Rapid7 Nexpose Helps to Protect Huge IT Infrastructure at Virginia Tech

An IT Leader

Virginia Tech has long been in the forefront of information technology. The campus has been fully networked since the early 80s, and more than 15 years ago, the school, in collaboration with what was then Bell Atlantic – now Verizon – and the Town of Blacksburg spearheaded the development of the Blacksburg Electronic Village. This project represented the first attempt anywhere in the country to make the vast resources of the Internet available to everyone throughout a university community.

Because of the University's vast size and scope, IT security is a major issue at Virginia Tech. One indication of its importance is that the University's vice president for IT reports directly to the school's president. A key element within Virginia Tech's IT department is the Office of IT Security, which has three components: Awareness, Training, and Policies; Identity Management; and the IT Security Lab. Randy Marchany is director of that lab, and Brad Tilley is an IT security analyst there. Marchany describes the lab in this way, "It is a product testing facility, an academic research facility, and an operational center for security functions within Virginia Tech."

IT Security Office staff members develop policies, coordinate training, and conduct awareness presentations throughout the University. Every student, faculty, and staff member at Virginia Tech is assigned what is called a universal ID, and the IT Security Office is responsible for creating, maintaining, and defining the appropriate authorization level for each of these thousands of IDs.

Client
Virginia Tech

Industry
Higher Education

Website
www.vt.edu

PCI Drives the Need for Vulnerability Scanning

In 2007, the IT Security Office initiated a security self-assessment. The driving force behind the project was to ensure that all University departments that handled credit card transactions were in compliance with the Payment Card Industry (PCI) standard. To conduct this activity, the Security Office adopted a strategy of using one Freeware tool – Nessus – and an equivalent commercial tool, which prompted the purchase of Rapid7 Nexpose.

Case Study Highlights

Challenge
In a large univerisity like Virginia Tech, IT security is a major issue. The Office of IT Security conducted a self-assessment of their compliance with the PCI standards, and found they needed a commercial scanner with capabilities beyond Nessus.

Solution
Virginia Tech began using Nexpose to scan all of their assets– servers, web applications, networks and databases. They found Rapid7's product and tech support to be tremendously helpful in securing their large network.

Tilley remembers the research that preceded their decision. "We had been using Nessus for several years as an inexpensive and easy vulnerability scanner," he says. "We set up a scan website that uses Nessus as its backend, and we started looking for a commercial scanner that could go beyond the capabilities that Nessus offered, which was how we found out about Rapid7 Nexpose. Now, we use Nexpose to scan everything – servers, Web applications, networks, databases."

"All Security is Local"

One of the guiding principles of the Security Office is "All Security is Local," and they try to disseminate this philosophy throughout the University. Marchany says, "We were seeking a tool that enabled us to monitor systems from a central standpoint, but one that would also give local system administrators throughout the school the ability to scan their own systems whenever they wished."

> "[Role-based access] gives system administrators around the campus a sense of empowerment."
>
> **Randy Marcheny**
> Director of IT Security Lab
> Virginia Tech University

The role-based access feature of Rapid7 Nexpose helps the Security Office to do just that. Role-based access enables the security staff to allow an administrator to access the scanner and use it without interfering with anyone else who may be doing the same thing. As Marchany says, "This capability gives system administrators around campus a sense of empowerment. They say, 'I can run a security scan whenever I need to, and I can review the results before the IT Security Office tells me I need to fix something.' This functionality has helped them to be more pro-active, and it has helped us tremendously."

Benefits

Better control of the network

With Nexpose, Virginia gained more visibility and a greater ability to manage their vast network than they had with free tool Nessus.

Large network scan capabilities

32,000 Nodes scanned with Rapid7 Nexpose.

Great customer support

"They are very responsive and they know what they're talking about... With Rapid7, the people you deal with are knowledgabe right up front." said Brad Tilley, IT Security Analyst at Virginia Tech.

Finer Scans

There are at least 32,000 nodes on the Virginia Tech network. "We don't have a border firewall," says Marchany. "Most of our systems have host-based firewalls, and they play an important part, but we also have a fairly extensive wireless network. All of this means that the sheer number of machines out there makes it extremely challenging for us to identify where sensitive data resides. That's why we appreciate the finer scans available through Rapid7 Nexpose. It is one of the tools that has been very valuable in our PCI compliance effort."

Accessible and Knowledgeable Technical Support

Rapid7 earns high marks from Marchany and Tilley for technical support. "They are very responsive," says Tilley, "and they know what they're talking about. With some companies, when you call tech support, you have to go through layers of support personnel before you find someone who can actually help you. With Rapid7, the people you deal with are knowledgeable right up front."

About Rapid7

Rapid7 is a leading provider of IT security risk management software. Its integrated vulnerability management and penetration testing products, Nexpose and Metasploit, and mobile risk management solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT environment, users and threats relevant to their organization. Rapid7's simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital and Technology Crossover Ventures. For more information about Rapid7, please visit http://www.rapid7.com.