

Widener University Uses Top Layer Devices to Protect from Incoming Classes' Unpatched Computers – MS Blaster and Welchia Expelled from School Systems

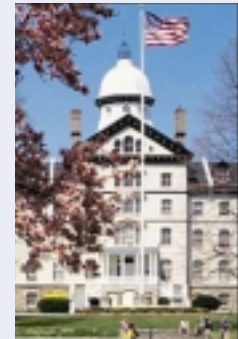
Solution Overview

Profile: Widener University, a comprehensive, private, doctoral/research-intensive institution of eight schools and colleges with its main campus located in Chester, PA, has nearly 7,000 students and more than 300 faculty and staff that rely on its network availability to live, learn, and work at the university.

Challenge: At the start of each semester, Widener students often brought laptop and desktop computers with them that had been infected with viruses and worms while in the outside world. Having dealt with the time-consuming, costly clean-ups that infected systems can create once inside university firewalls, Widener needed to act quickly before students returned for school and plugged into the university networks – especially after a summer that saw the explosion of the MS Blaster and Welchia worms around the world. Widener University sought a solution that would supplement its existing firewalls and easily integrate with the university's existing security infrastructure.

Solution: Larry Pfeifer, network engineer at Widener University, had already seen the benefits of a Top Layer Attack Mitigator [™] IPS, having been an early adopter of the solution. He had initially purchased a Top Layer IPS to minimize the false positives that Widener's intrusion detection systems were producing. As Pfeifer observed the additional benefits of an Attack Mitigator IPS in action - consistently neutralizing Denial-of-Service (DoS) attacks, hybrid worm and other network traffic anomalies – he determined that Top Layer's IPS technology would play a critical role in protecting the university's network and critical online resources from the arrival of a new wave of student devices in September 2003. To deflect the coming onslaught of viruses and worms, Pfeifer and his team choreographed a unique, effective security infrastructure utilizing the Top Layer technology: locating an Attack Mitigator IPS on each side of the university's firewall.

Benefits: With the flood of students in September 2003, Widener placed an Attack Mitigator IPS both outside and inside the firewall to help alleviate instances of viruses and worms and traffic anomalies that would be let loose as students plugged in their infected machines to the school network. With the Attack Mitigator IPS on each side of the firewall, Pfeifer was able to ensure network availability and high performance levels. "We witnessed many instances of the MS Blaster and Welchia attacks both inside the network trying to spread, and from the outside trying to penetrate the Widener network. With the Attack Mitigator IPSes in place, we didn't skip a beat, and the students, faculty, and staff were able to remain focused on education, rather than problems with the computing infrastructure," summarized Pfeifer.



Full Case Study

More than a University Network

With its main campus located in Chester, PA, Widener University is the home of more than 2,100 full-time undergrads, 1,100 evening undergrads, nearly 2,000 graduate students and more than 1,600 law students. In addition to serving these students and the faculty and staff, the university serves as an ISP for local school

districts. All-in-all, more than 7,000 people rely on the university to live, learn, and work.

Each Fall, thousands of students converge on the campuses of Chester and Harrisburg, PA and Wilmington, DE, and the Widener University IT staff must deal with the technological consequences. In recent years, viruses, worms, hybrids and hackers have posed an increasingly severe threat to the availability of Widener's network and online assets. Larry Pfeifer, network engineer at Widener University knew all too

well that 2003 could prove to be the worst year of post-move-in computer threats – after a summer that saw the proliferation of fast-spreading worms such as MS Blaster and Welchia.

Preparing for the Entrance Exam

Pfeifer and the Widener IT staff thought they'd get a head start, and strengthen the university's defenses. "We knew that our firewall alone wasn't going to be enough as students came back this year. With the amount of new attacks that had been unleashed in the Summer of 2003, we knew that our firewall would become quickly overwhelmed if we didn't provide it support." Fortunately, Pfeifer had already experienced how technology from Top Layer Networks could eradicate online nuisances and threats such as DoS attacks while minimizing false positives that consumed his team's time and attention. "Earlier in 2003, we installed an Attack Mitigator IPS to help alleviate the strain on our IT team by minimizing the false positives that our security infrastructure produced. The Attack Mitigator IPS really enhanced our Intrusion Detection Systems' (IDS) abilities. Putting the Attack Mitigator IPS in front of ISS's IDS sensors allowed us to weed out false positives while better identifying actual attacks that required our immediate attention. Seeing how well it worked for its original purposes, we thought the Attack Mitigator IPS may be able to play a bigger role in our network architecture, and gave it a try before the students hit the campus full throttle."

Pfeifer called upon Corporate Networking Inc. (CNI), a Top Layer reseller, to provide four Attack Mitigator IPS's for a temporary period as students began returning from Summer vacation, during the critical time when computers were being plugged into the university network. CNI's Tim Slattery rushed the Attack Mitigator IPS boxes to Widener University, playing an instrumental role in expediting the installation process to meet Pfeifer's aggressive timeline.

A Unique Solution to a Common Problem

Pfeifer's team needed to protect Widener University not only from external threats, but also internal threats as students inevitably connected to the network with infected computers – and began accessing files and resources from inside the firewall. This was a problem

that Widener had addressed in years past by simply cleaning up the aftermath of such an uninhibited internal spread of infection. This is a

challenge many institutions and corporations also have as they open their networks to mobile workers, students, and other authorized guests. The key questions for Pfeifer were, "How do we stop the spread of infection when these threats are launched from inside the firewall? Further, and equally important, how do we protect our firewall from being overwhelmed by the mass amounts of traffic generated from within, so that it can properly do its job of stopping threats from outside?"

Pfeifer's team decided that a key technology to protect their employer's network would be Top Layer's Intrusion Prevention System, the Attack Mitigator IPS. To provide optimal protection to the University's online assets, students' computers and the firewall, Pfeifer installed Attack Mitigator IPS devices on both sides of the firewall. With these devices on either side of the firewall, Pfeifer could ensure that the firewall operated at its maximum capacity – with each IPS device dropping malicious traffic attempting to enter or exit the Widener University network. The solution was a tremendous success. In fact, "As we expected, we saw immediate attacks of MS Blaster and the Welchia worm as students connected, but we didn't skip a beat nor were we adversely affected, simply because of the Attack Mitigator IPS and how well it worked in conjunction with our firewall," Pfeifer said. "The Attack Mitigator IPS is now an essential fixture in our network and security infrastructure – once one puts it in their network, you just don't take it out."

"We knew many students would bring more back to the university than they anticipated – many of them came back with infected computers. Of course, as they connected to our network, those infections looked to spread aggressively," explained Pfeifer. "However, we knew what to expect and were properly prepared with the right technology. Those attacks were nipped in the bud and the first day of class was a breeze ... at least for those of us in the network department," said Pfeifer.

