workers Discovering Affinity for Remote Work. Gallup. https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx

The Coronavirus Outbreak Has Become the World's Largest Work-From-Home Experiment. Time. https://time.com/5776660/coronavirus-work-from-home/

Amid Disruption, Identity Access Takes Center Stage. RSA. https://www.rsa.com/en-us/blog/2020-04/amid-disruption-identity-access-takes-center-stage