

GORE-TEX® Creators Plug Spyware Gap with FaceTime

CASE STUDY



ABOUT FACETIME RTGUARDIAN™

- Prevent spyware at the gateway
- Prevent unauthorized IM and P2P connections
- Ensure safe and secure IM by blocking high-risk features
- Ensure non-stop protection with automated updates
- Rapid set up plus simple ongoing administration and management
- Multiple custom and configurable reports
- Central administration for multi-appliance installations

“ A perimeter solution like RTGuardian integrates easily with existing systems, so we were able to experience the product's benefits in a relatively short period of time...The support for multiple communications or greynet channels, along with the substantial database of spyware signatures, efficient updating process, depth of research behind the signatures and a sensible approach to pricing, made FaceTime an easy choice as our preferred solution. ”

Tim Yates
Senior Network Engineer
W.L. Gore & Associates

“ FaceTime made our choice easy. The RTGuardian appliance is simple to deploy, does exactly what it says it will do, and gives us a trouble-free solution to managing spyware at the perimeter. It does its job quietly and efficiently, leaving IT staff free to pursue other tasks. ”

Tim Yates, Senior Network Engineer, W.L. Gore & Associates
FaceTime customer since October 2005

Overview

W L Gore & Associates was founded in 1958 to explore opportunities for fluorocarbon polymers; within 12 years, the company had wire and cables on the moon and operations worldwide. While Gore may be best known for their high-performance GORE-TEX® fabrics, their fluoropolymer expertise also delivers next-generation electronics and medical products. The company has repeatedly been named among the '100 Best Companies to Work for in America,' and its culture of trust is a model for contemporary organizations seeking growth by unleashing creativity and fostering team-work.

Challenge

While Gore is a private company and thus not subject to many of the data privacy and security regulations public companies are required to follow, the company has chosen to follow best practices in these and other key areas of corporate governance. With world-famous patented technology and annual revenues in excess of \$1.5 billion, Gore has the potential to be an attractive target for hackers and potential intellectual property (IP) thieves. And with 6,500 associates in 45 locations around the world, the company has plenty of potential points of vulnerability.

Gore operates manufacturing facilities at two locations in the United States, as well as in the UK, Germany, and Asia, and sales offices in all its major markets. The IT environment is mixed, with most desktops running Windows on Dell hardware and back-office systems running on AS400, Sun, Linux and Wintel platforms. The core communications infrastructure is Lotus Notes, so the internally-sanctioned Instant Messaging (IM) system is Lotus Sametime, but there is also widespread use of public IM platforms such as Yahoo and MSN. All corporate Internet access is routed through the company's headquarters in Delaware.

Because of the company's culture of trust, there has not been any organized drive towards usage policy for IM, and web access restrictions are limited to blocking sites with overtly offensive content. While the vast majority of users act responsibly, IT must, however, remain vigilant to the dangers posed by spyware, which can easily fool users, or even bypass them altogether and infect systems silently during an otherwise innocent-seeming website visit. An unsuspecting user clicking on a link forwarded in an IM conversation could wreak havoc on the network in short order.

Although Gore has not experienced any significant security events as a result of spyware, the company felt strongly that it needed to take steps to ensure the security of its IP and the productivity of its workforce, particularly given the increased number of targeted attacks by spyware developers on specific organizations.

In 2004, Gore took its first steps in perimeter malware blocking with the deployment of McAfee® IntruShield® intrusion prevention system for general-purpose perimeter security, and in late 2005 the company began to roll out McAfee AntiSpyware to desktops and laptops. However, it was clear that client anti-spyware, which doesn't act until spyware infection has already occurred, and perimeter intrusion prevention would not provide the degree of spyware-specific defenses necessary to guard the central corporate Internet access point. So the search began for a solution that was both gateway-based and designed specifically to address the spyware problem.

Solution

It was important to Gore to retain the culture of trust that has served them so well over the years, so the right solution for the company needed to continue to allow responsible users freedom of access to pursue their online activities, while putting in place safety nets that would protect the company and its valuable intellectual property against accidental vulnerabilities caused by less careful employees. Lockdown solutions that might work in other company cultures were not acceptable for W L Gore & Associates.

Gore considered a number of solutions, both software and hardware, to fill the perimeter spyware protection gap. Fortuitously, as the company was beginning its search, FaceTime was beginning public beta testing for Real-Time Guardian™ 3.0 (RTGuardian), and Gore became an active and enthusiastic participant in the testing program.

The company was immediately impressed with the speed and ease with which they were able to get RTGuardian up and running. The installation was simply a matter of connecting via a monitor port at the perimeter; from that point, “discovery mode” (monitoring) and “enforcement mode” (protection) could immediately be applied to all Gore locations around the world. The centralized administration enables the company to manage both the appliances and the corporate-wide standard policies from a single point, and network performance is

unaffected since RTGuardian looks at packets rather than scanning data inline. From a protection standpoint, the reports tell a clear story: RTGuardian is effectively preventing drive-by infections by blocking the download of spyware file types and preventing tell-tale phone-home behavior. The built-in extensibility of the solution is also welcome. Gore can easily add FaceTime's Greynet Enterprise Manager (GEM) module enabling the company to add targeted remediation and inoculation for hard-to-protect clients such as sales department laptops and desktop machines. Targeted remediation will eliminate the need for Gore to initiate broadbased scanning and cleaning of all employee PCs, allowing them to focus only on infected machines identified by RTGuardian at the perimeter. The entire process – from gateway to desktop remediation – can be automated, so IT resources can be focused on more productive tasks.

Results

Tim Yates, Senior Network Engineer at W L Gore & Associates, has no doubt that the decision to use FaceTime's RTGuardian to complete the company's perimeter spyware protection was the right one.

“FaceTime went out of their way to make this an easy decision for us,” says Yates. “Other vendors we considered were looking for us to make a much bigger upfront commitment than was appropriate for our needs. RTGuardian has a great interface, excellent reporting, and it's so easy to get just the information we need. Spyware protection must always address both the desktop and the perimeter, and FaceTime's technology clearly has an important role to play.”

In fact, Yates has been so impressed by the smoothness of putting the RTGuardian solution in place that the company is considering using FaceTime solutions as the foundation for a more formal IM usage policy in the future.

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, P2P file sharing, web conferencing and instant voice. FaceTime's award-winning solutions are used by over 600 customers, among them seven of the eight largest U.S. financial institutions. FaceTime supports or has strategic partnerships with all leading public and private IM network providers, including AOL, Google, Microsoft, Yahoo!, IBM, Bloomberg, Jabber and Reuters.

