A T.H.E. JOURNAL
CUSTOM WHITE PAPER
www.thejournal.com

SECURING THE K-12 NETWORK

An Endpoint Security and Network Management Solution for Education

Table of Contents

EXECUTIVE SUMMARY

IT departments everywhere face the challenge of finding cost-effective ways to guard against increasingly sophisticated security threats to the network. Those threats are particularly difficult to parry in a K-12 network, where protection involves highly distributed networks and diverse groups of users, including students. To compound the challenge, school districts must manage networks with many different users per endpoint, ever-greater inclusion of Internet material in the classroom and at home, and constantly shrinking budgets. To address those challenges, endpoint security and solid network management offer a powerful way to bring the K-12 network safely under control. This paper describes such a solution, and how it can be used to securely lock down the K-12 network, while reducing management costs and headaches

INTRODUCTION: A NETWORK UNDER ATTACK

A close call with the Conficker virus[1] in 2009 was a warning flag to Florida's Bay County School District that a better security solution was imperative. As Network Administrator Russ Goldbach explains it, the virus hit when the district was at its most vulnerable, during a move from Novell to Microsoft Windows and Active Directory. The worm—which had been lurk-

Sponsored by:
TREND MICRO

[1] *According to Wikipedia, the* ***Conficker*** *virus targets Microsoft Windows and was first detected in late 2008. It attacks by co-opting machines and linking them into a virtual computer that can be controlled remotely. Conficker is believed to be the largest computer worm infection worldwide since the 2003 SQL Slammer infection, affecting more than seven million government, business and home computers in over 200 countries. The virus is a worm, meaning it self-replicates using the network, and is unusually difficult to counter because it uses many advanced malware techniques.*

ing undetected on the district's network for some time—attacks Windows networks using file shares, bombarding the network with authentication traffic and often bringing a network to its knees with bandwidth overload.

With responsibility for some 10,000 endpoints throughout the district, network administrators quickly moved into emergency mode to deal with the threat. Unfortunately, though, "our virus software couldn't repair or remove the virus," Goldbach recently recalled. The district turned to engineers at Trend Micro for help. Working from a remote location, the team of engineers met with district's technical team and resolved the problem within three days—making a believer of Goldbach and of the school district. "We realized that we needed true enterprise-class anti-virus software" Goldbach said. Along the way, the district has cost-effectively added additional tools from the security company's suite of products to enhance network management and security, especially at the endpoint level.

THE SECURITY CHALLENGE AT BAY COUNTY SCHOOL DISTRICT

With main offices in Panama City, Florida, the heart of the Bay County School District lies two hours east of Pensacola and two hours west of Tallahassee, near beaches along the Gulf of Mexico. The district currently serves 19 elementary schools, five middle schools, six high schools, and a couple of adult education and general purpose schools. In all, Bay County is responsible for educating close to 27,000 students yearly.

The IT group has a large responsibility, with computers in 39 locations, including high schools, middle schools, a one all-in-one K-12 school -- a total of nearly 10,000 endpoints. The network includes 15 Citrix XenServers that act as virtual servers that can be combined on one physical piece of hardware – located at the district office and at specific schools. In addition, the district maintains 150 physical servers – many with additional virtual servers running on them.

The district's staff consists of about 3,500 people, with just a handful devoted to IT – four network support staff, two on the communications team, ten desktop support and help desk staff, and nine Programmer / analyst positions. Russ Goldbach is a network administrator (his technical title is instructional network specialist), one of four people in charge of the Bay County SD network.

In Bay County classrooms, all teachers have computers, either desktops or notebook computer that can be taken home. In addition, most classrooms have at least five PCs per classroom for students, and at least one computer lab per school.

And as with virtually any school district, especially in today's economy, Bay County faced budget limitations and efforts by IT staff to "do more with less" whenever possible.

CHALLENGING TIMES IN K-12

As Bay County SD's story illustrates, one of the toughest challenges that IT faces today is securing the network. A tall order for any IT director or system administrator, network security for a school district is an order of magnitude harder. Consider a typical school district's constrained budget, distributed locations, and various levels of users, from elementary to high school students, to teachers, staff and administrators. Add to that the strict security requirements mandated by laws regarding minors, schools, and Internet access—and you have the makings of a daunting security challenge.

Endpoint security—making sure that the outer edges of the network, where a wide variety of users are active around the clock on PCs and mobile devices like notebook computers and even smart phones, are safe—is a tremendous challenge in a K-12 setting. Managing a district-wide network to ensure the security and visibility of all devices on the network can be expensive and time-consuming. In addition to a wide variety of users and locations, with varying levels of expertise and usage needs, network administrators are faced with new types of devices, new Web 2.0 uses of the Internet that encourage lots of user sharing of various kinds of content, and of course, a push to cut expenses all the while.

Security experts calculate that the network's endpoints are perhaps the most vulnerable to attack, simply because they are so difficult to adequately protect. For starters, consider that your network has many more endpoints than it does servers, making the chances of an endpoint security breach that much more likely from a numbers standpoint. Many of your endpoint users, in addition, unlike the trained employees who manage your central servers, are unlikely to have much experience in recognizing and dealing with network threats. To make matters more difficult, in a K-12 environment, many users are schoolchildren.

When schools offer remote learning options over the network, as is increasingly common in K-12, or assign homework that requires Internet research, that challenge is made even more difficult. Students, a security challenge to protect at any time, now aren't even in a classroom location at all times. Regardless, they must be given reasonable access to the school network and to the Internet in order to do class work, homework and research—but still must be protected from malware and viruses, as well as security threats to the general network.

The answer comes from a software package that not only offers solid endpoint security features, but includes powerful network management capabilities as well—since proper management is part of a secure network. The combination of security and network management tools in a single suite offers some advantages—for example, it can lower costs by reducing the number of vendors used for content security and network management

TREND MICRO’S ENDPOINT SECURITY PLATFORM (ESP)

The Endpoint Security Platform offers a number of modules with different types and levels of security protection, along with network management tools. ESP is unique in that it frees up significant computing power to network endpoints—PCs and laptop computers, as well as remote servers — by installing two intelligent agents on each device (one for systems management, one for security). Once the agents are in place, additional software modules can then be added remotely—a feature that Bay County School District, portrayed in this paper, is taking copious advantage of—at any time in the future.

The agents, which use resources only lightly, are updated as needed using an intelligent relay network that chooses a network path based on availability and efficiency, rather than forcing a large update package through an often already-clogged path. For highly distributed organizations such as school districts, where network administrators often have little control over remote users, this solution can be ideal. Security protection includes anti-virus and anti-spyware software, along with root kit protection, web threat protection and vulnerability patching.

The ESP platform can include:

- Core Protection Module: A complete set of anti-malware and removal capabilities, including spyware protection. Blocks users and applications from accessing malicious web content. Moves malware signature files and web reputation assessments offsite and into the cloud to minimize endpoint load.

- Web Protection Module: Uses Trend Micro’s Web Reputation to block users and applications from accessing malicious web content.

- Patch Management Module: Delivers patch management capabilities for multiple operating systems—Bay County SD used the product on both a Novell and Windows network as it migrated to Active Directory.

functions. School districts can consolidate on security software, so that instead of using two, three, or more vendors for various security and management purposes, administrators can use a single software solution. Using a single vendor also reduces the amount of hardware needed to support the product, since that single product typically has a smaller footprint than repeated installations of various point solutions.

Moving to Better Network Security and Management at Bay County SD

Bay County School District's decision to bring Trend Micro's Convergence Endpoint Security Platform (ESP) product on board began with a migration from a Novell network to Windows during the 2009 school year. Reasons behind the move included desktop management challenges under Novell, and the need to implement Microsoft's network services technology, Active Directory.

But the real kicker was a serious security breach just weeks earlier, and the resulting realization that the district did not have the enterprise-level network management, security, and endpoint protection it really needed.

As Bay County School District Network Administrator Russ Goldbach explained, the district now uses Trend Micro's endpoint security platform for four essential functions:

1. Virus protection
2. Patch management
3. Asset discovery
4. Power management

Combined, the four features add not just security protection to the network, but also strong network management capabilities that lower risk and save the district time, money, and peace of mind.

"As a school district, we must have the best solution possible for security and protection," Goldbach explained, regardless of budget. "With the current solution, we feel that we do."

1. Virus Protection

Students, of course, are by definition a huge challenge to keep secure and safe on the Internet. Not only must their web activities as minors be monitored and protected to a higher standard than an adult user (see sidebar, "The Special Security Risks Facing K-12,") but because students tend to push computer systems to their limits with social networking activities, web browsing, and potentially unauthorized activities like gaming, monitoring their activities is that much more difficult. Teachers and staff, on the other hand, have their own slate of uses, including laptop computers that must function in both the classroom and in an office or at home, and a wide range of high-bandwidth needs, including multimedia, content sharing, and other Web 2.0 type uses.

To address some of those challenges, virus protection at Bay County SD is a two-phase process, Goldbach explained. First is a desktop-level security system, which ensures that each endpoint throughout the network is protected at that level. At the next level, the web security system uses databases from Trend Micro that are updated in real-time in order to check, nearly instantaneously, every single web site a user visits. Those that have been deemed potential security risks for a variety of reasons are blocked.

At Bay County SD, the software doesn't work as a filtering device and isn't used to block visits to sites specified by the school district. Rather, the district relies on Trend Micro's virus, worm, malware and security risk lists, which are updated constantly on servers around the world. "Every time a user goes to port 80 or port 443," Goldbach explained, which means the user is leaving the local network and venturing onto the Internet, "the software runs a quick check."

The real-time endpoint protection is an especially important feature in a K-12 environment, according to David Silverberg, who is Trend Micro's global product marketing manager for the ESP product. The endpoint protection feature means that every time a user—a student for example—accesses the Internet from an endpoint computer anywhere on the network, the endpoint agent in ESP instantly accesses Trend Micro's constantly updated set of risky sites maintained offsite in the cloud and checks whether that web site is a security risk. If it is, user access is blocked, period. Trend Micro threat in-

THE SPECIAL SECURITY RISKS FACING K-12

An IT director in K-12 faces a very specific set of unique challenges, according to Trend Micro's Lynette Owens, who is director of corporate outreach for the company's Internet Safety for Kids & Families Program. Not only do most school districts face compressed budgets, she pointed out, and a very diverse group of constituents, but they must also wrestle with legal compliance issues such as the very specific Children's Internet Protection Act (CIPA). CIPA is a federal law that addresses access to offensive content over the Internet on school and library computers. It applies to any school or library that receives funding for Internet access or internal connections from the federal E-rate program, which makes communications technology more affordable for eligible schools and libraries.

In addition to meeting the challenges of CIPA, Owens said, the increasing interest of teachers in Web 2.0-type learning adds to the risk. As the model of shared user content in the so-called Web 2.0 phase of the Internet grows, IT is literally caught between constituencies – while teachers need unfettered access to content in order to incorporate Web 2.0 models in their teaching style, parents remain rightly concerned about their child having unrestricted access to the Internet.

In fact, the responsibility of protecting minors rather than adults is a huge challenge in itself. "School districts have so many challenges [above and beyond corporations] in terms of Internet access. I really feel for IT directors" in K-12," Owens said.

Another challenge, she pointed out, is that while corporations can usually count on one employee using one computer consistently across the network, that model doesn't hold in K-12, where shared resources mean that IT never really knows who might be using any one endpoint at any one time. Because of the potential range of users for any endpoint, Internet safety is enhanced when whole categories of URLs are blocked. CIPA requires that schools block all pornography, but other site classifications can be added. Beyond blocking malicious sites that have spyware or other risky code, all gambling sites can be added, for example.

Owens also mentioned child identify theft, which is showing a steady rise lately among minors. Armed with only a name and place of birth, criminals can obtain a social security code and steal a child's identity for years without being detected. That makes it more important than ever that a school's Internet security software block access to any web site that can be an identity theft security risk.

No education institution, of course, wants to be known as a place where security is poor and where students might possibly be exposed to problems, Owens said. To prevent that, tight network security that takes into consideration the special needs of K-12 is imperative.

telligence—threat collection from multiple sources combined with advanced threat analysis—feeds into its well-known, constantly updated global set of databases listing security-risk sites throughout the Internet. "We were first to market with that kind of solution for the endpoints," Silverberg said.

For locations with endpoint users doing lots of Internet surfing—a good definition of many K-12 networks—that part of the solution is critical. "There's lots more risky behavior in that population," confirmed Silverberg. "With this solution, as soon as the user types in an address, it's run against a list in the cloud that tells us if it's a dangerous site or not. If it's risky, we block access."

That real-time aspect of virus protection takes advantage of Trend Micro's cloud-client architecture. Locating virus protection resources away from the school district and "in the cloud" can dramatically lower system resource consumption and bandwidth. It's not only a fast and efficient way to identify and block actions such as phishing, incoming malware and viruses, and inadvertent visits to spoofed sites, but it saves money, since less hardware and network bandwidth is needed to keep the network running smoothly. In addition, existing computers can often be kept in play much longer, since less processing power is demanded of them.

The access and checking is completely transparent to the user, and because software already running on the endpoint handles the check, there is virtually no performance degradation.

2. Patch Management

Managing software updates, or patches, can be an unending—and expensive—nightmare for IT administrators in any enterprise, but doubly so in large K-12 environments. School districts with a number of remote locations—typical of many districts—can understandably find it challenging to visit each site when an update needs to be made. Products for remote patch deployment are common, but many have high bandwidth demands and cannot be counted on to successfully reach every endpoint on the network.

That granular visibility offered by ESP makes for significant cost savings, since ESP's remote management features allow IT personnel to see and pinpoint problems from their desks. Rather than sending an IT staff member to a remote location to fix a problem, or even to first troubleshoot by determining if a security agent is on or off, IT administrators can stay put. Instead, using ESP, they can determine the status of the endpoint and the problem, then contact the help desk to remotely make the required fix. "A security fix that might have taken an hour, can take five minutes," Silverberg said. Multiplied over time, that's a huge savings in an IT technician's time.

Even the district's software engineers found it hard to believe: could virus software really be deployed to that many devices that quickly?

At Bay County, IT administrators have configured the ESP software to automatically look for patches and updates to standard everyday products like Adobe, Flash and Windows. The system is set up to automatically update software as needed on every machine across the network at a specified time. For example, Goldbach said, "We can quickly get a list of PCs [using ESP] that don't have [Windows] Service Patch 3 on them and update them." Larger updates that take extensive bandwidth can be set to run at night, when few or no users are on the system.

Once it had the ESP client installed on each device, the district used the distributed network architecture technology to communicate with its desktop computers initially, including sending registry settings and applications. During its move to Windows and Active Directory, Goldbach wrote a script to wake up each computer individually during the night, then import that endpoint's relevant information into Active Directory. "We realized we could pull this off in no time flat," Goldbach said, and the conversion to Windows was finished nine weeks ahead of schedule.

Instead of individually visiting every computer at the various schools sprawled across the district, all of the upgrades could be done remotely. "It saved us so much footwork," Goldbach says. "We now know that anything we have to deploy in a large scale can be done through the agent."

The intelligent relay system is a key feature that distinguishes ESP from competitors, Global Marketing Manager Silverberg said. It's a feature that's especially important to administrators in a K-12 environment, he points out, which typically have a distributed network with number of different locations to manage and a variety of users, including students and teachers, accessing the Internet. ESP's intelligent relay system makes for less network traffic, Silverberg explained, since instead of constantly having to pass very large update files to the agent over a static path, ESP dynamically looks for the nearest server or machine with available bandwidth to send the update. That contrasts with security products that consistently rely on one path and one connection—if that path fails, the update fails.

For example, when Bay County decided to deploy virus protection to every endpoint on the network, it was able to remotely distribute the software to 6,500 computers on the network using the intelligent agent already installed on each device. "That's probably the most important feature with this system," Goldbach said. "It's the only software we have seen that could do that." To heighten the challenge, the network at that point was still made up of a mixture of Windows Active Directory and Novell, and as Goldbach tactfully puts it, "remote deployment procedures in Novell are always challenging."

Even the district's software engineers found it hard to believe: could virus software really be deployed to that many devices that quickly? Turns out that it could—and the process made a believer of Goldbach, a long-time IT veteran.

That use of ESP, as a powerful systems management tool that can deploy other solutions remotely, even complicated rip-and-replace upgrades, offers a significant cost savings for IT. Creating rule sets that can be used repeatedly and thus free up IT staff for other tasks, and otherwise automating tasks so that IT can spend time on other work all are important aids in reducing the time spent on—and thus the cost of—network management and security.

Goldbach's experience converting the network points to another important technology – the so-called Wake-on-LAN feature, a networking standard commonly used in network management. Most Wake-on-LAN implementations use a central server to send mes-

SAVING ON SECURITY COSTS

Working under a constrained budget is a virtual certainty in most of today's public schools. Trend Micro's ESP solution addresses that issue in several ways.

First, the inherent cost of constantly addressing security incidents stemming from un-patched, improperly configured, outdated and insecure systems is huge. Studies show that improved security can cut network security management costs by 40 percent, as a result of saved IT time and employee productivity alone.

Combining security and network management software into a single solution from one vendor also cuts cost by:

- Reducing to one the number of products that must be licensed, supported and maintaine
- Cutting the training needed for IT personnel, who are now using one system rather than many. Time spent managing a single system is also less than time spent managing a handful of different solutions for various purposes.

Significant network savings can also be realized with Trend Micro's ESP solution, because it requires far fewer servers to secure the endpoints. ESP can scale to manage 250,000 endpoints per server, many times more than other solutions. That means fewer servers to manage, back up, and keep current, and servers previously used to run security solutions can be redeployed for other purposes.

A final cost of a security breach is dealing with the aftermath. For a school district, the damage to a school's reputation and loss of parental trust may be the biggest -- if most difficult to quantify -- cost of all.

[2] *"Cloud-Client Enterprise Security Impact Report Increased Protection at a Lower Cost," An Osterman Research White Paper sponsored by Trend Micro, January 2009.*

sages to the subnet to wake up a system and check it. The drawback to that method is that it uses a blind call across the network—since no reply is required from the device, there's really no way of knowing for sure that the device was reached. ESP takes a different approach, using its sophisticated knowledge of PCs and subnets on the network to essentially bombard the LAN and ensure a reply. "It's much more efficient," Goldbach explained, "and far superior to anything else we've seen."

3. Asset Discovery

ESP's use of intelligent agents on every endpoint comes into play again with asset discovery. At Bay County SD, Goldbach explained, special software agents (the software, which is not a Trend Micro product, is available for purchase as a separate module and can be added to an ESP installation) are used to run certain services on a timed setting, allowing the agents to "scan a subnet, recognize PCs that we didn't even know existed on the network, including printers, and query them to find out what kinds of devices we have out there."

In a school district environment, that kind of functionality is critical—Goldback runs the asset discovery software regularly to find new PCs on the network. "Students will bring in a PC [and attach it to the network], or someone else at a school will connect, or little network hubs will be put in place somewhere in the district," he said. It takes less than 15 minutes scan the district's entire network and prepare a report. Bay County network administrators use the tool regularly to scan the district's 43 subnets at a pace of one per day, producing a full report each week.

"The nice thing about it is that the system is smart enough to recognize the network," Goldbach said. "It's a very clean and efficient system—we haven't seen any [increased] load on the network when it's running."

Again, that sort of granular visibility offers significant savings when it comes to network management, since network admins can quickly pinpoint problems remotely, eliminating the need to visit locations. And with no measurable increase on the network load, there's no need to spend on additional servers or bandwidth.

4. Power Management

Reducing power consumption is a popular and environmentally friendly move, and is a sure-fire method of saving money and energy across the board in IT—hence its popularity in K-12. Directives to users advising them to turn off computers and printers when they are not in use can only go so far. An approach that has proven to be far more effective is network management software that is set to physically shut down PCs across the network at a given time.

Bay County has cut its power use, and cost, dramatically, slicing power consumption in half through remote power management.

At Bay County, power management through the software has shown dramatic results. Using the Trend Micro ESP agent to turn off all computers at 7 p.m. has cut power consumption in half, Goldbach said. The agent works by powering off both computers and monitors. During the day, the district sets unused systems to a standby power-saving mode, in which a move of the mouse powers them back on. Sleep timers are set across the board to turn off personal computers on the network at night; any user on the system at night receives a reminder that reappears regularly. Bay County also has an energy awareness program to remind users to power down, Goldbach said, but the forceful shutdown approach gives the district another way to enforce the policy – and clearly one that has yielded impressive savings.

SUMMARY: A NETWORK MANAGEMENT AND ENDPOINT SECURITY SOLUTION

Tough, dependable and affordable security is clearly an essential item on any K-12 network, and Bay County's experience illustrates what can happen when security isn't made a priority. Virus, malware and rogue attack protection is critical today, combined with good network management practices like asset control and power management.

All of those features are possible because of what is perhaps the biggest benefit of the ESP system for Bay County SD: its cost-saving powerful overall remote management capabilities, made possible by the unique distributed network architecture. Bay County takes advantage of that architecture in numerous ways to both enhance security and save costs – for enterprise-level virus and malware checking and protection, for patch and power management, and for asset tracking. Each feature is increasing efficiency, helping protect students, dramatically cutting network management costs, and reducing the district's overall risk.

About Us

About T.H.E. Journal

THE Journal is dedicated to informing and educating K-12 senior-level district and school administrators, technologists, and tech-savvy educators within districts, schools, and classrooms to improve and advance the learning process through the use of technology. Launched in 1972, *THE Journal* was the first magazine to cover education technology.

THE Journal's franchise consists of the monthly print magazine (which is also available in digital format), the web site thejournal.com, six newsletters (THE News Update, T.H.E. Journal Insider, IT Trends, THE SmartClassroom, School Security, and Collaboration 2.0), and targeted list rental opportunities.

With a distribution of 100,000 circulation, T.H.E. Journal is the leading resource for administrative, technical, and academic technology leaders in K-12 education.

About Trend Micro

Trend Micro provides solutions in endpoint, messaging and Web security. With operations globally, Trend Micro is focused on innovating smarter security solutions that protect against a wide range of insidious threats and combined attacks including viruses, spam, phishing, spyware, botnets, and other Web attacks, including data-stealing malware. Trend Micro's goal is to provide customers with the most timely, most effective threat protection with the least amount of complexity, thus ensuring secured data and reputation, reduced administrative costs, regulatory compliance and business continuity despite rapidly increasing and ever-changing security threats

Trend Micro's vision is to create a world safe for exchanging digital information by offering a comprehensive array of customizable solutions to enterprises, small and medium businesses, individuals, service providers and OEM partners.