



CUSTOMER CASE STUDY

“There’s really only so much you can accomplish with a manual audit of your network, and that kind of audit doesn’t always give you the in-depth information you need.”

Jeremy Wood
Information Security Analyst
Norwich University

Rapid7 Nexpose Enables a Small IT Staff to Manage a Large IT Infrastructure at Norwich University

A Sophisticated Computer Network

Norwich provides students, faculty, and staff with a comprehensive computer infrastructure. There are wired and wireless connections in all dorm rooms, as well as a recently overhauled campus-wide wireless network which is fully redundant, from the edge to the core. While this redundancy offers maximum flexibility, it also means that there are twice as many network intrusion points.

Jeremy Wood, Information Security Analyst at Norwich, describes the situation they faced in early 2008. “Our infrastructure was already pretty large, and it was continuing to grow,” he says. “We knew that we had a number of Windows servers and a number of Linux servers, but we didn’t have a really clear idea of exactly what was on each of them. In addition, it was becoming increasingly difficult to manually audit all of those servers and all of our network equipment. There’s really only so much you can accomplish with a manual audit of your network, and that kind of audit doesn’t always give you the in-depth information you need.”

The Choice of Rapid 7 Software

To address these issues, the Norwich IT department decided to upgrade their computer security. After defining critical needs, they chose Rapid7 Nexpose software and were impressed with it from the start. “It was easy to set up,” according to Wood, “and we began scanning IPs almost immediately. Within the first day, we were already scanning and getting back excellent results. We then had a clear picture of our vulnerabilities and exactly what we needed to do to fix them.”

The Norwich IT staff has required little support from Rapid7, but when they did need assistance, Rapid7 was there. Early on, there were some licensing questions, so Wood called Rapid7. “Within one day, they had addressed and fixed those problems,” he recalls. “They also went ahead on their own and activated our external scan engine, which saved me from having to make another call about that.” The second encounter with Rapid7 was equally fruitful. After Wood submitted a product enhancement suggestion, he received a message back the same day saying that his suggestion was being evaluated and considered.

Rapid7 Nexpose has provided a visible increase in efficiency at Norwich University, where, as is the case at many schools, a small IT staff must manage a large IT infrastructure. “We save a ton of time by having Rapid7 Nexpose do all the scanning,” says Wood. “It handles a lot of the tasks that we would otherwise have to do manually.”

Eliminating 1,500 Network Vulnerabilities in Two Months

Rapid7 Nexpose’s first scan identified about 3,000 network vulnerabilities, some small and some critical. Within the first month, the IT staff was able to eliminate about 1,000 of those vulnerabilities, followed by another 500 the next month, meaning that they were able to halve the number of vulnerabilities within just two months, quite an impressive feat.



Norwich University is a military college in rural Northfield, Vermont, not far from the state capital, Montpelier. Founded in 1819, Norwich was the first private military college in the United States and the birthplace of the nation's ROTC program. Its current student body of 1,900 includes men and women from more than 40 states and 20 foreign countries, who choose one of two educational tracks – traditional or military. The latter group may earn a commission upon graduation.

Now, everyone on the IT staff uses Rapid7 Nexpose. The systems are broken down another level into asset groups for ease of management. The Windows person can see all the Windows issues, for example, and the Linux person can see all the Linux ones. By segregating the issues in this way, each staff person can quickly and easily identify what needs to be fixed without sifting through additional information.

Compared to other products, Rapid7 Nexpose has been a clear winner at Norwich. "Our previous product was adequate for simple scans," says Wood, "but Rapid7 Nexpose can do a lot more, like checking our policy levels and the software on our servers."

Future Plans for Rapid7 Nexpose

The Norwich IT team's future plans for Rapid7 Nexpose include scanning all images before they are sent to any university-owned machine, thereby providing a baseline assessment of each image before it goes out to the university community.

Furthermore, after they have reduced the number of network vulnerabilities to under 100, the IT staff plans to make better use of Rapid7 Nexpose's ticketing system for future tracking.

Wood sums up his group's assessment of Rapid7 Nexpose this way, "You can have all the information in the world, but if you have a tool that cannot give you good reports on that information, then it's really useless."

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 is the only solution that includes support for web applications, databases, operating systems, and network devices in a single system. It separates real threats from the noise common to most vulnerability management systems, giving direct, actionable visibility into the real threats to mitigate risk and remain compliant. For more information on Nexpose products and services, visit www.rapid7.com

NU CS 1208