Security in Higher Education: A Model for the Modern Institution

The University of Florida protects apps and data while freeing students, faculty and staff to work anywhere on any device

Introduction

Institutions of higher learning are responsible for providing a secure environment for their students, faculty and administrators to work and study. To protect personal information, intellectual property and other sensitive data from breach, universities must find a way to secure applications and data across an increasingly complex array of devices, applications, network connections and usage scenarios. At the same time, the institution must meet the demands of users for a simple, high-quality experience on any device they choose to use, including personal laptops, smartphones and tablets, wherever they work. The cost of failure can be high, from reputational damage, to regulatory fines, to the loss or compromise of valuable research. Layering point solutions onto an aging infrastructure only adds complexity without building strategically robust security. As the threat of malware, hacking and other attacks continues to rise, the need for a more comprehensive and effective approach is becoming urgent.

Citrix solutions enable institutions to secure the delivery of applications and data on any device students, faculty and staff use, over any network. As shown by the experience of the University of Florida, the solution provides a complete foundation to:

- Enable secure student access and mobility on any device while protecting applications, data and intellectual property
• Protect against malware and the loss or theft of data
• Facilitate compliance with demanding regulatory requirements
• Simplify and reduce the cost of IT operations while future-proofing the environment to meet new requirements to come

A rapidly evolving environment poses new security challenges for educational institutions

Universities and other institutions of higher learning face increasingly complex and urgent security requirements. The IT environment grows more complex by the day as students, faculty and administrators embrace new types of devices and applications in exploding numbers. The volume of data is growing quickly as well, along with the number of places it must be kept secure—in on-premises datacenters and third-party cloud services, on personal and university-owned devices, in transit over public networks, in personal email and hard drives, and more. People connect to campus resources in more ways from more locations as well, bringing new requirements for secure remote access as well as authentication and authorization. Given the highly distributed and collaborative nature of education today, IT must also provide secure access to students, employees, contractors and business partners from remote campuses, dorms, home offices and workspaces across the globe.

At the same time, the stakes of IT security have never been higher. From hackers and organized crime, to disgruntled insiders, to well-intentioned users who unwittingly put data at risk, the institution is at constant risk of a damaging breach. No university wants to be in the headlines for compromising the records of its students or the intellectual property of its researchers—especially in a field where a reputation for expertise and excellence is paramount. Even before research is conducted—or tuition payments are processed, healthcare is provided or a wide range of other essential functions are performed—the institution must maintain compliance with demanding regulatory standards governing data privacy and security.

The need for effective security can’t be allowed to interfere with the essential functions of higher education, the free flow of ideas and information, and the successful collaborative pursuit of knowledge. Students, faculty and administrators must be able to pursue their work while adhering to security procedures and policies. It’s a reasonable expectation, but the implications have become increasingly daunting for IT. These include:

• The ability to work anywhere, with a consistent user experience, from PCs, Macs, laptops, tablets and smartphones
• Flexibility to use personal devices within a campus environment through bring-your-own-device (BYOD) programs
• Freedom from outdated IT security policies 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 many institutions, the security challenge is compounded as much by outdated campus infrastructure as by disruptive technologies. Application delivery technologies may date back a decade or more, implemented in layers and silos that make it difficult to secure applications, keep track of the location and movement of data, and maintain a consistent and easily manageable environment.
The security situation at University of Florida

One of the nation’s top public research universities, the University of Florida is a global institution encompassing 16 colleges and 150 research and service centers across 50 countries. The university’s 52,000 students are instructed and supported by 15,000 faculty and staff members. “Our diverse community and ever-changing IT landscape makes it difficult to develop a consistent security strategy,” says Mehdi Ramdane, a systems administrator at the university. “Our user base is more mobile and dictates a flexible learning space, and they want to use their own devices and access data from anywhere.” These devices run on a variety of platforms including Windows, Mac, iOS and Android, and may or may not be locked down. Meanwhile, the university community generates vast amounts of data each semester, all of which must be protected wherever and however it is stored and accessed.

While addressing these needs for secure mobility and BYOD, the university also needs to ensure that students don’t face financial obstacles to learning due to the high cost of applications, especially those used for only a limited time in a specific class. “If professors need to teach a certain function of a program, then we need to make sure that it’s readily available to students,” says Ramdane.

University of Florida IT views the security challenge of course-related application delivery as threefold:

- Provide users with secure access from anywhere, anytime, to an environment that allows them to use applications for no direct cost
- Allow students and faculty members to bring their own devices
- Handle data in a secure and compliant fashion

Secure access and mobility for students, faculty and administrators

IT security strategy at many organizations has traditionally amounted to adding layer after layer of security products. Most campuses currently have multiple access points and authentication procedures to support different use scenarios; three different gateways and authentication procedures might be needed to handle one student connecting from a PC in a dorm, another student connecting over the Internet from a tablet on campus, and a third student connecting from a smartphone while visiting family elsewhere. The tools used to manage local controls on endpoints vary widely as well across different types of laptops, tablets and smartphones. Now today’s educational institutions are turning to a more effective and sustainable approach. Instead of accumulating a complex, costly and unmanageable assemblage of point solutions, schools like the University of Florida are changing 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.

Built on this model, the Citrix solution for secure application and data delivery in higher education begins with Citrix XenApp®. XenApp 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 faculty anywhere, on any device. Applications and data remain protected within the hardened datacenter and only screen updates, mouse clicks and keystroke commands are sent across the network to the user’s endpoint device. Applications that live natively on mobile devices, whether iOS, Windows or Android, are containerized, and their data is encrypted on the device as well. These measures dramatically reduce the risk of exposure without the need to configure extensive security features or add-on security products.
The hosting of applications in the same location as their backend data enhances application performance even when accessed from distant locations.

**Secure application and data delivery at University of Florida**

The University of Florida uses XenApp to power UFApps, a free service available to all university students and faculty. Four years after its introduction, UFApps publishes 127 applications to students and faculty on campus and around the world. The XenApp infrastructure helps fulfill its three goals of securing access to applications, making them available to any student or faculty whenever they need them, and protecting the integrity of that data that the application handles. Before any application is deployed in UFApps, the university's Information Security Office completes a risk assessment to ensure the application will not cause any loss of data confidentiality or integrity. The application is then tested for compatibility issues and middleware dependencies and added to a trusted software repository that stores all applications.

Users access their UFApps applications through Citrix Receiver™, a lightweight client that can be downloaded and installed on any type of desktop or mobile device. IT administrators can securely enable application access from any type of personal or institution-owned device while ensuring that IT security procedures and processes are enforced. New students and faculty are automatically provided with access to UFApps applications, and access to applications and data can be revoked in seconds for graduates or departing faculty. Because data is stored in the datacenter, not on user endpoints, IT doesn’t have to worry about sensitive data remaining on personal laptops or mobile devices belonging to students, faculty or staff. Access control and data encryption are performed by Citrix NetScaler™, a secure application, desktop and data access solution that provides granular application and device-level policies and action controls.

With NetScaler, University of Florida 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. Users can be allowed to 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 can be restricted to a small subset of resources under all conditions. Users connecting via public kiosks or workspaces could be limited to viewing data and nothing else. Access can also be limited based on the security posture of the endpoint, including the presence or absence of up-to-date antivirus software, client firewalls and hard drive encryption utilities. Policies can be applied dynamically as users move between different devices, applications and locations. In this way, administrators can enforce compliance with rules that govern privacy and the secure storage of the institution’s data.

**Meeting the expectation for BYOD with a great experience**

Many college students now rely on as many as three devices for their work—a smartphone and a laptop to begin with, and often a tablet as well. Among this population, bring-your-own-device is seen not as a perk, but as an assumption, for students accustomed to meeting their own technology needs and choosing the best way to get their assignments done. The same is true for an increasing number of faculty and administrators. As they move from location to location and device to device, these users expect the same kind of simple, seamless and consistent experience they've become accustomed to with consumer services like Netflix, Spotify or Amazon.
With Citrix Receiver, NetScaler and the XenApp-powered UFApps service, the University of Florida can allow complete freedom for students and faculty to use BYO devices of any kind while maintaining control over how and where applications and data are accessed. Single sign-on and transparent policy enforcement masks complexity and eliminates the need for repetitive or cumbersome authentication and authorization processes. The solution automatically determines the best way to deliver each application to each user based on location, device type and application requirements to ensure a high-quality experience in any scenario.

Data loss prevention and recovery

Universities and other educational institutions host and manage a wide variety of information, and face an equally diverse array of risk factors. Research data and intellectual property must be protected against loss or theft—whether by external actors or others within the university community itself. University systems and applications must be shielded from hackers, malware, ransomware and other attacks.

XenApp protects data in motion by making it possible for users to work with data without ever having it transferred over the network. Instead, data is accessed remotely in the datacenter, where it can be 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. At the same time, 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. Because no unencrypted data resides on the endpoint, a lost or stolen device will not result in lost or compromised data; the user can simply use a replacement device to regain access to centrally hosted and managed data.

The University of Florida complements the inherent security of the XenApp architecture with measures such as segregated environments for sensitive projects, regular vulnerability scanning and a data classification policy governing the usage of different types of data in various scenarios.

Taken as a whole, the Citrix solution enables a complete framework for the University of Florida to secure its environment and protect its applications and data. This framework encompasses:

- Identity and access — including two-factor authentication for all users and access control based on use context
- Network security — with secure remote access for mobile and third-party users
- Application security — through the centralization and encrypted delivery of applications, and containerization for applications accessed on mobile devices
- Data security — including the centralization and hosted delivery of data, secure file sharing to reduce data loss, and containerization for data in transit and at rest
- Monitoring and response — with auditing and accounting of resource access to support compliance
Business continuity and operational benefits

Beyond its immediate benefits for security, mobility and user flexibility, the Citrix solution helps the University of Florida achieve simpler, more efficient IT operations. Centralized application delivery vastly simplifies provisioning, administration and maintenance, which lowers overall costs. Security measures and policies can be applied consistently across devices and scenarios through a single point of management, becoming both more comprehensive and more efficient. Vulnerabilities can be patched or remediated in a central location, instead of across hundreds of remote PCs and devices. Centralized tracking of access to applications and data eliminates the need to collect logs from remote devices, greatly simplifying audits and regulatory compliance. In the event of a disaster, a dual-datacenter strategy keeps University of Florida applications and data up and available to users.

As new types of endpoint devices and applications enter the environment, the secure foundation provided by the Citrix solution enables the University of Florida to maintain security without having to reinvent the wheel or expend resources on a new generation of endpoint solutions. This allows campus IT to embrace innovation without the fear of undermining security or incurring new complexity. Emerging user, institutional and the regulatory requirements can be addressed simply and efficiently.
Conclusion

Facing the security challenges of an increasingly complex and diverse technology environment, including mobility, BYOD and remote access, educational institutions need to update their approach to data protection. The University of Florida uses integrated Citrix solutions including Citrix XenApp, Citrix Receiver and Citrix NetScaler to enable the secure delivery of applications and data on any device students and faculty use, over any network. Conditional access policies reduce risk in diverse user scenarios, while virtualization keeps data centralized in the datacenter, not on vulnerable endpoints. In this way, the University of Florida—and other institutions like it—can allow users to work productively from anywhere, at any time, while simplifying IT, facilitating compliance and providing a secure foundation to meet future needs.

For more information about Citrix solutions for education, please visit www.citrix.com/education.