Securely deliver digital workspaces

Strengthen security and compliance – down to the endpoint – while delivering a satisfying, consistent user experience with virtual, SaaS, and web applications.
Dynamically control user access and actions and defend against cyberthreats while delivering a high-performance experience

Citrix ADC (application delivery controller) addresses multiple networking challenges facing government agencies – with a single solution:

• **Security.** Protect apps and services against cyberattacks and deliver secure, remote access for employees, contractors, and partners.

• **Compliance.** Meet current or anticipated requirements for FIPS 140-2 compliance.

• **Performance.** Accelerate app performance for users in demanding scenarios, including remote locations, poor connectivity, and multimedia apps.

• **Availability.** Make sure applications – especially public-facing web apps – remain highly available to users during peak usage periods or business interruptions.

• **Experience.** Simplify access to multiple applications and maintain a consistent experience across geographies and devices.

Citrix ADC is a comprehensive solution for protecting, controlling, managing, and optimizing apps and services. It is the ideal front end for:

• Citrix Virtual Apps and Desktops environments

• Web applications

• Database applications

**How it works**

Citrix ADC is deployed in front of server infrastructure for virtual apps and desktops, web apps, and database apps. It delivers advanced access and data control features, multi-layer threat protection, and security management capabilities. More than a powerful security and compliance solution, Citrix ADC also helps IT managers substantially improve the availability and performance of applications.

Citrix ADC is available as a single or multi-tenant hardware appliance or a flexible, software-based virtual appliance. It works seamlessly with Citrix SD-WAN, which optimizes app performance over the WAN for branch and mobile workers.

Now, let’s look at how Citrix ADC handles networking use cases often encountered by government IT teams.

**At a Glance**

As security threats grow and compliance requirements become stricter, your government organization may find it harder to meet worker needs for flexible access to applications and data. It seems the more you tighten security, the more restrictive the work environment becomes. But this outcome isn’t inevitable. Citrix ADC allows you to strike the best balance between data protection and employee productivity in each user scenario. Plus, this versatile solution load-balances local and global servers for high availability; supports single sign-on (SSO) for simplicity; optimizes performance across poor connections and low bandwidth; and provides secure, remote application access.

**Key Benefits**

• Improved compliance through context-aware endpoint controls

• Protection against network- and app-layer threats

• High availability with load balancing/global server load balancing (GSLB)

• Fast performance over bandwidth-constrained networks

• Streamlined SSO access to virtual, SaaS, and web apps

**Verifying endpoint compliance**

The popularity of mobile work, telework, and bring-your-own-device (BYOD) programs means IT organizations struggle to control application access on untrusted devices and connections. On the one hand, employees need certain functionality to work effectively. On the other, IT must be sure that user devices and connections are secure.

Citrix ADC solves this dilemma with powerful, policy-based management of user access and actions.

_**Endpoint Analysis (EPA) allows Citrix ADC to scan the user device for required security measures (such as antivirus and the latest software patches) and determine**_
user location and identity. Based on the results, EPA technologies including SmartAccess and SmartControl determine what resources the user can access, and which actions are allowed – such as printing, saving, and downloading.

Because EPA technology is contextual, the type and extent of access will change based on the situation. For instance, if a user’s device, location, or identity do not pass muster, Citrix ADC can refuse to allow full VPN access and instead limit the individual to the Citrix protocol, which delivers only an image of the application interface.

EPA is delivered through Citrix Gateway, a single, secure point of access to applications and data that is a key feature of Citrix ADC.

Protecting against threats
Government agencies must constantly guard against cyberattackers and fraudsters attempting to steal citizens’ personally identifiable information or other confidential data. As the front end for government servers, Citrix ADC provides strong protections against cyberthreats, including:

Network-layer shielding: Firewall functionality (provided by the integrated Citrix Web App Firewall) enables the solution to stop unauthorized and potentially malicious traffic from gaining access.

Application-layer shielding: The firewall defends against a wide range of pervasive application-layer threats, such as SQL injection, cross-site scripting, and buffer overflow attacks.

Optimizing server availability
Most agencies operate public-facing websites that citizens depend upon for information, transactions, application submissions, and other needs. These platforms must remain available even when high traffic volume puts stress on the network – such as during peak enrollment periods. Another challenge is maintaining server availability during an interruption, so employees can continue serving the public throughout a crisis or disaster.

Citrix ADC helps ensure high availability and performance of applications:

Multi-layer protocol shielding: Citrix ADC thwarts attacks that rely on perversion of common protocols by validating and enforcing rules for acceptable usage.

Load balancing and GSLB technologies direct requests to the least-busy server.

In the event of a data center failure, Citrix ADC can automatically redirect traffic to a secondary site, with no interruptions for users.

Improving the user experience
Network latency can reduce productivity and cause frustration among remote and mobile...
government workers, such as scientists, engineers, aid workers, and military personnel in the field.

**Citrix ADC** accelerates application performance over the network through technologies including caching, compression, and TCP optimization.

Based on policies, it can prioritize different types of traffic (such as real-time audio and video) by associating them with individual virtual channels within the Citrix protocol.

**About Citrix ADC**

This award-winning ADC features unmatched security, superior L4-7 load balancing, reliable GSLB, and increased uptime. It helps control costs by scaling capacity up when you need it and down when you don’t—and you can even share capacity across instances on premises and in the cloud.

---

**Customer Use Case**

**U.S. Department of Defense organization**

**PROFILE:**

Plays a major role in human health and safety nationwide and internationally

**CHALLENGE:**

Securely deliver access to internal systems to users anywhere in the world, on government-issued and BYO devices, and over secure and non-secure connections including satellite and LTE.

**RESULTS:**

Citrix Gateway provides flexible access including full VPN, clientless VPN, and Citrix HDX connections. Endpoint Analysis strengthens security by determining each user’s location and device type/encryption level, and then connecting them to the appropriate access point based on device requirements and security level.