



CUSTOMER CASE STUDY

“In my experience NeXpose has been extremely useful. We use it for both general and target scanning, and love that it can pinpoint a particular device and scan more deeply. It’s great for finding problems and demonstrating what’s really going on in networks. It’s helped educate a lot of people here.”

Michael King
CISO
City of Philadelphia

VA in PA: The City of Philadelphia Gains an Eagle Eye View of their Network

With the number of network attacks on the rise, data security is an issue of increasing concern. Government agencies in particular have an enormous responsibility to ensure that their IT systems are secure. Their systems contain a wealth of sensitive information, and vulnerabilities in the servers, switches, routers, firewalls, and databases leave these systems susceptible to unauthorized access and attack. Proactive protection of the network is critical to the integrity of the agency and the safety of those who rely on it.

The City of Philadelphia exemplifies the benefits an organization can reap when using a highly developed and multi-faceted vulnerability management solution. Used across the entire city government, NeXpose, the award winning vulnerability management system, ensures complete system coverage and strong protection of over 85 city departments.

In early 2006, the City of Philadelphia hired a new IT management team to deploy information systems that would support and enhance city government operations. Vulnerability management was immediately deemed a priority, and a product review began. A third party consultant recommended the evaluation of NeXpose.

The expert system in NeXpose outshined the competition in the evaluation process, achieving better results than rival products. The product’s capabilities met all the needs of the City’s IT department, and the price point was right. Michael King, the newly appointed CISO, made the final decision in choosing Rapid7’s NeXpose as the City’s vulnerability management solution. The City of Philadelphia purchased enough IP’s to cover a Class B network, as well as an appliance.

NeXpose provided greater visibility to their network, enabling the City to better manage it. The product’s complete coverage of the network is the primary reason it was chosen as the vulnerability management solution for the City of Philadelphia; but there are certain features that made it a great fit:

- **Reporting Aptitude** – NeXpose has the most comprehensive reporting of any product of its kind. After it scans a network, it provides a detailed remediation report, giving a step by step guide to patching the vulnerabilities it detects. The reports are extremely customizable, offering a variety of detail options. For those at the executive level, NeXpose will create a summary comprised entirely of graphs, for a simple, yet complete understanding of the scan results
- **Scanning Capabilities** – It was important to the City to be able to do a variety of scanning, and Michael was extremely impressed by the variety of platforms NeXpose can scan; Windows, Linux, and SQL to name a few. He was particularly impressed by the tool’s ability to scan databases, such as Oracle. Despite all the valuable information at stake, database security is not addressed by other vulnerability solutions. NeXpose scans databases and finds security, configuration, and operational vulnerabilities that, left



The City of Philadelphia is the largest city in Pennsylvania, one of the most populous in the U.S. and a major commercial, educational, and cultural center for the nation

unattended, would compromise the security of the network.

“In my experience NeXpose has been extremely useful. We use it for both general and target scanning, and love that it can pinpoint a particular device and scan more deeply. It’s great for finding problems and demonstrating what’s really going on in networks. It’s helped educate a lot of people here,” Michael says.

- **Availability as an Appliance** – NeXpose is offered as software, hosted service, or as a black box appliance; which is what the City chose to do. Michael explained: “The fact that NeXpose had the appliance option was a huge draw. Spending time and resources loading everything on to our servers was an extremely unappealing prospect. The appliance made NeXpose a ‘plug and play’ solution. Implementing NeXpose was extremely smooth, and user interface has never been a problem”.

“NeXpose not only provides system protection, but is instrumental in redirecting the resources of the City of Philadelphia to streamline the infrastructure of the IT department”, Michael reiterates “Thanks to NeXpose, we have a better picture of our entire network. We can easily run scans on a daily basis, and identifying our risks allows us to prioritize and use our resources in best way possible.”

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. For more information, go to www.Rapid7.com.