Delivering secure apps and data across devices, networks and campuses

How XenApp dramatically simplifies data protection, access control and other critical security tasks.
Most discussions of application and desktop virtualization focus on cost reduction, simplifying IT operations and increasing convenience for students and faculty. 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 protecting student and research data, access control, user provisioning and compliance. They can also give administrators extremely granular control over how students, 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 learning and business continuity.

**IT security challenges sweep education**

Across campuses, IT groups are continuously challenged to support critical new business initiatives and improve student and employee 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. The expectations of modern students and faculty now include:

- The ability to work anywhere, with a consistent experience, from PCs, laptops, tablets and smartphones.
- Flexibility to use personal devices within a campus environment through bring your own device (BYOD) programs.
- Freedom from rigid IT security controls that restrict performance and inhibit teaching, learning and administration.
- Secure access to student, research and institutional data as well as on-demand self-provisioning for applications.

At the same time, data breaches, cyber criminals, hackers, zero-day threats, new types of malware and stealthily planned targeted attacks make frequent appearances in news headlines and IT feature stories. As these risks grow, fundamental changes in the way students and employees work and waves of new consumer technologies are shattering the old methods of enabling student and employee productivity while protecting institutional information:

- Students and employees use an estimated three connected devices on average for teaching and learning.
- Students and employees are supplying their own personal endpoint devices, making it difficult or impossible to mandate and enforce an institutions’ security standards.

1 Audience Survey on Technology in Higher Ed, University Business, June 2014
• IT must provide access to students, employees, contractors and business partners from remote campuses, dorms, home offices and workspaces across the globe.

Rethinking security for the modern educational institution

In light of these trends, traditional approaches to security and remote access are clearly not sustainable. While addressing more sophisticated threats, IT groups must also enable easier access to resources from proliferating user devices. The challenge goes beyond the quantity of endpoints to defend; their increasing diversity adds further complexity. Each type of device—PC, laptop, tablet and smartphone—requires different security products, protecting against different threats, through 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.

Citrix 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 students and employees anywhere, on any device. Keeping applications and data protected within the hardened datacenter, and hosted in the same location as their backend databases, further enhances application performance even when accessed from distant locations.

The numerous application access and performance benefits of XenApp are well known, but the security advantages of a centralized application deployment model are often overlooked. XenApp provides an inherently secure architecture that dramatically reduces the quantity of data exposed outside the datacenter without the need to configure extensive security features or add-on security products. All apps, data and information remain secured in the datacenter and only screen updates, mouse clicks and keystroke commands are sent across the network to the user’s endpoint device.

XenApp keeps sensitive student and research information protected in the datacenter, but students and 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 institution-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. Students and employees in any location can download Citrix Receiver and securely access XenApp published applications making it easy for IT to meet everyone’s demands without compromising security standards.
**Citrix NetScaler Gateway**

XenApp deployments can be further enhanced with Citrix NetScaler Gateway™, 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 students and employees 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 the actions allowed to students and employees. Administrators can strike the right balance between security and end user convenience in every situation 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 students and employees can access a wide range of applications and data while on the LAN, a subset of those resources while on a tablet in dorms or 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 students in insecure environments to copy, email or print data, or to save confidential files to removable media. They could limit students and employees on public kiosks or workspaces to viewing data and nothing else.

Access can also 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 an institution’s data. This is critical for institutions that are affected by regulations such as those in some European countries that require data about its residents to 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, but also create policies so that nobody located outside of the country, or using a mobile device, could access that data.

**Reduced security complexity**

The architecture and core features of XenApp with NetScaler Gateway make security far more reliable and easier to manage. With 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 datacenter 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 antivirus products deployed on endpoints, and are far easier to update.

XenApp keeps research, intellectual property
and other sensitive information protected from eavesdropping, man-in-the-middle attacks and other threats to data in motion by making it possible for users to work with student and research data without ever having it transferred over the network. If policies are enabled to allow data transfer, that data is encrypted from end to end.

Application and desktop virtualization with XenApp also simplifies an institution’s 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. Students, faculty and 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 inclement weather, a major outage or a natural disaster.

Access control
Controlling access to applications and institutional 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 campuses 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 student connecting from a PC in the dorms, a second student connecting over the Internet from a tablet on campus, and a third student connecting from a smartphone while visiting family in another state or country.

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. This can include the addition of 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 students and employees fast, on-demand access to Windows applications and application updates. By providing an enterprise app store, IT can provide consumer-type flexibility to students and free operations and support staff members from providing applications to individual students and employees. Provided with convenient access to corporate-approved and tested applications, users are less likely to download infected apps from dubious app stores and compromised sites on the web.

Provisioning and de-provisioning
Provisioning and de-provisioning access to resources for students and employees can be a burdensome activity for IT administrators, especially when students graduate, or when employees, contractors and others are terminated. War stories abound of students or contractors retaining application access months after graduation or when their work is complete, and of fired employees walking off with student data and intellectual property. With XenApp, new students or employees can be provided with access to applications with a few clicks, and access to applications and data can be revoked in seconds for graduates or terminated employees and contractors. If terminated employees have been using their own laptops or mobile devices, the sensitive data they have accessed has remained stored out of reach in the datacenter, not on their own equipment.

Incident response and disaster recovery
Incident response and disaster recovery are 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-datacenter” 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
As rising threats and evolving work styles pose new security challenges for IT groups at educational institutions, Citrix XenApp gives students, faculty and employees more power and flexibility to securely access applications and data anywhere, using any device. Application and desktop virtualization 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, and compliance while enabling secure, efficient remote access. Security improvements are inherent in a virtualized architecture and a centralized application and desktop delivery model, reducing the work needed to provide better security. As a result, the institution 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
Citrix Education Solutions