citrix

White Paper

Ensure the Secure, Reliable, Delivery of Citrix Workspace to Any User, Over Any Network

Citrix ADC improves the Citrix Virtual Apps and Desktops experience for both end users and IT administrators

Application and desktop virtualization have dramatically improved end-user productivity and data security. They have also simplified the work of IT administrators and decreased overall computing costs. Yet the flexibility businesses need to ensure they are competitive means IT must now consider:

- How to ensure the security posture is extended to the endpoint in order to maintain compliance. IT must manage secure access across all the different use cases while deploying applications securely to users on any device, over any network.
- And then—once users are securely connecting—how to provide them a seamless experience when working from any device in any location. In order to do this, users need their apps to be available and responsive, with simple and easy access.
- What to do if users run into issues accessing their published apps—how to pinpoint those issues and troubleshoot them. The proliferation of networking protocols and products has made it almost impossible to obtain end-to-end visibility of application traffic. Without end-to-end visibility, it is extremely difficult to troubleshoot performance problems. Proponents of application and desktop virtualization need to overcome these challenges in order to protect and extend the gains they have made in simplifying the end-user experience, increasing the reliability of application performance, strengthening security, and improving management of IT resources.

Citrix ADC specifically addresses these challenges. Citrix ADC brings together the capabilities of application delivery controllers (ADCs) and secure remote access (in the case of this white paper, for access to Citrix Workspace powered by Citrix Virtual Apps and Desktops). The goal of Citrix ADC is to ensure compliance to the endpoint by enabling the secure, reliable delivery of applications and virtual desktops to any user, anywhere. This white paper provides a brief overview of Citrix ADC and how it addresses these challenges:

- Maintaining compliance by extending security to the endpoint.
- Simplifying the end-user experience with fast, seamless remote access to virtual apps/desktops
- Speeding time to troubleshoot Citrix Virtual Apps and Desktops access issues with end-to-end application visibility

- Striking a balance between security and productivity.

Citrix ADC enhances Citrix Workspace

Citrix ADC is a secure remote access solution that secures and optimizes Citrix Workspace for end users, while providing compliance, reliable and simplified access. Citrix ADC includes secure remote access functionality found in all editions of the Citrix ADC product line. Citrix Workspace allows secure delivery Windows, Linux, web, SaaS apps, and full virtual desktops to any device so your teams can work how they want, from anywhere. With Citrix Workspace, customers can leverage an integrated solution for securely delivering apps, desktops, files, and services to any user, on any device, over any network, with a high-performance user experience. Citrix is the only vendor that offers the established leadership and proven technologies in all the areas needed—from app and desktop virtualization, to mobile app and device management, to cloud networking—to enable the delivery of comprehensive and personalized digital workspaces.

Citrix ADC enables IT organizations to:

- Ensure compliance to the endpoint outside the corporate network
- Gain end-to-end visibility of Citrix Virtual Apps and Desktops traffic to quickly resolve issues
- Secure applications, desktops, and data with centralized, contextual access control polices to dynamically adjust user access
- Provide users with the best experience to maximize their productivity

Extend compliance to the Endpoint

ICA Proxy
With ICA Proxy for Citrix Virtual Apps and Desktops, Citrix ADC provides secure remote access to Citrix apps and desktops without the need to create a full SSL-VPN tunnel into your network. Users can access all their apps and desktops from one URL via single sign-on (SSO) with the same rich application, desktop, and data experience that users enjoy when connected to the local network.

When Citrix ADC is paired with Citrix Workspace, users can access their workspace from any device, anywhere. It enables you to do SSO passthrough to StoreFront. SSO capabilities remove the hassle of multiple authentication checkpoints when switching between desktops and applications within Citrix Workspace. Users no longer need to configure complex and risky network tunnels to access their applications and data and are no longer restricted to a single device in a single location. With Citrix ADC, users can be productive anywhere, using any device.

Citrix ADC encompasses several key networking features and tools. As shown in Figure 1, these include the load balancing, SmartAccess and SmartControl, and HDX Insight as part of the Citrix Application Delivery Management (ADM).

Contextual Security with SmartAccess and SmartControl
The SmartAccess and SmartControl technologies provide a flexible way to balance user convenience against risk. IT can calibrate login challenges by adjusting the amount of access offered based on attributes such as a person's role or location, the device type, and the sensitivity of the resource being requested. Administrators can make access extremely simple when conditions are appropriate, or more difficult when risks are higher. For example, an employee in a corporate office might be able to authenticate with only a password, while a remote user requesting access from an unknown device might need to use two-factor authentication or answer special challenge questions. By making access simpler and more consistent across applications, devices, and environments, Citrix ADC:

- Increases end-user satisfaction and acceptance
- Lowers help desk and support costs

- Improves security by raising the bar for access requests with high-risk characteristics while simplifying authentication for users in low-risk environments

Citrix ADC also provides a mechanism to create and distribute access control policies, including sophisticated adaptive access control policies, to Citrix ADC appliances throughout the enterprise. SmartControl facilitates centralized policy management that:

- Greatly increases the productivity of administrators
- Improves end-user satisfaction by ensuring a consistent set of access rules across all devices and location
- Enhances security by strengthening access control at the edge of network, and by reducing the opportunity for human error in distributing and applying access policies

Multi-factor Authentication
With nFactor, Citrix's solution for multi-factor authentication, customers can fine-tune the authentication schemes for various user groups while using the same Citrix ADC endpoint (or the same FQDN for all users). This allows IT admins to manage all users from a single entry point to enhance control and monitoring capabilities while reducing operational and infrastructure costs.

nFactor is designed to provide more context to the users connecting. For instance, on the login portal, depending on the user and where he/she is connecting from, nFactor is able to intelligently determine what authentication fields to display; for example, do you only require a name and password, or are there additional levels of information? You can select a particular domain users are connecting to based on who the user is. There is a lot more flexibility in being able to validate a user when he/she is connecting. IT can now provide additional layers of validation to see who a user is.

Citrix ADC for Maximum Workspace Availability

Load Balancing
Citrix ADC is an industry-leading application delivery controller that sits in front of application or web servers in corporate data centers and cloud environments. It improves the resiliency, performance, and security of enterprise applications, SaaS applications, and virtualized applications such as Citrix Virtual Apps and Desktops and Citrix Endpoint Management. Form factors include appliances for the data center, and cloud-ready virtual appliances for data centers and cloud environments such as Amazon Web Services (AWS) and Microsoft Azure

High Availability
A high-availability deployment of two Citrix ADC appliances can provide uninterrupted operation in any transaction. When you configure one appliance as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary. If for any reason, the primary node is unable to accept connections, the secondary node takes over.

The secondary node monitors the primary by sending periodic messages (often called heartbeat messages or health checks) to determine whether the primary node is accepting connections. If a health check fails, the secondary node retries the connection for a specified period, after which it determines that the primary node is not functioning normally. The secondary node then takes over for the primary (a process called failover).

Citrix ADC also performs server load balancing. This increases application resiliency and performance by distributing traffic evenly across clusters of servers, by monitoring the health of servers, and by providing seamless failover when a server goes down. Citrix ADC can redirect traffic to servers located in entirely different data centers and in the cloud. It even has the ability to balance queries and updates across SQL databases.In addition, Citrix ADC improves application

performance by compressing and caching network traffic and offloading tasks from servers and network devices (discussed in the Improving Application Performance and Quality section, below).

Global Server Load Balancing
Global Server Load Balancing (GSLB) provides load-balancing services across different geographical regions. It operates under same general principles as load balancing and evaluates server health to distribute traffic amongst multiple data centers. GSLB works via Domain Name Servers (DNS) to maintain business continuity during site-level disasters and distribute the network and server load across multiple sites.

Citrix ADC's GSLB and spillover features provide seamless failover and redirection of users to a backup site in the event of a disaster, and can be used to intelligently spread user requests across multiple sites during normal business operations.

IT can designate GSLB by the least loaded data center, the closest data center, the data center that responds most quickly to requests from the client's location, a combination of those metrics, or SNMP metrics. Citrix ADC keeps track of the location, performance, load, and availability of each data center and uses these factors to select the appropriate data center to send the client request.

End-to-End Visibility

Major industry trends such as mobility and virtualization have transformed the way users work and where they work. Users are accessing their applications over a variety of networks and on several different devices. These networks can range from secure, corporate networks to home networks to Wi-Fi. There are several reasons why users may be unable to access or run their applications:

- Mobile networks, like 3G/4G are unreliable, causing latency.
- There can also be problems with the network or the device.
- Home networks have their own challenges—ISPs and Wi-Fi issues can impact the network.

At the end of the day, users may have a poor experience, leading to lack of productivity.

With all the networking protocols and products, it is almost impossible to obtain end-to-end visibility of application traffic. Without this end-to-end visibility, it can be extremely difficult for IT to troubleshoot performance problems. For example, a user calls the help desk with an application issue such as a slow running application. The IT help desk has trouble pinpointing the issue and passes it to the desktop admin, who then passes it to the network admin, until the help desk must finally contact the vendor for support. The vendor may even have to escalate the issue within their IT. Meanwhile, the user is extremely frustrated and unable to be productive. The IT help desk can have long or missed SLAs as a result.

So, how can Citrix ADC solve this with a better troubleshooting solution?

Within the powerful Citrix Application Delivery Management (ADM) solution, there is a tool for end-to-end visibility for Citrix Virtual Apps and Desktops, called HDX Insight. Citrix ADM is a centralized network management, analytics, and orchestration solution that serves as a critical data aggregation point for applications serviced by Citrix ADC. Application-specific data points and transactions are presented to an administrator with insights into performance and reliability. It manages large numbers of Citrix ADCs(in the tens of thousands) and acts as a valuable source of data that provides insights and analytics and identifies user experience issues all the way down to the transaction level. Having data across your network allows you to identify potential problems and address them quickly.

HDX Insight

HDX Insight is the only solution that offers end-to-end visibility for Citrix Virtual Apps and Desktops environments. For Citrix Virtual Apps and Desktops specific environments, HDX Insight delivers data analytics for Citrix Virtual Apps and Desktops traffic flowing through Citrix ADC.

With HDX Insight, Citrix ADC is uniquely able to parse, decrypt, decompress, and decompose ICA packets, even at the level of individual virtual channels, to provide in-depth visibility into network traffic that uses the ICA protocol, a standard used by Citrix applications.

HDX Insight includes management tools for monitoring, analyzing and reporting application performance metrics and related data, giving enterprise IT unparalleled visibility into Citrix Virtual Apps and Desktops traffic. IT admins can get information on user device and network issues. For example, IT admins can identify users experiencing issues related to a specific published application, as well as users affected by excessive latency, by too many current users coming in via a particular Citrix ADC instance, or by a faulty network segment. In short, HDX Insight allows IT administrators to deliver a compelling user experience by analyzing HDX data and performing business intelligence, failure analysis, and capacity planning for the networks.

As part of Citrix ADM, HDX Insight provides end-to-end visibility of Citrix Virtual Apps and Desktops (ICA) traffic on both LAN and WAN links. HDX-based access sessions help IT quickly pinpoint issues such as latency and application health. HDX Insight provides unparalleled monitoring and auditing of HDX traffic associated with Citrix Virtual Apps and Desktops environments.

Only Citrix ADC can provide full benefits of the ICA protocol—not just for optimizing ICA traffic, but for end-to-end visibility of both application and network traffic in Citrix Virtual Apps and Desktops environments.

Alerts and notifications on the thresholds set for your environment help you proactively monitor access issues. HDX Insight provides the ability to export the data to third-party products like Splunk. It has the option to provide historical as well as real-time analytics data, and customizable and exportable reports allow for external reporting. All this helps you maintain your SLAs, provide a better user experience, and improve user productivity.

Citrix ADC is also ideally positioned to deliver application flow visibility, because all the application traffic flows through it. This capability to monitor and

Figure 1: HDX Insight provides end-to-end visibility down to the level of individual applications and users

provide visibility is enabled by Citrix ADC's support for AppFlow. Citrix AppFlow is an innovative and open standards-based technology that extends the TCP-level information already captured by IPFIX—the IETF standard for NetFlow—to include per-flow application-layer data records. AppFlow has recently been extended to include support for the HDX protocol. The result is an extensible instrumentation technology that conveys both network- and application-level data for Citrix Virtual Apps and Desktops

To ensure a consistent end-user experience, HDX Insight gives IT the ability to proactively manage application health and performance with end-to-end application- and network-level visibility from a single console within Citrix ADM or Citrix Director.

Through the console, IT administrators can:

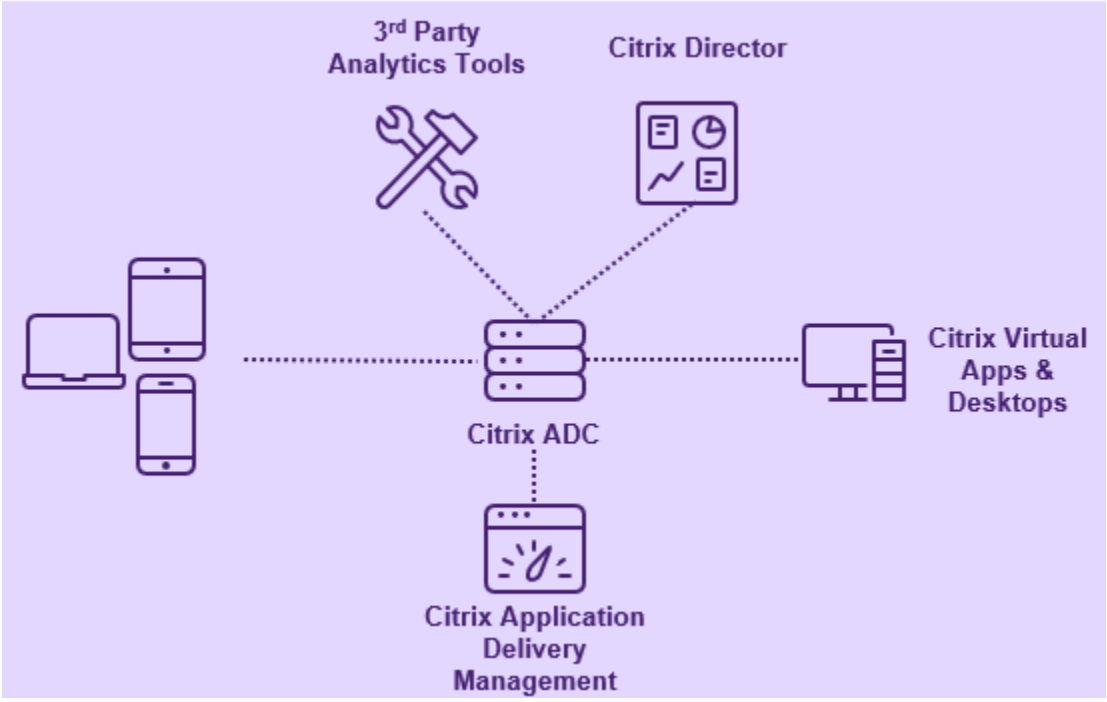
- Troubleshoot performance and quality issues raised by users
- Manage performance proactively by identifying and resolving performance issues before they are perceptible to users
- Perform capacity planning to ensure that resources are in place as networking and appliance demands grow

Simplifying the End-User Experience

One of the key objectives of Citrix ADC is to make the end-user experience as simple and uniform as possible for finding and accessing virtual applications and desktops across all devices, in every type of location, across all types of network. Another objective is to enhance security without complicating life for end users.

StoreFront Integration
StoreFront manages the delivery of desktops and applications from Citrix Virtual Apps and Desktops servers, and from Citrix Endpoint Management servers in the data center to user devices. StoreFront enumerates and aggregates available desktops and applications into stores. Citrix ADC with StoreFront provides secure remote access for users outside the corporate network and Citrix ADC to provide load balancing.

Figure 2: Citrix HDX Insight for end-to-end visibility of Citrix Virtual Apps and Desktops deployments



Director
Director integrates with Citrix ADM for network analysis and performance management. Network analysis obtains HDX Insight reports from Citrix ADM and provides an application and desktop view of the network. With this feature, Director provides an advanced analytics view of ICA traffic in your deployment. Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

HDX Insight reports provide you with the following information in Director:

- Latency and bandwidth effects for applications, desktops, and users across your deployment
- Manage performance proactively by identifying Latency and bandwidth information specific to a particular user session

Support for mobile devices
Users can connect remotely from Android or iOS devices through Citrix ADC to mobile apps and resources in the internal network. Users with Android and iOS devices connect using Citrix Workspace and Endpoint Management to establish a Micro VPN tunnel.

Improving Application Performance

Of course, the end-user experience also reflects application performance. That is particularly true for virtual applications and desktops accessed from remote locations. The challenge is to maintain or improve application performance in the face of additional application delivery, increasingly complex network infrastructures, and tight budget constraints.

TCP Optimization
The Citrix ADC is proven to improve application performance through load balancing, TCP compression, content caching, and protocol-level optimization for TCP and ICA. Citrix ADC also improves application performance by reducing loads on networks and servers. It does this by decrypting SSL/TLS traffic before it reaches the server. Features to speed up the delivery of web pages to mobile devices include converting large GIF files into efficient PNG formats, and compressing scripts and cascading style sheet (CSS) files.

Thinwire Support
Thinwire is Citrix's display remoting technology that allows graphics to be generated on one machine to be transmitted, typically across a network, to another machine for display. Thinwire enables a highly interactive user experience that is similar to that of a local PC. It utilizes a range of complex and efficient image analysis and compression techniques to maxmize server scalability while consuming less bandwidth.

Support for Adaptive Transport
Adaptive transport, a data transport mechanism for Citrix Virtual Apps and Desktops, makes Citrix Virtual Apps and Desktops traffic faster and more scalable while improving application interactivity over challenging bandwidth situations. With Citrix ADC, it benefits off-net workers such as work-from-home employees.Adaptive transport maintains high-server scalability and efficient use of bandwidth by allowing ICA virtual channels to automatically respond to changing network conditions.

Adaptive transport helps the ICA channels intelligently switch the underlying protocol between the Citrix protocol called Enlightened Data Transport (EDT) and TCP to deliver the best performance. It improves data throughput for all ICA virtual channels including Thinwire display remoting, file transfer (Client Drive Mapping), printing, and multimedia redirection.

Subscription-based Citrix ADC with Citrix Workspace Essentials
For customers interested in moving their Citrix Virtual Apps and Desktops deployments to the cloud with Citrix Cloud, there is Citrix Workspace Essentials, a complementary service to Citrix Virtual Apps and Desktops Service on Citrix Cloud that delivers the same high-quality user experience as an on-premise Citrix

ADC, but without the need to configure firewall ports, TLS certificates, or register a DNS domain..

Citrix Workspace Essentials provides the easiest way to ensure security and availability of virtual app and virtual desktop services from Citrix Cloud. Citrix Workspace Essentials provides high value and is the simplest approach to deliver secure remote access in the cloud.

- ***There is no hardware to buy or maintain.*** Maintenance is on Citrix. A reduced on-prem software and hardware footprint means lower data center maintenance costs. ***It's highly scalable.*** Scale up to add new users seamlessly
- ***There are seamless service upgrades.*** Get easy access to latest service.
- ***It's always up to date.*** Software updates are made in real time and without affecting the service.***Get fast time-to-value.*** With "out-of-the-box" productivity, there are no changes required in the DMZ.
- ***There is just one vendor.*** Citrix Workspace Essentials integrates tightly with Citrix Virtual Apps and Desktops.
- ***Get fast time-to-value.*** With "out-of-the-box" productivity, there are no changes required in the DMZ.

Get improved security. Reduce the security attack surface by putting the remote access point of presence in the cloud, rather than on-prem

Conclusion

You are not alone in confronting the challenges of more devices and applications, more users and use cases, and a lack of tools for end-to-end visibility and management. Citrix is dedicated to continually improving application and desktop virtualization for end users, for administrators, and for IT management.

This paper has outlined just a few of the ways that Citrix ADC can make your organization's Citrix Virtual Apps and Desktop deployments more robust:

- Maximize enterprise compliance beyond the data center.
- Leverage end-to-end application and network visibility to troubleshoot problems and ensure high performance
- Simplify the end-user experience by providing always-on access from all types of devices to all authorized applications from a single portal, adaptive transport support, Thinwire support, and other ease-of-use features

These are only a sampling of the features and advantages, so please explore the resources listed below.

Citrix ADC for Business Continuity

Protect your APIs and Applications with Citrix ADC

Ensuring Business Continuity with Citrix ADC & ADM

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