SECURING THE CAMPUS WITH FORTINET'S SECURITY SOLUTIONS FOR HIGHER EDUCATION

KEY SECURITY CHALLENGES FOR HIGHER EDUCATION

As institutions of higher education embrace technology to enable learning and collaboration, they are accelerating their adoption of cloud services, bring-your-own-device (BYOD) access, and mobile application use. With the influx of these new services, however, come increased risks to network security.

The volume, speed, and sophistication of new cyber threats mean that it's 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. Boards of trustees are increasingly aware of these vulnerabilities, putting IT leadership in the hot seat.

There is also external pressure to demonstrate security due diligence. Students, faculty, and staff members are using the institution's network to access and transmit a lot of personally identifiable data and other sensitive information. 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). In addition, IT managers 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 a unified effort from security technologies that communicate with one another 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. A security solution 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. These distributed-but-connected security tools can help enforce data security policies, protect data privacy, and prevent attacks in one segment from spreading throughout the campus.

> *"With the FortiGate in the mix, we can manage, monitor, and log traffic, access, and security, and do it simply."*
>
> *– Doug Stewart*
> *IT Senior Manager*
> *University of Georgia*

Take unrelenting user demand in stride. As the volume of transactions and data flowing over the institution's network expands, security technology must have the capacity to monitor, inspect, and filter it without hampering application performance. When there's a need to add security tools, such as firewalls, email and web access gateways, unified threat management, or endpoint security, these 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 time and resources. By consolidating the management of all security functions into a single console, IT can gain a unified view 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 network segmentation, and analytics for real-time response. The Fortinet Security Fabric allows universities and colleges of all sizes to leverage existing investments while moving towards a more resilient integrated security architecture.

Fortinet's Security Fabric protects the campus's entire attack surface by incorporating the following elements:

Network Security. Protects the network from known and unknown threats. FortiGate Next-Generation Firewalls include 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. Reduces complexity by protecting the expanded attack surface across Software-as-a-Service (SaaS) applications as well as private and Infrastructure-as-a-Service (IaaS) cloud deployments, all with a single solution.

Endpoint Security. Detects and blocks malicious objects from web, email, network, and personal storage targeting endpoint devices. FortiClient delivers easy-to-manage, automated, fully customizable endpoint security for a wide range of devices.

Email Security. Inspects email for unwanted and malicious messages and inappropriate/sensitive content. FortiMail provides comprehensive security for both incoming and outgoing messages and is easy to deploy, operate, and manage.

Web Application Security. Protects web applications from threats targeting known and unknown exploits. FortiWeb (web application firewall) uses the latest threat intelligence to protect web applications from sophisticated attacks while lowering management and operational costs.

Advanced Threat Protection. Detects intrusions that have evaded conventional, established defenses. FortiSandbox isolates and inspects any suspicious files detected by security tools to stop them before damage is done.

Management and Analytics. Enables visibility and management of Fortinet and partner products for smooth operation and greater insight. Reduced cost and complexity with centralized control of the entire network from a single console drive a lower TCO. Automated reporting helps track compliance.

Unified Access. Fortinet's secure access solutions deliver comprehensive security and access control for secure Wi-Fi and enable secure user/admin connectivity.

"As more of our customers migrate into our data centers, virtualizing and firewalling their systems, we needed to ensure that our firewalls weren't a bottleneck for available bandwidth. Fortinet's solution provided us with the throughput, flexibility and manageability that both our customers and engineers appreciate."

– David Hunter
Manager, Campus LAN Infrastructure
Indiana University

FORTINET—THE BEST CHOICE FOR COLLEGES AND UNIVERSITIES OF ALL SIZES

With more than 500 educational institution customers and 340,000 customers globally, Fortinet is the fastest-growing enterprise network security company in the world and the #1 most adopted network security solution.

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 Fortinet firewalls to deliver the best price per performance in the industry.

To ensure top protection from the latest threats, Fortinet's 200+ in-house threat intelligence experts 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.

Similarly, the research and advisory firm, Gartner, provides insights on technology and vendors to help business leaders make purchasing decisions. Multiple Fortinet solutions can be found in Gartner Magic Quadrants, including Enterprise Network Firewall, UTM, Wired and Wireless LAN, and Web Application Firewall.

FORTINET NETWORK SECURITY EARNS TOP MARKS

Fortinet provides a complete, scalable solution for higher education institutions large and small that delivers proven security validated by ongoing third-party testing.

Integration, automation, and single-pane-of-glass management simplify operations to save IT staff time.

With top threat intelligence, a large customer base, and a strong track record in education, Fortinet is the ideal higher education security partner.

> *"In Fortinet, we have found a partner with the foresight to help us forge the next generation of cybersecurity professionals."*
>
> *- Professor Kris Rosenberg*
>   *Program Director, Information*
>   *Technology and Cybersecurity*
>   *Oregon Institute of Technology*

F⊡RTINET.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

May 18, 2018 12:00 PM

Macintosh HD:Users:US:Documents:FORTINET:Higher_Ed_Solution_Brief:Higher_Ed_Solution_Brief_ck