IT IN HIGHER EDUCATION: BALANCING SERVICE, LEARNING, AND ACCOUNTABILITY

Higher education is a challenging environment for IT. On one hand, universities prioritize openness and sharing for the sake of learning. On the other, they are subject to intense security pressures that you'd expect to find in highly regulated verticals and resemble enterprises in their complexity. They have thousands of users and applications, tiers of users, from students and faculty to administration and research facilities, and they need to find cost-effective ways to protect their networks. These networks are required to meet the next-generation campus demands of students and staff while being developed within a tight budget often determined by both state and federal governments. At the same time, the attack surface continues to grow wider and weaker, making it a more appealing target for cybercriminals around the world.

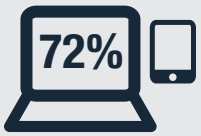
Threat vectors antagonizing the next-generation campus include:

- Traditional malware delivery methods: With the threat landscape growing at a rapid rate, well-known attacks, such as phishing, distributed denial of service (DDoS), and ransomware are making their way into higher education. When student records and sensitive research datasets are involved, risk should be assumed.
- Mobile devices like cell phones and laptops: Connected devices are often unmonitored and not designed for optimal security.
- Internet of Things (IoT) devices: Inherently unsecure, these devices are targets of opportunity for hackers, and they can also be weaponized.

Universities house a lot of valuable information. Where there is enrollment and scholarship data, for example, there are identities to be stolen. Where there is proprietary institutional research, thought leadership is at stake. In addition, where there are thousands of connected devices on one campus, service disruptions and breaches can wreak havoc.

Higher Ed institutions face enormous complexity but are nevertheless required by the marketplace and their constituents to offer seamless IT services. Now more than ever, they are looking for trusted partners to shepherd them through this churning IT landscape.

DIGITAL TRANSFORMATION IN NUMBERS



of students connect at least two devices to the campus network at the same time

Educause Review July/August 2016, The Internet of Things in Higher Education

Today's students spend **140+ hours** a week with their tech devices

Refuel Agency Unveils the 2015 College Explorer, Febuary, 2016

of higher education institutions now look to cloud options first when considering new investments

MeriTalk Study, "Destination Cloud: The Federal and SLED Cloud Journey," September 2016

CHALLENGES UNIQUE TO HIGHER EDUCATION

Gone are the days of computer labs and centralized infrastructure. Today, with each student bringing two to three devices to campus, IT services are highly distributed and fluid. Disparate teaching, testing, and research applications must also be integrated and protected. The types of data they contain are as diverse as they are valuable. In addition to protecting the network and everything connected to it, Higher Ed institutions must prove regulatory compliance, particularly PCI DSS, HIPAA, and FERPA.

Above all, universities and their administrations are accountable for providing advertised learning outcomes. Today's Higher Ed consumers – parents as well as students – are savvy and outcome-oriented. Disruption to a university's core business of learning can spell disaster for recruitment, incoming tuition revenue, and reputation.

SECURITY REQUIREMENTS FOR ED TECH LEADERS

Today, a couple of best practices can ensure schools remain protected and able to carry out their missions.

1. MEET KEY EDUCATIONAL NEEDS

- Encourage online learning and free inquiry: Today's courses and majors embrace a wide range of centralized and decentralized learning

tools – many of which are housed online. In addition, students are empowered to find their own answers and innovate in virtual groups, which means they're vulnerable to cyberattack and difficult to track.

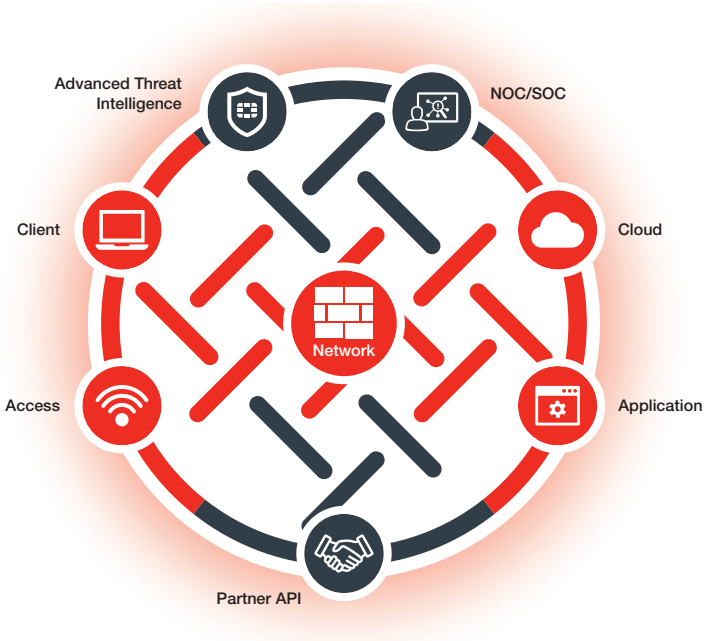
- Accommodate many diverse devices: The average student walks onto campus with two or three devices – not including the laptop or other connected equipment they're also likely to use.
- Allow access to specific applications related to research, administration, and even fundraising: In higher education, teaching is only one component of the IT infrastructure. With multiple business processes at work at all times, functionality and uptime are mandatory, even throughout periods of upgrade and change.
- Secure email and Wi-Fi access points: These are two of the most frequently used tools on campus – and the most obvious points of attack for would-be data thieves.
- Use firewalls/sandboxes: Schools must protect their IT infrastructures with advanced security.

2. EMBRACE A SECURITY FABRIC APPROACH

- Provide complete protection and cohesion: A security fabric provides a comprehensive solution comprised of integrated security and networking products that share intelligence for faster response. It also delivers visibility into the entire network through a single pane of glass. Many universities, unfortunately, have developed IT in a piecemail fashion, where very specific knowledge and training is required to make changes and updates, leaving gaps in security and visibility.
- Maintain long-term security and visibility: By contrast, a fully developed security fabric ensures compatibility, scalability, easy upgrades, and simplified management. Fewer IT staff are required – especially important in under-resourced institutions.
- Ensure affordability: The first obstacle for institutions is often monetary, but fortunately, a security fabric-based solution creates enormous efficiency and consolidation that can finally move universities beyond old, entrenched IT expenditures and subscriptions.
- Efficiently prove regulatory compliance: Ensuring and demonstrating compliance can be difficult and time-consuming, but a security fabric delivers automated compliance auditing and detailed reports to ease this burden.

IMPROVING SECURE STUDENT LEARNING

To address their unique challenges and requirements, Fortinet offers Higher Ed a new approach to cybersecurity, the Fortinet Security Fabric, which promises security that is broad, powerful, and automated.



- **Broad:** The Security Fabric covers the entire attack surface. Security can be applied to the network, endpoints, access, applications, and cloud.
- **Powerful:** The Security Fabric uses security processors to reduce the burden on infrastructure, delivering comprehensive security without affecting performance.
- **Automated:** The Security Fabric enables a fast and coordinated response to threats. All elements can rapidly exchange threat intelligence and coordinate actions.

With the Fortinet Security Fabric, Higher Ed is well positioned to meet both current as well as future security needs. With integration that provides true end-to-end protection, the Fortinet Security Fabric can easily secure Higher Ed's next-generation campus in its entirety, enabling organizations to provide safe, quality learning environments today, tomorrow, and well into the future. For more information visit www.fortinet.com/education or contact us at education@fortinet.com.

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

September 28, 2017 8:33 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:SB-IT-in-Higher-Education:sb-it-in-higher-education