



Sallie B. Howard School for the Arts Removes the Risk behind Internet Browsing

Challenge: Protecting School Computers from Internet Threats

The Sallie B. Howard School for the Arts and Education (SBH), like many schools, is struggling to keep up with the times. To prepare students for life after school, the integration of technology is a must. However, relying on technology creates risks.

This was the problem Soron Foster, technology support specialist for SBH, needed to address. As students relied more heavily on computers and the Internet, teachers and administrators noticed much of the activity wasn't school-related.



Customer:

Sallie B. Howard School
for the Arts and Education

Fast Facts:

Located in Wilson,
North Carolina

700 Students

328 PCs

Key IT challenges:

Enforcing security policies that prevent students from accessing unauthorized sites without hindering their schoolwork and research, protecting against malware, securing internal data, ensuring privacy of student records

The knee-jerk reaction would be to severely limit Internet access. Foster knew better. Located in Wilson, North Carolina, which is about a half hour east of Raleigh, SBH is a charter school that serves many underprivileged students who have few creative outlets. The Internet is both a vital learning tool and creative one as well: Foster needed to control its capabilities without limiting the student's potential.

"We're an arts school," said Foster. "Our students are doing much more than run-of-the-mill research for reports. They're calling up reference images for art projects. They're studying videos of modern dance, and students are using programs like GarageBand to help them compose their own music."

Unfortunately, the existing security that was in place was not keeping in lock step with the way students were using the Internet. Viruses had slipped through, and non-education-related sites were seeing heavy traffic.

Even with URL blocking in place, a supposedly trusted site could be compromised and contain malicious code. A new and inappropriate site could fall through the cracks, not yet blacklisted. Technically-savvy students had already found ways to bypass the school's defenses.

It's Not Secure if It's Easy to Bypass

When Foster started working at SBH, the school had two layers of security in place. They used Symantec's antivirus protection and SonicWall's firewall with content filtering. Symantec's antivirus had a few flaws. It didn't protect against zero-day threats, didn't offer centralized administration, and didn't allow administrators to drill down into the specifics of flagged incidents.

Foster was pleased with SonicWall as a firewall; however, students were finding ways around the content filtering. Some students used proxies to reach blocked sites such as MySpace.



Students weren't the only problem. Teachers also put the network at risk. Since their existing Symantec email protection was a blunt instrument, several teachers had clicked on email links and attachments. "They fell for a social engineering attack that told them that someone had sent them a Hallmark e-card," Foster said.

As a result, several email accounts were turned into Botnet zombies, which were later used by attackers to send out spam. As is typical with zombie attacks, the infection evaded detection because it occurred late at night when the school was not in session.

Selection Criteria:

Finding an Endpoint Security Product that Protects Different Types of User

Foster knew that the school's security needed to be upgraded. First, he looked at Symantec's updated antivirus program. Not only was it expensive and restrictive, but the new version still didn't protect against zero-day attacks.

Next, Foster considered adding SonicWall's antivirus to their existing firewall. Again, pricing was a sticking point, and the program didn't have a robust enough feature set.

"Our users have a wide range of capabilities," Foster said. "Some have little experience with technology and can easily be duped by social-engineering attacks. Others are computer whizzes. We needed a security solution with enough flexible features to address both types."

As he was investigating various solutions, Foster learned about eEye Digital Security on a podcast. "It sounded too good to be true," Foster said. "But I figured I should at least check it out."

The Answer:

eEye's Integrated Threat Management Solution

What Foster found was a comprehensive security solution that offered everything he was looking for - zero-day protection, centralized management and behavior-based settings, rather than signature-based protection - at a much lower price point than other solutions he had considered.

eEye's Blink Endpoint Security protects client devices 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.

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





“The zero-day protection is critical,” Foster said. “Even when you don’t have all of your patches up to date, Blink still protects you. That certainly makes my job easier.”

Another reason Blink is different than other endpoint security solutions on the market 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 other eEye products, including Retina Network and Web Security Scanners and REM Security Management Console.

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.

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 wizard makes monitoring an entire network simple and quick.

The Hidden Benefits of Blink and REM

Since the school’s infrastructure hadn’t been upgraded in a while, the deployment was a little trickier than usual. Network settings had to be updated and patches had to be deployed.

“It took a little time to get the network settings right, but the eEye support team stepped in and walked us through it,” Foster said.

Foster soon realized that with eEye he could streamline his workflow. “Before eEye, we didn’t have any central administration. Updates and patches were done manually. Policy changes were also manual.” In a school with 328 PCs, it’s easy to see how patches would get out of date and why policies would pretty much stay as-is.

“Now, I don’t have to walk the building. I just go into REM, and with a few clicks, the changes are done,” he said.

Foster also gained visibility into each and every PC through Blink. “When I go into the Blink console, I immediately know more about what’s going on the device than the users do,” he said. In other words, students trying to get access to restricted sites through proxies would now hit a wall. Proxies are detected and the sites blocked.

Foster also gets network visibility and correlation through REM. “With REM, when I open it up, the first thing I see is a report. It graphically shows me exactly what’s going on that day. I see network activity. I see our vulnerabilities, and I see the risks associated with them. REM keeps me informed,” he said.

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





Achieving ROI

SBH saved money with eEye right from the start. Blink was priced well below the other options the school considered, while offering a much more complete feature set. "Blink is so much more than your typical antivirus program," Foster said. "With Blink, what you get is a full security suite. Along with antivirus, you get a firewall, system protection, zero-day protection, and centralized administration – all for a lower price than most antivirus programs alone."

SBH also saves money by saving time. "The last time we were hit by an email virus, I spent a couple of days going from machine to machine to machine. All of the fixes had to be done manually," Foster said.

Compare that to Blink. The minute Blink was installed; it immediately found viruses that had been evading detection. These were from the Hallmark email mentioned earlier. When spam engines woke up late at night and tried to start sending out spam, Blink blocked them. Foster was alerted to the activity, and the process of patching PCs was centralized. Blink then pointed out vulnerabilities on the school's SMTP server and suggested email policy changes.

Foster immediately made the changes, but even before patches were applied and configurations changed, Blink protected against any suspicious behaviors.

"The other thing to keep in mind is that eEye is constantly upgrading their software," Foster said. "In the short time I've been a client, they've already made performance improvements and further simplified administration."

"When I go into the Blink console, I immediately know more about what's going on the device than the users do. With REM, when I open it up, the first thing I see is a report. It graphically shows me exactly what's going on that day. I see network activity. I see our vulnerabilities, and I see the risks associated with them. REM keeps me informed."

- Soron Foster, technology support specialist for the Sallie B. Howard School for the Arts and Education



eEye Digital Security®

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



eEye's Integrated Threat Management Suite:

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.

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.

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.

Retina On Demand simplifies the entire vulnerability management process by allowing an organization to rapidly deploy Retina Security Management Appliances within an environment and manage all of the job scheduling, reports, and results through a hosted version of REM. There is no need to set-up servers, configure databases, or even install any software to benefit from Retina On Demand. eEye has created true black-box technology that can be plugged into any environment and managed via the Internet for a hands-free approach to vulnerability management and regulatory compliance.



eEye Digital Security®

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

