Case Study

mojo

Hesperia Unified School District Prevents Use of Unmonitored Wireless Internet

> "As we discovered these rogue access points, it became apparent that wireless LANs from neighboring businesses or homes could also be used by students who have their own laptops to access the Internet, And the presence of a municipal wireless network could also allow students to access the Internet from school property. This is of grave concern as it would jeopardize our certification to uphold the Children's Internet Protection Act and ultimately our E-rate designation."
>
> -David McLaughlin, Director of IT for
> Hesperia Unified School District

Highlights

- Prevent students from accessing the Internet through wireless signals from neighboring schools, businesses or municipal Wi-Fi networks.
- Prevent rogue access points without on site scanning
- Ensures district remains in compliance with Children's Internet Protection Act
- Remote management enables IT staff to administrate and monitor policy compliance from central site
- Automatic prevention stops threats immediately, eliminating need for IT staff to travel to school

Keeping Students Safe

Like many school districts, Hesperia Unified School District in Southern California strives to improve the learning and teaching experience for its over 20,000 students in 22 elementary, middle and high schools through use of the Internet. The School District believes that appropriate use of technology can enhance critical thinking skills and has provided computers for almost all classrooms along with Internet access.

To facilitate Internet access, a pilot was begun with a limited number of secure wireless access points (APs) in select classrooms. While not providing comprehensive campus coverage, they enabled untethered use of laptops for teaching purposes. As with many organizations, this small installation of wireless bred desire in others for the same freedom of connectivity.

Discovering the Wireless Threat

After the access points were installed, the IT team began receiving strange help desk requests. Teachers would report that their laptop was connected to an access point, but they couldn't reach the Internet. These reports lead to an investigation which revealed that new, unauthorized APs had been installed. The teachers' laptops were associating with the rogue APs instead of the authorized access points! The rogue APs were providing IP addresses that were invalid, preventing the laptop from reaching the Internet. Without these incidents, months might have gone by before the IT team discovered the rogue access points, potentially leaving the school's network open to unauthorized hackers.

Ensuring Compliance with the Children's Internet Protection Act

As a result of these incidents, the IT team at Hesperia Unified decided to move forward with a comprehensive wireless LAN installation. In addition to creating a centrally managed wireless LAN, a key objective is also to automatically identify and secure the school against wireless threats. The team was concerned not only about rogue access points that might expose the school's network to outsiders, but also the ability for students to connect to the Internet without virtue of a web content filter.

“As we discovered these rogue access points, it became apparent that wireless LANs from neighboring businesses or homes could also be used by students who have their own laptops to access the Internet,” said David McLaughlin, Director of IT for Hesperia Unified School District.

“And the presence of a municipal wireless network could also allow students to access the Internet from school property. This is of grave concern as it would jeopardize our certification to uphold the Children’s Internet Protection Act and ultimately our E-rate designation.”

The Children’s Internet Protection Act (CIPA) is a law designed to protect minors from accessing inappropriate adult content while in schools or libraries. School districts must certify that they are in conformance with this law when applying for E-rate discounts. E-rate discounts are vital in helping schools make the best use of tight budgets for telecommunications equipment.

Schools commonly use a web content filter to ensure that inappropriate Internet web sites cannot be viewed by students when they are on school property. Unfortunately, unmonitored wireless connections will completely bypass this protection, putting the school at risk of being in violation of CIPA.

Enforcing a Comprehensive Wireless Use and Security Policy

Due to this risk, Hesperia Unified looked for a comprehensive solution that incorporated not only a centrally managed wireless LAN, but also a wireless intrusion detection and prevention solution. After researching their options, the team came to a decision to deploy the Mojo AirTight, the wireless intrusion prevention and Mojo Wireless Manager performance management solution along with Extreme Networks wireless LAN. “A key reason we chose this solution was because of the close partnership of Mojo Networks with Extreme Networks,” said David McLaughlin.

Combined, the two are a powerful combination that enables the IT team to take back control of the air space. Comprehensive wireless coverage will significantly mitigate the risk of rogue APs as teachers and students will have wireless access through the campus. The Mojo AirTight allows the IT team to set up policies to automatically identify and prevent wireless threats such as ad hoc networks and clients connecting to neighboring wireless LANs. “A key selling factor for us is the ability to have automatic prevention,” said David McLaughlin. “We’re not onsite at the schools, so we need to ensure that these wireless threats are stopped immediately.” The IT team also positively views Mojo AirTight’s ability to prevent ad hoc networking that might be used to facilitate cheating during exams.