SECURING AND SIMPLIFYING NETWORK ACCESS FOR HIGHER EDUCATION

Enabling Secure, Automated, High-Capacity Connectivity

EXECUTIVE SUMMARY

Colleges and universities offer target-rich environments for cyber criminals. From financial, medical, and personal data to government and commercial research, educational networks can contain a wealth of data, numerous access points, and large volumes of endpoint access—all of which require unique security solutions. Institutions must define and implement a comprehensive security architecture that provides end-to-end network visibility, dynamic access control, and automated threat responses. FortiNAC offers an ideal network access control (NAC) solution. Part of the Fortinet Security Fabric, it offers compatibility with a wide range of third-party security solutions to help schools secure sensitive data while maximizing the value of their existing infrastructure investments.

DIGITAL CHALLENGES FOR HIGHER ED—BYOD AND IOT

Today's digital campuses require connectivity for numerous types of devices—from the mobile solutions of faculty, staff, and students to smart devices in classrooms and dormitories. Securing the network while enabling easy, automated access for a large volume and variety of endpoints is one of the greatest challenges for colleges and universities. Schools must balance technology controls with simplified access to ensure a productive and secure campus environment.

A recent survey finds that 99% of students have at least one digital device, the vast majority of students have two devices, and approximately one-third of students have three or four digital devices on campus.[1] The quantity of devices per student has increased steadily over the last few years, rapidly expanding the number of endpoints that must be controlled. In addition to greater mobile access demands as a result of bring-your-own-device (BYOD) policies, colleges and universities are also facing a surge of new Internet of Things (IoT) devices that are flooding campuses. With thousands of new IoT devices introduced each year, students and campuses alike are now connecting IoT-enabled devices—such as printers, cameras, lighting, and climate controls—to the campus network.

Moreover, campus facility managers are often unintentionally complicating this already intricate network. By adding even more devices to networks without notifying campus IT and security teams, facility managers run the risk of creating new Shadow IT issues that add to the already growing risk of vulnerabilities.

FORTINAC PROVIDES:

- Complete visibility and automated onboarding for endpoints (BYOD and IoT)
- Pre-connect and post-connect device monitoring
- Granular network access controls to enforce minimum security requirements (OS, antivirus)
- Ability for custom access levels by user or role
- Automated threat responses to quarantine suspicious IoT devices, BYOD, and other endpoints
- Quick and easy scalability—up to 10,000 devices from a single solution instance

FortiNAC profiles every endpoint and infrastructure device on the network, and provides contextual awareness about the device, user, and applications. It also tracks and monitors all activity.

Northeastern University is even piloting an Amazon Echo Dot integration program that links a student's own personal digital assistant product with their university account to answer questions and reduce wait times throughout the campus.[2] As these kinds of programs expand, students may be using IoT-enabled devices to do everything from managing enrollment and payment accounts to ordering pizza delivery via their student meal plan. But since most IoT devices have little to no built-in security, these connected devices offer an easy target for hackers to exploit.

THE NEED FOR AUTOMATION—PROVISIONING, ACCESS, AND RESPONSES

Without compensating security controls, introducing countless new endpoints onto a university's network can be dangerous and expose a school to a wide variety of attacks. Universities must be able to monitor and control endpoint access, as well as set minimum security standards for students, faculty, contractors, and guest devices. Schools must also ensure an automated and efficient way for these tens of thousands of devices and users to access the system with the appropriate level of access for each.

Additionally, with thousands of security alerts per day, overwhelming network traffic, and scarce IT resources, colleges and universities cannot manually review all potential issues. For effective security, schools must also automate policy-based event triage and quarantining of suspect users and devices.

SOLVING THE CAMPUS SECURITY CHALLENGE

As part of the Fortinet Security Fabric architecture, FortiNAC offers a NAC solution designed to protect networks with IoT devices. Security leaders in these environments need to be aware of each and every device and user on their networks and allow them appropriate access.

FortiNAC equips security leaders with the tools they need to successfully manage and secure their complex IoT networks. The Fortinet solution provides the visibility to see everything connected to the network, as well as the ability to control those devices and users, all while providing dynamic, automated responses to threats.

VISIBILITY

With thousands of endpoint devices, identifying "who, what, when, and where" is critical to locating and securing compromised devices. FortiNAC provides the deepest level of network endpoint visibility. It profiles every endpoint and infrastructure device on the network, and provides contextual awareness about the device, user, and applications. It also tracks and monitors all activity.

For IoT devices, FortiNAC identifies headless devices each time a device connects to the network. When new devices connect, it notifies the device sponsor to authorize the device onto the network and records every action taken by the device. With simple, centralized management, FortiNAC ensures that if a device is compromised, it can be located quickly, even if the device is in a remote location.

With simple, centralized management, FortiNAC ensures that if a device is compromised, it can be located quickly, even if the device is in a remote location.

CONTROL

FortiNAC provides contextual awareness for scalable onboarding and dynamic network access control. Network access can be assigned using automated, predefined profiles—saving a significant amount of time when onboarding large numbers of students, faculty, contractors, guests, or staff.

To manage high volumes of BYOD devices, FortiNAC helps institutions set and enforce minimum security requirements for things like current operating system patches and antivirus software. Using a pre-connect scan, FortiNAC only grants access for devices that meet requirements and can automatically direct users to a self-remediation page for those that don't qualify. FortiNAC also provides continuous post-connect scanning to look for devices and/or users that act suspiciously or fall out of network compliance.

In addition, FortiNAC provides granular control of endpoint access policies and permissions by role or by user to ensure users only receive the necessary amount of access. Integrated within the Fortinet Security Fabric, FortiNAC provides centrally managed, end-to-end control of the entire fluid network, including satellite campus locations.

AUTOMATED THREAT RESPONSES

FortiNAC supports automated threat responses including immediate quarantining of suspicious devices/users, triaging of events, and streamlining analyst reviews by delivering all contextual information along with the alert. By leveraging contextual awareness from the broader Fortinet Security Fabric, FortiNAC helps analyze and prioritize security events. It streamlines multistep workflows and integrates with ticketing systems to provide real-time endpoint containment. This speeds the time to resolution and reduces the burden on strained IT resources.

FortiNAC also acts as a compensating control for IoT devices with weak security. It monitors the devices for unusual behavior and automatically quarantines devices that act suspiciously. For example, if an IoT device starts pinging a DNS server, it will be tracked, an alert is generated, and the port can be immediately locked down while awaiting analyst review.

To manage high volumes of BYOD devices, FortiNAC helps institutions set and enforce minimum security requirements for things like current operating system patches and antivirus software.

FortiNAC supports automated threat responses including immediate quarantining of suspicious devices/users, triaging of events, and streamlining analyst reviews by delivering all contextual information along with the alert.

HIGHER EDUCATION CASE STUDY: PEPPERDINE UNIVERSITY

Pepperdine University is a liberal arts and research university with about 8,500 students and 2,000 faculty at its main campus near Malibu, plus five graduate schools across Southern California. Dr. Kim Cary, CISO at Pepperdine University, has some key insights about the role of a university network in the BYOD era. "Our students compare the university's ease of wireless connection to places like McDonalds and Starbucks, so we don't want to be super-intrusive and make people jump through a lot of hoops."

Cary also notes that if Pepperdine faculty come to campus with a new device, it needs to connect and function seamlessly. "They come to class, turn on their device, and expect to get network access to the resources they need. And they expect the process to be easy regardless of the device they're using."

But how do you ensure a quality experience for thousands of users bringing every conceivable type of device onto campus? How do you block infected devices without restricting the vast majority that are safe? These questions led Cary to another key insight: "The device type doesn't matter—what's important is to provide appropriate access and respond immediately to any security threat."

Cary created a new kind of network control for BYOD at Pepperdine that could meet the needs of a dynamic campus community. "We need to know who is on our network, give them appropriate access, and let them know where they stand at all times. And we need a solution that's fully automated and user-friendly, which is easy to do with FortiNAC."

Designed with scalability in mind, FortiNAC also helps lower total cost of ownership (TCO) by not requiring a server in every deployment location. It leverages existing directory, networking, and security infrastructures to protect existing investments and minimize disruption.

FLEXIBLE AND SCALABLE NAC DEPLOYMENTS

FortiNAC offers unparalleled visibility, control, and automated responsiveness for educational network access. Beyond those core capabilities, FortiNAC can be deployed as a hardware appliance, a virtual appliance, or a cloud service—offering school security architects a flexible, third-generation NAC solution that can adapt to the unique needs of any network environment. Designed with scalability in mind, FortiNAC also helps lower TCO by not requiring a server in every deployment location. It leverages existing directory, networking, and security infrastructures to protect existing investments and minimize disruption.

[1] Joseph D. Galanek, Dana C. Gierdowski, and D. Christopher Brooks, "ECAR Study of Undergraduate Students and Information Technology, 2018," EDUCAUSE, October 2018.

[2] Elizabeth Weise, "Exclusive: Alexa, when's my next class? This university is giving out Amazon Echo Dots," USA TODAY, June 20, 2018.

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
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

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

303124-0-0-EN
October 29, 2018 3:01 PM
D:\Fortinet\Work\October 2018\102718\sb-network-access-higher-education