Citrix Workspace for First Responders and Public Safety
Managing information access with a flexible, cost-effective, and secure workspace

Public safety and first responders, whether police, fire, rescue, or aid organizations such as FEMA, have complex and critical information technology requirements. They must balance the need for fast, accurate response with increasing concerns about data security and privacy protection. These public safety personnel tend to be heavily weighted towards mobile working via satellite or wireless connections, or operating at smaller, remote sites, so user experience and connectivity become critical concerns.

Installing, updating, and supporting applications on devices in the field is time-consuming and expensive. Meanwhile, the first responders who depend on these applications, which are often delivered from multiple agencies/municipalities, face lengthy security processes such as multiple, unique logons, which can cause delays in access. Legacy or custom software, which can be hard to support and maintain, plays a critical role in the mission of these vital workers.

Instead of tackling each issue and scenario individually, you should consider a single strategy: a secure digital workspace. It’s a flexible and integrated method to deliver and manage applications, desktops, data, and documents that first responders, call center staff, and public safety officials rely on.

A complete secure digital workspace should be:

- **Unified**: Provides a single pane of glass for configuring, monitoring, and managing your entire technology infrastructure to deliver a unified user experience
- **Contextual**: Adapts to each user’s patterns and exceptions through machine learning so work can be done securely, from any location
- **Secure**: Grants safe access and full visibility across the network and user ecosystem, and includes predictive analytics so you can proactively address threats

At a Glance

A secure digital workspace from Citrix gives first responders and the entire public safety department a flexible, integrated way to support your mission. It provides secure, mobile access to critical applications from patrol cars and emergency vehicles; streamlines IT management and supports less-expensive endpoints to conserve budget; and optimizes system uptime and reliability for rapid response. This workspace also enables you to adopt cloud or hybrid cloud services to boost scalability and reduce IT administration.

Key Benefits

- Secure delivery of computer-aided dispatch (CAD) system to first responders
- Optimized application delivery to remote facilities with bandwidth constraints
- Fast, centralized application security patching for increased protection
- Data storage in the datacenter instead of the endpoint for privacy protection and compliance with regulations such as FBI CJIS
- Cost reduction from centralized IT management and support for thin-client devices
- Government-grade, hybrid cloud-ready solution

A secure digital workspace can contribute to your public safety goals by:

- Improving staff efficiency, productivity, and choice
- Strengthening regulatory compliance and information security
- Streamlining adoption of new technologies (cloud services, FirstNet, NG911, Windows 10, etc.)
- Improving the user experience in the field, in transit, and at remote locations
- Conserving scarce IT budget for other uses
A secure digital workspace from Citrix can help you accomplish all this. It also enables you to realize the full benefits of hybrid and multi-cloud environments while simplifying management and overcoming security challenges. Let’s look at some of the leading scenarios—and benefits—for public safety departments.

Improving regional communications dispatch and 911 computing

County-wide communication dispatch centers for fire, police, and emergency medical services enable rapid deployment of the closest units for emergencies and better leverage of regional specialty teams. Often dispatchers are required to operate multiple desktop computers, each with access to specific systems and/or municipalities. Prepping training labs and maintaining CAD interoperability across participating agencies can be a time-consuming undertaking.

Using Citrix Workspace to deliver virtual desktops (VDI) to these call centers can reduce the need to maintain multiple physical desktops for each dispatcher. A unified desktop can improve user speed and efficiency while reducing hardware and backend IT costs. Also, a digital workspace can help with prevention of and recovery from malicious attacks such as ransomware. This is accomplished by creating a secure digital perimeter with a web application firewall. Meanwhile, the virtual desktops can operate in a stateless fashion, allowing them to be rapidly re-provisioned in the case of an infection. Following are other important benefits of Citrix Workspace for dispatch centers.

Experience
- Equipment footprint and costs can be reduced by eliminating the need for multiple desktops at each dispatcher station.
- VDI allows dispatchers to log in faster, access information more quickly, and experience fewer interruptions.
- Administrators can rapidly deploy changes or updates to dispatcher desktops for training or production upgrades without having to visit each endpoint.
- Citrix virtual desktops are optimized to fully support Skype and other VoIP communication suites.

Security
- A digital workspace can provide protection from ransomware: first by protecting the network from incoming threats; and second by making it easy for IT staff to rapidly redeploy desktops to a known good state prior to a compromise.
- Desktop virtualization features centralized management that makes it easier to stay current with security patches and updates for both Windows 10 and critical applications.
Choice:
• A digital workspace separates the desktop image from the endpoint device, allowing an organization to mix and match devices, including thin clients, without impacting the ability to support them.
• Allowing workloads to reside on premises, in a public or government cloud, or using a hybrid approach provides flexibility in migrating to the cloud.

Increasing efficiency of in-vehicle and remote computing for first responders

The laptops within police vehicles have become mobile command centers, providing access to as many as a dozen independent systems that enhance law enforcement capabilities. Examples of common remote workloads include computer-aided dispatch (CAD), Department of Motor Vehicles access, National Crime Information Center (NCIC), and FBI Criminal Justice Information Systems (CJIS). Each of these systems typically requires an officer to authenticate using a unique set of credentials, adding both time and complexity to the daily workload.

In an extreme example, one state sheriff’s patrol officers required 13 unique logins to gain access to all the applications involved in their workspace. To avoid repeating this tedious login process every time they started their patrol vehicles, the officers kept the squad cars running continuously. This practice eventually caught the attention of the state chief financial officer, who was looking for an explanation for a spike in fuel consumption—and costs.

Fire and rescue organizations similarly struggle with the ability to provide consistent connectivity and a quality user experience to their first responders, either in vehicles or at remote substations. Additionally, these organizations are often left with legacy applications that cannot be installed or supported on modern operating systems. A digital workspace can make a major difference in the computing efficiency of first responders.

Experience
• Integrated single sign-on to applications reduces the number of credentials that must be manually entered, saving time for patrol officers.
• Virtualizing patrol car desktops allows officers to access information more quickly, improves application performance, and allows direct upload of media content rather than having to visit a substation to transfer data.
• Administrators can rapidly deploy changes or updates to the endpoints in patrol cars without the need to be on location with each vehicle.
• Citrix desktop virtualization lets organizations retain the ability to support multiple peripherals, such as GPS devices, which are often unique to law enforcement.
• Remote users enjoy better network performance and responsiveness through optimized delivery and load balancing.

Security
• A digital workspace can safeguard against ransomware by protecting the network from the threat and making it easy for IT staff to rapidly redeploy patrol car desktops to a known good state prior to compromise without having to visit the vehicle.
• Windows 10 versions and security updates can be easily kept current without interacting with the endpoint device.
• If a legacy application cannot be migrated to a modern operating system, its security risks can be mitigated by virtualizing the software within the datacenter and exposing only the required components to a properly secured endpoint.
• Citrix Workspace technologies offer FIPS 140-2 support and compliance with CJIS requirements.
Choice

• With a digital workspace, the desktop image is independent of the endpoint device, allowing organizations to look for alternatives to the current practice of deploying MILSPEC laptops in patrol cars. The ability to use an officer’s mobile phone for both communications and computing has gained traction recently. Citrix Workspace offers a consistent, unified experience across all devices.

• Organizations gain flexibility by allowing workloads to reside on premises, in a public or government cloud, or using a hybrid approach when migrating to the cloud.

Empowering digital workspace on mobile devices

First responders and public safety workers increasingly rely on mobile devices to transform their workflows for the digital age. On endpoints from smartphones and tablets to ruggedized devices, Citrix Workspace offers a consistent experience and a single platform to manage all applications, including SaaS applications, and data delivered to those devices.

Citrix believes that protecting endpoint devices, whatever they may be, wherever they are, is a critical component of a secure digital workspace. This is why enterprise mobility management (EMM) functionality is a core feature of Citrix Workspace. This functionality includes integrating with and extending the capabilities of Microsoft Intune. Mobile devices can be configured to be securely shared by multiple users, a scenario that is ideal for first responders, relief workers, or rapid response teams. Any mobile application can be secured by enabling data encryption, FIPS 140-2 compliance, and micro-VPN capabilities. Apple DEP (Device Enrollment Program) and derived credentials are also supported.
Security is a primary concern for law enforcement. It’s important to be able to wipe lost or stolen endpoints (laptops and mobile devices), including specific configurations and sensitive applications. Citrix Workspace supports both MDM (mobile device management) policies for full control of agency-owned devices, and MAM (mobile application management) policies to containerize government data and secure it without modifying personal data. This flexibility in configuration helps give your officers peace of mind knowing their personal information is safe from deletion, while your organization maintains full control over agency data.

**Experience**

- You can enhance user productivity and satisfaction by providing a consistent experience across all devices with secure management and containerization of apps and data on any device running Windows, MacOS, iOS, Android, Chrome, or KNOX.
- IT administrators can push applications and configuration changes to all devices and receive confirmation that the changes have been delivered.
- Secure sharing of files, including digital evidence, in compliance with chain of custody controls, can be accomplished without the need to manually upload documents at substations.
- For remote users and locations, network performance and responsiveness are improved.

**Security**

- Sensitive applications such as CAD and connections to external agencies can be remotely wiped in case of loss or theft. Micro-VPN connections can be established to ensure encryption of data in transit.
- FIPS 140-2 encryption, required for connections to FBI CJIS, is available for data in transit and for data at rest in storage containers.
- Geo-fencing can be used to control access to applications and data by devices based on their geographic location.

**Choice**

- Devices can be fully managed with MDM policies or with MAM policies to manage only organizational data on a personal endpoint.
- Endpoint device protection can be optionally integrated with Microsoft Intune to enhance capabilities.
- You gain organizational flexibility by allowing workloads to reside on premises, in a public or government cloud, or using a hybrid approach for migration to the cloud.

---

**Case Study**

**County Sheriff’s Office**

**PROFILE:**
Oregon’s Linn County Sheriff’s Office provides patrol services, detectives, corrections services, civil services, 911 emergency services, and emergency management. The Sheriff’s Office employs 184 full-time employees who serve in six different operational divisions covering a 2,300-square-mile jurisdiction.

**CHALLENGE:**
Saving files to standalone desktop computers required deputies to spend valuable time driving back to their offices to resume working on a report or access a file. Additionally, slow and/or unreliable WAN connectivity from multiple sites and patrol cars was impacting productivity. For the lean IT team, supporting hundreds of individual devices across a large geography was very time-consuming.

**RESULTS:**
With Citrix virtualization, deputies save reports and media, including audio and video, to rights-based, networked case folders stored in a datacenter, rather than visiting a substation to manually transfer the data. Officers now have fast access to information, including internal reports and databases from the state Department of Motor Vehicles and the Federal National Crime Information Center. The IT staff is using time saved since deploying the Citrix solution to modernize a 25-year-old records management system and CAD application.
**Citrix Workspace:** A seamless work experience regardless of the type of app, device, network, or location, without a lot of extra steps. IT maintains control and visibility of SaaS, mobile, virtual, and web apps with a simple and integrated solution that enhances a user’s experience, giving them the best tool to do their job efficiently. Available in Citrix Cloud, Citrix Cloud Government, on-premises implementation or a hybrid approach. ([https://citrix.com/workspace](https://citrix.com/workspace))

**Citrix Cloud:** Citrix Cloud services simplify the delivery and management of Citrix technologies, helping you to extend existing on-premises software deployments or move one hundred percent to the cloud. Create and deploy secure digital workspaces in hours, not weeks, while placing your sensitive app, desktop and data resources on any cloud or hybrid cloud. ([https://cloud.com](https://cloud.com))

**Citrix Cloud Government:** The first digital workspace built for government. Citrix Cloud Government platform empowers your agency to securely deliver apps and data to your workforce while improving IT efficiency and enhancing user experience. Built on a FedRAMP High Baseline certified government infrastructure as a service (IaaS) it enables your agency to leverage our industry leading digital workspace technology on any government grade infrastructure ([https://cloud.us](https://cloud.us))