Securing the Campus with Fortinet Security Solutions for Higher Education

Executive Summary
As institutions of higher education embrace technology to enable learning and collaboration, they are accelerating their adoption of cloud services and their support for mobile applications. They are also deploying a wide range of Internet-of-Things (IoT) devices as part of smart campus initiatives. With the influx of these new technologies, however, come increased risks to network security and to the intellectual property and personal data connected to it.

University CIOs can competently manage these risks with the Fortinet Security Fabric. A broad, integrated, and automated security platform, the Security Fabric gives CIOs visibility into their entire security infrastructure, both on and off campus and in the cloud. It also provides robust analytical tools and controls to protect ever-evolving higher-education networks. Certified, recommended, and validated by trusted testing and research organizations such as NSS Labs and IDC, Fortinet solutions are securing the networks of more than 4,000 educational institutions worldwide.

Key Security Challenges for Higher-Education
The volume, speed, and sophistication of new cyber threats mean that it is not a question of if, but when, attacks will occur. Detecting these attacks and mitigating their impact has become increasingly difficult. Visibility is limited across disparate parts of the institution: residence halls, research facilities, classrooms, and offices. And when an attack occurs, it can spread rapidly, either through technology flaws, such as large, unsegmented internal campus networks and lack of endpoint protection, or through human vulnerabilities to social engineering and other cyber-criminal tactics.

Meanwhile, the attack surface on university campuses is expanding rapidly. Technology is becoming ubiquitous in classroom environments, and students are arriving on campus with an average of eight or nine personal devices that they expect to connect to the university network. Students, faculty, and staff members are using the institution’s network to store, access, and transmit both valuable research data and sensitive personally identifiable information (PII).

Boards of trustees are increasingly aware of the vulnerabilities in universities’ IT networks, putting IT leadership in the hot seat. There is also external pressure to demonstrate security due diligence. IT managers must protect each type of data in compliance with government regulations. Student education records are protected by the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA). The privacy of student and employee medical information is governed by the Health Insurance Portability and Accountability Act (HIPAA). And any entity that accepts credit card payments—such as the bursar, the campus store, or the cafeteria, to name a few—must comply with the Payment Card Industry Data Security Standard (PCI DSS).

Understanding the Risk
“Many institutions have extremely limited to no real insight regarding the depth of their security risks in schools, departments, and labs. They can range from exceptionally well-managed servers and devices to those that are compromised or unpatchable.”

– Bradley C. Wheeler, CIO Indiana University

Six research areas of interest for higher-ed cyberattackers:
1. Scientific
2. Medical
3. Defense
4. Public policy
5. Nuclear issues
6. Economic forecasting
In addition, universities must establish identity theft prevention programs under the Federal Trade Commission's (FTC) Red Flags Rule to protect covered accounts such as bursar and student accounts, payment plan agreements, and institutional loans.

**Higher-education Solution Requirements**

To meet all these challenges, a security solution must cover all attack vectors in the network, from the cloud, to web applications, to the network, to the endpoint. It must scale to be future-proof, and it must be integrated for centralized visibility, compliance reporting, and fast, automated response to threats.

**Deflect pervasive threats.** Nearly every network-connected wireless device and mobile or cloud application has become a vector for cyber threats. Defending this exploding attack surface requires an automated, orchestrated response to threats by security technologies that communicate in real time and are fueled by up-to-date threat intelligence.

**Thwart attacks on the inside.** Openness and sharing are inherent in academic institutions. Allowing data to traverse the campus network unchecked, however, invites disaster. The security infrastructure must not only protect the campus perimeter but must also be deployed between departments, faculty, staff and student user groups, and other internal network segments. As part of a zero-trust access strategy, university network security solutions should incorporate adaptive trust mechanisms between network segments to enforce data security policies, protect data privacy, and prevent attacks on one segment from spreading laterally throughout the campus.

**Take unrelenting user demand in stride.** As the volume of transactions and data flowing over the institution’s network expands, security technologies must have the capacity to monitor, inspect, and filter traffic without hampering application performance. Additional security tools, such as firewalls, email and web access gateways, unified threat management, or endpoint security, should slot seamlessly into the existing security environment, allowing protection to scale cost-effectively.

**Rationalize IT operations.** When network security evolves organically, IT winds up with a hodgepodge of disparate devices and management tools. This not only hampers threat detection and response across the network but also wastes staff time and resources. The security infrastructure needs to provide broad visibility of the entire attack surface, orchestrate security policy enforcement, automate security provisioning and threat response, and easily provide proof of regulatory compliance.

**The Fortinet Security Fabric: A Strategic Differentiator**

Fortinet delivers a unique approach to security for higher-education institutions. This architecture, called the Fortinet Security Fabric, provides deep automated visibility, distributed intent-based segmentation that enables zero-trust access, and analytics for real-time response. The Fortinet Security Fabric allows universities and colleges of all sizes to leverage existing investments while moving toward a more resilient integrated security architecture.

The Fortinet Security Fabric protects the university’s entire attack surface by incorporating the following elements:
**Network security.** Protecting the network from known and unknown threats, a broad range of FortiGate next-generation firewalls (NGFWs) offer multiple security and networking controls as well as a Wi-Fi controller in a single platform for reduced complexity, ease of management, and lower total cost of ownership (TCO).

**Multi-cloud security.** Augmenting cloud-native security controls, Fortinet cloud security solutions offer single-pane-of-glass visibility and unified security across multiple cloud deployments. FortiGate VM is a cloud-based virtual NGFW that protects traffic moving between campuses and clouds as well as between different cloud services. Meanwhile, FortiCWP cloud workload protection (CWP) provides superior visibility and control of the entire multi-cloud infrastructure, helping university CIOs to accurately assess and manage their security infrastructure.

**Application security.** These Security Fabric components include web application firewalls (FortiWeb), application delivery controllers (FortiADC), and sandboxing (FortiSandbox) to address the latest threats that target specific applications as well as unknown exploits. Configuration templates facilitate compliance for the vast array of data that universities store, which may be subject to different regulations. The Security Fabric also includes FortiMail, which secures cloud-based email applications, complementing the built-in capabilities of Microsoft Office 365 or Google G Suite.

**Security operations.** The Fortinet management and analytics solutions (FortiAnalyzer, FortiCloud, FortiManager, and FortiSIEM) provide efficient administration, transparent visibility, and real-time insights across the entire Security Fabric. They simplify management workflows, shorten deployment times, and reduce the chances of misconfiguration caused by human errors. Security operations solutions also encompass advanced threat detection capabilities powered by FortiGuard Labs to spot threats like new malware variants. Another security operations tool, FortiDeceptor, deploys decoys to analyze threat activity and share information across the Security Fabric.

**Secure access.** Large universities are increasingly looking to software-defined wide-area networking (SD-WAN) to reduce the cost and complexity of connecting multiple campuses and satellite sites. But moving from traditional dedicated multiprotocol label switching (MPLS) links to the internet-based connectivity employed by SD-WAN carries a security risk. Fortinet SD-Branch integrates FortiGate Secure SD-WAN with the LAN at each campus or satellite location and includes common management tools on a single pane of glass.

**Endpoint and device protection.** Helping universities to provide the right access to the right person at the right time, FortiAuthenticator supports intent-based segmentation by centralizing user identity information. Fortinet Single Sign-On (SSO) simplifies secure access for end-users, and FortiToken provides a scalable, low-cost solution for two-factor authentication. Once users are signed on, FortiClient detects and blocks malicious objects from web, email, network, and personal storage targeting endpoint devices. At the same time, FortiInsight user and entity behavior analytics (UEBA) bolsters protection against insider threats by detecting behavioral anomalies that might signal a threat.

With the expansion of IoT, university networks are inundated with access requests from cameras and printers, HVAC sensors, and various other devices that are part of smart campus initiatives. To provide visibility of every user-operated or headless device attempting to access the university network, the FortiNAC network access control solution orchestrates automated responses to a wide range of networking events, helping to contain threats before they spread.

**Fabric APIs and Fabric Connectors.** The open ecosystem of the Fortinet Security Fabric unifies Fortinet and third-party security solutions, enabling them to work seamlessly together and eliminating security gaps. The ecosystem includes Fabric APIs, which enable technology providers (Fabric-Ready Partners) to develop integrations for their products with the Fortinet Security Fabric, and Fabric Connectors, which provide deeper, API-based integrations that can be deployed with a click.

**Network operations.** The Security Fabric helps university CIOs bridge the gap between their security operations and network operations, leading to campus networks that are driven by security, rather than hampered by it. This benefit is enabled by a combination of Security Fabric technology and services.

First, FortiManager provides single-pane-of-glass management, zero-touch provisioning of new security solutions, and centralized configuration, with out-of-the-box workflows and scripts and Fortinet open APIs. Second, the Security Rating Service leverages the end-to-end visibility of the Security Fabric to provide an objective risk score against accepted benchmarks and peer institutions, with actionable advice on how to achieve a better risk management posture. Finally, FortiOS, the security operating system powering the entire Fortinet Security Fabric, delivers automation and orchestration features that optimize operations across the university.

**Fortinet—The Best Choice for Colleges and Universities of All Sizes**

With more than 4,000 educational institution customers and 340,000 customers globally, Fortinet is the fastest-growing enterprise network security company in the world and the number one most deployed network security solution.7
Fortinet invests heavily in research and development (R&D) and holds four times more patents than any other network security vendor. One key benefit of in-house R&D is the custom, purpose-built security processors that radically boost performance, enabling FortiGate NGFWs to deliver the best price per performance in the industry.

To ensure top protection from the latest threats, the 200-plus in-house threat-intelligence experts at FortiGuard Labs work around the clock to discover and analyze threats and to deliver countermeasures in the form of continuous updates to the Fortinet Security Fabric.

In order to validate product effectiveness and performance, Fortinet frequently participates in third-party tests, consistently earning top scores. Fortinet has earned “Recommended” ratings for nine different products in tests by NSS Labs, an independent research and testing organization. This is more than any other network security vendor. Fortinet also regularly receives certifications from ICSA Labs, Virus Bulletin, and more. These unbiased validations let consumers know which products perform the best and deliver the lowest TCO, helping them make informed decisions.

Higher Education Positioned to Lead in Cybersecurity

Containing a wealth of intellectual property and personal data, and a highly mobile and transient user base, university networks present some of the most lucrative targets for cyber criminals. Yet institutions of higher education also boast some of the richest intellectual resources for combatting cyber crime. Students of computer science, information systems, and the increasingly common cybersecurity studies are learning about the latest best practices and technologies needed to protect networks in a wide range of industries in the public and private sectors. Where better to see advanced cybersecurity in action than right on their own campuses?

In partnering with Fortinet—the number one network security innovator—university CIOs have the opportunity not only to ensure the security of their own institution’s network but also to serve as a living lab for their students and for other institutions and organizations.

2 Ibid.
4 Ibid.
10 Ibid.
11 As of June 2019, Fortinet has 598 U.S. patents issued by the U.S. Patent and Trademark Office, more than three times as many as the next closest competitor. See “Accelerating and Securing the Cloud On-Ramp: The Fortinet Security Fabric,” July 29, 2019.