Putting the “Security” in Secure Remote Access

Learn how Citrix ADC delivers a comprehensive secure remote access solution for your application environment
Citrix ADC is not only a leading Application Delivery Controller (ADC), but also a secure remote access solution that provides security and compliance beyond the corporate network to users that are accessing their Citrix Workspace, as well as other applications, from anywhere, on any device. Citrix ADC addresses the challenges organizations have with securing the endpoint and ensuring compliance outside the data center. Because it incorporates the capabilities to support all types of remote access scenarios including VDI, Web, Enterprise, Mobile and SaaS applications, from a single platform via one URL through a unified workspace experience, ADC not only eliminates the need to implement additional gateways, but also provides an opportunity to consolidate a wide range of existing remote access solutions and deliver a single sign-on experience for end users. Leveraging Citrix ADC in this capacity enables CIOs to substantially improve employee productivity and end-user satisfaction, while reducing the TCO and complexity of their remote access infrastructure and associated operations.

This white paper explores the core strengths that makes Citrix ADC, THE choice for remote application security requirements including contextual security, single sign-on across applications and end-to-end application visibility. These security capabilities empower IT to deliver secure digital workspaces to all users—on any device, from anywhere, over any network.

The Security Challenge with “Secure Remote Access”

User authentication and encrypted tunnels are well—recognized, long—standing staples for ensuring the confidentiality and integrity of remote access sessions (and data) traversing untrusted networks. When remote access deployments were limited to a well-defined subset of an organization’s employees using corporate-managed devices to reach a handful of applications, these basic VPN technologies were even deemed sufficient. Little else, if anything, was considered necessary from a security perspective.
These days, however, the remote access landscape is much different. More often than not, IT departments are now under pressure to enable remote access for any user, operating in any location with any type of device, to any type of resource—including enterprise web, mobile, cloud/SaaS and client-server applications, hosted desktops and data. Establishing comprehensive protection for this greater (and still growing) set of remote access use cases requires thinking about security in a more holistic manner. One helpful approach is to consider the need for security across three distinct dimensions:

- **The Physical Dimension.** In addition to the access network, other components of the end-to-end path requiring attention include the client device, enterprise network and accessible systems, apps and data. Not to be overlooked, too, is the security of the access gateway itself, as well as any “downstream” resources that become accessible as a result of having obtained access to the enterprise network—such as cloud/SaaS apps.

- **The Logical Dimension.** Providing protection for network-level protocols and services is really only a starting point. Many threats today are capable of completely bypassing controls that operate solely at this level. Establishing comprehensive protection, therefore, also requires paying attention to higher layers of the computing stack—most notably those pertaining to individual applications, associated business logic and the data itself.

- **The Functional Dimension.** Having defenses that combine multiple security technologies, methods and mechanisms is essential to thwarting today’s multi-vector threats. Beyond user authentication and network/transport encryption, other types of security countermeasures that require attention include: dynamic access control, DDoS protection, data security, and malware/advanced threat detection.

**Citrix ADC: The Ultimate Remote Access Security Blanket**

Citrix ADC is a secure and unified front-end for all applications that provides administrators granular application and device-level control, while enabling users to single sign-on across all applications from one URL, and giving them access to these applications from anywhere, and by using any device. Built on top of the market-leading Citrix ADC application delivery platform, Citrix ADC combines an extensive portfolio of remote access security features with a powerful set of broader, data center security capabilities to deliver the complete multi-layer, multi-function, end-to-end protection that today’s complex remote access deployments require.
Comprehensive User and App-Centric Access Management

For Citrix ADC, providing end-to-end protection begins with enabling granular control over which users and devices are able to access specific resources under different operating conditions. With a combination of powerful proxies, discrete tunneling options and adaptive user and app-centric controls at their disposal, IT administrators can render risky, loose-putting, one-size-fits-all security policies and access mechanisms—and the legacy solutions that require them—a thing of the past.

Identity-Based Access Control

Citrix ADC serves as an authentication and authorization proxy that not only delivers a powerful layer of protection but also helps standardize this part of the access experience for users who, historically, have had to navigate an inconsistent morass of mechanisms and policies when trying to obtain access to different types of resources.

With Citrix ADC, all inbound application requests are blocked until the identity of the corresponding user and their device is validated. Access is then strictly confined to those parts of the enterprise network and the specific applications for which each individual user is authorized. To maximize compatibility with existing identity and access management tools and protect investments, Citrix ADC provides SAML 2.0 federated identity and supports extensive set of authentication mechanisms including local authentication, RADIUS, LDAP, TACACS, Digital Certificates, NTLM and Kerberos constrained delegation. Enabling single sign-on (SSO) to all web, cloud, Citrix Virtual Apps and Desktops resources further simplifies and enhances the user experience.

Multi-Factor Authentication

User identity and role-based application access control are paramount to security; however, this should not force end users to maintain a long list of credentials leading to security risks and a deteriorating experience. Taking a compromised approach either on security or on experience will lead to direct negative impact on the business outcomes.

IT needs a way to authenticate these different group of users in different ways. Adaptive multi-factor authentication and group based authorization ensure user identity is verified before providing access to any applications or data. This ensures different stakeholders such as employees, partners, vendors and others gain the right access to apps and data from a variety of locations and using a variety of devices. While different gateways can be used for different groups of users, the maintenance and consistency in experience is negatively impacted with this approach. Citrix ADC provides a very powerful authentication infrastructure that provides capabilities to create flexible and policy-driven authentication schemas.

IT can fine-tune the authentication schemes for various user groups using the same gateway endpoint (or FQDN for all users). This allows IT administrators to manage all users from single point of entry, thereby enhancing control and monitoring capabilities while reducing operational and infrastructure costs. Citrix ADC has comprehensive single sign-on capabilities that provide a seamless experience for end users for any type of application located anywhere (on-prem, hybrid or multi-cloud, etc.). Using these capabilities, IT can extend Citrix ADC to access any application including Citrix technologies.

Dynamic Access Control and Centralized Policy Management

A combination of endpoint analysis capabilities and the innovative SmartControl feature set enables administrators to avoid the limitations of fixed access control policies and instead provision remote access services that automatically adapt to changing conditions.
**Endpoint Analysis (EPA).** Integrated endpoint scanning establishes whether client devices are in compliance with enterprise security and management policies, such as having the latest versions of their respective operating systems, anti-virus software, client firewalls, hard-drive encryption utilities are present, running and up-to-date and all software patches installed. For devices that fail these checks, access can be restricted to a limited set of applications and data or pre-defined remediation zones where users can obtain the tools needed to bring them into compliance.

**SmartControl.** With SmartControl, administrators can now manage user policies from Citrix ADC console. The policies are enforced in the DMZ as opposed to in the Intranet and improves security at the network edge. With SmartControl, Citrix ADC assigns the access privileges and a layer of restrictions are created at the network level before reaching the Citrix Virtual Apps and Desktops environment. This made Citrix ADC the secure gateway giving it the ability to determine how much access users need. SmartControl can override any individual settings on the Citrix Virtual Apps and Desktops farms, depending on which is the more sensitive in nature. Because Citrix ADC includes in-depth knowledge of the ICA protocol, administrators can even control actions of Citrix Virtual Apps and Desktops users that might be considered risky in certain situations, such as local print, copy, paste and save-to-disk operations. IT administrators can configure one rule that allows a strongly authenticated mobile salesperson using a corporate device access to the full suite of hosted sales tools, while a second rule limits members of the sales team using password-only authentication from unknown devices to a Citrix Virtual Apps-hosted app for generating and managing proposals.

**Secure Tunneling Options and Controls.** All access sessions are protected from eavesdropping by standards-based SSL/TLS encryption. With the classic SSL VPN capability (latest industry standards for SSL encryption capabilities), the resulting tunnel can be used to provide access to a broad set of resources, including entire networks. Alternately, administrators can use the solution’s innovative MicroVPN feature to define a secure tunnel for a single, designated application. This approach inherently restricts the reach of client devices, thereby limiting the impact of any that might be compromised. Closely related split tunneling and browser cache controls provide yet another important

---

**Figure 2: Citrix ICA connection**

![Citrix ICA connection diagram](image-url)
layer of data protection. With the basic split tunneling feature, users are blocked from accessing any other network (or networked resource such as a printer) for the duration of their remote access session. Available as a pre-defined configuration option, an enhanced alternative instead blocks access to the Internet and other networks while still allowing access to services on a client’s local subnet (e.g., print and file shares). The browser cache cleanup feature, on the other hand, ensures that all objects and data are flushed from local browser cache immediately upon completion of each and every access session.

Mobile Application Management and Mobile Device Management

Citrix ADC provides integration with two major MDM/MAM vendors, i.e. Citrix Endpoint Management and Microsoft Intune.

Citrix Endpoint Management

Together with Citrix ADC, Citrix Endpoint Management offers a complete end-to-end FIPS 140-2 compliant solution for all data in transit and at rest. Citrix Endpoint Management and Citrix ADC provide the ability to scale, ensure high availability for apps and maintain security while reducing mobility deployment and management costs. Through Active Directory integration, Citrix Endpoint Management and Citrix ADC provide a solution that supports SSO (Single Sign On) capabilities and access to all apps with a single one-time PIN number. Citrix ADC delivers an extensive portfolio of essential datacenter security capabilities that are significant for mobile users, their apps and data. Citrix ADC provides critically important application security, network/infrastructure security, and identity and access management, which when combined with Citrix Endpoint Management, delivers a tightly coupled solution that enables IT to support the security needs of mobile users and the enterprise. Citrix ADC provides Micro VPN support for Citrix Endpoint Management Apps and, enterprise (in-house) apps wrapped with MDX, MDX technology enables business apps on user end point devices to tunnel securely back to corporate networks via an on-demand application VPN connection, ensuring that non-corporate apps have no visibility into this enterprise tunnel. Citrix ADC allows configuring forward proxy that is leveraged by Citrix Endpoint Management. Using this feature, you can monitor and analyze web traffic through Citrix ADC for corporate compliance and user behavior. It also allows setting up access control policies for users, logging of all denials, and users trying to access web sites not meeting corporate compliance.

Microsoft Intune

Citrix and EMS integration allows organizations to harness the power of Citrix ADC and Microsoft Intune to help IT control access to on-premises data and resources, while still enabling people to do their best work from any device. This integration gives you on-premises conditional access—allowing you to set policies to ensure that only managed and compliant devices can connect to your on-premises corporate network.

Compliance policy settings in Microsoft Intune evaluate the compliance of employee devices against a set of rules you create. As a first check, Citrix ADC captures the device ID to check if the device is enrolled and compliant with Microsoft Intune. If the end-user device is not enrolled or in compliant status, Citrix ADC redirects the user to the Intune enrollment process. An Intune agent will guide the user to complete the enrollment process and maintain the end-user device status with Intune. When the user comes to Citrix ADC again, device state will be verified before access is granted, thereby enforcing the conditional access policies.

When you combine a device-compliance policy with conditional access, only authorized users will gain access, and only from compliant devices. The integration of Citrix ADC and Microsoft EMS provides a cost-effective solution with conditional access and improved end-user device security.
Powerful Proxies

Embedded proxies deliver unparalleled application-specific control and protection.

ICA Proxy. An integral proxy for ICA—the communication protocol for Citrix Virtual Apps and Desktops—enables Citrix ADC to secure and optimize associated remote access sessions like no other solution available in the market. While alternatives suffer from incomplete and outdated efforts to reverse-engineer ICA functionality, Citrix ADC benefits from intimate knowledge of the protocol and the ways Citrix Virtual Apps and Desktops are designed to use it. One result, for example, is the ability for administrators to set and enforce policies for individual app-level functions such as local printing and copy/paste.

ActiveSync Proxy. Citrix ADC can also serve as a termination and policy enforcement point for inbound ActiveSync traffic (used to enable native email services for mobile clients). The embedded ActiveSync proxy provides an important layer of protection for back-end Exchange servers and allows administrators to control email access based on a wide variety of parameters, such as whether the associated device is jail broken, in an undesirable geographic location, or out of compliance in some other way. The ability to leverage client-side certificates further enhances security by eliminating the need to cache Active Directory credentials on each mobile device requiring native email access. Similar proxy coverage and security capabilities are also available for RDP- and PCoIP-based services and applications.

Powerful Security Monitoring and Management

Equally important to its extensive access management capabilities are the powerful security monitoring features of Citrix ADC that allows IT to quickly pinpoint and resolve user logon and gateway issues that may arise without negatively impacting user productivity.

Citrix Application Delivery Management Gateway Insight

As part of Citrix Application Delivery Management, Gateway Insight provides specific Citrix ADC statistics and analytics in a centralized console. It provides specific HDX protocol monitoring information relevant to the Citrix ADC. Gateway Insight provides visibility into issues related to user authentication and authorization to any application via Citrix ADC including failures encountered by all users at the time of logging on to Citrix ADC. It provides visibility into all login and app-launch issues for the user. Gateway Insight leverages AppFlow data to provide visibility into data for the errors that users encounter when logging onto the Citrix ADC, regardless of the access mode. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity. IT can get details on user sessions as they pertain to endpoint analysis, authentication, SSO, application launches, active sessions and termination reasons. Identifying login and authentication failures helps improve IT help desk troubleshooting and SLAs.

Comprehensive Threat Protection

As powerful as they are, however, providing granular control over access to networked resources and robust security management capabilities are only two parts of the equation for end-to-end protection. Companies today require a comprehensive security solution that provides multi-vector threat protection, insight, and analytics. With Citrix ADC, organizations also benefit from an extensive set of security capabilities focused on the direct prevention and mitigation of numerous types of threats targeting organizations today.

For more details on Citrix ADC comprehensive security please refer to the white paper “Citrix ADC - a Foundation for Next-Generation Datacenter and Cloud-based Security.”
Conclusion

Put the brakes on the proliferation of access methods and infrastructure that is commonplace among organizations today. Citrix ADC can offer multi-dimensional security and protection by providing granular control over access to networked resources, robust security management capabilities as well as an extensive set of security capabilities focused on the direct prevention and mitigation of numerous types of threats targeting organizations today.

Start your security journey with Citrix and find out more by going to: www.citrix.com/it-security.

For further information on consolidation, read Consolidate Your Secure Remote Access Delivery Infrastructure with One URL click here.