

Electronic Charter School Secures Education Infrastructure and Protects Students with FaceTime

CASE STUDY



ABOUT FACETIME RTGUARDIAN™

- Detects, manages and secures all Internet activity with zero network latency
- Prevents incoming malware at the gateway
- Detects “phone home” behavior of adware/spyware for targeted remediation of client infections
- Supports all major enterprise and public IM networks
- Ensures safe and secure IM use by blocking high-risk features
- Prevents unauthorized IM and P2P connections, including Skype
- Monitors and controls access to Web sites to prevent inappropriate use of company resources
- Provides non-stop protection with automatic updates from FaceTime Security Labs
- Rapid set up plus simple ongoing administration and management
- Insight into bandwidth abuse, source and destination IP addresses, and port abuse
- Triggers targeted, clientless remediation process for malware on infected endpoints using Microsoft sanctioned technologies to efficiently clean and inoculate PCs



“ Without Real-Time Guardian in place, our entire network could be out for up to ten days because of a worm-enabled DDoS attack accidentally introduced through a student’s PC. With 7,300 students depending on ECOT for their education, we simply can’t afford that kind of down time. ”

Brad Scott, IT Manager, Electronic Classroom of Tomorrow
FaceTime customer since October 2006

Overview

The Electronic Classroom of Tomorrow (ECOT), based in Columbus, Ohio, was founded in 2000 to provide students throughout the state with secure, Intranet-based education for Grades K through 12 as a quality alternative to traditional public schools. ECOT and its 500 staff currently serve 7,300 students between the ages of five and twenty-one through a home-based online learning environment designed to meet the needs of students who - regardless of academic ability, mental, emotional, or physical disability, socioeconomic status or location - do not thrive in a traditional classroom setting.

What sets ECOT apart from other public schools is its home-based online learning environment. ECOT's ability to provide a statewide K-12 educational environment through its own secure Web-based network, or Intranet, is unique. The Intranet restricts access to Web sites not approved by ECOT, while providing a wide range of teaching tools and educational sites that are appropriate for students of all ages. Just like other public school students, ECOT students have teachers, counselors, class discussions, report cards and out-of-class trips. Unlike other public school students, however, ECOT students are required to use computer and Internet technology to access their lessons.

Students may use their own computer systems and log into the Intranet via the Web if they have appropriately-equipped machines, but 80% use computers and VPN connections provided by ECOT.

Challenge

Because Web access is a core requirement for ECOT, if the Intranet goes down, students and teachers are disconnected and the educational continuum is broken. Equally, because 7,300 students and 300 teachers are connecting into the system remotely every day, the opportunity for a crippling malware attack is extremely high. So protecting the network from attack and consequent downtime is IT Manager Brad Scott’s top priority.

“We’ve had incidents where a worm has gotten into the system and spread to every node on the network in a matter of hours. Windows VPN security can’t deal with infection prevention on the scale we need, and getting thousands of remote systems cleaned is a mammoth task that really gets in the way of the learning process,” says Scott.

The networks are configured for high levels of security with VPNs, domain policy, and redundant local user policy for students, who must connect through a proxy in order to access approved sites. But it's not as simple as it might seem to find an appropriate solution to manage the malware threat.

Explains Scott: "Our students are all over the state and there's no common denominator among their connection speeds. We have students in urban environments who are able to access the Intranet via cable modem, but we also have students in remote rural areas who are connecting at 9600 baud. The key for us was to find a security solution that supports this vast range of connection speeds without impacting students' ability to interact with the system effectively."

ECOT clearly needed to avoid any solution that required code to be pushed out to the remote machines – not only would this create a major vulnerability gap in the organization's security, but the students with slow connection speeds would suffer a negative impact on their whole educational experience. So Scott and his team of five – two staffers and three contract workers from Xerox, which provides ECOT's network and server support – set out to find a solution that would meet their very specific requirements.

Solution

Fortunately, the search was short, and the shortlist even shorter. The only product the team found that provided centralized malware scanning and remediation *and* promised zero latency was FaceTime's Real-Time Guardian.

"As soon as we read about RTG, we were pretty sure it was the right solution for ECOT," said Scott. "Not only would it prevent infected traffic from entering the Intranet – whether from the Web or via VPN – but it would allow us to centrally manage mitigation and remediation, a key issue with our network, which has little in the way of remote management capabilities because of the connection speed disparity."

ECOT's management approved the purchase and Brad's team installed Real-Time Guardian 500 at the gateway.

Results

ECOT has been extremely happy with Real-Time Guardian's protection in the four months since the device was installed.

"Other than one minor incident caused by an accidental factory default reset, which FaceTime's technical support staff fixed right away, RTG has been an incredibly useful addition to our network security toolbox," says Scott. "It's also great to have the real-time reports of what's going on with bad traffic on the network. The graphs look really good, and I'm looking forward to having the time to explore the system in more detail, now we don't have to worry about malware attacks leaving us scrambling to get the network back on line and reconnect the students to their studies."

ECOT is in the process of modifying its network topology to be more hierarchical than the current flattened approach, with a view to improving and extending the protection afforded by Real-Time Guardian.

"When technology works the way you want it to - as RTG is doing for us - it is truly a beautiful thing."

*Brad Scott, IT Manager,
Electronic Classroom of Tomorrow*

About FaceTime Communications

FaceTime enables the safe and productive use of greynets like instant messaging, Skype, web conferencing and P2P file sharing. Ranked number one in market share among instant messaging management vendors for the third consecutive year, FaceTime's award-winning solutions are used by more than 800 customers including nine of the ten largest U.S. banks. FaceTime Security Labs delivers the industry's first IMPact Index, which assesses "point-in-time" risks posed by viruses, worms and other malware propagating through greynet applications. FaceTime supports or has strategic partnerships with all leading public and private IM network providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM, Reuters, and Jabber.

FaceTime is headquartered in Foster City, California. For more information visit <http://www.facetime.com> or call 888-349-FACE (3223).