Citrix Workspace Microapps Service Security Overview

Contents

Introduction

Citrix Workspace is a digital workspace platform that is designed to help give employees everything they need to be productive in one unified experience. Citrix Workspace provides IT with the visibility, simplicity, and security required to enable and control their employees' experience.

We believe that protecting our customers' data is one of our most essential responsibilities, and providing information about our security practices, policies, and processes helps empower customers to make informed and critical decisions about their IT spend. This security overview has been created to answer the most common customer questions and describe our approach to security of the Microapps service, which is a part of Citrix Workspace.

Workspace intelligent features give users a single unified experience no matter where they reside while incorporating new microapps and microworkflows to guide and enhance productivity. Analytics and automated intelligence make it possible for admins to customize the experience for individual users. Citrix Workspace is designed with security in mind—all data and keys are encrypted.

We are creating new ways to interact with your existing systems and to provide your end users with simple actions right within the Citrix Workspace interface. Actions are user-initiated activities taken within the microapps that provide inputs to regularly accessed business applications. The actions a user performs within a microapp are designed to address specific common problems and use cases quickly and easily, adding to increased user productivity (for example: request PTO, submit a help desk ticket). Write-back actions are performed using the user's own account and not a generic service account, which makes the action auditable. Citrix Workspace can also push event-driven microapps and notify users of something that requires their attention (for example: approval of an expense report, new course available for registration).

To learn more about Citrix Workspace with intelligent features, visit Citrix Tech Zone to watch a short video, read a technical brief, or read a complete reference architecture. To learn more about how Citrix handles Customer Content in Citrix Cloud services, read Citrix Cloud services customer content and log handling article.

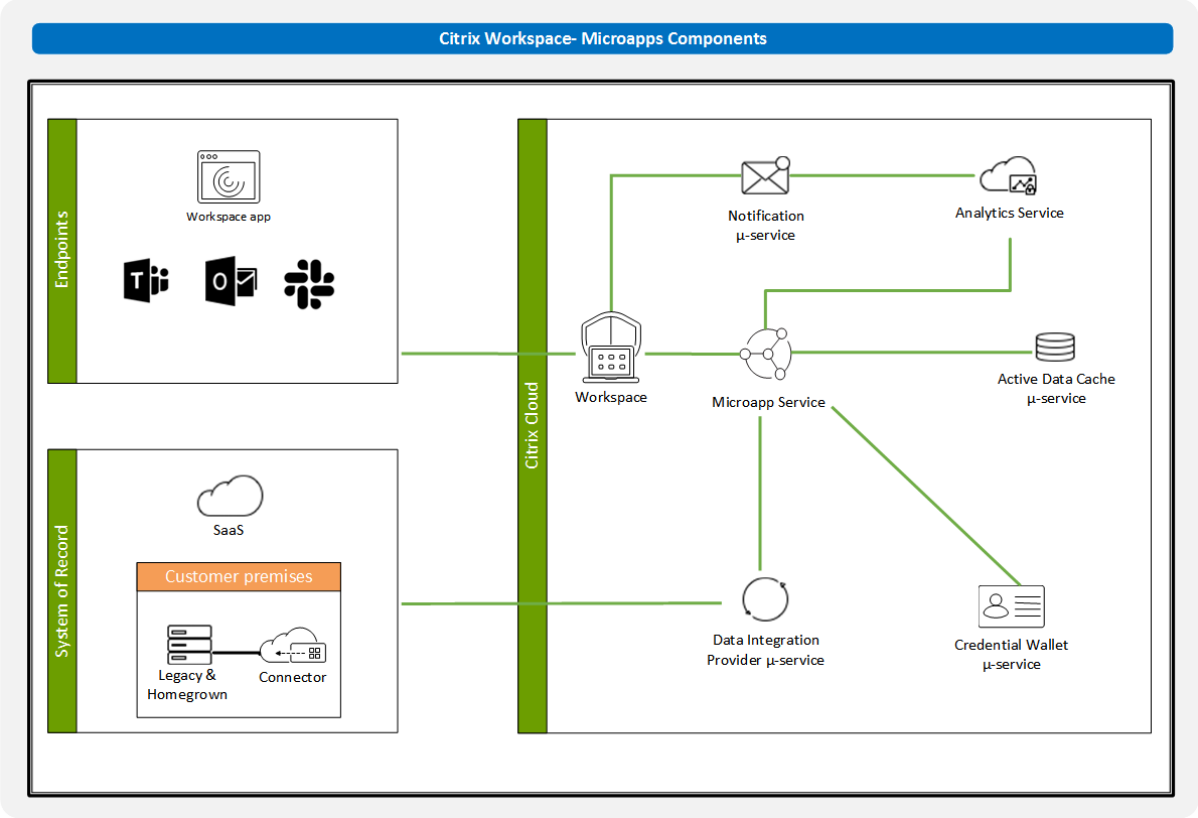
Note: *this information is provided on an "AS IS" basis without warranty of any kind, for information purposes only, and is subject to change at any time at Citrix's sole discretion.*

Service Architecture

At the core of the next generation workspace with intelligence is our proven Citrix Secure Digital Workspace with new micro-services. Citrix services are hosted on the Citrix Cloud platform, which can connect through Citrix Connectors to any cloud or infrastructure you choose (on-premises, public cloud, private cloud, or hybrid cloud).

Many of the relevant security questions about the Microapps service are related to the Citrix Workspace platform itself and not directly to this specific service. For example, Citrix Workspace handles end users' authentication.

The overview of the Microapps service components and interactions can be found in the following diagram:



Service Components

The Microapps service components can be roughly divided into three separate categories:

- **Clients** – Endpoint clients used to access Citrix Workspace
- **System of Record** – Data source, typically SaaS, or web applications used by customer
- **Citrix Cloud** – Components hosted in Citrix Cloud. These components are part of the service

Clients

Citrix Workspace is primarily accessed by end users through the Citrix Workspace app (formerly known as Citrix Receiver), however alternative endpoints can be also used (extended by vendors or customers). For example Microsoft Teams or Slack. The Citrix Workspace app is available for various platforms – native clients for Windows / Linux / macOS, mobile clients for Android/iOS and as HTML5 and Chrome packaged app.

System of Record (SoR)

A System of Record (SoR) is an existing customer application that the Microapps service interacts with. These applications can be SaaS applications, legacy applications, custom applications and can be hosted on-premises or in the cloud. Consider Workday, Salesforce, or ServiceNow as common examples. Each SoR integration can support multiple microapps (for example ServiceNow can support a microapp to get notified about new support tickets assigned to you, also another microapp to create support tickets).

Microapps Service

The Microapps service is a single-tenant service that acts as a central orchestration layer and data cache for microapps functionality. The Microapps service is responsible for credentials management, reading and writing data from the SoR and forwarding events to analytics / notifications service.

It periodically polls the SoR to update its local data cache. The event engine then generates raw notification events based on changes observed in the data cache, then sends them to the Citrix Analytics service to score them for relevancy.

You can read more about the data cache in the data security section.

Integrations Provider

For each connected SoR, a data integration is responsible for synchronizing data between the SoR and the Microapps service. It defines how to authenticate to the source SoR, what is the expected schema of data and how to retrieve it. There are template integrations available from Citrix Workspace for various SoRs or you can create your own application integrations.

Credential Wallet

The Citrix Cloud platform includes this secure service for storing service credentials and OAuth 2.0 client tokens. The Microapps service uses the Credential Wallet service to store and retrieve required credentials that are used to synchronize data with the SoR and to perform user actions against the SoR using the user OAuth token.

Analytics

The Microapp service is NOT sending notifications directly to the notification service, instead it forwards raw events to the Citrix Analytics service. The Citrix Analytics service processes the raw events and creates scored notifications that it then sends to the notification service. Machine learning is used to prioritize events that are then forwarded to users. You can find

more information about data collected and processed by Citrix Analytics service in the product documentation.

Notification Service

The notification service processes the notifications created and either stores them in a database to be later served as notification cards or sends them out immediately as a push notification to the end-user.

Connector Appliance for Cloud Services

The Connector Appliance for Cloud services is a Linux-based virtual appliance that serves as a channel for communication between Citrix Cloud services and customer on-premises (or public/private cloud) locations. It enables the Microapps service to interact with home-grown applications without requiring any complex networking or infrastructure configuration.

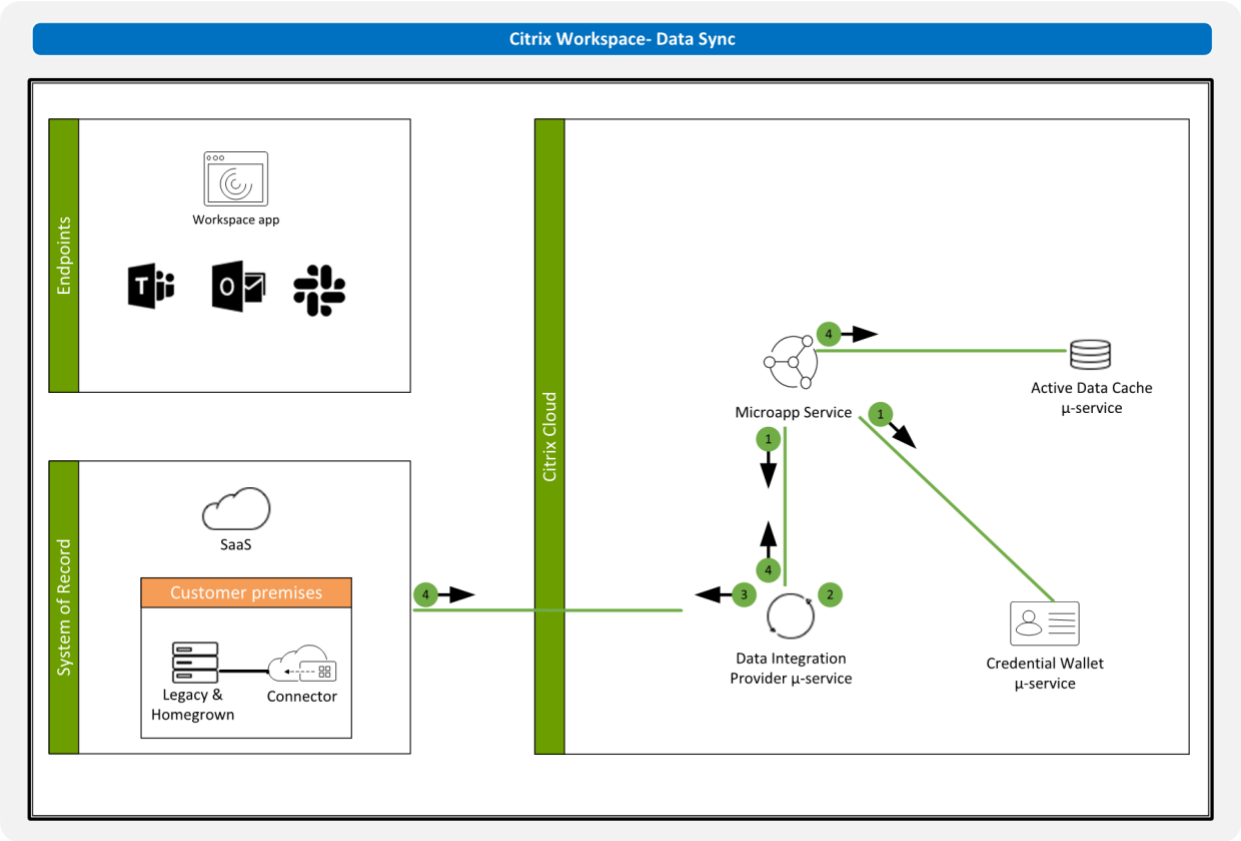
Service Processes

In this section, we talk about different processes in the Microapps service – how data is retrieved from SoRs and how notifications are pushed to the end users.

Data Retrieval

The Microapps service retrieves data from a customer's SoR and stores it in the Microapps service data cache, based on which notifications and/or actions can be generated. The sync intervals can be scheduled to be different based on the SoR or the customer's specific implementation.

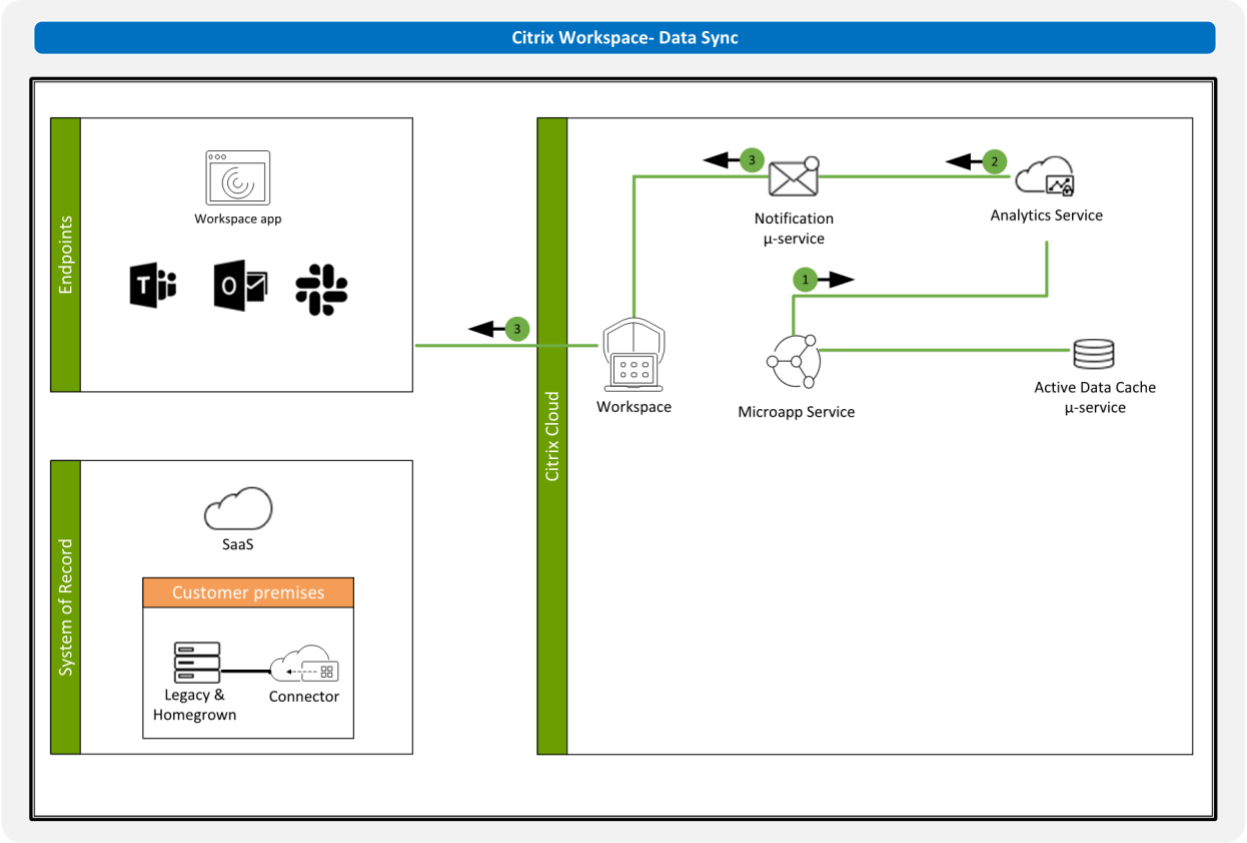
The following steps are taken during a synchronization process:



1. The Microapp service retrieves encrypted service account credentials for the requested SoR from the Credential Wallet and requests a sync from the integration
2. The integration decrypts the service account credentials
3. The integration retrieves data from the SoR using provided credentials
4. The integration streams data from the SoR to the microapp service which then stores the data in the data cache

User Notifications

The microapps service reads data from the data cache and generates events based on the change notification logic defined by the customer as part of each microapp. Each notification is sent to Citrix Analytics service to process / assign scores and based on various algorithms to determine the priority ranking within each user's feed. Scored and personalized notification cards are then forwarded to the Notification service.

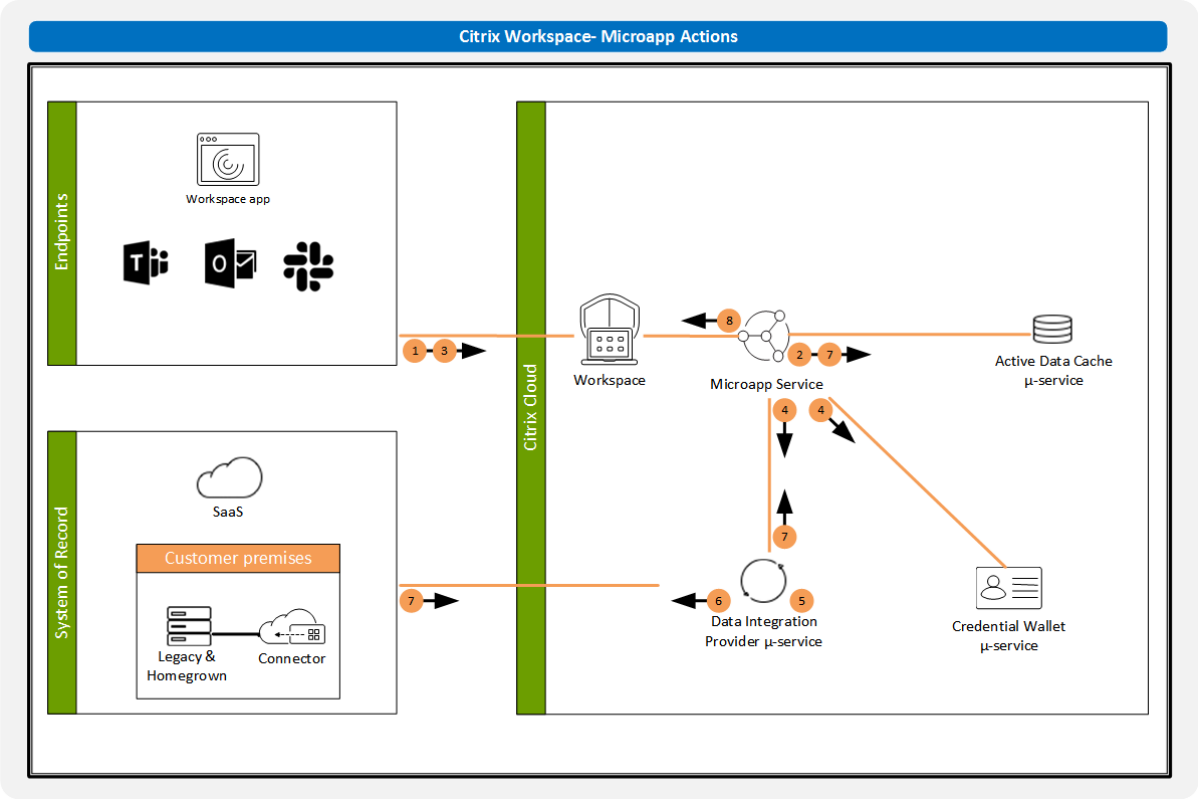


1. The microapp service sends raw events to Citrix Analytics service
2. Citrix Analytics service processes this data, creates scored notifications and sends them to the notification service
3. Endpoints receive the notification

User Actions

From a security perspective, read-only operations such as displaying a notification are less critical than making changes to a SoR. “Actions” are operations that result in change to the source SoR and it is important to understand security implications for write operations. Example of an action is approving a PTO request.

The following steps are taken during the processing of actions:



1. The endpoint retrieves data from the microapp service to render a microapp details
2. The microapp service retrieves data from the data cache to support rendering
3. A user invokes an action from the microapp. The microapp service receives the action. Microapp service performs a validity check on the requested action to ensure that the underlying request is still valid
4. The microapps service retrieves an encrypted OAuth 2.0 token from the credential wallet and forwards action to the integration
5. The integration decrypts the end user's OAuth 2.0 token for the SoR action
6. The integration writes the action to the SoR using the identity of the end-user
7. The integration reads back the changed data and the data cache is updated
8. The endpoint receives feedback that the action has successfully completed

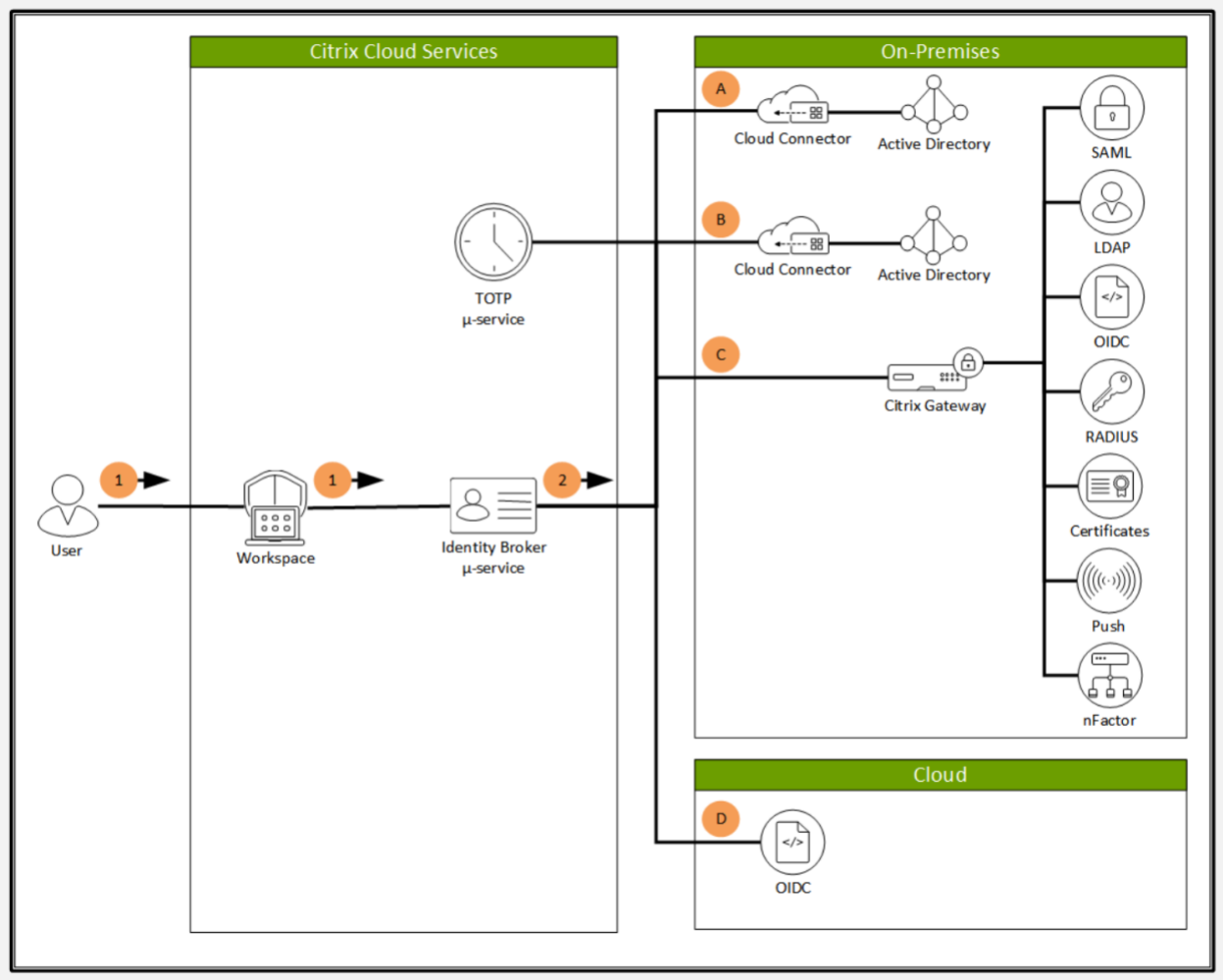
Citrix Security Controls

Citrix is highly focused on implementing strong security controls for all components of Citrix Workspace with intelligence. In this section, we talk about access security, infrastructure security, computer security, and protection of data at rest and in transit.

Access Security

End User Authentication

For end user authentication, Citrix Workspace supports multiple identity providers, authentication methods, and industry standards such as SAML or OpenID Connect with a strong focus on multifactor authentication.



1. An unauthenticated user accesses Citrix Workspace, forwarding the request to the identity broker
2. Based on the configuration of Citrix Workspace, the user authenticates with an appropriate identity provider
    a. The identity broker uses the Cloud Connector's communication channel to authenticate users with Active Directory
    b. The identity broker uses the time-based one-time password (TOTP) to validate the user's temporary token and then uses the Cloud Connector's communication channel to authenticate users to Active Directory
    c. The identity broker uses OpenID Connect to communicate with an on-premises Citrix Gateway, which supports multiple authentication providers
    d. The identity broker uses OpenID Connect to communicate with cloud-hosted identity providers like Azure Active Directory or Okta

With Citrix Gateway, more advanced and complex access control scenarios are supported. Customers can use **nFactor** for context-aware authentication, integrate smart cards or

certificates. You can watch a short tech insight video to learn more about Citrix Gateway authentication features.

Citrix Analytics for Security is an add-on service that further improves context-aware access security. It continuously assesses the behavior of Citrix Workspace users and applies actions designed to protect information. You can learn more by watching this short video, read a technical brief or documentation

To learn more about Citrix Workspace supported identity providers and our approach to authentication, read the Workspace Identity tech brief or Identity and access management documentation.

To provide the best user experience, single sign-on is an important consideration. To learn more about Citrix Workspace and single sign-on, read the technical brief.

System of Record Authentication

Two different kinds of accounts are used by the Microapps service when authenticating against SoRs: service accounts (to update data cache) and authorization tokens (to perform actions in user's context). Both credential types are securely stored in the Credential Wallet.

Each integration has a separate **service account**. A service account can use various methods to authenticate (for example API key, OAuth 2.0 token, password), depending on which authentication standards are supported by the SoR. Depending on the SoR, it is recommended to provide service accounts with minimum required privileges, ideally limiting the data that it can read if there is a misconfiguration.

The SoR service account is responsible for generating a single data cache object for ALL users of that application. Before this data is exposed to end users, it is important to use filters that affect which data is visible to which user.

Example: If you are using Jira, only one cache object is created for all users. Before displaying any data to the end users in a microapp notification or page, it is important to specify a condition (filter) that displays data only if tickets are assigned to current user ('assignee_email = logged-in user email`). It is important to understand that if these filters are not correctly configured, data can be exposed to users that should not be able to see it. Filters are often based on an email but can be any other attribute or conditions.

The second type of credential is a user's OAuth 2.0 token (**authorization token**). Tokens are used to perform actions against the SoR in a user's context. Whenever possible, it is recommended for administrators to pre-consent OAuth (user is not asked to approve access to attribute / permissions by resource provider). While it is possible to use a service account to make changes to a SoR, it is preferred to rely on user context and use authorization tokens instead.

If possible, use service accounts in the SoR with read-only permissions. The write-back actions should use a user's actual account to enforce all actions in a manner that is consistent with the policies of the system you are interacting with. Using a service account without impersonation can make it difficult to determine which user performed an action.

Customer administrators are able to limit access to microapps on Citrix Cloud to specific users and/or groups. Customer administrators with the Microapps admin role have full access to all data integration configuration and data cache content, but no access to existing integration credentials.

Infrastructure Security

The Microapp services are managed by Citrix and hosted on a third party platform (currently Microsoft Azure). Access to the hosted environment is restricted and only possible from Citrix data centers.

Management access to this third-party platform is allowed only from Citrix data centers. To limit access to Citrix data centers, Citrix maintains a Physical and Environmental Security Policy and Program. You can read more in Citrix Services Security Exhibit.

Compute Security

Citrix Workspace consists of many micro-services. The microapps service and data cache is single tenant to provide customer data isolation, while other services are multitenant.

- Microapps service and data integrations – single-tenant
- Credential Wallet – multitenant
- Analytics service – multitenant
- Notification service – multitenant

Multitenant services use per-tenant isolation with separate customer partitions that are using per-tenant encryption keys and credentials (with exception of notification service, which relies on token-based security for access). Microapps service is a single-tenant component to better help isolate the data in data cache (single-tenant SQL database).

Data Security (data-at-rest)

Customers may select their cloud instance geo during Citrix Cloud onboarding, which is where data is both processed in-flight and stored at rest. Citrix does not control the location of cloud SoR. The same limitation applies to SoRs that are hosted on-premises.

Service Components

Data collected and stored by various Microapps service components is described below using the definitions provided in the Service Components section.

Components with no data at rest

- Microapp service

- Connector Appliance for Cloud services
- Data Integration Provider

Components with stored data

- Analytics service – Contains user scoring data, no data from SoR
    - Database is multitenant with customer partitions, encrypted with a multitenant encryption key
    - Data is retained for 13 months
- Notification service – Contains notification card data
    - Database is multitenant with customer partitions, encrypted with a multitenant encryption key
    - UI elements of microapps (visible cards) should preferably not contain any sensitive information
- Data Cache – Contains per-SoR data
    - Database is single-tenant with per-tenant DB-level encryption key and per-tenant DB credential
    - Information stored here should be filtered to include only information required by microapps (must be supported by SoR)
    - Only data from last 90 days is synchronized (default). This period is configurable by customer.
    - During full synchronization, previous content of the cache is automatically deleted.
- Credential Wallet – Contains encrypted system account credentials and OAuth 2.0 tokens
    - Database is multitenant with customer partitions, encrypted with a multitenant encryption key
    - Uses FIPS 140-2 level 2 validated cloud HSM (Azure Key Vault) with non-exportable, per-tenant keys

Customer Components

Most customers are interested in data storage used for their business data (**data cache**) and credentials (**credential wallet**). While data cache content depends on the source SoR and implementation, credentials security is provided by Citrix.

Credentials are stored using a key vault. The Credential Wallet service performs service-level authentication to govern API access. Only approved services are permitted to retrieve and decrypt secrets.

Understanding data cache is critical to get a better view of the business data that is stored there. Data cache content, behavior, and synchronization schedules are highly dependent on the integration provider implementation and should be carefully reviewed regularly. Capabilities of the SoR and exposed APIs can affect both synchronization frequency and content of data collected. It is important to understand the permissions model of the SoR and

requirements – if data is filtered by user or more complex system is being used (for example contextual security or group-based security).

The Microapps service uses a pull synchronization to retrieve data from SoR. Default (full) synchronization with SoR has an interval of 24 hours and is configurable by customer (can be as short as 15 minutes). Depending on the SoR capabilities and available APIs, synchronization can be full or incremental (preferred). Typical implementation is performing a full sync daily (or weekly) and incremental synchronization every few minutes.

Data that is retrieved during this synchronization also depends on the SoR capabilities and APIs – it can be either a full data retrieval or filtered data retrieval. With filtered data retrieval, only a subset of attributes is collected and saved in cache. This also makes it possible to limit personally identifiable information and other data elements that are stored in a data cache. Data cache content can be reviewed by a full administrator role using data cache explorer functionality.

Example: When retrieving information about ServiceNow tickets, you don't need to collect hundreds of attributes, but only Assignee, Description, Ticket Number, and Priority. This filter is configurable per customer.

For template integrations that are managed by Citrix, we provide a complete list of attributes that are stored. You can find a list of available integrations in product documentation. Each article contains instructions for implementation and link to connector specifications. For example, see SAP Ariba integration instructions and SAP Ariba connector specifications.

Understanding your applications, available APIs and capabilities is critical for a successful Microapps service implementation.

Network Security (data-in-transit)

Citrix Cloud minimizes and manages the externally facing attack surface using processes such as monitoring, automation, and security testing. Cloud platform providers provide a significant number of native security capabilities as well including host-based and perimeter firewalls, intrusion detection and prevention systems, anti-DDoS capabilities, and centralized visibility using services like Azure Security Center. Furthermore, the products, services, and components hosted within public clouds ship logs to Citrix's security information and event management system (SIEM), which provides alerting and event correlation capabilities.

Firewall devices for Citrix are configured to restrict access to the Citrix environment by limiting the types of activities and service requests that can be performed from external connections.

Firewall rules follow an established standard that uses least privilege permissions approach, among other leading practices. Access to specific entities within the network is restricted and exceptions are only authorized when necessary for a short (<24 hour) period. Automation patrols any exceptions and removes them nightly as needed.

Protection with an external network firewall with a 'default deny' ruleset is a mandatory requirement. Citrix corporate and non-cloud facilities are protected with network-layer firewalls.

Endpoint to Citrix Workspace

When users are connecting to Citrix Workspace, data in flight stays in the customer geo in the Citrix Cloud and uses industry standard TLS 1.2+ (AES 256) with the strongest cipher suites. Customers cannot control the TLS certificate in use, as Citrix Cloud is hosted on the Citrix-owned cloud.com domain. To access Citrix Cloud, customers must use a browser capable of TLS 1.2 with strong cipher suites.

Citrix Workspace to SoR

To access SoRs that are on-premises, the connector appliance for cloud services requires only outbound TCP port 443. The connector appliance supports customer web proxies, uses RSA key pairs with trusted service identity store and signed, single-use tokens. An administrator can connect to any on-premises resource through the connector and it is recommended to put it in DMZ and configure firewall rules to limit access to other resources.

It is recommended that data to retrieve by service account should be filtered (only required attributes should be collected). If supported by the SoR, it is also advised to provide this account with minimum required privileges, ideally limiting the data that it can read if there is misconfiguration. Read more about data cache behavior and limiting of data in SoR Authentication section.

In the best-case scenario, the solution uses service accounts in the SoR with read-only permissions. The write-back actions utilize a user's actual account to ensure all actions performed are compliant with data policies of the system we're interacting with.

Citrix Services Security

Citrix Services Security Exhibit describes the security controls implemented in connection with the performance of Citrix Cloud services, technical support services or consulting services under the relevant Citrix license and/or services agreement and the applicable order for the Services. The Exhibit does not apply to beta or lab/tech preview services, including Citrix Cloud Labs.

The Exhibit describes the administrative, physical and technical security controls Citrix employs to maintain the confidentiality, integrity, and availability of its Services. These controls apply to Citrix's operational and Services systems and environments. Citrix employs ISO/IEC 27002 as the baseline for its Services security program.

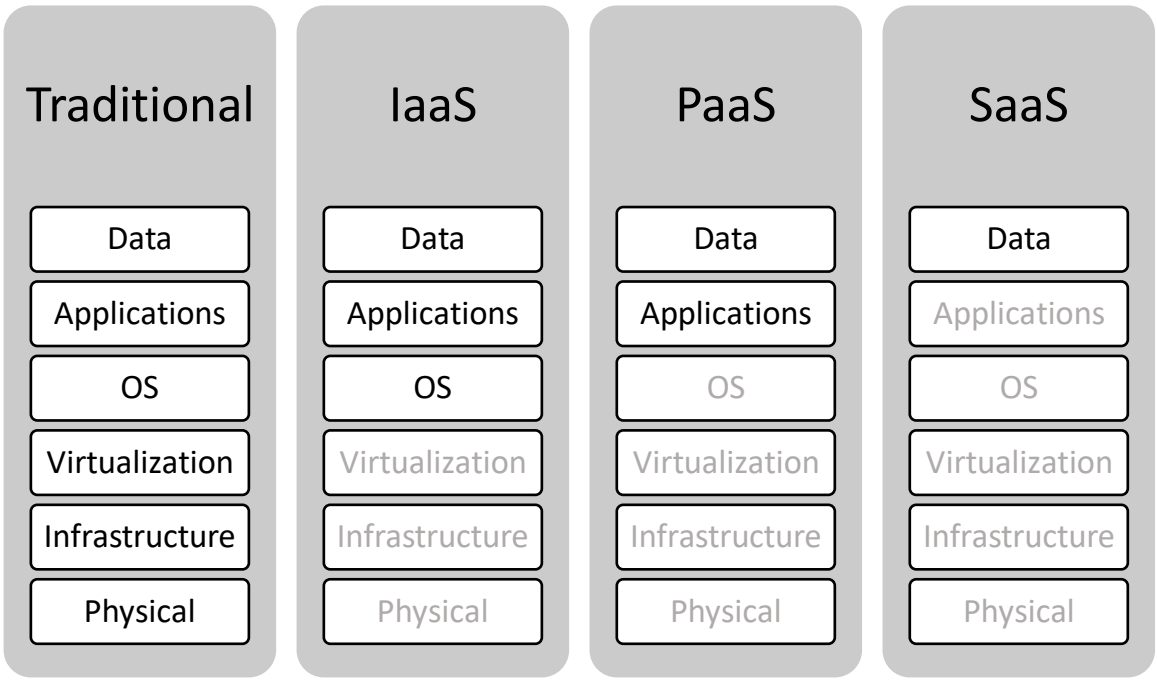
Citrix has appointed a Chief Information Security Officer (CISO), who is responsible for security oversight and policy strategy, compliance and enforcement.

Latest version of Citrix Services Security Exhibit is available on the Citrix Trust Center.

Shared Responsibility Model

Most critical security threats in the cloud today are the result of service misconfigurations. According to Data Breach Investigations Report 2019, 45% of data disclosures in the information industry have been caused by misconfiguration and 24% by publishing errors. While the Citrix Workspace platform has been designed with security in mind, it is important to understand how Citrix and our customers share ownership of security responsibilities. Understanding this shared responsibility model and taking all the required steps to secure your implementation are critical to success in the cloud today.

In a traditional (on-premises) model, your organization is responsible for all aspects of the implementation covering all 6 layers of the deployment stack. With a cloud deployment, the responsibility for some of these layers no longer fall to your IT organization.



Organization responsibilities in shared responsibility model

Citrix is fully responsible for all aspects of physical, infrastructure, virtualization and OS areas that are hosted primarily in Microsoft Azure. That said, there are two important areas that the customer is fully responsible for – implementation and configuration.

While the Microapps service has been designed as a highly secure solution, if a customer does not implement or configure it properly or completely, the result can compromise the security of the solution. Each customer implementation is unique, with a different combination of requirements and portfolio of applications. Customers need to understand their implementations, and the responsibilities and associated security impact their decisions can have. The following are a few examples of important security responsibilities that customers have.

First, assessing and segmenting your applications is a critical step in building a successful workspace solution. Many customers are dealing with hundreds or thousands of unique applications. Understanding their capabilities and limitations is critical for implementation. This assessment needs to include, among other things, information about available APIs and their capabilities and limitations. All applications must be evaluated, so security risks can be identified before implementation, especially for legacy systems. New microapps should always go through a security review before being added to the production library. Implementing proper change management is important, and we recommend a separate service subscription for test/QA purposes.

Second, identity and access management plays an important role in security access to your data. Service accounts (or tokens) that retrieve data from a System of Record (SoR) are the customer's responsibility and need to be properly secured. Provide only minimum required privileges to a SoR - read-only access and access limited to required fields. Identify which resources these accounts need to access and what are the required permissions for them as well as implement monitoring of their access.

Third, always minimize the amount of data retrieved from the SoR and stored in the Microapps service data cache by synchronizing only filtered data and using incremental synchronization. Data retrieved should be limited both in scope (only required fields) and in time. This depends on applications and the SoR capabilities. When the Citrix Connector appliance is used to provide access to a SoR, network access must be limited only to required resources and monitored for suspicious behavior. When displaying notifications to end users, make sure that filters are implemented, and only relevant information is visible.

While these are three illustrative examples of customer responsibilities in the SaaS shared delivery model, there are many more customers need to consider and assess. You can find more information about security best practices in product documentation.

Compliance and Certifications

ISO 27001: Citrix is certified for the internationally recognized ISO/IEC 27001 standard for its implementation of Information Security Management Systems. You can download the ISO 27001 certificate here.

Service Organization Control (SOC) Reports: Citrix Workspace has undergone a SOC 2 audit. A copy of the most recent report is available here after signing an NDA.

Other compliance initiatives that may not necessarily include Citrix Workspace are located here: https://www.citrix.com/about/trust-center/privacy-compliance.html

Resources

Microapps Overview - Citrix Tech Zone is home for technical, in-depth articles that are inspired and driven by technical communities and enthusiasts.

Microapps Documentation –Microapps product documentation.

Microapps Reference Architecture - Citrix reference architectures are comprehensive guides that assist organizations in planning their Citrix Workspace implementations complete with use cases, recommendations, and more.

Citrix Trust Center - The Citrix Trust Center provides the latest information on our approach to security, privacy, and compliance. Learn how we support and protect our customers.

Citrix top 20 security FAQs - Explore common questions and key information on Citrix security best practices and controls.

Citrix Services Security Exhibit - Describes the technical and organizational security controls for Citrix Cloud services, technical support services, or consulting services.

Revision History

Author: Martin Zugec

Special Thanks: Daniel Feller, Ana Ruiz, Radovan Hrabcak, Marek Jalovec, Tomas Kmec, Allyson Kuegel, Andrew Cooper, David Le Strat, Jay Tomlin, Eric Beiers, Slavomir Jelen, Christian Reilly, Alexis Goltra, Lisa Mundrake, Brenda Oakley