citrix

Solution Brief

Secure remote access to any application from anywhere, on any device

At Citrix, we empower our customers to provide contextual and secure access to applications deployed on-premises, in the cloud, or delivered as SaaS. In addition, we also provide security controls like web filtering and web isolation for customers who want to control what users access on the Internet. Currently, we offer three choices to customers looking to implement secure access and single sign-on solutions for their applications, network and data.

Citrix Secure Workspace Access

Citrix Secure Workspace Access offers a comprehensive, zero trust approach that delivers secure and contextual access to all applications you need and provides an enhanced user experience while maintaining security control. It allows for consolidation of traditional security products like VPN, single sign-on and browser isolation technologies with one solution. This allows for a holistic security approach based on principles of zero trust. Over and above consolidation, it provides cloud app control policies to protect intellectual property in SaaS and web applications.

In addition to allowing access to corporate data from managed devices, Citrix Secure Workspace Access provides security controls to protect user and corporate information even when accessed from BYO and unmanaged devices. With browser isolation technology, it helps users access applications in an isolated environment to protect applications from any malicious content on user devices. In addition, app protection policies in Citrix Secure Workspace Access protect user and corporate information from being stolen by key logger and screen capturing malware. This allows IT to let their users access corporate data from BYO and unmanaged devices; thus making life easier for both IT and end-users.

Citrix Workspace Essentials

Citrix Workspace Essentialsis a component of Citrix Secure Workspace Access that can be purchased separately as well. This service, provides single sign-on and zero trust VPN-less access to web and SaaS apps and secure remote access to Citrix Virtual Apps and Desktops. It allows customers to replace their traditional

VPNs and consolidate SSO solutions for SaaS applications. However, it does not provide advanced security policies like copy, paste control, isolated browser, and app protection policies that come with Citrix Secure Workspace Access. If you are looking to provide basic access to applications with single sign-on experience then this is a good service to begin with.

Citrix Gateway

Citrix Gateway is a customer-managed solution that can be deployed either on-premise or on any public cloud, such as AWS, Azure, or Google Cloud Platform. It comes in both hardware and virtual form-factors that can run on any hypervisor environment. Citrix Gateway provides users with secure access and single sign-on to all the virtual, SaaS and web applications they need to be productive. It also provides a complete SSL VPN solution for access to network resources.

Citrix Secure Workspace Access– common use cases

Citrix Secure Workspace Access helps customers adopt cloud and SaaS applications while removing concerns around unauthorized access and securing confidential data in SaaS applications. Common challenges that are solved by Citrix Secure Workspace Access include:

1. Secure VPN-less access with zero trust network access

Unlike a traditional VPN, Citrix Secure Workspace Access is a cloud-based offering that provides secure and contextual VPN-less access with single sign-on (SSO) to on-premises web apps. In addition to SSO, it also provides controls for protecting information shared in web applications. Administrators can enforce security controls to govern data exfiltration including preventing copy, paste, print and navigation, and enabling watermarking on-screen for sensitive applications. Additionally, it provides security controls like web filtering and an isolated browser environment to protect users accessing embedded and app-shared malicious links, adding security as they access web apps from their personal or BYO devices. These security policies along with Citrix Analytics for Security, enable organizations to deliver zero trust outcomes by reducing the attack surface, securing the log-in process, enabling continuous authentication and authorization, providing data and device protection, protecting users from web-based threats, and automated risk prevention.

2. Secure Access to sanctioned SaaS apps with security controls

The increase in use of SaaS apps creates security risk as users have to juggle multiple log-ins for different services, leading to poor password practices like reusing passwords or passwords that are easily hacked. Secure Workspace Access provides the ability to Single Sign-On to SaaS applications and additionally enforces security controls to govern data exfiltration including preventing copy, paste, print and navigation, and enabling watermarking on-screen for sensitive applications. These features provide a way to allow end-users to gain secure access with Single Sign-On to all of their SaaS applications configured within Citrix Workspace.

3. Browser isolation for gray sites to augment anti-phishing and anti-malware capabilities

Citrix Secure Workspace Access provides the ability to isolate and render websites in a cloudhosted browser leveraging the Citrix Secure Browser Service. Citrix Secure Browser Service isolates web browsing to protect the corporate network from browserbased attacks. It delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration. Administrators can orchestrate secure browsing as a web filtering policy within Secure Workspace Access. By isolating internet browsing, IT administrators can offer end users safe internet access without compromising enterprise security. In addition to browser isolation, administrators can also implement traditional web filtering policies to allow/deny access to one or more websites.

Citrix Workspace Essentials – common use cases

Citrix Workspace Essentials provides secure remote access solution with a diverse Identity and Access Management (IDAM) capabilities, delivering a unified experience into SaaS apps, heterogeneous virtual apps and desktops, and internal web applications. Customers who choose Citrix Workspace Essentials are typically looking to solve the following challenges:

1. Single sign-on to SaaS and web applications

Today's end users require easy access to their web, cloud or SaaS applications across multiple devices and connections. A cumbersome sign in process can significantly impede productivity—although IT must require secure logins to protect corporate data. In order to ensure a high-quality user experience while still maintaining security and control, IT teams must provide users with single sign-on (SSO) across all applications, whether they're hosted on premises, in the cloud or delivered as SaaS. By leveraging contextual Secure Workspace Access and multi-factor authentication, IT can maintain productivity and end-to-end oversight across all application traffic.

2. VPN-less and zero trust secure access to internal web applications

Traditional VPNs are complex and tough to manage especially when IT teams are trying to scale quickly. Citrix Workspace Essentials securely connects to an on-premises data center with the Citrix Gateway Connector, which is deployed on-premises. The connector acts as a bridge between internal web applications and Citrix Workspace Essentials by establishing a TLS connection without a VPN connection.

Citrix Gateway–common use cases

Citrix Gateway is a secure and remote access solution that has solved these key customer challenges:

1. ICA proxy to on-premises deployments of Citrix Virtual Apps and Desktops

Citrix Gateway provides advanced functionality for delivering remote access to Citrix Virtual Apps and Virtual Desktops applications. It is the only solution that provides security, performance and complete end-to-end visibility for Citrix environments. Its core strengths are:

- **Security –** Citrix Gateway provides contextual Secure Workspace Access policies for Citrix Virtual Apps and Citrix Virtual Desktops. These policies, referred to as SmartAccess and SmartControl policies, allow enforcing controls on actions a user can take once they successfully login to these applications.
- **Improved performance –** Only Citrix Gateway supports HDX Enlightened Data Transport, a protocol developed on UDP, to provide a better user experience for traffic over high-latency networks like home and public WiFi.

2. VPN for remote access to corporate network and datacenter resources

Citrix Gateway is a full SSL VPN solution that provides users, access to network resources. With both full tunnel VPN as well as options for clientless VPN, users can access applications and data deployed on-premises, or in a cloud environment. Core strengths for our SSL VPN solution include:

- **Clientless access to all apps:** Citrix Gateway offers browser-based access to all web and legacy applications that are deployed on-premises or in a cloud.

- **nFactor authentication framework:** Citrix Gateway provides a robust nFactor authentication framework that allows IT to authenticate users based on their location, state of end user device, and more.
- **Always-on connection:** Citrix Gateway provides an always-on connection that allows a user to move from office LAN to a remote or WiFi connection without affecting the SSL VPN session. As the user transitions from office LAN to home, or public WiFi , they are automatically reconnected to their corporate networks as soon as internet access is available.
- **Integration with 3rd party authentication providers:** Citrix Gateway integrates with 3rd party authentication providers that support RADIUS, LDAP, TACACS, Diameter based mechanisms.

3. On-premises single sign-on to all SaaS and web application

In addition to being an ICA proxy and SSL VPN solution, Citrix Gateway also provides a complete single sign-on solution to SaaS and web applications. Core strengths of Citrix Gateway include:

- **Support for all federation standards:** Citrix Gateway supports SAML 2.0, OAuth 2.0, and OpenID Connect standards for federation and SSO across all SaaS applications. It also supports form-based, Kerberos, NTLM/ domain pass-through mechanisms for applications deployed onpremises.
- **Works with your existing authentication infrastructure:** Citrix Gateway integrates with 3rd party vendors like Symantec, RSA, DUO security (now Cisco), to provide multi-factor authentication options. It also natively provides a one-time password that customers can use for a second-factor.
- **Complete end-to-end visibility:** Citrix Gateway with Citrix Application Delivery Management, provide Gateway Insight dashboard that provide usage statistics as well as help troubleshoot any authentication and single sign-on issues, a user may be facing.

Feature		Citrix Gateway	Citrix Workspace Essentials	Citrix Secure Workspace Access
Citrix-managed cloud service (SaaS)			●	●
Customer-managed (on-premises or cloud deployment)		●		
Single Sign-On to all applications	**Federated Identity** Citrix provides a SAML 2.0 identity provider (IdP) to enable single signon to all SaaS applications	●	●	●
	Single Sign-on to Intranet Web Apps	●	●	●
	Zero trust-based VPN less access to intranet apps		●	●
	One URL – Portal page to access all applications	●	●	●
	Support for FAS for Citrix Virtual Apps and Desktops and Citrix Workspace	●	●	●
	Support for multiple identity providers, including Microsoft AD, Azure AD, Okta, and more	●	●	●
Citrix Analytics	**Operational Analytics** Gain insight into devices, apps, files, and networks	●	●	●
	Security Analytics	Add on	Add on	Add on

Feature		Citrix Gateway	Citrix Workspace Essentials	Citrix Secure Workspace Access
Easy desktop, application and data access Provides secure access to all desktops, applications and data from any device from a single point that simplifies the user experience.	**Secure access to virtual desktops and applications** Provides secure access to Citrix Virtual Desktops, and Apps sessions	●	●	●
	Secure access to mobile apps, web apps and Citrix Content Collaboration data with MDX Micro VPN Provides secure access to AppController delivered web and SaaS applications, native mobile applications and enterprise data.	●		
	Secure network access Full VPN support enables network level access to any server within the protected network.	●		
	Browser-only access (CVPN) Provides secure access to web applications, email and file shares using only a browser (no additional client components required).	●	●	●
	Custom Portal A customizable landing page for users to easily access all their applications, files, email and other IT resources.	●	●	●
Easy desktop, application and data access Provides secure access to all desktops, applications and data from any device from a single point that simplifies the user experience.	**User Interface localization** Localizes user interfaces in English, Spanish, French, German and Japanese.	●		
	Broad client support for receiver plugin Supports major platforms including Windows® 32- and 64-bit operating systems (including Windows 8.1), Mac® OSX 10.9, Linux, iOS and Android.	●	●	●
	Support for Workspace experience		●	●

Feature		Citrix Gateway	Citrix Workspace Essentials	Citrix Secure Workspace Access
Endpoint analysis (EPA) Ensures that devices are safe to connect to the network and users have a method to easily update their devices to meet established policies.	**Integrated endpoint scanning** Continually scans client devices to determine if client security products (antivirus, personal firewall or other mandatory corporate programs) are active. It also scans for device location, device configuration.	●		
	Enhanced device identity scans Authenticates a device by scanning for a valid company issued device certificate	●		
	Quarantine groups/remediation Provides clients that fail endpoint analysis scanning with limited access to remediation sites to bring these devices into compliance with the organization's security policies	●		
	Advanced endpoint analysis Advanced endpoint analysis capabilities using industry-standard APIs like OPSWAT	●		
Apply security policies and controls	**Cloud App Control for SaaS and web applications** Gain control over how their users access and interact with SaaS apps. Capabilities include the ability to restrict copy/ paste, printing, watermarking, restrict downloads, and more. App Protection policies protect SaaS and web apps against keylogger and screenshot malware.			●
Security policies to control users access to Internet content	**Web filtering** Block users from accessing risky sites that may infect their network with malicious software			●
Balance productivity and security with web isolation or isolated browser	**Cloud-based web isolation protects against web threats** Isolate browsing from the company network, protecting from web-based threats. No files or data will reach the corporate network and copy and paste is controlled by policy, keeping possible attack contained in the cloud.			●
Multi-Factor Authentication	Support MFA with RADIUS (and 3rd party integrations)	●		
	Native one-time password (OTP)	●	●	●

Feature		Citrix Gateway	Citrix Workspace Essentials	Citrix Secure Workspace Access
Scenario-based policy control (SmartAccess) Provides controls, to configure the most secure access to data and applications by dynamically adjusting access based on EPA scan results and the user identity/group information	**Adaptive Secure Workspace Access for virtual hosted applications and desktops** Provides dynamic Secure Workspace Access to resources based on EPA results. The session is terminated if the EPA scans fail during a session.	●		
	Adaptive application and action control Controls the behavior of Citrix Virtual Desktops and Apps sessions by preventing operations like print, copy/ paste etc. if accessed using a personal/ insecure device.	●		
SmartControl	**Centralized Policy Management** Provides centralized application policies for Citrix Virtual Desktops and Apps environments	●		
Monitoring and Visibility	Monitor and troubleshoot network latency for Citrix Virtual Apps and Desktop sessions (HDX Insight) with Citrix Application Delivery Management (Citrix ADM)	●		
	Monitor application usage, and troubleshoot authentication issues for end users (Gateway Insight)	●		
Application and data security Protects and keeps private all data transmitted between the client and the datacenter.	**Standards-based security** Ensures that all communications are secure through the use of SSL/TLS encryption.	●	●	●
	MDX MicroVPN Ensures secure access to web and mobile application content hosted in the data center with per-app VPN connections rather than full device-level tunnels	●	○	○
Application and data security Protects and keeps private all data transmitted between the client and data center	**Split tunneling control** When turned ON, Citrix Gateway intelligently classifies internal/ protected network traffic from Internet traffic and tunnel only the internal/protected network traffic through SSLVPN. Internet traffic does not go through the SSLVPN tunnel. When turned OFF it enforces both internal/ protected network traffic as well as public Internet traffic to go through the SSL/ VPN tunnel.	●		
	VPN-less access to intranet apps		●	●
	SSO to SaaS and virtual apps and desktops	●	●	●
	Browser cache cleanup Removes objects and data cached on the local browser once the SSL VPN session is terminated.	●		

Feature		Citrix Gateway	Citrix Workspace Essentials	Citrix Secure Workspace Access
High Availability/ Fault tolerance Creates secure access deployments that guarantee a high level of availability and reliability	**Basic high-availability configuration** Links gateway appliances to create an active-passive pair, ensuring sessions remain active if the master fails.	●	●	●
	Global server load balancing (GSLB) Routes client connections to the best VPN site based on availability, health, proximity and responsiveness. This feature is only available in Citrix Networking Enterprise and Platinum editions.	●	●	●
Simplified administration Maximizes the efficiency of the IT organization by simplifying common installation and management tasks.	**Centralized administration using** Citrix Application Delivery Management Configures and manages Citrix Gateway appliances from a single command center console	●		
	Wizard-driven configuration Provides an intuitive series of click- through screens and simple instructions to guide administrators through installation and configuration	●		
Simplified Administration Maximizes the efficiency of the IT organization by simplifying common installation and management tasks	**Multiple VPN servers** When A single appliance can emulate multiple SSL VPNs by hosting one or more virtual servers, each with a unique IP address, FQDN and certificate	●		
	Administrative auditing Monitors all configuration changes made by administrators to ensure accountability and easy rollback of configuration errors using command center.	●		
	Auto-downloading/Auto-updating client plug-in Automatically downloads the Citrix Gatewayvplug-in when the user connects to Citrix Gateway, and ensures that the user always receives the latest version of the client software. (Workspace App in case of Citrix Workspace Essentials and Citrix Secure Workspace Access)	●	●	●
	Agentless access to apps		●	●
	Support for automated distribution of Citrix Gateway plug-in Simplifies client installation by allowing deployment of the Citrix Gateway plug- in through systems and client management solutions.	●		
	Data entitlements Data consumption by end user, but can be shared across user base	N/A	1 GB per user/ per mo.	10 GB per user/ per mo.

◒ Supported with Gateway on-premises as identity provider for Citrix Workspace

○ Supports only Citrix Secure Mail and Citrix Secure Web

Platform Specifications

For platform specifications for Citrix Gateway, please refer to our Citrix ADC datasheet Notes

Notes

1. Citrix Secure Workspace Access is sold as part of Workspace Premium and Premium Plus packages only. Citrix Analytics for Security may be purchased as a standalone add-on.
2. Customers need to purchase a universal license for adding CCU users for SSL VPN and SSO sessions, if using Citrix Gateway. For Citrix ADC/Gateway versions after 11.1, the Standard edition includes (500) Universal licenses, Enterprise or Advanced editions include (1000) Universal licenses, and there are no Universal license requirements with Platinum or Premium editions. For versions previous to NetScaler ADC 11.1, the Standard and Enterprise editions include (5) Universal licenses, and the Platinum edition includes (100) Universal licenses.
3. Maximum no. of SSL VPN users on a VPX appliance is based on various parameters like underlying hardware, licensing etc.
4. HDX Insight is available with NetScaler MPX/SDX/ VPX appliances running NetScaler EE or PE license. Customers will be required to use Citrix Application Delivery Management (Citrix ADM) to see this information.
5. Customers can get up to 35,000 concurrent users per appliance by using Citrix ADC/ Gateway appliances. For more information, please refer to the Citrix ADC datasheet. Citrix ADC datasheet.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States