



eEye Protects High School from Dangerous Computing Activities

Challenge: Making Sure Students Adhere to Acceptable Use Policies

Bishop Verot Catholic High School in Fort Myers, Florida provides students with a number of PCs that they can use to complete homework or conduct research. The trouble is that even in the controlled environments of the library and computer labs, students' online activities can't be that closely supervised. There aren't an unlimited number of teachers to watch over their shoulders, after all.

At the beginning of each year, students have to sign an acceptable use agreement, which says that they'll only use computing resources for school purposes. But teens will be teens, and they'll do their best to challenge authority.



Customer:

Bishop Verot Catholic High School

Fast Facts:

Located in Fort Myers, FL

750 students

130 PCs

8 servers

Key IT challenges:

enforcing security policies that prevent students from accessing unauthorized sites without hindering their school work; protecting against malware; securing internal data; ensuring privacy of students' records

Antivirus and Web filtering software give the school some protection and control, but students are savvy and would prefer to have unfettered access to the Internet. "After we installed Web filtering, students began using proxies," said Jason Castaldo, Bishop Verot's systems administrator. "We needed more sophisticated security just to keep up with their workarounds."

Bishop Verot also had to protect the network from malware. No matter how much security training you offer, every IT person knows that end users are still the weakest link in the security chain.

"Even with Web and mail filtering in place, things slip through. Even teachers occasionally click on things they shouldn't, like those 'click here for unlimited income' links in spam," Castaldo said.

Starting from Scratch

When Jason Castaldo started working for Bishop Verot six years ago, the school's PCs were poorly secured. Antivirus programs weren't being updated. The bare-bones Windows XP firewall was the school's only firewall, and, of course, when Castaldo looked into the situation he found an array of problems.

"The first thing I noticed was how slow all of the machines were," he said. "They were bogged down with multiple viruses and spyware. I had to reformat each one, both servers and workstations, and start from scratch."

This situation actually presented an opportunity. As Castaldo started purchasing appropriate security solutions, he also established an informal security policy. Now, whenever a subscription expires, Bishop Verot doesn't simply renew. Instead, the school looks to see if they can get even better security at the same price. That could mean staying with the same vendor and upgrading to a new suite, but often it means looking for something new altogether. This is how Bishop Verot first learned about eEye Digital Security.

The Selection Criteria: Squeezing More out of Each Security Dollar



When Bishop Verot's antivirus subscription expired, the school started to study the security market. Bishop Verot had been using Panda Security's AdminSecure. The school was pleased with the product's performance but sought more protection at a similar price point.

"We wanted additional features that would protect our network in the event that malware made it past our initial lines of defense," Castaldo said. With traditional antivirus software, there's always the threat of zero-day attacks. Traditional antivirus programs rely on signatures,

so if you don't have the signature you're at risk. Research labs can take weeks or even months to develop signatures for new threats. "We wanted security that didn't need to know what exactly the threat was in order to provide protection," he said.

Bishop Verot considered products from Computer Associates and eTrust. Both offered more functionality - but at a much higher price. Finally, the school looked at eEye Digital Security.

The Answer: eEye's Integrated Threat Management Solution

eEye's Blink Endpoint Security offers an array of security features at a much lower cost than competing security products. Blink protects clients by identifying behaviors, not signatures. Offering integrated multi-layered endpoint protection, Blink is a single, lightweight client that replaces multiple security agents, protecting against known exploits, zero day attacks, and all other attack vectors.

"With the other solutions, we would have had to piece together several different modules, or even entirely separate security solutions, to get the same functionality of Blink," Castaldo said. "Eventually, it came down to cost. When we found ourselves asking 'how many products do we have to buy to do what Blink does?' the answer was obvious. We needed Blink."

Aside from cost, what makes Blink different than other endpoint security solutions is that it is part of a larger security suite. While Blink can operate as a standalone endpoint protection solution, it is designed to work with the Retina Network and Web Security Scanners and the REM Security Manager.

Taken together, the eEye solution represents a new class of security product: integrated threat management. eEye detects vulnerabilities and threats, prevents intrusions, protects all of an organization's key computing resources, from endpoints to network assets, all while providing a centralized point of security management and network visibility.

Key Benefits:

Policy creation
and enforcement

Antivirus protection

Zero-day protection

Quarantining of suspicious
machines

Centralized security
management

Reporting and auditing



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276





REM acts as a central control console and correlation engine – the brains of the operation. With REM in place, Blink agents throughout the network can report back and correlate threats, policy abuses and attack vectors. An intuitive user interface and installation wizards make monitoring an entire network simple and quick. For a one-person IT staff like Jason Castaldo, speed and ease of use are necessities.

Finding Vulnerabilities without Looking for Them

The advantage to eEye customers is that the knowledge developed for one product is shared with the others – even if you only subscribe to a single component. eEye’s research team is consistently the first to identify new threats in the wild, and its products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself.

For instance, Bishop Verot is currently only using Blink and REM. The Retina Network Scanner, which pinpoints security vulnerabilities, is something they believe exceeds their needs. However, that hasn’t prevented them from finding vulnerabilities.

“We ran into an issue during the install. Not all computers had Windows Vista SP1 on them. Blink triggered the update,” Castaldo said. “That may seem trivial, but unpatched computers are a serious risk.”

Blink also takes the knowledge developed for eEye’s vulnerability scanning tools and leverages it to rate an organization’s security level. Bishop Verot learned that they needed to patch or update several programs, including Adobe Acrobat and Flash.

“Blink points out system vulnerabilities,” Castaldo said. “It makes me aware of what is on our network and what needs to be addressed.”

“Blink points out system vulnerabilities. It makes me aware of what is on our network and what needs to be addressed.”

– Jason Castaldo, Systems Administrator, Bishop Verot Catholic High School

Other Key Benefits:

Automated notification when problems occur

Streamlined incident response

Centralized security management that provides a single point of visibility into and control over the network

Offers remote administration features, so updates don’t require manually visiting each PC

Ability to apply policies to USB storage devices



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276





Enforcing Policy to Monitor Students' Behaviors

Instead of relying on malware signatures, Blink prohibits a range of risky behaviors, while also enabling IT to restrict activities that pose risks to their particular institutions. In a high school, for instance, that means blocking MySpace.

“Our acceptable use agreement says that students can only use computing resources for school purposes, but we try not to be too heavy-handed,” Castaldo said. “If a student is on ESPN, they’re probably not doing schoolwork, but we’ll usually let that slide. We try to give them some leeway.”

MySpace, on the other hand, presents a different problem. The site has been used for cyber-bullying and cyber-stalking, and the school needed to block the site for liability reasons.

Bishop Verot's Web filter blocked MySpace, but its logs also showed that students were trying to find a backdoor to the site. “After we blocked MySpace, we found a student using Google to search for ‘hack school security,’” Castaldo said. This potential security/liability risk was averted and instead became an issue for the school's principal.

Blink can set and enforce policies that protect against those behaviors. “It prevents students from running executables, so they can't download password sniffers or keyloggers,” Castaldo said. Even if the hacking software changes, Blink won't care. By protecting against bad behaviors, rather than specific programs, Blink helps ensure that students are surfing only where they should be.

eEye's Integrated Threat Management Suite:

Blink delivers multi-layered endpoint protection in a single, lightweight client that replaces multiple security agents, protecting against known exploits, zero-day attacks, and all other attack vectors.

Retina Network Security Scanner provides multi-platform vulnerability management. Retina identifies known and zero-day vulnerabilities and provides security risk assessment, enabling security best practices, policy enforcement, and compliance with regulatory audits.

Retina Web Security Scanner rapidly and accurately scans large, complex web sites and web applications to tackle web-based vulnerabilities, ensuring privacy, security integrity and compliance.

REM simplifies the security management of complex networks. Designed for enterprise scalability, REM provides a single point of visibility into and a centralized point of control over enterprise networks.



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276

