

## Eastern Kentucky University Taps FaceTime to Keep Spyware off Campus

### CASE STUDY



#### ABOUT FACETIME RTGUARDIAN™

- Prevents incoming spyware at the gateway
- Detects, manages and secures all Internet activity with zero network latency
- Prevents unauthorized IM and P2P connections, including Skype
- Detects “phone home” behavior of adware/spyware for targeted remediation of client infections
- Monitors and controls access to Web sites to prevent inappropriate use of network resources
- Supports all major enterprise and public IM networks
- Ensures safe and secure IM use by blocking high-risk features
- Non-stop protection with automatic updates from FaceTime Security Labs
- Insight into bandwidth abuse, source and destination IP addresses, and port abuse
- Fast and easy to deploy, with low administrative overhead

*“RealTime Guardian gives us the perimeter protection and manageability we need to prevent spyware from getting onto our network, taking care of the problem before it can turn into a labor-intensive clean-up operation for the helpdesk.”*

**Ed Riley, Assistant Director**  
 Networking, Telecommunications and Systems  
 Eastern Kentucky University  
 FaceTime customer since 2007

#### Overview

Founded in 1906, Eastern Kentucky University offers 168 degree programs and serves more than 16,000 students a year, supported by 2,000 faculty and staff, across four campuses. But with small classes and an active campus life, the university prides itself on retaining a small-college feel. The IT department has 80 members of staff, 16 of whom are responsible for the network, systems, telecommunications, and residential technical support under Ed Riley, Assistant Director and a 25-year veteran of the department.

IT infrastructure is largely based around Windows and Cisco, with additional Unix systems in the data center. Multi-tiered security comprising anti-virus, anti-spam, and network access control is in place to protect the university’s single wide-area network. Every student is supplied with a copy of Norton Anti-Virus when they first arrive on campus; network access control policy requires the presence of fully updated virus protection and the latest Windows updates for students logging into the network from the residence halls.

Faculty, staff, and students make extensive use of real-time communications. The Blackboard e-Education enterprise software application is increasingly used for distance learning, and Skype and instant messaging are used for interpersonal communications at many levels across campuses.

#### Challenge

Over the past year, IT and helpdesk staff have seen a significant rise in spyware infiltrating the network. It became clear that the user-based anti-spyware software that had been the sole defense against these attacks was no longer effective.

Recent research data\* clearly points up the growing cost to IT departments of repairing PCs after a spyware incident. The average cost incurred in recovering from malware infections that entered the network over real-time communications channels has more than doubled over the course of a year. In 2007, IT managers reported spending an annualized average of nearly \$289,000 to repair or re-image PCs after such infections, compared with \$130,000 in 2006. On average, almost 40 PC-related incidents a month require some kind of repair or remediation and each repair takes an average of nine hours.

“I’m a firm believer in perimeter-based defense systems,” said Riley. “By relying on a user-based approach, we were essentially relying on people, and I think anyone in IT would agree that people are the weakest link in any security system.”

The extent of the university's reliance on web-based systems for distance learning means that, not only was it essential to keep the network spyware-free to continue to deliver teaching programs effectively, but any viable anti-spyware solution had to offer zero latency to maintain an effective transmission speed.

"A particular challenge of any security system in an academic environment is providing protection without privacy invasion," added Riley. "While we would never be able to block real-time communications, we can exercise some 'back-end' control through packet shaping and other non-intrusive measures."

The concept and practice of free speech has always been a focal point of academic life, and that freedom of speech has extended through all the myriad communications channels now available on campus, from inter-student IM and chat to the eBlackboard distance learning program.

### Solution

Riley's team evaluated a number of edge-defense anti-spyware solutions, focusing on those that had received high ratings in independent reviews and tests. FaceTime's Real-Time Guardian was an immediate front runner, exhibiting effective spyware blocking, no network latency, and, importantly for acceptance in an academic environment, no censorship of communications channels. It also offered a good foundation for future management of real-time communications that would allow an element of control without intruding on the freedom of those communications.

"Installation and deployment of RT Guardian went extremely smoothly," said Riley. "Some minor tweaking was needed to ensure cooperation with the Cisco routers, but the FaceTime team sorted that out for us in no time."

The system has so far been deployed to all 2000 staff and faculty members and to the 5000 students living in the residence halls at Eastern Kentucky University.

### Results

Riley is pleased with the results of the RT Guardian deployment "but I'd guess my colleagues in the helpdesk department are even happier," he added. "Not only are they not getting calls complaining about system slow-downs and other performance-related issues directly attributable to spyware, but they're not spending time fixing the problems the user-based anti-spyware couldn't deal with.

They're able to work on more productive tasks like rolling out new PCs and making sure everyone's patched and up to date."

An additional benefit Riley discovered was the ability to monitor real-time communications usage and come up with some of those important "back-end" controls to keep the network humming. "By combining the use of Cisco packet-shaping products to curtail P2P traffic on our Resnet network with RT Guardian to block most P2P traffic, we are able to establish broad operating controls for bandwidth-sapping P2P networks.

Large data packet transfer could indicate music or video file sharing that may constitute a breach of copyright. Notable legal action by the Recording Industry Association of America (RIAA) for illegal music downloading in violation of copyright laws has prompted concern among many IT professionals at colleges and universities. Identifying and preventing such transfers keeps both institution and individuals on the right side of the law.

Riley also appreciates the reporting and analysis tools. "Anti-spyware programs can generate a huge amount of data, some of which is extremely useful in configuring the protection to best effect. When we were using client-based protection, that data was essentially unavailable to us, but with RTGuardian we can get a number of different reports to help us optimize the system."

"We believe that RTGuardian is an excellent foundation for the future protection of all our communications channels against spyware and other malware. University environments are generally more open and less centrally controlled than commercial environments, so this kind of edge-based protection is really essential to our network security."

---

### About FaceTime Communications

Founded in 1998, FaceTime Communications is the leading provider of security solutions for the management and control of greynet applications such as adware/spyware, instant messaging, webmail, peer-to-peer file sharing, web conferencing and VoIP. FaceTime is ranked #1 by SC Magazine for IM Security, and has been rated #1 by IDC for two consecutive years. FaceTime solutions are used by almost two million people in over 800 organizations, among them eight of the ten largest U.S. financial institutions. FaceTime supports all leading public and private IM network providers, professional community networks, P2P networks including Skype, and WebEx web conferencing.

