Senforce Technologies Secures Neumont University's Mobile Network

Neumont University is on the fast track to becoming well known for its students' competitive edge in this technology-laden world. Neumont only offers two accelerated degrees, Bachelor of Science in Computer Science and Master of Business Administration, yet that is all Neumont University graduates need to be some of the most sought-after software developers in the world.

The university is not short on history, or prestige. Neumont received the CIO 100 Award last year and was recently dubbed by MSNBC, "one of the most talked about colleges in America." and the University is accredited by the American Council for Independent Colleges and Schools.

Neumont University's curriculum is project-based and focuses on the skills most valued by today's employers. Students are mentored by some of the industry's most distinguished faculty members, and receive advanced training in modeling, architecture, and business processes. Neumont is also not short on big-name technology backers, as IBM and Microsoft are partners of the university's development environments.

Neumont University is committed to preparing students for today's demanding technology careers through real-world, interactive curriculum, as well as outfitting students, faculty and staff with the best technology available.

Neumont University's mobile security challenges

"Everyone here from students to administrators is highly advanced in the complexity of technology systems and software," says Peter Green, director of IT at Neumont University. "Basically, we know as IT administrators our target audience is the same profile as a hacker. We have people with very good computing skills, to say the least, and they have the ability to compromise our corporate data."

Considering practically every student, faculty and staff member at Neumont University uses a Lenovo ThinkPad®, so the network is in constant motion day and night. Mobile computing in the classrooms and labs is not enough, as students take their schoolwork and enterprise-sized projects home, to the nearest restaurant, or to partner businesses.

With so much critical data residing on the university's endpoints, specifically the students' laptops, the endpoint security solution needed to provide IT administrators with a comprehensive ability to secure and monitor data as it moved in, out and through the university's network.

"A high security priority is absolutely ensuring the integrity of our grading system is preserved," Green emphasizes. "We have to say that the degrees that we were handing out are valid."

Grading, students' personal data, and flexible connectivity are among the high priority security policies that Neumont University's IT administrators are most concerned about. Secure grading data is, of course, of utmost importance considering needed accreditations and the integrity of faculty and their curriculum. Visitors, students, enterprise partners, and professors needed highly flexible connectivity for projects that are worked on the university's main campus, as well as from a variety of remote locations away from the university.

"Yes, student connectivity was a huge challenge, not to mention the fact that, for our program, using anything other than a wireless environment was out of the question," Green says. "We weren't going to be able to tether students to a board at all times, because at a minimum they had to at least be mobile enough to move from classroom to classroom and in between with their laptops. However, the security methodology we started out using to control the laptops as they were leaving from and returning to our environment didn't give us comprehensive control and was too internal network centric."

Approaching endpoint security from the outside in

Neumont's mobility and wireless network connectivity requires 80 Aruba A-band access points on two floors, connecting 400 laptops to 35 servers, four of them Senforce endpoint security and intelligent network access control (INAC) servers, over two networks. One of the four servers from Senforce is a security policy update server that Green says has helped them do everything regarding endpoint security from the "outside in."

"If we want to publish any policy or change any settings, we just work those features through the main console and the policies stretch out to all the endpoints from there," says Green. "Overall management has been significantly reduced and we are a lot more secure than we were before Senforce."

Like many organizations, Neumont's IT security team began securing their wireless network and its endpoints by getting to the low-hanging, security-challenging fruit first. They added and configured separately antivirus, patching methodology, and firewall security features.

"We started by approaching endpoint security from the inside out," says Green. "We wanted to protect our network from our endpoints, which is a limited approach. And, the security policies we had on our endpoints were also limited and incomplete. Yes, it was a layered approach, but we were trying to piece together separate security configurations and applications."

Green credits Senforce Technologies and its Endpoint Security Suite (ESS) for providing Neumont University with a comprehensive solution with all of the features they needed to completely control what each laptop was doing while the devices were connected to the wireless network.

Wi-Fi networks are inherently insecure and Neumont IT was mainly on guard for rogue and unsecured access points, accidental associations, man-in-the-middle attacks or Evil Twins, Ad hoc networks, and dual homing security threats.

These typical Wi-Fi threats were compounded by other threats that could also potentially punch holes or open gaps in the university's perimeter defenses. With the employees and students working and studying at home, on the road, etc., having security policies to control removable storage devices through Senforce ESS has also proven invaluable.

Controlling data in motion

Through ESS, Senforce focuses on securing PCs, laptops and tablet PCs (endpoints) by providing a comprehensive, 360-degree view of endpoint security management. The suite gives IT and security administrators the ability to secure and control data in motion as it moves in and out of an organization, and delivers this through centralized management functionality to create, distribute and enforce security policies on endpoint devices.

The addition of removable storage security in ESS 3.2 to Senforce's existing wireless security, advanced firewall, endpoint integrity, Location-Aware™, data security and centralized management and reporting capabilities increases IT departments' control over users' endpoint devices, without compromising their productivity.

ESS enables IT administrators to enforce the security policies that are appropriate or allowed for each endpoint device. Senforce believes that no single security policy fits everyone, every threat profile, and every situation.

The suite's key foundational feature, Location-Aware technology, ensures that the appropriate security policy is automatically enforced based on the location of the laptop, tablet PC or desktop PC. The addition of removable storage device security allows security administrators more granular control to determine what a user may connect to their laptop or PC and where they are allowed to do it, as well as controlling how much data may be transferred from or to their endpoint device.

Security administrators can now choose to give users complete freedom over the attachment of external devices via USB, FireWire, Bluetooth, Infrared, and PCMCIA ports, or limit them to only having data transfer capability within the safe office environment.

When employees are on the road, they may be limited to only reading external storage devices, or have no ability to connect anything at all, other than a mouse and keyboard. Stricter controls may be implemented, whereby users are restricted to attaching only those devices that have a specific serial number.

Trust in the system

“With Senforce we have a complete endpoint solution and a single console for our security management,” says Green. “We’ve seen a great return in our time reduction of working to prevent security problems, and the trust in the system that we have from Senforce has increased exponentially.”

Green says Neumont IT management knows Senforce ESS is doing its job not only from all of the reporting functionality and single management console, but also from students having to come to them and request more functionality.

“This increases our trust factor in the security system,” says Green. “Our average user here is capable of some amazing security circumventing maneuvers. Knowing that ESS has locked down everything from the outside in is a great feeling for us.”

ABOUT SENFORCE TECHNOLOGIES, INC.

Senforce Technologies® is a market leader of endpoint security management and enforcement. Senforce enables IT organizations to protect employee computers, networks and data from malicious attacks, unauthorized access and misuse. Senforce products automate and control security practices by location (at the office, on the road or at home) through centralized policy-enforcement. Senforce customers, including financial services, government and major enterprise organizations use Senforce products for removable storage device control, wireless security, network access control, personal firewall, security policy and compliance enforcement. For more information on Senforce, or any of its solutions, visit www.senforce.com or call 1.877.844.5430.