White Paper

Securing virtual desktop infrastructure with Citrix ADC

Learn how Citrix ADC delivers business-critical security capabilities to advance the many benefits of virtual desktops.

Today's modern enterprises are rapidly adopting app and desktop virtualization as a way to reduce operating costs, enable workplace flexibility, increase business agility, and bolster their information security and compliance posture. Actually realizing these benefits depends, however, on ensuring the security, availability and visibility of the virtual desktop infrastructure. This paper explains how Citrix ADC has been designed to meet these requirements. By integrating an extensive set of advanced access and action control features, multi-layer threat protection mechanisms, powerful security management and a wealth of additional network delivery capabilities, Citrix ADC not only preserves the benefits promised by virtual desktops, it maximizes them.

The security conundrum with app and desktop virtualization

Migrating from traditional desktop deployment and management approaches to virtual desktop technologies offering centralized management is a key initiative for many enterprises. Indeed, Gartner expects adoption of hosted virtual desktops (HVDs) for installed base (total users) alone to exceed 53 million users by 2017[1.] Driving this growth is a compelling set of benefits. With a full-featured app and desktop virtualization solution, enterprises can substantially and sustainably reduce desktop ownership and operating costs, enable complete workplace flexibility and increase business agility by providing rapid support for strategic initiatives such as mergers and acquisitions, geographic expansion and dynamic partnership arrangements.

Another major advantage of app and desktop virtualization is that it significantly strengthens an organization's information security and compliance posture by centralizing all data and applications in the corporate datacenter. Because users view and manipulate their desktops remotely, there is no need to distribute or store potentially sensitive material to their local devices. At the same time, maintaining centralized control over desktop applications and operating systems not only makes it easier for IT to pursue standardization that reduces complexity, cost and an organization's attack surface, but also boosts the ease, speed and thoroughness of implementing updates and security

[1] Forecast: Hosted Virtual Desktops, WW, 2014 Update," Gartner, December 2014

patches. With a centralized administration model, granting and revoking access rights and privileges is also quick and efficient.

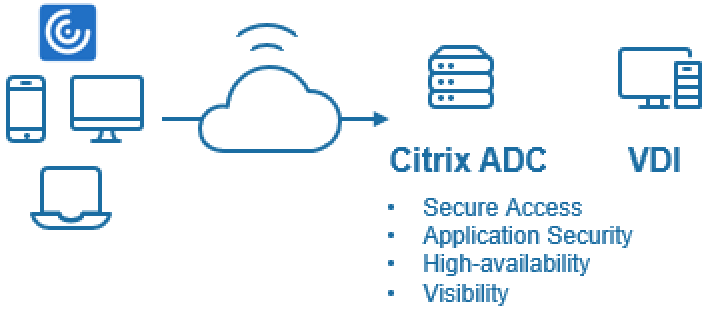
Although app and desktop virtualization has a lot to offer today's enterprises, preserving potential gains – including the security advantages of a centralized deployment and administration model – depends on ensuring the security of the associated virtual desktop infrastructure (VDI) and the datacenter within which it resides. This may sound a bit circular—organizations must invest in one set of security measures to effectively gain the benefits of the second—but that's exactly the point. In order to realize the desktop and data security benefits of virtual apps and desktops, it's critical to make sure that the VDI itself is secure. Indeed, a few aspects of app and desktop virtualization that require particular attention include:

- ***Remote access.*** With enterprise mobility and telecommuting initiatives on the rise, a substantial percentage of users are likely to require access to their apps and desktops from a remote location, and often over an insecure public network.
- ***Device proliferation.*** Consumerization of IT has sparked the need to support a rapidly expanding portfolio of client devices with widely varying security characteristics and profiles. Further complicating matters is the fact that most of these devices are no longer owned or controlled by the enterprise. The crucial point to acknowledge is that even though app and desktop virtualization can eliminate local retention of sensitive data, a compromised client device still poses a threat. Sensitive data can still be viewed and the rights attributed to the user/device can still be exploited
- ***Extent of access.*** With desktop virtualization, users obtain access not only to the applications and data "resident" on their virtual desktops, but also to any networked resources – such as databases, the Internet or SaaS applications – to which those desktops in turn have access. This elevates the importance of security in general, and access control in particular.
- ***Concentration of resources.*** The importance of robust defenses is also elevated because app and desktop virtualization involves putting many of an organization's eggs in a single basket. In contrast to the conventional, distributed model of desktop computing, a single successful attack now has the potential to impact a substantial number of users and desktop systems.

There is also the big picture to consider. Today's hackers are highly organized and motivated to do damage and make off with valuable data. As a result, robust defenses are generally required, if for no other reason than to provide protection from an increasingly sophisticated and hostile threat landscape.

How can Citrix ADC help

Citrix ADC is deployed in thousands of networks around the globe to optimize, secure and control the delivery of all enterprise and cloud services, and to maximize the end user experience across all device types. As such, it is also the ideal solution for front-ending an organization's app and desktop virtualization infrastructure. Particularly relevant in this case are the numerous security mechanisms and features that Citrix ADC delivers to help protect VDI. These are grouped into three distinct categories - - access security, threat protection and security management – and work together to address each of the aforementioned issues requiring attention.



User and app-centric access security

For Citrix ADC, protecting an organization's VDI begins with enabling granular control over which users and devices are able to access which specific virtual desktops under different operating conditions. Offering a combination of adaptive user and app–centric controls and discrete tunneling options. Citrix ADC allows IT administrators to lock down their virtual desktop and app resources like never before.

Identity based access control

Citrix ADC serves as an authentication and authorization proxy that not only delivers a first, 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.

All inbound session 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 virtual desktops for which each individual user is authorized. To maximize compatibility with existing identity management tools and investments, support is available for an extensive set of authentication mechanisms, including local authentication, RADIUS, LDAP, TACACS, certificates, NTLM, SAML2 and Kerberos.

Dynamic access control

A combination of endpoint analysis capabilities and the innovative SmartControl feature set enables administrators to avoid the limitations and risks of rigid, one-size-fits-all policies and instead provision services for accessing virtual desktops (and other resources) that automatically adapt to changing conditions.

Endpoint analysis.

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 and all software patches installed. For devices that fail these checks, access can be restricted to pre-defined remediation zones where users can obtain the tools needed to bring them into compliance.

SmartControl.

With SmartControl, the extent of access a user obtains is dynamically adjusted based on a variety of attributes, such as the user's role, strength of authentication, endpoint scanning results and sensitivity of the target resources. For example, administrators can configure one rule that allows a strongly authenticated mobile salesperson using a corporate device access to a virtual desktop configured with their full suite of sales tools and associated sensitive data, while a second rule limits members of the sales team using password-only authentication from unknown devices to an alternate virtual desktop with a limited set of resources for generating and managing proposals. Because Citrix ADC includes in-depth knowledge of the ICA protocol, administrators can even control actions of XenDesktop users that might be considered risky in certain situations, such as local print, copy, paste and save-to-disk operations.

Secure tunneling options and controls

All access sessions are protected from eavesdropping by standards-based SSL/TLS encryption. With the classic SSL VPN capability, the resulting tunnel can be used to provide access to a broad set of resources, including, of course, virtual desktops. Alternatively, administrators can use the solution's innovative MicroVPN feature to define a secure tunnel for a single, designated resource. 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 layer of data protection. With the basic split tunneling feature, users are blocked from accessing any other network for the duration of their access session (remote or otherwise). 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). In addition, the browser cache cleanup feature ensures that all objects and data are flushed from local browser cache immediately upon completion of each and every access session.

Extensive, multi-layer threat protection

With Citrix ADC, enterprises also benefit from an extensive set of threat detection and prevention capabilities.

Network-layer shielding

Independent of its many app and user level access controls, Citrix ADC also incorporates core network firewall functionality. In particular, support for access control lists (ACLs) provides the means to preemptively filter inbound traffic based on attributes such as source port/IP, destination port/IP, protocol, VLAN tags, ICMP type and many others. In addition, the default configuration setting to automatically drop packets that are not explicitly allowed by policy (i.e., "default deny") enables Citrix ADC to inherently stop all sorts of unwanted, unauthorized and potentially malicious traffic from gaining access – and subsequently doing harm – to the enterprise network.

Application-layer shielding

Moving up the computing stack, another significant Citrix ADC design feature is its proxy architecture. Coupled with HTTP/URL re-write and L7 content filtering capabilities, this allows Citrix ADC to:• shield connection brokers and other downstream VDI components from direct TCP and UDP connections initiated from external users, thereby reducing their exposure to malware and other types of attacks•   provide cloaking and content security for these same components to effectively hide server error codes, real URLs and other pieces of information that could give hackers the details they need to formulate custom attacks

In addition, many VDI implementations contain web-based components that also need robust protection against attacks. In this case, the integrated Citrix Web App Firewall provides: •

- a flexible, hybrid-security model that protects against known vulnerabilities using an updated attack-signature database and a positive security model to defeat zero-day attacks for which signatures do not yet exist.
- protection from a wide range of pervasive application-layer threats, such as SQL injection, cross-site scripting and buffer overflow attacks
- an extensive set of XML protections, including content/schema validation mechanisms (to defend, for example, against manipulation of front-end app store features as a way to gain unauthorized access)
- easy-to-configure security policies and templates for simple and fast deployment and management

Multi-layer protocol validation

Many types of cyber threats operate by perverting protocols that are commonly allowed by policy, such as TCP and HTTP. Citrix ADC thwarts all attacks relying on such techniques by validating and enforcing rules for acceptable usage of these protocols.

TCP validation. Citrix ADC features a high performance, standards-compliant TCP/IP stack that has been enhanced to (a) automatically drop malformed packets that could pose a threat to back-end VDI resources, and (b) prevent disclosure of connection and host information (e.g., server addresses and ports) that could prove useful to hackers intent on perpetrating an attack.

HTTP validation. Enforcing RFC compliance and best practices for HTTP usage is a highly effective way that Citrix ADC eliminates an entire swathe of attacks based on malformed requests and illegal HTTP protocol behavior. Custom checks and enforcement rules can also be added to the security policy by taking advantage of integrated content filtering, custom response actions and bi-directional HTTP re-write capabilities.

Multi-layer DDOS Protection

Distributed denial of service (DDoS) attacks designed to take down one or more of an enterprise's computing services – such as its hosted virtual desktops – are a constant and growing threat. Citrix ADC defenses in this area include:

- an integral API call-out mechanism that can be used to automatically trigger external DDoS protection services based on real-time traffic conditions;
- a high-performance architecture and extensive set of mechanisms for mitigating flood-oriented attacks targeting common network and connection layer services; and
- numerous features for countering more insidious low-bandwidth, application-layer variants, without impacting legitimate transactions.

To learn more about these capabilities, please refer to: Citrix ADC: A powerful defense against denial of service attacks

No-compromise SSL

By incorporating dedicated SSL acceleration hardware with support for both 2048 and 4096 bit keys, Citrix ADC delivers essential encryption capabilities that avoid the need to make tradeoffs between having stronger security and maintaining a high-performance user experience.

For those organizations requiring a high-level of cryptographic assurance,Citrix ADC is also available in FIPS 140-2 Level 2 compliant models.

Extensible threat and malware protection

The Citrix ADC SDX service delivery platform provides another substantial layer of threat protection. Featuring an advanced virtualized architecture,Citrix ADC SDX is a multi-services platform that enables consolidated operation of multiple independent instances of key services, including Citrix ADC itself and third-party applications. Its extensible design results in a future-proof approach for delivering a wide range of traditional and advanced threat protection technologies, both now and in the future. One compelling example is the ability to run the Palo Alto Networks VM-Series on Citrix ADC SDX and thereby supplement the extensive security capabilities of Citrix ADC with the power of a next-generation enterprise security platform capable of stopping both known and unknown threats, including advanced malware and targeted attacks

Powerful security management and visibility

Equally important to its extensive access management and threat protection capabilities are the powerful security management and visibility features of Citrix ADC.

As a consolidated front-end for practically all of an organization's internal and web resources, Citrix ADC provides a convenient, centralized approach that simplifies the creation and administration of otherwise disparate access policies. Users benefit from a more consistent set of access rules, while less potential for things to "slip through the cracks" reduces IT security risk.

With Citrix ADC, administrators also obtain complete end-to-end visibility into all HTTP and ICA-based access sessions. Coupled with extensive event logging, full RADIUS accounting, a complete audit trail of administrative actions and robust reporting capabilities, the result is the ability not only to investigate known security incidents, but also to proactively uncover misuse and other telltale signs of compromised clients or attacks against an organization's VDI

Beyond Security

Adequately securing VDI is not sufficient to fully preserve the benefits of app and desktop virtualization. Enterprises also need to ensure the availability, performance and scalability of whatever solution they decide to implement. After all, what good is a highly secured virtual desktop environment if it’s not consistently available? Or if performance is so poor that users perceive it to be unavailable, even when it isn’t? This is another area where Citrix ADC truly excels as a front-end solution for an organization’s app and desktop virtualization infrastructure. In addition to its compelling set of network security features, Citrix ADC delivers:

- a combination of enterprise-class server load balancing, global server load balancing, and health monitoring capabilities to ensure virtual desktop availability and business continuity
- an extensive collection of mechanisms that not only enhance virtual desktop performance over the network but also streamline the user experience
- intelligent load distribution and server offload capabilities that enable seamless scalability of virtual desktop infrastructure

Conclusion

Available as a high-performance, single or multi-tenant hardware appliance or a flexible, software-based virtual appliance, Citrix ADC is easily and cost-effectively deployed as a front end to today’s virtual desktop solutions. By delivering a robust set of advanced access and data control features, multi-layer threat protection and powerful security management and visibility capabilities, Citrix ADC not only preserves but also extends the benefits organizations have come to expect when embracing app and desktop virtualization. More than just a security solution, Citrix ADC also helps IT managers substantially improve the availability, visibility, performance and scalability of their virtual desktop implementations.

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