



Delivering applications anywhere,
anytime with maximum security
and control over data



Executive summary

Information security continues to be a significant challenge for enterprises. Nearly every day, new threats target vulnerabilities exposed within new and existing applications and technologies. The distributed approach to application deployment and management compounds matters even further. With traditional application deployment, applications are routinely distributed beyond enterprise boundaries, thereby putting critical information at risk and requiring a similar, distributed deployment of numerous countermeasures. Extending defenses to each individual endpoint is costly, has questionable effectiveness and is not always practical given the diversity of users and device types most businesses need to support. The result is often an expensive, ineffective and difficult-to-secure solution.

Citrix® XenApp™ replaces traditional application deployment with on-demand application delivery, allowing users operating anywhere with any device to have instant access to applications while ensuring the highest levels of security and control over sensitive data.

Security challenges of traditional application deployment

The traditional, distributed approach to application deployment and management—installing, maintaining and supporting applications on individual endpoints—has become extremely complex and costly in the face of rapid change in today’s computing environments and trends, such as an increasingly distributed workforce and the proliferation of applications and devices.

Distributed computing is also inherently insecure. Users are often configured with risky administrator privileges to fix issues they encounter and to add applications. Moreover, sensitive data and application code residing directly on user endpoints are highly exposed and can easily be lost or stolen.

Challenges adding to the security concerns of IT include:

- The need to maintain compliance with stringent privacy and security regulations
- The need to support a highly mobile and increasingly distributed workforce
- The need to provide third-party users (e.g., partners and contractors) with access to applications and organizational computing resources
- The need to support numerous endpoint operating systems and a burgeoning collection of device types and configurations
- The growing need to support bring-your-own-computer (BYOC) initiatives and employee-owned devices in the workplace

Common solutions come up short

Common technical solutions used by organizations to address their security and application access requirements in a distributed application management environment are fraught with challenges. Two examples are the locked-down asset and the use of virtual private network (VPN) technology.

With locked-down assets, user endpoints are loaded with security software—which itself, must be deployed and maintained—meticulously configured to enforce the principle of least privileges, and barred from leaving the corporate network or facility. This is an expensive approach and although it should yield robust security and simplify compliance, the data is still at risk. For example, social engineering attacks can still wreak havoc. Worse, user productivity inevitably suffers due to overly restrictive policies and settings, which limit remote and mobile access.

Choosing to take a more moderate locked-down approach is hardly an improvement. Providing broader access and support for additional scenarios—such as off-network operations and selected third-party users—creates greater complexity and cost, and also more exposure and weaker overall security.

Another approach, VPN technology, provides an authenticated and encrypted tunnel for providing secure, remote access to applications and other information resources. It is an improvement for external users, but access is typically granted to everything on the network, and data that is accessed can be transferred to the user's machine, thus cannot be secured.

These traditional, distributed measures, in addition to being inadequate from a security perspective, have proven to be challenging, costly and incomplete in the coverage they provide—particularly given the expanded and ever-changing needs of the modern business.

On-demand application delivery with XenApp

A powerful alternative to traditional, distributed application deployment and management methods, on-demand application delivery enabled by XenApp provides users anywhere on any device instant access to the applications they need while allowing administrators to maintain complete control over corporate data.

Keys to the capabilities of XenApp are:

- (1) Virtualization technologies that centralize, manage and maintain applications in the datacenter and subsequently deliver them as an on-demand service to users anywhere using any device
- (2) A robust set of security features that are integral to the XenApp infrastructure, as well as Citrix Ready partner solutions



XenApp – Secure by design

XenApp relies on a combination of application and session virtualization to overcome many of the challenges of traditional application deployment solutions.

Application virtualization improves the security, manageability and compatibility of applications by isolating them from the underlying operating system and other applications. With application virtualization, applications are not installed at the endpoint. Instead, they are packaged in a way that provides each application with its own isolated runtime environment where it will operate using its own virtualized (i.e., imaged) instance of necessary system services, settings and data. When an authorized user requests an application, the corresponding package is streamed to the user's endpoint. Application virtualization also provides access to applications when users are offline and enables organizations to more fully leverage the computing power of distributed endpoints.

Session virtualization, a significant differentiator for XenApp, makes applications available as:

- Server-hosted applications, installed on, or virtualized and streamed to, a centralized Windows Server® running Remote Desktop Services
- VM-hosted applications, implemented within a virtual machine that is then run on a centralized blade PC, dedicated workstation or as part of a virtual desktop infrastructure (VDI) implementation

XenApp delivery infrastructure delivers robust protection and control

XenApp hosts and runs applications in a centralized location, as opposed to on endpoint devices. Users remotely access them via a client-side agent or an ordinary web browser and interact by exchanging only mouse and keyboard movements, and the corresponding screen updates, over the network. Applications become accessible from anywhere, at anytime and with any device; performance is enhanced; and, most importantly, sensitive code and data need never leave the datacenter.

XenApp addresses security issues and concerns with a comprehensive set of protection and control capabilities in four functional domains:

1. Centralized data retention and administration
2. Secure access, delivery and containment
3. Fine-grained access and usage controls
4. Comprehensive monitoring

Centralized data retention and administration

One of the most powerful security features of XenApp is its centralized architecture, which yields three distinct benefits:

- **Reduced exposure** – With the hosted, or online, delivery scenarios enabled by XenApp, settings can be applied so that data and sensitive application software never leave the datacenter. Applications are run on centralized servers and users can view and interact with real-time screen updates, or images, of what they're working on, but none of the associated information is actually delivered to their devices.
- **Centralized protection** – Hosted applications are also fully protected by the robust, centralized security infrastructure characteristic of most organization's central offices and datacenters. This is in contrast to the inconsistent and often ineffective level of protection typically afforded mobile and distributed endpoints.
- **Simplified remediation** – Because all applications are managed and maintained centrally, software vulnerabilities can be remediated in a more thorough and efficient manner. Administrators need only patch and maintain a single, centralized image for each application rather than hundreds or even thousands of images on devices scattered around the globe.

Secure access, delivery and containment

XenApp security features that control who has access to virtualized resources, ensuring the confidentiality of user sessions and protecting any data made available for offline operation, include the following:

- **User authentication** – XenApp natively supports a wide variety of authentication mechanisms, including Active Directory, Active Directory Federation Services, RADIUS, Kerberos, pass-through authentication—where user desktop passwords are transparently submitted to the server—and multiple options for two-factor authentication, such as RSA SecurID tokens and smart cards. Biometric and other forms of authentication can also be accommodated by leveraging the available SDK and using existing Citrix Ready security solutions.
- **Single sign-on** – Integrated single sign-on technology provides detailed password management and control. This enables automated application logon, policies to control password strength and expiration, and self-service password reset—an essential capability for enforcing password discipline without increasing the burden on users and system administrators. Users need only a single set of logon credentials to securely launch multiple password protected applications delivered by XenApp.
- **Session encryption** – Sessions can be encrypted using standard protocols and high-performance algorithms such as Transport Layer Security (TLS), Secure Sockets Layer (SSL) and Advanced Encryption Standard (AES). This can be accomplished for XenApp-delivered applications or via the integrated line of full-featured SSL VPN appliances that enable secure remote access not just to XenApp hosted applications, but to all of an organization's other centralized computing services as well.



- **Offline data protection** – Integrated with Citrix Receiver™, the Encrypted Data Plug-in provides an encrypted workspace, or safe zone, for application data stored on user endpoints to support offline access. Policies can be set so that only approved corporate applications are able to see and write to the AES-256 encrypted space, so that stored data is automatically wiped clean after an administrator-specified expiration period. Remote kill functionality is also available to delete protected data in the event that an endpoint is lost or stolen.

Fine-grained control for access and usage

Another major strength and significant differentiator for XenApp is the ability to exert fine-grained control over user sessions and how data can be used within those sessions.

Who can get to what and how—whether via offline access, online access or both—is established via publishing and application delivery policies. Providing control based on user identity, however, is only the beginning. When, for how long, from where and the state of the user’s computing device can also be factored into both access and usage policies. The result is a superior degree of control and protection compared to alternative solutions.

XenApp enables highly granular policies to be set on an individual user or group basis to restrict whether hard drives, printers, com ports and clipboard functions (i.e., copy and paste) are accessible during user sessions to prevent data download and copy from the datacenter.

Furthermore, SmartAccess, enabled by the Citrix® Access Gateway™ SSL VPN component of Citrix® XenApp™, Platinum Edition, provides integrated endpoint scanning. Client systems can be scanned and evaluated against administrator-defined criteria to enforce approved, secure configurations—such as having up-to-date security and operating system software. The results can then be used as factors that determine whether access is granted, and to what extent. For example, a configuration can be implemented where users with systems meeting corporate criteria for full access will be able to access and interact with all resources; whereas that same user accessing applications and data from a less secure location, connection or device may be provided access to the exact same applications with the ability to print and save files limited to the corporate network.

The net benefits of this set of security features are that (a) access to applications is not an all-or-nothing proposition, rather, it is a tightly controlled and variable experience based on a user’s overall security context, and (b) control is extended to also apply to the data involved in any session.

Comprehensive monitoring

The extensive monitoring, tracking and auditing capabilities of XenApp help administrators identify and react to misuse due to malicious intentions, undetected compromises, policy gaps, errors or oversights. They also provide extensive support for compliance with corporate policies, and with security and privacy regulations.

- Session shadowing enables a given user session to be duplicated and displayed in real time on an administrator's workstation. This functionality can be used either for troubleshooting purposes or to watch a user's activities to confirm suspected misuse.
- Activity logging creates a visual record of a user's on-screen activity while accessing online applications and stores it as a video file on a secure server. Session recording can be initiated based on triggered rules, for example, when a specific user in a watchgroup connects to a specific application. This technology can be used to help with regulatory compliance, risk mitigation and troubleshooting.
- Configuration logging supports a similar set of goals as activity logging, but in this case relative to administrators, rather than users. Each configuration change made to a XenApp server farm is tracked to maintain a record of who made it and when.
- Reporting provides a long-term mechanism for revealing the nature of user activities and their tendencies. When gathered and selectively displayed, these details can be used not only to help refine access and usage policies, but also to support forensic analysis—for example, by piecing together a timeline of user activity and correlating that with log data from other systems.

XenApp meets all critical business and security requirements

Citrix XenApp replaces traditional application deployment with on-demand application delivery, which replaces a fundamentally weak security model with an architecturally robust model. The extensive collection of integral authentication, access control, encryption and monitoring capabilities of XenApp further ensures the highest degrees of security and comprehensive control over sensitive data, while enabling users operating anywhere with any device to instantly gain access to the applications they need. The result is a solution that significantly simplifies application management, strengthens enterprise security and helps achieve regulatory compliance while also enabling IT to seamlessly and safely address the business-driven challenges of extending application access to an increasingly distributed workforce, third-party users and a rapidly growing number of new mobile devices.



Worldwide Headquarters

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309, USA
T +1 800 393 1888
T +1 954 267 3000

Americas

Citrix Silicon Valley
4988 Great America Parkway
Santa Clara, CA 95054, USA
T +1 408 790 8000

Europe

Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen, Switzerland
T +41 52 635 7700

Asia Pacific

Citrix Systems Hong Kong Ltd.
Suite 6301-10, 63rd Floor
One Island East
18 Westland Road
Island East, Hong Kong, China
T +852 2100 5000

Citrix Online Division

6500 Hollister Avenue
Goleta, CA 93117, USA
T +1 805 690 6400

www.citrix.com

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2009 was \$1.61 billion.

©2010 Citrix Systems, Inc. All rights reserved. Citrix®, XenApp™, Citrix Receiver™ and Access Gateway™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.