

Rock-Solid Environmental Protection

Oregon Department of Environmental Quality Cleans Up Hazardous Malware with NETGEAR® STM Stream Scanning Technology

Profile

INDUSTRY: Government

Organization

State of Oregon Department of Environmental Quality
Portland, Oregon, USA www.deq.state.or.us

Challenge

Defending 1,000 computers against new Web-based threats with minimal administration

Solution

NETGEAR® STM Stream Scanning Technology proactively stops Internet-based spyware and viruses at the gateway without any impact on network performance

Background

The State of Oregon Department of Environmental Quality (Portland, Oregon; Oregon DEQ) is a regulatory agency responsible for restoring, maintaining, and enhancing the quality of Oregon's air, land, and water. The state agency protects and enhances Oregon's water and air quality, cleans up spills and releases of hazardous materials, and manages the proper disposal of hazardous and solid wastes. The Environmental Protection Agency delegates authority to Oregon DEQ to operate federal environmental programs within the state such as the Federal Clean Air, Clean Water, and Resource Conservation and Recovery Acts. Oregon DEQ's network environment includes 1,000 computers distributed across 16 locations throughout the state.

PROBLEM/OBJECTIVE

CODE RED ALERT

As Web usage at Oregon DEQ grew over the years, so did the risk of being attacked by Web based threats. Employees browsing the Web were jeopardizing their IT systems, opening up the door for new threats to come in. They had defenses against email borne threats such as spam and email viruses, but nothing to protect against Web based malware. The risk of exposure to such threats was very apparent, but due to resource constraints nothing was ever put in place to stop such threats. Risk finally turned into reality when several years ago, the Code Red worm was unleashed upon the world, and Oregon DEQ.

Code Red was one of the most disruptive worms in history, attacking government entities such as the White House and the Pentagon and causing an estimated \$2.6 billion in damage worldwide. It was also one of the first worms to use the Web as an attack vector. Code Red exploited a buffer-overflow vulnerability in Microsoft IIS based Web servers by sending a malformed HTTP request to the Web server being attacked. It was so effective due to the fact that at the time there was little to no network protection against Web based threats. For Oregon DEQ, Code Red was a wake-up call. The incident exposed the vulnerability of the agency's undefended Web traffic and highlighted how Web-based malware could pose a greater threat than email-based malware.

SOLUTION

DOING MORE WITH LESS

Oregon DEQ recognized that it needed to protect its Web traffic from sophisticated new malware threats, and it needed to do it with minimal administration. Patrick Irvine, the agency's email administrator, is responsible for all aspects of IT communications and security. Patrick had certain key requirements for a gateway security solution: "Zero administration. Zero hassles. We needed a product to take care of our security needs, but we really don't have the staff to watch it like a hawk." The product had to have (1) an excellent detection rate for viruses and spyware, (2) extremely easy deployment, and (3) zero administration.

Patrick contacted a government IT security reseller and evaluated gateway anti-malware appliances from a leading European anti-virus (AV) vendor and the Content Security Gateway (CSG) appliance using NETGEAR STM Stream Scanning Technology.

The contrast between the two products was, according to Patrick, like "night and day." The European AV company's product was difficult to deploy and kept crashing, even after the vendor sent several replacement appliances. "In the end, we never got the product to work," said Patrick.

When Patrick evaluated the CSG appliance using NETGEAR STM Stream Scanning Technology, the product handily exceeded his expectations. "It really is an appliance," said Patrick. "We didn't take more than 30 minutes to set it up, do some updates, and we were done. You set it up and it goes. The best part, though, is knowing that spyware and viruses are not coming in through Web traffic, and the speed and performance of the network isn't suffering."

RESULT

ROCK-SOLID GATEWAY DEFENSE

The CSG appliance using NETGEAR STM Stream Scanning Technology is now the frontline defender for the entire agency. Since deploying the CSG, Oregon DEQ has experienced no malware attacks and no Web traffic latency. Prior to using the CSG with NETGEAR STM Stream Scanning Technology, Patrick fought spyware at the desktop level with four different anti-spyware products that "just worked OK, not fabulous." Now he is winning a proactive, preventive war against spyware at the Web gateway: "I haven't had anything inside our network get spyware." Patrick also enables the appliance's email scanning, which has detected and stopped email-based malware that a leading email security appliance deployed upstream missed. Even with both Web and email scanning enabled for the entire network of 1,000 computers, "everything ran as usual," there has been no Internet slowdown. Patrick concludes: "The appliance has proved itself to be a rock-solid, stable product. The NETGEAR STM Stream Scanning Technology inside the appliance has enabled all 1000 computers on our network to enjoy safe and virtually latency free Web browsing. We are well protected on all ends and I don't need to do any administrative work. To me that says it all."

"NETGEAR STM Stream Scanning Technology running on the CSG appliance has proved itself to be a rock-solid, stable product. We are well protected on all ends and I don't need to do any administrative work. To me that says it all."

Patrick Irvine
 Email Administrator
 State of Oregon Department of Environmental Quality