

Blackhawk Technical College

A customer success story

Blackhawk Technical College needed to update its email, web and endpoint security to offer staff and students a consistent work environment. Sophos helped the school move to a secure environment with an endpoint agent, web appliance and email gateway, giving the IT services team better control over and visibility into systems at Blackhawk's five campuses. With Sophos, Blackhawk:

- Saves hours that were spent manually weeding out spam email
- Reduced help desk calls due to antivirus alerts
- Cut down drastically on the number of infected machines requiring re-imaging

Business challenges

Blackhawk Technical College, based in Janesville, WI, has seen something positive in a tough local economy: a 52% jump in enrollment over two years after the shutdown of a nearby General Motors plant. The increase represents the highest enrollment the school has ever handled as new students seek workforce training. The school also offers degree programs and community education, with 14,000 student accounts and 1,100 full- and part-time employees across its 5 Wisconsin campuses.

Server systems engineer Jason Thoms is part of Blackhawk's IT services department, which supports both staff and student workstations. Before implementing Sophos Endpoint Security and Control, Sophos Email Security and Control and Sophos Web Security and Control, Thoms had to contend with spotty email filtration and unchecked web threats.

Blackhawk's former security solution—Trend Micro's endpoint and server protection and message appliance—wasn't up to the task of protecting the school's email accounts. "Using it and deploying it was pretty challenging," says Thoms. "We couldn't ensure that laptops in the wild were being updated or protected or even installed and running correctly." It was expensive, too, and "the reporting functionality was an obvious afterthought," according to Thoms.

Customer at a glance



Positive business outcomes:

- Proactively monitor and repair infected student workstations
- Can easily, centrally enforce school policies for email and internet use
- Give the IT services team control over all system workstations
- Lets IT services see all web and email threats in one location
- Provide a consistent experience for users

Sophos solutions

- Sophos Endpoint Security and Control
- Sophos Email Security and Control
- Sophos Web Security and Control

Number of License

- 1,500 enterprise

Thoms had to manually maintain Blackhawk's email gateway to try to reach a balance between blocking threats and allowing legitimate emails. "I would spend two or three hours a week tweaking expressions," he says, "trying to weed out the phishing scams, image spam and other messages it should have picked up." The IT team also had to deal with user complaints about spam by writing custom rules. "It was like playing whack-a-mole because it would pop up somewhere else a little bit different," says Thoms.

Consistency was a major goal of endpoint security at Blackhawk, so that users saw the same thing on every computer. It was common for PCs to have unwanted applications like Yahoo! Messenger or MSN toolbars. "When someone new logged in they were bombarded with all this stuff that wasn't supposed to be there," says Thoms. "And then the workstation next to it was just fine but we had no idea" which ones were affected. That included virus threats, which slipped through filters unbeknownst to the IT team. "In a full classroom, if you've got one compromised machine, that could be one student that couldn't participate," says Thoms.

Without a web appliance, "all the high risk sites had to be blocked at the DNS filtration level or at the workstation itself," says Thoms. "Once a threat hits the workstation, you're kind of doing it wrong."

Technology solutions

When Thoms narrowed down his security solution decision to recommend Sophos for purchase, "reputation was one of the big things," he says, along with Sophos' enterprise focus.

"I'm a realist. I know it's expensive to support consumers," he says, "and that makes the product more expensive. Eventually that cost is going to find us too."

"Before Sophos, there were a lot of unknowns. This is a product that's a lot easier to manage and maintain."

Protecting email security was a top priority at Blackhawk when choosing a new provider. "Reducing the amount of spam was pretty much paramount," says Thoms. "And I wanted to leverage having an email gateway that was a hardened appliance, something I didn't have to manage that was monitored."

A web proxy wasn't part of his original set of requirements for their new security solution. "But I couldn't imagine our environment without one of those," he says. "That's our first line of defense for our students and workstations." It's helped the IT team regain system-wide control. They can view statistics on blocked threats in real time with Enterprise Console: screen shows the web proxy dashboard and another shows the email gateway. "Visibility is the biggest thing," says Thoms.

Deploying Sophos took about a week across Blackhawk's five facilities, since Thoms wanted to be in each location as the product was being rolled out. "I think I spent more time traveling to the campuses than actually deploying it," says Thoms. "We planned ahead to make things as fast as possible," setting up local shares so installations happened on LAN rather than WAN links.

After installation, the application and help desk support teams tackled remediation issues, as the Sophos antivirus tool discovered infected computers that the previous solution had missed. “It was pretty messy,” says Thoms, “so I guess that was an indication that there was a lot of stuff out there that wasn’t being blocked.

Business results

In the first year of Blackhawk’s Sophos implementation, “we just hit 15 million blocked spam messages,” says Thoms. Time saved and peace of mind also figure into measuring the success of Blackhawk’s solution.

“We’re not so much running around putting out fires when professors complain about broken workstations—We’re able to preempt that and fix that before it becomes an issue.”

“It’s hard to put a number to the number of hours somebody spends disinfecting a machine,” says Thoms. “Before, there were a lot of unknowns. Maybe machines weren’t checking in every hour, maybe they were. This is a product that’s a lot easier to manage and maintain.”

Antivirus protection has eased worries for Thoms team of administrators. While a lot of antivirus software is hit or miss with pulling updates correctly, they have peace-of-mind knowing clients are being updated consistently. His team also appreciates that the products features are easy to find and use.

Thoms also gives PureMessage (part of Sophos Email Security) top marks for spam filtration. “I don’t think there’s a better product out there that’s priced sanely,” he says. “It’s accurate, updated often, and if there’s a problem with the hardware, knowing Sophos is watching remotely gives an added layer of protection.”

And, further adding to Blackhawk’s increased systems visibility, “the reporting functionality has been really helpful,” says Thoms. “We’re able to get a sense of why classrooms might be more susceptible to threats.” That might include a user with elevated privileges, or a suspicious file from a student’s CD. “We can identify and be proactive about leveraging all the policies and rules,” Thoms says. “Then when someone gets an error or warning on the screen, maybe they’ll act on it. If they don’t, we know it’s in Enterprise Console, or as a last resort, it’ll be in the report we get every week.”

And Enterprise Console alerts IT services as soon as a problem arises. “We’re not so much running around putting out fires when professors complain about broken workstations,” says Thoms. “We’re able to preempt that and fix that before it becomes an issue.” Remote monitoring and automated cleanup scheduling have also saved time.

Sophos Endpoint Security and Control also contributes to the flexibility that Thoms and IT services need to provide at a technical college. “We have a network security class that lights our console up like a Christmas tree when they start their hacking tools,” says Thoms. “We were able to tweak policies a little bit in that room so we’d only see the worst of the worst, but still allow the students to learn and

Blackhawk Technical College

A customer success story

use the tools that they'll be protecting their networks from.” Thoms also uses policies to block kiosk machines from handling financial data, for example.

Most importantly, Thoms is confident that Sophos will be there for him during current and upcoming projects. His sales rep set the tone during his evaluation process. “She was tenacious, to say the least—in a good way,” says Thoms. “I talked to her more often than Trend would return calls. I didn't hear from Trend Micro the whole year I was a customer.” And communications haven't subsided, he says. “Even to this day, she follows up on any questions I have and expedites cases we think are important.”

And support experiences with Sophos have been a huge improvement over Blackhawk's previous vendor. Removing Trend's anti-competitor removal tool to install Sophos was tricky, but “Sophos support was pretty aware of what was going on and gave me step by step instructions,” says Thoms. “I was on hold less than a minute and in another few minutes was speaking to someone who knew exactly what to do. That was a great first impression.” Thoms usually hears back on any support questions within 24 hours, “which is more than adequate.”

“I don't have to use support very often because the product works,” says Thoms. “But it gives me good peace of mind.”

Boston, USA | Oxford, UK

© Copyright 2011. Sophos Ltd. All rights reserved.

All trademarks are the property of their respective owners.

cs/110208

SOPHOS
WWW.SOPHOS.COM