WHITE PAPER

Protecting Higher Education with the Fortinet Security Fabric

Executive Summary

As institutions of higher education embrace technology to enable learning and collaboration, they accelerate their adoption of cloud services and 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 across cloud deployments. It also provides robust analytical tools and controls to protect ever-evolving higher education networks and supports a number of use cases.

Key Security Challenges for Higher Education Environments

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.[1] 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).

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."[2]

– Bradley C. Wheeler,
CIO Indiana University

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. CIOs 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, 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 Security Use Cases

The above challenges break across various use cases for higher education:

The smart campus

Many smart university campuses function similarly to smart cities—students can access services across campus with just one identification card or mobile application including food, housing, and entertainment. While this provides an optimized student experience, it creates a vulnerable environment for cyber criminals to exploit. To fully protect this infrastructure from advanced threats, universities need a unified set of solutions that integrate to provide an end-to-end, multilayer defense, detection, and response.

The Fortinet Security Fabric delivers a broad, integrated, and automated security solution with integration from data center to cloud. Universities gain centralized visibility and control across the entire campus.

The Security Fabric is powered by industry-leading FortiGate next-generation firewalls (NGFWs) as well as artificial intelligence (AI)-based threat intelligence from FortiGuard Labs. In addition, university CIOs can integrate security orchestration, automation, and response (SOAR) tools and security analytics tools with FortiAnalyzer and FortiManager to enable a strategic and coordinated response to advanced threats. Advanced endpoint protection, detection, and response tools work together with FortiNAC network access control (NAC) to protect endpoint and IoT devices.

Fortinet cybersecurity solutions seamlessly integrate into the Security Fabric, along with dozens of third-party solutions delivered by Fabric-Ready Partners. This means university CIOs can leverage parts of their existing security infrastructure and break down silos. Extensive application programming interface (API) tools enable integration of third-party tools.

Fortinet Dynamic Cloud Security solutions break down silos between multi-cloud environments. FortiCASB cloud access security broker (CASB) enables complete visibility and control, while FortiCWP cloud workload protection (CWP) helps teams keep track of their cloud security posture, analyzing traffic across hybrid clouds. FortiWeb web application firewall (WAF) leverages powerful machine-learning (ML) capabilities to define benign and malicious cloud traffic, and then blocks malicious traffic.

Six research areas of interest for higher education cyberattackers:[3]

1. Scientific
2. Medical
3. Defense
4. Public policy
5. Nuclear issues
6. Economic forecasting

Growing Expectations

Students may arrive on campus with eight or nine different devices, expecting that each will have wireless internet access. Pervasive and high-speed Wi-Fi may even be a differentiator in some students' college-selection process.[4]

The decentralized campus

It is not uncommon for universities to extend services from the main campus across multiple branch campuses, remote research locations, or locations abroad. Not only does this add security complexity to the network but also requires greater bandwidth demands from branch locations. Connections between every location must be secure, cost effective, high performing, and scalable to the influx of school traffic throughout the year.

Fortinet solutions for decentralized campuses enable institutions to provide secure, high-performance networking with branches. FortiGate NGFWs include secure, cost-effective software-defined wide-area network (SD-WAN) technology. SD-WAN enables campus locations to achieve direct internet access so networking traffic can travel between clouds, or over a virtual WAN (vWAN) within select public clouds. The Fortinet Secure SD-WAN solution is built into the FortiGate NGFW itself, removing the need for additional point products and simplifying network complexity.

At remote campus locations, Fortinet SD-Branch extends Secure SD-WAN to the access layer that enables secure networking at branches. In addition, Fortinet SD-Branch provides consistent security across the internet, wireless network, and switching infrastructure.

Integrated CIO and cybersecurity education

While universities often offer courses and training focused on cybersecurity, the curriculum may be more theoretical and less focused on the current threat landscape and how to proactively defend against it. Consequentially, students may not graduate with the full spectrum of knowledge to successfully work in the field.

University CIOs can help combine academia and real-world experience with the threat landscape by partnering with industry experts who can provide the latest threat intelligence and explain burgeoning trends and cybersecurity best practices The Fortinet Network Security Academy enables CIOs to help both students and staff to hone their knowledge with industry-recognized cybersecurity certifications.

The Fortinet Network Security Academy offers an eight-tiered Network Security Expert (NSE) certification program that validates a security professional's expertise. These programs include a range of both self-paced and instructor-led courses, along with practical exercises that demonstrate mastery of complex network security concepts.

Campus safety

Ensuring physical student safety is of paramount importance for universities. It is a university's moral obligation to keep students safe from all types of physical harm ranging from criminal activity to sexual assault, as well as to prevent these types of crimes from occurring on campus.

Universities need a comprehensive approach to cyber and physical security with single-pane-of-glass monitoring to ensure campus safety.

Yet, implementing connected physical security across multiple buildings, walkways, and housing can be a complex process. Universities need to survey indoor and outdoor areas, while ensuring that the physical security is integrated with the cybersecurity infrastructure.

The Fortinet Security Fabric integrates cyber and physical security, allowing the entire security infrastructure to be viewed and managed with a single pane of glass. University CIOs gain the peace of mind that security cameras, recorders, emerging facial recognition and weapons detection technologies, and recordings are a seamless part of their overall security architecture.

> "In two short years, there could be nearly 30 billion autonomous Internet-of-Things devices on [university] networks."[5]

Fortinet Differentiators for Higher Education Cybersecurity

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

The Security Fabric protects the university's entire attack surface by incorporating the following elements:

Integrated platform

The open ecosystem of the 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 Security Fabric. It also includes Fabric Connectors, which provide deeper, API-based integrations that can be deployed with a click.

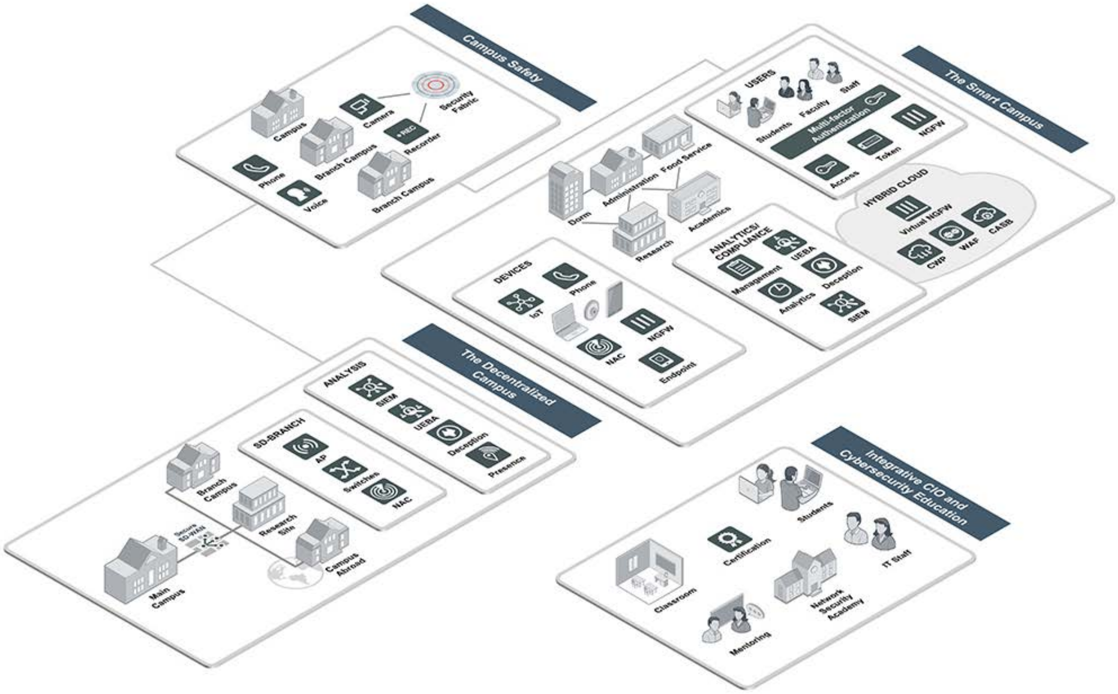

Figure 1: Higher education security architecture and use cases.

Secure branch campus

Large universities are increasingly looking to 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 Fortinet Secure SD-WAN with the LAN at each campus or satellite location and includes common management tools on a single pane of glass.

Networking, cybersecurity, and physical security

Fortinet protects the network against known and unknown threats with industry-leading physical and cybersecurity that seamlessly integrates. When networking, cybersecurity, and surveillance functions combine with single-pane-of-glass management, universities can take a more proactive security posture across main and branch campus locations.

Insider threat protection

Fortinet delivers insider threat protection from malicious and unintentional threats with a range of tools. FortiAnalyzer and FortiToken deliver identity and access management to authorize users, and FortiNAC orchestrates automated responses to a wide range of networking events, helping to contain threats before they spread. FortiInsight, which uses ML to hone its accuracy while reducing false positiives, bolsters protection against insider threats by detecting behavioral anomalies that might signal a threat, while FortiDeceptor deploys decoys to analyze threat activity and share information across the Security Fabric.

Robust threat intelligence

To ensure top protection from the latest threats, FortiGuard Labs collects and analyzes real-time threat intelligence. An AI-powered self-evolving detection system (SEDS) has been using ML capabilities for nearly eight years, uncovering the latest known and unknown threats. FortiGuard Labs delivers countermeasures in the form of continuous updates to the Security Fabric to protect university networks. These AI-enabled capabilities that are integrated across all of the security elements enable higher education CIOs to keep pace with the rapid changes taking place in the threat landscape.

Industry-leading Threat Protection

FortiGate NGFWs have the industry's lowest TCO per protected Mbps.[6]

NSS LABS RECOMMENDED

In tests by NSS Labs, Fortinet has earned "Recommended" ratings for nine different products—more than any other network security vendor.[7]

Industry leadership

Fortinet is continuously recognized as an industry leader with best-of-breed security and networking solutions. Fortinet has achieved the best score in the NGFW Security Value Map from NSS Labs, and has achieved nine "Recommended" ratings from NSS Labs.[8]

Conclusion

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 combating 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. And there is no better place to see advanced cybersecurity in action than right on their own campuses.

In partnering with Fortinet, 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.

[1] Lindsay McKenzie, "At What Cost Wi-Fi?," Inside Higher Ed, April 17, 2018.

[2] Lindsay McKenzie, "On Red Alert," Inside Higher Ed, March 6, 2019.

[3] Ibid.

[4] "Ohio State University trustees approve contract with Apple to launch Digital Flagship Initiative," Ohio State News, April 6, 2018.

[5] Eli Zimmerman, "How Universities Can Mitigate IoT Risk on Campus," EdTech, January 15, 2019.

[6] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October, 2019.

[7] Ibid.

[8] Ibid.

January 24, 2020 12:39 AM
D:\Fortinet\White Paper\Vertical Marketing - Higher Education\wp-FA-protecting-higher-education-with-the-fortinet-security-fabric
521372-0-0-EN