Secure app and data delivery—across devices, networks and locations

How XenApp dramatically simplifies data protection, access control and other critical security tasks.

CITRIX®

Most discussions of application and desktop virtualization focus on cost reduction, simplifying IT operations, and increasing convenience for employees. These factors are extremely important, but IT professionals should not overlook the immense impact of workspace virtualization on information security. In fact, application and desktop virtualization have profound advantages for key security functions such as data protection, access control, user provisioning and compliance. They can also give administrators extremely granular control over how employees, contractors and business partners use and share application data.

This white paper examines how Citrix® XenApp® can dramatically reduce the effort required to protect mission-critical information, while giving users fast, simple, flexible remote access that enhances business productivity.

Growing IT security challenges

Corporate IT groups are continuously challenged to support critical new business initiatives and improve end user computing experiences, while facing limited budgets and mounting pressures to improve information security. Many of these challenges involve making computing resources easier to utilize, regardless of physical and geographical boundaries. Employees are demanding the following:

- Work anywhere, with a consistent experience, from PCs, laptops, tablets and smartphones.
- Utilize personal devices within a corporate environment through bring your own device (BYOD) programs.
- Freedom from rigid IT security controls that restrict performance and inhibit productivity.
- Access to corporate data and self-provision applications on-demand.

At the same time, today's headlines announce data breaches and IT news websites feature stories about cyber criminals and hackers spreading zero-day attacks, new types of malware, and stealthy planning targeted attacks.

Fundamental changes in the way people work and waves of new consumer technologies are shattering the old methods of balancing employee productivity and IT security. IT admins are facing powerful workplace trends that disrupt routine protocols and processes for protecting corporate information:

- Since 2014, each knowledge worker is expected to have an average of 3 devices connected in the workplace.

- Employees are supplying their own personal endpoint devices, making it difficult or impossible to mandate and enforce corporate security standards.
- IT must provide access to employees, contractors and business partners, from remote offices, home offices, hotel rooms and even kiosks, across the globe.

Rethink security

Clearly these trends are not sustainable with current approaches to security and remote access. How can IT groups provide easier access to resources, in the face of more sophisticated threats, with multiplying endpoints to defend? And the challenges are not just related to the quantity of end points, but to the increasing diversity. Each type of device—PC, laptop, tablet and smartphone—requires different security products, protecting against different threats, and applying different access policies.

The remedy is not adding yet another layer of security products that require more management. Instead, it is to change the game by moving to a computing model that is inherently secure, with an architecture that dramatically simplifies fundamental security functions such as data protection, access control, provisioning and secure remote access.

XenApp

XenApp is an application delivery solution that enables any Windows®, Linux, Web or SaaS application to be virtualized, centralized and managed in the datacenter and instantly delivered as a service to users anywhere on any device. With XenApp, applications execute in the data center and are securely accessed from any location. Keeping applications and data protected within the hardened data center and hosted in the same location as the back-end databases further enhances application performance even when accessed from distant locations.

The application access and performance benefits of XenApp are numerous, but many times the security advantages of a centralized application deployment model are overlooked. XenApp provides an inherently secure architecture that dramatically reduces the quantity of data exposed outside of the data center without configuring extensive security features or add-on security products. The fundamental design of XenApp is to keep all apps, data, and information secured in the data center and only send screen update, mouse click and keystroke commands across the network to the user's endpoint device.

XenApp keeps sensitive corporate information protected in the data center, but employees still need secure access to the XenApp infrastructure. Applications published using XenApp are accessible through Citrix Receiver™—a lightweight client that can be installed on any type of device, including iOS, Mac®, Android®, Windows and more. Citrix Receiver makes it easy for IT administrators to securely enable application access from any type of personal or corporate-owned device while ensuring that IT security procedures and processes are enforced. Citrix Receiver is in constant communication with the XenApp infrastructure, making it easy to identify the optimal application delivery method for any user based on device features, available network connection, and specific application-related tasks. Users in any location can download Citrix Receiver and securely access XenApp published applications making it easy for IT to meet the employee demands without compromising security standards.

NetScaler Gateway

XenApp deployments can be further enhanced with NetScaler Gateway™. NetScaler Gateway is a secure application, desktop and data access solution that provides granular application and device-level policies and action- controls. NetScaler Gateway secures remote access to XenApp infrastructure and provides users with a secure, single point of access to published applications and desktops from any type of device. NetScaler Gateway ensures secure remote access by using secure Citrix ICA® proxy technology to encrypt data without the need to establish a full VPN tunnel from remote devices.

NetScaler Gateway leverages HDX SmartAccess™ technology to give IT managers a single point of management for controlling access and limiting actions allowed to users. With HDX SmartAccess, IT administrators can strike the right balance between security and end user convenience in every situation. They do this by defining a precise set of policies based on users, devices and locations. For example, administrators might want to create policies so that one group of users can access a wide range of applications and data while on the LAN, a subset of those resources while on a tablet at home, and a smaller subset from a smartphone connected through a public network. Another, less trusted group could be restricted to a small subset of resources under all conditions. Administrators can go even further by restricting the ability of users in insecure environments to copy, email or print data, or to save confidential files to removable media. They could limit users on public kiosks to viewing data and nothing else.

Further, access can be limited based on the security posture of the endpoint. HDX SmartAccess includes endpoint analysis software that can scan remote computers and determine if security tools like anti-virus software, client firewalls and hard drive encryption utilities are present, running, and up-to-date. If these requirements are not met, the user can be restricted to a limited set of applications and data, or redirected to a remediation site where the security deficiencies can be remedied. These policies can be applied dynamically as users move between different devices, applications and locations.

Administrators can enforce compliance with rules that govern privacy and the secure storage of data. This is critical for enterprises that are affected by regulations such as those in some European countries that require data about its residents be stored within the country's borders. With HDX SmartAccess, an organization could not only prove that the data resides in a virtual environment located in the country, it could also create policies so that nobody located outside of the country, or using a mobile device, could access that data.

Reduce security complexity

The architecture and core features of XenApp with NetScaler Gateway make security far more reliable and easier to manage. By opting for a solution that is inherently secure, some of the most vexing challenges of protecting data on endpoints simply disappear or are dramatically reduced in complexity.

Data protection

Sensitive data can be centralized in the data center and protected by a complete set of network and host security products such as next-generation firewalls (NGFWs), intrusion protection

systems (IPSs), and host anti-malware and anti-spyware tools. These defenses are generally much more powerful and effective than the local firewall and anti-virus products deployed on endpoints, and are far easier to update.

With XenApp, data is never transferred over the network, and if policies are enabled to allow data transfer, that data is encrypted. Keeping intellectual property and sensitive information protected from eavesdropping, man-in-the-middle attacks, and other threats to "data in motion."

Application and desktop virtualization with XenApp also simplifies the operational aspects of data protection. Databases and files in a central location are far easier to monitor and back up than those residing on distributed devices.

Employees are easily protected from data loss due to hardware and software failures, accidents and human errors. Data can be recovered faster in the event of a major outage or disaster.

Access control

Controlling access to applications and data residing on endpoints is extremely challenging, especially since the tools available to manage those local controls vary widely across different types of laptops, tablets and smartphones.

Further complicating the picture is the fact that most organizations have multiple access points and authentication procedures to support different use scenarios. Three different gateways and three different authentication procedures might be needed to handle one employee connecting from a PC in the office, a second employee connecting over the Internet from a tablet at home, and a contractor connecting from a smartphone at the airport.

With XenApp, administrators can use one set of tools to create and enforce a single set of access control policies for all users, regardless of their locations and the devices they are using. They could also add multi-factor authentication to any Windows or legacy application, including tokens, smartcards, RADIUS, Kerberos and biometrics.

These same access controls and authentication methods can be used to manage access to all resources delivered by XenApp while providing a self-service, enterprise app store that gives users fast, on-demand access to Windows applications and application updates. By providing an enterprise app store, IT can provide consumer-type flexibility to users and free up operations and support staffs from providing applications to individual employees. It also enhances security by giving users convenient access to corporate-approved and tested applications, so they don't potentially download infected apps from dubious app stores and compromised sites on the web.

Provisioning and de-provisioning

Provisioning and de-provisioning employees can be a burdensome activity for IT administrators. It is particularly challenging to cut off application and data access when employees, contractors and others are terminated. War stories abound of contractors retaining application access months after their work is complete, and of fired employees walking off with customer lists and intellectual property.

With XenApp, new users can be provided with access to applications with a few clicks, and access to applications and data can be revoked in seconds from terminated employees and contractors. If terminated employees are using their own laptops or mobile devices, sensitive data is stored out of reach in the data center, not on their equipment.

Incident response and disaster recovery

Incident response and disaster recovery are also inherently simpler with application and desktop virtualization. Centralized data is easier to monitor and analyze than data spread around distributed systems. Vulnerabilities can be patched or remediated in a central location, instead of across hundreds of remote PCs and devices.

For disaster recovery, administrators can set up a "two data center" configuration where applications and data are mirrored between two sites. If one site goes down, users can quickly be switched to the other with no loss of data or productivity. If laptops and other devices are destroyed or unreachable in a disaster, employees can access their applications and data from other devices in safe locations.

Compliance

XenApp can simplify audits and regulatory compliance. Investigators can use a complete, centralized audit trail to determine who accessed what applications and data. There is no need to collect extensive logs from remote devices.

Conclusion

This paper outlines how XenApp solutions from Citrix give users more power and flexibility to securely access applications and data anywhere, using any device. It also explains some of the ways application and desktop virtualization can simplify difficult and time-consuming IT security tasks related to:

- Data protection
- Access control
- Policy enforcement
- Provisioning and de-provisioning
- Incident response and disaster recovery
- Compliance
- Secure, efficient remote access

XenApp solutions reduce the work needed to provide better security. Security improvements are inherent in a virtualized architecture and a centralized application and desktop delivery model. That means that organization can enjoy the benefits of simpler and more reliable security, without having to implement and manage complex new security tools.

Additional Resources

App Virtualization Solutions

Compare XenApp vs. VMware Horizon

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2015 of $3.28 billion, Citrix solutions are in use at more than 400,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.