TRANSFORM SECURITY AND COMPLIANCE

Improve Data Security, Protect Personally Identifiable Information (PII), and Keep Intellectual Property (IP) Safe

Addressing Higher Rates and Risk of System Intrusion

Information security is now cited as the number one issue for higher education leaders.[1] High-profile data breaches and cyber threats are forcing institutions to increase their focus on information security. Nearly 10 percent of security breaches in the U.S. targeted education institutions in 2016.[2] Overextended and siloed IT staff makes it difficult for academic institutions to detect and quickly remediate issues within the complex and diverse environments they manage. In higher education, research, intellectual property and financial and personal data is of high value to malicious parties. Data is at risk and it, along with student privacy, must be protected.

Factors such as highly sensitive data environments (e.g., health, financial, research), sprawling and complex campus networks, large numbers of unsecured devices accessing networks, and overextended and siloed IT staff put a bull's-eye on higher education for malicious threats. Institutions of higher learning are meeting threats head-on by safeguarding student privacy with an innovative identity-based solution that delivers and secures data and apps on any device while improving the end-user experience to access needed educational resources. They also need to protect valuable intellectual property and research data by unifying access and securing data centrally as well as on endpoints.

Securing highly sensitive health, PCI, financial and personal data is critical and can be done with VMware solutions. Moreover, VMware can help ensure compliance with HIPPA, PCI, FERPA and other standards with virtual network, virtual desktop, security, and mobility solutions.

Addressing Enterprise Requirements

Students, faculty, and staff demand always-on access to learning resources and campus IT teams are ready to help with the caveat that they remain in control of infrastructure and applications. VMware meets both requirements, offering a transformative approach to security—through a ubiquitous layer of software—that provides comprehensive, unified end-point management and network security technology, purpose-built for providing IT with granular control that starts in the data center and finishes at the device. VMware's approach helps better safeguard data from both internal and external threats. It also provides defense-in-depth security for full protection of data and infrastructure in the modern world

Secure Sensitive Data Environments

A public data breach can ruin the trust of students, faculty, and staff as well as the reputation of a college or university. For these reasons, campus IT teams are diving deeper than traditional, policy-based checklists of security functionality to institute preventative measures. New defense-in-depth approaches to security include protecting devices, networking, applications, and clouds.

[1] Center for Digital Education, "8 Cybersecurity Challenges Facing Higher Education," May 18, 2016.

[2] Ibid.

> "VMware NSX helps to protect our students and staff, which ultimately helps protect the University."
>
> IAIN RUSSELL
> HEAD OF INFRASTRUCTURE
> INFORMATION SERVICES DEPARTMENT,
> EDINBURGH NAPIER UNIVERSITY

OVERVIEW

Preventing data theft and system intrusion to steal personally identifiable information (PII) and intellectual property (IP) from academic institutions has become a campus IT imperative. VMware provides a holistic approach that transforms security and streamlines compliance by providing a ubiquitous software layer across application infrastructure and endpoints. The end-to-end solution enables campus IT teams to reduce risks, lower costs, and better protect their data and reputations.

BENEFITS

- A holistic approach to strengthen campus-wide IT security
- Distributed and integrated security functions across the data center
- Identity and endpoint security for BYOD initiatives
- Streamlined compliance

Brian Pietrewicz, Director of Computing Platforms at the University of New Mexico (UNM), describes the value VMware vRealize® Automation™ and VMware NSX® together provide to his campus, ultimately securing data and giving IT the ability to meet compliance requirements. He says, the solutions give UNM the confidence to "double and triple in size without increasing the amount of staff."

Safeguard Student Privacy and Intellectual Property

The job of ensuring information is secure on campus is challenging. There are more devices and apps on campuses than ever, and IT must protect the identities associated with them as well as the networks they access from intrusion. Moreover, increased collaboration between academic institutions and private or governmental partners requires strengthening intellectual property protection and limiting extortion opportunities such as ransomware. Personalized learning, virtual labs, and online courses further complicate data stewardship strategies.

Academic institutions striving to prevent on-campus incidents of malicious and untended data theft as well as stop hackers are turning to VMware for a best-practices approach that more effectively counters digital attacks and thwarts cybercriminals. The University of York, for example, uses VMware NSX as a backbone to a new agile IT security approach, providing services to students, faculty, and more than 2,000 researchers across 30 academic departments.

Streamline Risk and Compliance

Traditional perimeter security models don't adequately protect workloads inside of a data center. VMware delivers granular, workload-specific security that guards against dangerous lateral threats. NSX makes micro-segmentation economically and operationally feasible, providing the networking and security foundation for the software-defined data center (SDDC), enabling isolation and segmentation with advanced services.

VMware solutions keep data safe by ensuring it stays in the data center, not on mobile devices. Through conditional access policies, IT can enforce access decisions based on a range of decisions, including strength of authentication, network, location, and device compliance. UNM, for example, uses NSX and vRealize Automation to offer access to environments only if they comply with regulatory requirements such as HIPPA and FERPA.

Learn More about VMware Transformative Security Solutions for Higher Education

Data theft and system intrusion prevention has become a business priority for academic institutions. While protecting their IT infrastructure and apps, campus IT teams also must keep up with regulatory changes. VMware helps colleges and universities adopt a multi-layered security approach—strengthening the security of the data center, desktop PCs and workstations, and endpoints—to mitigate the threats of ransomware, malware, phishing, and other breaches—at lower cost.

Learn more at http://www.vmware.com/go/edu.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com