Case Study

Frenship Independent School District

PROFILE:

COUNTRY: USA
INDUSTRY: Education
SIZE: 10,000 students

OBJECTIVE:

Frenship ISD needed a way to identify and block rogue applications that allowed students to bypass the district's web filter, creating security breaches and using precious bandwidth for non-educational activities.

SOLUTION:

The district found what it was looking for in ContentKeeper App Defender, a revolutionary new product that can recognize the unique signatures of nearly 60 rogue applications (with more being added each month).

RESULTS:

- Better web security
- Greater control over bandwidth usage
- More effective policy compliance

Revolutionary New Solution Helps Frenship ISD Find and Block 'Tunneling' Applications

ContentKeeper App Defender prevents students from circumventing the district's web filter

When Frenship ISD Chief Technology Officer Joe Barnett first tried App Defender, a revolutionary new product from ContentKeeper that can detect and block rogue apps used to circumvent web filters, he was shocked at what he found.

In this district of 10,000 students in West Texas, it was not uncommon for Barnett to see 400 or even 500 examples per day of suspicious apps identified by the software. Large numbers of students were using freely available tunneling apps to bypass the district's filtering software, often so they could play computer games during school hours.

"We were using a firewall, but it wasn't effective at blocking these applications," Barnett says. "We were experiencing high bandwidth utilization at odd times which led us to SSL decryption and analysis."

Whereas the district's firewall failed to block these rogue apps, ContentKeeper App Defender succeeded. As a result, students are now being kept on task far more effectively as they use Chromebooks and other digital devices for learning—and precious bandwidth is no longer being wasted on gaming, VPN and other non-sanctioned activities.

How the Solution Works

ContentKeeper App Defender can recognize the unique signatures of nearly 60 rogue apps that students commonly use to get around their district's firewall and filtering software, creating a massive security hole.

What's more, this number is continually growing as a dedicated team of ContentKeeper specialists scours the web for the latest examples of rogue applications. These include peer-to-peer file sharing applications such as BitTorrent, HTTPS proxies such as Hide My Ass, and tunneling apps such as Psiphon or Ultrasurf.

When App Defender detects a suspicious app on a student's device, the product isolates that machine from the network. The student receives an automated message stating that his or her network access has been suspended until the offending app is removed. Once the app in question is deleted, the student's network privileges are immediately restored.

Barnett likens this capability to putting students in a "digital time out" until they comply with the district's Acceptable Use Policy. "We can stop the web activity on that device until the app is uninstalled. The result is a "soft" no instead of a hard stop" he observes.

"Our high school was exceeding 80 percent of its total bandwidth allocation, and we were at a point where severe restrictions would be needed to conserve existing bandwidth or adding additional capacity to ensure student learning impacts were minimized."

—Joe Barnett
Chief Technology Officer

Impressive Results

When Frenship ISD first rolled out App Defender, students who were blocked for using one particular tunneling app would try another and then another. As they began to learn they would not be successful, many students stopped trying to circumvent the district's web filter altogether, Barnett says.

Today, there are fewer than 100 instances per day of students trying to use rogue applications, mostly from students who had not made this type of attempt in the past.

Using App Defender has allowed the district to preserve essential bandwidth for classroom learning and other mission-critical uses. "Our high school was exceeding 80 percent of its total bandwidth allocation, and we were at a point where severe restrictions would be needed to conserve existing bandwidth or adding additional capacity to ensure student learning impacts were minimized," Barnett says. "Now, our bandwidth use is much more predictable and visibility into network activities is greatly enhanced. App Defender is an important resource-saving, increased visibility, and prioritization tool."

The product has also improved security and helped the district remain CIPA compliant. Combined with ContentKeeper's web filtering and intelligent SSL inspection, App Defender is an effective tool for guarding against malware and ensuring Internet policy compliance, preventing students and others from opening a back door into networks through which they can access high-risk websites or download malicious files.

"How can we efficiently utilize district resources while providing a safe secure learning environment? ContentKeeper App Defender helps us do this is a very effective way," Barnett concludes.

ContentKeeper.com
k12@ContentKeeper.com
US: +1 888.808.6848
Intl: +61 2 6261 4950