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

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

Citrix Access Control

Citrix Access Control service provides instant single sign-on to SaaS, and enterprise web applications. It also provides security controls for SaaS and web applications to control what actions users can take once they successfully login. These actions include things like ability to copy/paste, print a page, apply watermarks on SaaS and web pages. This provides data governance on SaaS applications and protects against insiders looking to steal information inside these applications. It also provides web isolation for customers looking to access the internet in a secure and locked down environment that protects them from browser-based attacks. Along with Citrix Analytics, the solution provides security tools and analytics that help IT easily manage user access and actions on cloud and SaaS applications while reducing the risks of internet browsing seamlessly.

Citrix Gateway Service

Citrix Gateway Service provides a secure remote access solution delivering a unified experience into SaaS apps, heterogeneous virtual apps and desktops, all delivered through the cloud and managed by Citrix.

Citrix Gateway

Citrix Gateway is a customer-managed solution that can be deployed on-premises or on any public cloud, such as AWS, Azure, or Google Cloud Platform. It comes in hardware, virtual, and containerized form factors (IR). 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 Access Control – Common Use Cases

Citrix Access Control 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 Access Control include:

1. Single sign-on and data governance for SaaS, web, and virtual apps

End users are accessing a wide range of SaaS, web, and virtual apps to stay productive. Each of these apps require a separate log-in and password, which proves too much for those end users to handle. This leads to poor password practices, including using the same password for multiple services, recycling passwords, or writing them down on a piece of paper.

Citrix Access Control enables single sign-on for your end users web, SaaS, and virtual apps, helping them to effortlessly navigate the apps they need to stay productive while keeping your data secure.

The modern workplace has become powered by SaaS apps, with large enterprises using nearly 125[1] of them to effectively run their business . End users love the anywhere, anytime access because it helps them stay productive no matter where they are. IT benefits from lower management costs, scalability, and simplified upgrades. However, securing them and preventing data exfiltration has proved challenging for IT, as they don't have the same level of control and oversight into SaaS apps as they would over on-premises apps.

Citrix Access Control enables IT to effectively protect the data that lives in SaaS and web apps while still providing end users with a best-in-class experience. Policies that include restricting clipboard access, printing, and downloading, among others, ensure that IT has the control and oversight they need to successfully prevent against data leakage from SaaS apps.

2. Control user access to the Internet with web filtering policies

While many of the SaaS apps that make their way into the enterprise are sanctioned by IT, some departments choose to buy and use an app without approval, creating a data leakage risk. Additionally, users put the entire organization at risk by browsing risky websites on corporate devices and networks. While it would be simple to just block access to a wide range of unapproved sites, this can be a productivity killer as end users are unable to access information and services they need to be successful in their role.

Citrix empowers IT apply security policies to SaaS apps, even if they've been deployed without their knowledge. Secure browsing gives the flexibility to block access to risky websites that may inject malware into corporate devices or networks, or to deploy a cloud-based browser that allows end users to access potentially dangerous sites without posing a risk to the network. While Citrix Access Control increases the security posture of your organization, it can also solve browser compatibility issues that end users may face when accessing the SaaS apps they need to stay productive.

3. Accessing the internet using an isolated and locked browser environment
With the rising amount of ransomware, malware and data theft attacks originating from users browsing the internet, organizations are looking for solutions to segregate the high-risk web traffic and execution of web code away from the internal, trusted network. IT must be able to provide users with secure access to run a browser in the cloud, while still maintaining control. Because all internet browsing is external, a secure browser solution reduces the risk of attack. The user receives a consistent browser experience, but without unwittingly introducing potential threats into the corporate network. By isolating internet browsing, IT administrators can offer end users safe internet access without sacrificing security.

Citrix Gateway Service– Common Use Cases

Citrix Gateway Service provides secure remote access solution with diverse Identity and Access Management (IdAM) capabilities, delivering a unified experience into SaaS apps, heterogeneous Virtual apps and Desktops, and so forth. Customers who choose Citrix Gateway Service 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 access controls and multi-factor authentication, IT can maintain productivity and end-to-end oversight across all application traffic.

2. ICA proxy to on-premises deployments of Citrix Virtual Apps and Desktops
ICA proxy is the most secure and optimal way for end users to access Citrix Virtual Apps and Desktops. This empowers IT to provide VPN-less access for those users to reach their business-critical virtual apps and desktops.

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 access control 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.
- **End-to-end performance visibility -** Included with Citrix Gateway and Citrix Application Delivery Management is HDX Insight, a dashboard to monitor how Citrix apps are performing over your existing networks. This is something no other solution provides today.

2. SSL 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 to a 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. 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 on-premises.
- **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 Gateway Service	Citrix Access Control[1]
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 sign-on to all SaaS applications	✓	✓	✓
	One URL – Portal page to access all applications	✓	✓	✓
	Support for FAS for Citrix Virtual Apps and Desktops	✓		
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			✓
User Behavior Analytics[1]	**Citrix Analytics** Gain insight into devices, apps, files, and networks to identify and take automated action against risky end-user behavior.			✓
Monitoring and Visibility	Performance Monitoring for Citrix Virtual Apps and Desktops (HDX Insight) with Citrix Application Delivery Management (ADM)	✓		
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, Apps, and Endpoint Management ICA sessions without requiring a VPN connection.	✓	✓	✓
	Secure access to mobile applications, web applications 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.	✓		
	Secure browser-only access (CVPN) Provides secure access to web applications, email and file shares using only a browser (no additional client components required). *Tech preview only*	✓	✓	✓
	Custom Portal A customizable landing page for users to easily access all their applications, files, email and other IT resources.	✓	✓	✓

Feature		Citrix Gateway	Citrix Gateway Service	Citrix Access Control
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		✓	✓
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 (anti-virus, 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 to SaaS applications	**Enhanced security policies for SaaS and web applications** Gain control over how their users access and interact with SaaS apps while giving them security controls to prevent data exfiltration. Capabilities include the ability to restrict copy/paste, printing, watermarking, restrict downloads, and more.			✓
Balance productivity and security with a web isolation/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 Gateway Service	Citrix Access Control
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 access control for virtual hosted applications and desktops** Provides dynamic access control 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 datacenter with per-app VPN connections rather than full device-level VPN tunnels.	✓		

Feature		Citrix Gateway	Citrix Gateway Service	Citrix Access Control
Application and data security Protects and keeps private all data transmitted between the client and the datacenter.	**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 SSLVPN tunnel.	✓		
	Browser cache cleanup Removes objects and data cached on the local browser once the SSL VPN session is terminated.	✓		
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	✓	N/A	N/A
	Wizard-driven configuration Provides an intuitive series of click-through screens and simple instructions to guide administrators through installation and configuration.	✓	N/A	N/A

Feature		Citrix Gateway	Citrix Gateway Service	Citrix Access Control
Simplified Administration Maximizes the efficiency of the IT organization by simplifying common installation and management tasks	**Multiple VPN servers** 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 Gateway plug-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 Gateway service and Citrix Access Control)	✓	✓	✓
	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	1 GB per user/ per mo.	1 GB per user/ per mo.	10 GB per user /per mo.

Platform Specifications

For platform specifications for Citrix Gateway, please refer to our Citrix ADC datasheets as below:

1. **For hardware appliances**
2. **For virtual appliances (includes appliances for cloud platforms)**

Notes

1. CItrix Access Control and Citrix Analytics are sold part of Workspace packages only (Workspace Standard, Workspace Premium and Workspace Premium Plus).
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, licensingetc.

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.

6. Learn more in the Resource Library