

# Providence College captures previously undetected attacks with FireEye

CUSTOMER STORY

## KEY COMPONENTS

- FireEye Network Threat Prevention Platform

Ranked by *U.S. News* as one of the top two master’s level colleges and universities in the northern United States 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.

### 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® Network Threat Prevention Platform. “What we immediately saw was extremely eye-opening! The FireEye platform was catching malicious code that had previously entered our environment completely undetected,” he recalled.

The FireEye Network Threat Prevention Platform 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

COMPANY	Providence College, Providence, Rhode Island
INDUSTRY	Education
DESCRIPTION	Providence College is a private, coeducational, Catholic college located in Providence, Rhode Island. With over 5,000 students the college specializes on academic programs focused on liberal arts
CHALLENGES	<ul style="list-style-type: none"> <li>• 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</li> </ul>
SOLUTION	<ul style="list-style-type: none"> <li>• FireEye Network Threat Prevention Platform</li> </ul>
BENEFITS	<ul style="list-style-type: none"> <li>• Protection against advance malware, zero-day and targeted APT attacks</li> <li>• Immediate visibility into previously undetected malicious activities</li> <li>• Cost savings through optimization of remediation process</li> <li>• Zero latency or user impact</li> </ul>

“There is some very sensitive data within the Providence College environment, **but with the FireEye Network Threat Prevention Platform we know that advanced malware never makes it onto our network undetected.**”

— **Donald J. Schattle II**, information security officer, Providence College

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-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 platform 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 platform immediately lets a user know why a web page was not delivered.”

The FireEye platform 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 Network Threat Prevention Platform gives us exactly that.”

**To learn more about FireEye, visit:**  
[www.fireeye.com](http://www.fireeye.com)