Public Sector

Securely share, sync, and store files

Content collaboration lets government workers securely access and send files from any device, and provides flexible storage options—on premises, in the cloud, or a hybrid.

Securely and easily access, share, and synchronize files residing anywhere—including on restricted networks and public clouds—from any device using email, web portals, and apps.

Sharing information internally and externally is essential to the mission of any government organization. Collaboration with coworkers, partners, contractors, and personnel at other agencies requires access to many types of files, some of which may contain sensitive or confidential data. But current ways of accessing, exchanging, and storing these files can be risky, complicated, and inflexible.

One problem is the common tendency for workers to go outside government IT channels and use unapproved file-sharing and storage programs. While these consumer-focused solutions make it easy and convenient to send and receive very large files, they usually lack stringent security.

Another risk is the use of unmanaged devices—typically smartphones and tablets—to access, share, and store files. Without IT oversight and control, these devices may fail to meet government security requirements and can expose files to cyberthreats.

Different processes for accessing files residing in various locations can reduce employee productivity. Government regulations may require some data files to be kept on premises, on restricted networks or shares, while others can be stored in a public cloud. Each repository may call for a separate access method. Similarly, the wide range of devices, operating platforms, and email software used by government workers can make file sharing and synchronization difficult.

The importance of content collaboration

According to Gartner, "Content collaboration platforms can transform how individuals and teams work." In its *Magic Quadrant for Content Collaboration* report from 2018, the analyst firm predicts: "By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration platform to implement document workflows and improve collaboration and productivity."

Gartner lists core user and IT functionality offered by content collaboration platforms:

Users

• Mobile access to content repositories.

• File synchronization across devices and cloud repositories.

• File sharing with people and applications, inside or outside an organization.

• Team collaboration, with dedicated folders.

• A content repository.
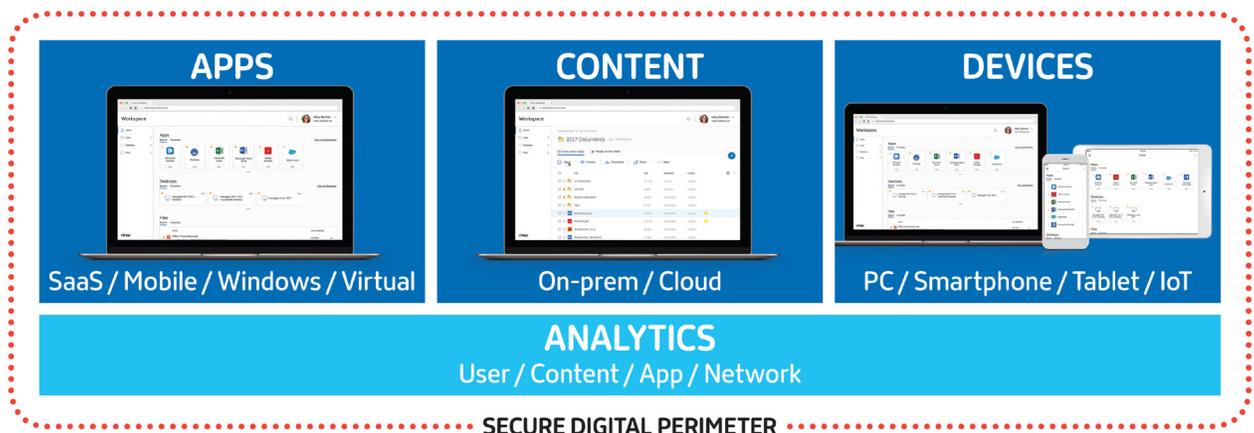
IT administrators

- Security and data protection on devices, cloud services, repositories or servers.
- Data governance, including file access control, retention, centralized oversight, classification and data residency.
- Content analytics and analysis for IT and business insight, including user preferences, work patterns, social interactions and touchpoints.

Citrix Content Collaboration (formerly ShareFile) was ranked with the Leaders in the 2018 Gartner Magic Quadrant. This enterprise-class solution simplifies collaboration for mobile, remote, and local users inside and outside your organization while maintaining IT control and providing reporting and auditing capabilities. Workers can securely access, sync, and share files from anywhere, on any device.

How it works

Citrix Content Collaboration is a file-sharing service that enables your workers to easily and securely exchange documents. The service enables your users to send large documents (up to 100 GB) by email, securely handle document transfers to third parties, and access a collaboration space from desktops or mobile devices. It provides a wide variety of ways to work, including Citrix Virtual Apps and Desktops, a web-based interface, mobile clients, desktop tools, and integration with Microsoft Outlook and Google Mail.

At a Glance

Replacing "shadow IT" solutions for file sharing with a highly secure yet flexible content collaboration platform can benefit government workers and IT administrators alike. Citrix Content Collaboration removes complexities from document sharing, sync, and storage by providing secure, unified access from any device to resources that are stored in diverse locations and subject to various data policies and compliance requirements. It addresses the challenge of "data sprawl" with centralized management of repositories. It also supports regulatory compliance and auditing with robust controls, reporting, and analytics on user activities.

Key Benefits

- Multi-layer security: Protect data with 256-bit AES encryption of files in transit and at rest, multi-factor authentication, and remote wipe for lost, stolen, or compromised devices.
- Regulatory compliance: Comply with NIST 800-53 security standards, HIPAA regulations, and other requirements, and securely archive files to support FINRA, SEC, and other compliance efforts. Gain the ability to work in a CJIS-compliant environment.
- Worker productivity: Send large files (up to 100 GB); access and edit files from any device; sync files automatically; obtain feedback and approval on documents; and reduce turnaround time with electronic signatures.
- Centralized management: Control access permissions to files or folders, receive download alerts, and generate detailed activity reports.
- Storage flexibility: Store and connect to files on premises, in a public cloud or Citrix Cloud, or a hybrid environment.

This Citrix solution is part of a complete, secure digital workspace that is:

- **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 worker'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
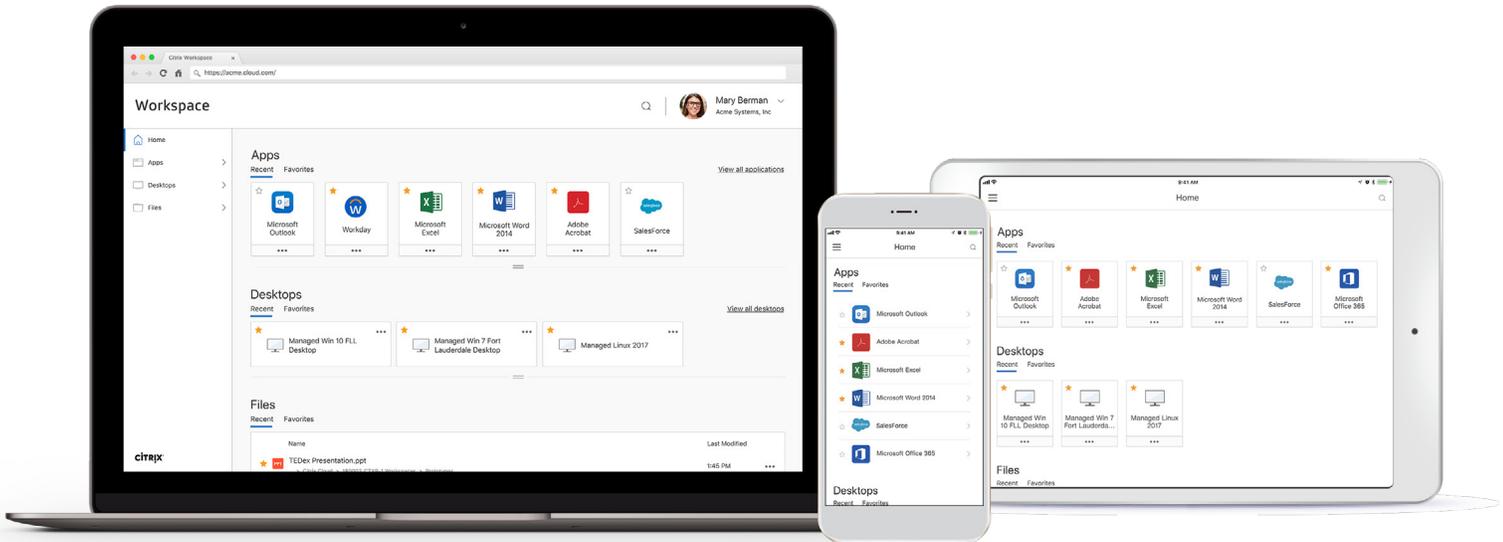
Citrix Workspace with Content Collaboration meets the needs of IT administrators for strong data security and control, while delivering on the file-sharing needs of users.

Content collaboration scenarios

Let's look at several major file-sharing challenges facing today's government agencies, and how a content collaboration platform can help.

Shadow IT

When government workers cannot easily access or send files using approved methods, they may turn to consumer-type file-sharing systems. Circumventing the established IT environment is risky: online tools may not provide adequate data security, and worker access and actions can't be monitored.

Common examples of shadow IT are SaaS applications and cloud services like Dropbox. Reasons for using them instead of agency-provided solutions include greater ease of use, compatibility with mobile devices, and superior performance—especially the ability to transmit large files that exceed the size limits of email applications.

To avoid the use of unapproved products and services, your IT team should consider offering a content collaboration solution that meets users' needs for simplicity, ease of access, flexibility, and performance. Citrix Content Collaboration encourages the use of secure, managed file sharing because it offers extensive functionality, easy access, device and OS choice, and powerful functionality.

Hybrid environments

Many government agencies are transitioning to cloud services for some or all of their IT functions. The use of public clouds as data repositories adds to the problem of "data sprawl." Besides the cloud, files and documents may reside on workers' devices, in agency storage zones such as SharePoint and OneDrive, and on network shares. Accessing all these different storage locations can be complicated and time-consuming—and it becomes even more complex when you factor in different endpoints and networks.

*Citrix Files for Windows and Mac allows users with a Content Collaboration license to interact with all their files directly from the Windows file system (see **Figure 1**) or the Mac Finder window. Access to network drives, OneDrive, SharePoint, and other cloud repositories appears as a mapped Windows drive, helping users stay productive in the native Windows experience. Citrix Files also provides access to data in hosted environments like Citrix Workspace and Virtual Apps and Desktops. The same file sync and share experience is used across both physical and virtual endpoints.*
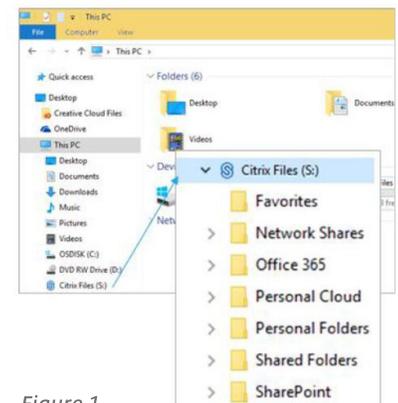

Figure 1

Auditing and compliance

When government data, particularly sensitive or confidential information, is being shared, IT administrators need tools to control, monitor, and report on worker access and actions. These capabilities are critical for auditing and regulatory compliance.

Citrix Content Collaboration gives IT administrators the ability to track and log activity in real time and create custom reports to meet compliance requirements. They can define policies to allow the appropriate level of secure access for each user, in any scenario. Users can be granted download-only access or full upload/edit/delete rights, depending on their location, role, or device. This solution also provides access to Citrix Analytics, which applies machine learning and artificial intelligence to data from network traffic, users, files, and endpoints to analyze malicious user behavior and application performance anomalies.

Citrix Workspace

Citrix Workspace offers a better way to work. It unifies Citrix technologies including virtual apps, virtual desktops, content collaboration, and endpoint management. This solution offers a user-centric experience where everything you need to work is in one app, with simplified access and performance based on user context and IT-designated conditions. By bringing all your apps, files, and data together in one easy-to-use interface, Citrix Workspace delivers secure access and high performance to your users.

Customer Use Case

Mid-Atlantic State Attorney General's Office

PROFILE:
A state AG office staffed by a team of 500 legal professionals handling case files.

CHALLENGE:
Attorneys and paralegals needed a way to easily share case files with opposing counsel for discovery, with an audit trail to document when and by whom these files are accessed. The AG office also needed a solution for responding to Freedom of Information Act (FOIA) requests by the public.

RESULTS:
Using Citrix Content Collaboration, the AG's office can easily collaborate internally and externally with granular levels of security. Citrix Content Collaboration also provides an easy way to grant information on a case to citizens as part of a FOIA request.

CITRIX®
Public Sector

0219/PDF