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. The bring-your-own-device (BYOD) movement has been a way of life at Pepperdine for many years. Thanks to the FortiNAC network access control (NAC) solution, students, faculty, and staff, as well as thousands of guests at special events, can use their personal devices safely on the campus network.

Dr. Kim Cary, chief information security officer (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 McDonald’s and Starbucks, so we don’t want to be super-intrusive and make people jump through a lot of hoops.” In addition, Cary notes that Pepperdine’s distinguished faculty sometimes come to campus and go directly to class with a new device. “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 NAC.”

“Dr. Kim Cary, CISO, Pepperdine University

CASE STUDY

Pepperdine University Enables Network Access Control for Rapid Threat Remediation

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. The bring-your-own-device (BYOD) movement has been a way of life at Pepperdine for many years. Thanks to the FortiNAC network access control (NAC) solution, students, faculty, and staff, as well as thousands of guests at special events, can use their personal devices safely on the campus network.

Dr. Kim Cary, chief information security officer (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 McDonald’s and Starbucks, so we don’t want to be super-intrusive and make people jump through a lot of hoops.” In addition, Cary notes that Pepperdine’s distinguished faculty sometimes come to campus and go directly to class with a new device. “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 NAC.”

Securing the Network for BYOD

Pepperdine selected the FortiNAC solution to enable a flexible, secure BYOD environment to enhance the university experience. The solution’s endpoint visibility and automated, policy-based access control enable thousands of varied users to safely access the university network with devices of their choice.

FortiNAC simplifies access permissions through group profiles to enable users to get on the network quickly with access according to their role. Students, faculty, and staff enter their credentials once to register their device, then access the appropriate university network. This is crucial to quickly on-boarding high volumes of new students each semester.
FortiNAC also regulates guest management. Contractors get access set by their sponsoring department, while guests get web access only to public campus sites and the internet. Furthermore, using FortiNAC’s guest management features, event sponsors at Pepperdine can create hundreds or thousands of accounts for conference visitors with just a few clicks, specifying parameters such as start date, end date, and time of day, which FortiNAC enforces automatically. FortiNAC also logs all connection events, allowing IT staff to track registrations, device types, operating systems, and changing trends to help manage service levels and plan for capacity.

The Secure, Responsive University

One of the key features that Cary likes about the FortiNAC solution is that it integrates with the university’s intrusion detection system (IDS). When the IDS detects an attack, FortiNAC identifies the device and automatically blocks it from the network. FortiNAC then notifies the device owner, via a webpage, that they’re quarantined and explains how to contact someone for help to fix the issue. “We have security, but we also have a great user experience to go with it,” Cary adds. “By providing the quarantine reason and remediation-help link to the student, staff, or visitor, we keep their frustration low and reduce troubleshooting calls to overworked network staff.”

The solution’s ability to seamlessly integrate with numerous best-of-breed security technologies is a huge benefit for Pepperdine. This saves numerous IT ticket remediation hours, enhances the user experience, and enables Pepperdine to leverage top security solutions to build a comprehensive network security solution.

The same approach helps protect the university from copyright violations. When Pepperdine receives a Digital Millennium Copyright Act (DMCA) takedown notice, information security staff use FortiNAC to identify which device was used when the violation occurred, quarantine the device, and notify the student that their computer is blocked due to a copyright violation. The resulting webpage instructs the student to contact Tech Central for help. “We have very few repeat offenders,” Cary observes. “By enabling us to follow the law, NAC helps protect the student and the university from liability.”

Automating Access for University-owned Devices

Pepperdine also uses FortiNAC to manage its own networked devices. For example, using FortiNAC’s security automation capabilities, the university can move their enterprise printers anywhere on campus, and FortiNAC automatically puts them on the appropriate virtual local-area network (VLAN)—which is on a dedicated network for security reasons—thereby eliminating a previously manual task. Pepperdine has been so impressed with FortiNAC that they are planning to expand usage to include automated threat response.

1 Formerly Bradford Networks.

Business Impact

- Provides fast, easy, and secure network access for thousands of students, faculty, and guests
- Identifies and blocks compromised devices, and provides self-service remediation
- Protects the university from copyright violations when students or staff download copyrighted materials onto their devices
- Reduces user frustration and troubleshooting calls to overworked technical staff
- Automates network provisioning for headless infrastructure devices that are often moved around campus

Solution

- FortiNAC

“We have security, but we also have a great user experience to go with it. By providing the quarantine reason and remediation-help link to the student, staff, or visitor, we keep their frustration low and reduce troubleshooting calls to overworked network staff.”

– Dr. Kim Cary, CISO, Pepperdine University