

Sourcefire Customer Case Study: Halesowen College: Won't Learn About the Need for Security the Hard Way

Will Davidson



Technical Resources Director,
Halesowen College

About Halesowen College

Halesowen College is a further education establishment based in Halesowen in the West Midlands county of the United Kingdom. The college offers a broad range of services, with over 40 AS/A Level subjects and 70 vocational programmes, including work-based learning. The college has three sites, including the main campus, a Hair and Beauty Academy, and the Coombs Wood Business Centre, all of which are within a mile of each other. In a typical year, Halesowen College has approximately 4000 full-time students, as well as 4000 part-time students.

OVERVIEW

When Halesowen College was looking for a commercial network security solution to replace its open source Snort® Sensors in order to improve efficiency and better manage the demand for IT services, Sourcefire® was its first choice.

Business Drivers: Delivering security, improving efficiency of the IT department, supporting expansion, and ensuring the availability of critical services

Industry Sector: Higher Education

Why Sourcefire? Threat analysis, Sourcefire RNA® (Real-time Network Awareness), Sourcefire Defense Center®, Impact Flags, and familiarity with Snort

Business Benefits: Dramatically reducing time spent monitoring and managing alerts, providing evidence for use in audits, and providing a best practice approach to security

SO MANY ALERTS, SO LITTLE TIME

Halesowen College has approximately 1700 PCs, which are supported by a mixture of networks and managed internally. The college relies heavily on Microsoft Windows, which accounts for around 70 percent of the network, although the college also uses a lot of open source, in particular Linux, which makes up the other 30 percent.

As a public-facing education establishment, security is a key priority because the systems are being accessed by young people, and ensuring their safety is a primary concern. Over the past nine years, Halesowen College has used open source Snort IPS technology to monitor and protect its Local Area Network (LAN). However, following an increase in service requirements and a need for greater efficiency, the organization decided it needed a more commercial solution which would reduce the pressure on the IT team and increase its ability to react to security threats.

Will Davidson, Technical Resources Director for Halesowen College, is responsible for the college's IT support teams and the development of IT services across the organization. Davidson explains:

"We had been using Snort and really liked it and found it could spot threats very well. However, there would be so much information coming in that it was very difficult for us to put the threats in priority order and act in time. One of my technicians was literally spending half his day just managing alerts. Our network and services were becoming increasingly critical, and as demand grew, we looked to expand these services. At the same time, we started to look for a tool that could make our monitoring more effective and manageable."

Sourcefire 3D System Benefits at a Glance

- Sourcefire RNA & Impact Flags dramatically reduce time spent monitoring & managing alerts
- Sourcefire Defense Center readout & logs provide evidence for audits
- Sourcefire 3D System provides best practice approach to security

"I would recommend Sourcefire, and I do! Whenever I talk to other colleges I tell them about the Sourcefire 3D System and how confident we are with our security. We are very happy with the system; it has delivered everything that we were looking for and more."

The Right Solution at the Right Price

Halesowen College reviewed a range of commercial solutions that could enable it to be more proactive. While the college isn't committed to using any particular purchasing framework, it is vigorously audited, both internally and externally, to ensure it is complying with best practices and achieving value for the money. After careful consideration of the options available, the college decided to implement the Sourcefire 3D® System.

Davidson continues:

"We came across Sourcefire while we were at the Infosecurity Europe exhibition in London, and after seeing a demonstration of the technology, we were really impressed. In particular, the threat analysis and RNA functions stood out as it correlates context and data so that you are only alerted to threats that you need to act upon. It basically does all the hard work for you, and then just tells you what you need to know. This was really appealing as it meant a huge reduction in the number of actionable events, which had been our main problem with the Snort system, while still providing total visibility of network activity. Additionally, as we had been using Snort for such a long time, we were familiar with the technology, and we trusted it."

"Our financial regulations state that we have to speak to a range of different vendors before we make any purchase decisions, so we had a look at Cisco and TippingPoint, but they didn't have what we were looking for. It was much more difficult to get the information we needed to do a comparison, but from what we could gather it would have cost us a lot more to get what we needed. The Sourcefire team was far more responsive and seemed really interested in what we were trying to do. The Sourcefire solution ticked all our boxes and came in within budget—so it was a fairly clear-cut choice really."

IT COULDN'T BE EASIER

In June 2008, Halesowen College installed two Sourcefire 3D® Sensors, one to monitor the college's Internet connection and the other for its wireless networks. This gave the college complete visibility of all traffic coming in from outside the campus. Additionally, the college has deployed Sourcefire RNA to gather network intelligence, with all information feeding into the central Sourcefire Defense Center.

The 3D System provides Halesowen College with all the network defense capabilities of its previous Snort system, along with more in-depth network and security information, by combining a number of security technologies. This integrated approach provides a greater level of understanding when it comes to security alerts and reduces the number of events that the security team needs to review.

To aid with the installation process, Halesowen College used the professional services of one of Sourcefire's partners, Armana Systems. Davidson comments:

"Armana was extremely professional, and the staff really knew their stuff. We had a much better dialogue going with them than any of the other service providers we considered. It was helpful to have them on board, as the initial set up was all done for us, which meant we were only left with the fine tuning, which halved the installation time."

“The threat analysis and RNA functions stood out as it correlates context and data so that you are only alerted to threats that you need to act upon. It basically does all the hard work for you, and then just tells you what you need to know. This was really appealing as it meant a huge reduction in the number of actionable events, ... while still providing total visibility of network activity.”

“We have made huge efficiency gains, with time spent monitoring events being cut right down from four hours to one hour a day. Effectively, RNA is giving our team back 15 hours a week.”

REAL-TIME SECURITY, CONTROL, AND PEACE OF MIND

Since deploying the system, Halesowen College has been able to meet its goal for tightening security across the network, as Davidson outlines:

“The Impact Flag functionality and alerts are fantastic. They’re very quick to come through, we get all the information in real-time, and it gives you added confidence that the sensor is doing its job. This makes it is much easier to spot trends, which means we can be more proactive and act quickly on threats. For example, we had a SQL injection attack on our website, and the 3D Sensor picked it up straight away and told us everything about the attack so that we could respond immediately. In the past, it would have taken us twice as long to find out about the nature of the attack.”

“RNA provides an even finer level of control so that we get far less events to review, which is excellent. We have made huge efficiency gains, with time spent monitoring events being cut right down from four hours to one hour a day. Effectively, RNA is giving our team back 15 hours a week. Additionally, the readout and logs provide us with an audit trail and evidence that the networks are secure, so that we can formalize our response during an audit and demonstrate that we are following best practice.”

WHAT MORE COULD YOU WANT?

Halesowen College is extremely pleased with the Sourcefire 3D System and is keen to extend its protection when it gets extra budget secured, as Davidson continues:

“I would like to put another sensor in, to monitor the gateway between the staff and student networks to protect us from internal threats. However, this is a longer term plan. But when we do, we will be using Sourcefire. I would recommend Sourcefire, and I do! Whenever I talk to other colleges I tell them about the Sourcefire 3D System and how confident we are with our security. We are very happy with the system; it has delivered everything that we were looking for and more.”

©2009 Sourcefire, Inc. All rights reserved. SOURCEFIRE®, Snort®, the Sourcefire logo, the Snort and Pig logo, SOURCEFIRE 3D®, RNA®, SOURCEFIRE DEFENSE CENTER®, CLAMAV®, SECURITY FOR THE REAL WORLD™, SOURCEFIRE RUA™, DAEMONLOGGER™, SOURCEFIRE SOLUTIONS NETWORK™, and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. Other company, product and service names may be trademarks or service marks of others.