

Providence College Captures Previously Undetected Attacks with FireEye Web Malware Protection System

Summary

Company	Providence College, Providence, Rhode Island
Industry	Education
Description	Providence College is a private, coeducational, Catholic college located in Providence, Rhode Island. With its 2010–2011 enrollments of 3,850 undergraduate and 735 graduate students, the college specializes in academic programs focused on the liberal arts.
Challenge	Identify and install a security solution that was easy to implement, didn't contribute to operational overhead and eliminated the shortcomings of signature-based detection technologies such as NGFW, IPS and AV, which cannot stop advanced malware.
Solution	Deployment of FireEye Web Malware Protection System 4000 Series appliance.
Benefits	Protection against advanced malware, zero-day and targeted APT attacks as well as immediate visibility into previously undetected malicious code and optimization of remediation processes permitted swift cost justification of project. Plus all college network traffic passes through the FireEye Web MPS appliance without latency.

Ranked by *U.S. News* as one of the top two master's level colleges and universities in the North for thirteen consecutive years, Providence College sits on a picturesque hilltop campus two miles west of downtown Providence, Rhode Island, the state's capital city. Just like any mainstream commercial enterprise, the college is tasked with protecting sensitive data; relating to its students, faculty, staff and research projects.

"There is some very sensitive data within the Providence College environment, but with the FireEye Web MPS appliance we know that advanced malware never makes it onto our network undetected."

– Donald J. Schattle II, Information Security Officer, Providence College

The Truth Can Be Scary

Recognition of the limitations of tools acting solely on signatures catalyzed an extensive period of research for Don Schattle, Providence College's Information Security Officer, that culminated in a pilot of the FireEye Web Malware Protection System. "What we immediately saw was extremely eye-opening! The FireEye appliance was catching malicious code that had previously entered our environment completely undetected," He recalled.

The FireEye Web Malware Protection System (MPS) appliance provides automatic, real-time blocking of next-generation Web malware. Inbound and outbound traffic is inspected to confirm and capture zero-day malware and targeted attacks. Risk is evaluated through the actual execution of suspected code in a full-featured virtual endpoint environment that precisely determines core intent.

Time is Money

"Early in the evaluation we meticulously tracked every single FireEye Web MPS-generated alert and found that in all cases, the notification was triggered by a real threat," said Schattle. "We instantly saw that our current security platform had missed a variety of malicious code." This accuracy allowed the college's IT team to dramatically reduce the time and cost associated with the detection and eradication of malware threats.

Schattle noted, "The inline installation of the FireEye Web MPS was a quantum leap forward for us. Not only will it detect and block a threat, it does so in a very elegant manner; the appliance immediately lets a user know why a Web page was not delivered."

The FireEye appliance sits directly behind the firewall and is the gateway to a 5,000+ node campus-wide network. Schattle observed, "It's never a bottleneck for the network even though all of the college's traffic passes through it. The significant processing power and throughput capabilities of the unit just make this a non-issue."

Schattle concluded, "Any device we deploy needs to deliver what was promised with a minimum of operator intervention and with a high level of reliability and autonomy: Our FireEye Web Malware Protection System 4000 Series appliance gives us exactly that."

Key Component

FireEye Web Malware Protection System 4000 Series appliance

FireEye is the world leader in combating advanced malware, zero-day and targeted APT attacks that bypass traditional defenses, such as Firewalls, IPS, AV, and Web gateways!

© 2011 FireEye, Inc. All rights reserved. FireEye, Inc. and all FireEye, Inc. products are either trademarks or registered trademarks of FireEye, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. -- CS.WMPS4000.052011