



## CUSTOMER CASE STUDY

“The role-based access feature in Rapid7 NeXpose gives the system administrators around campus a sense of empowerment. ... It has helped them to be more pro-active, and it has helped us tremendously.”

Randy Marchany  
Director, IT Security Lab  
Virginia Tech

## 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.

### 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.

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



Founded in 1872 as a land-grant college, Virginia Polytechnic Institute and State University –better known as Virginia Tech – is home to more than 30,000 students, the largest full-time student population in Virginia. The school, located on a beautiful 2,600-acre campus in Blacksburg, Virginia, offers more degree options than any other college in the Commonwealth, and its global reach includes facilities in Switzerland, the Dominican Republic, Egypt, and India.

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.”

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.”

#### **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 Rapid 7**

Rapid7 is a leader in [vulnerability management](#) and compliance, delivering a single unified solution across an organization’s entire infrastructure. Rapid7 NeXpose helps securities professionals to reduce their attack surface by providing actionable insights into the real threats from vulnerabilities across their entire IT infrastructure. Rapid7 NeXpose is the only solution that provides in-depth coverage of vital Web and database systems in addition to networked devices, servers, and operating systems. The NeXpose A.I. and Reporting Engines synthesize large quantities of raw data to provide direct insight into the vulnerabilities that represent the most risk to the business. From this insight the product delivers a set of prioritized remediation recommendations that help security professionals get protection fast. Organizations, including Black & Decker, Trader Joe’s, Florida State University, the New York Times, and the City of Philadelphia, continually rely on Rapid7 products and services to mitigate risk and remain compliant.