

“Nexpose catches stuff others won’t. It’s shown no false-positives.”

Eric Nooden
Information Security Specialist
Redflex Traffic Systems

Rapid7 Nexpose Busts Security Violations at Redflex Traffic Systems

Redflex Traffic Systems, Inc. (redflex.com) is the longest consistently operating company in the growing road-safety camera industry in the United States, with more than 20 years of experience partnering with cities to make an impact on dangerous driving behaviors.

Redflex technology has proven its impact on U.S. public safety. Its road safety cameras have helped create safer communities. Rates of running stop signs, red lights, and railroad crossings—and subsequent accidents—drop significantly when people know they might get a ticket. Advanced license-plate reading technology cross checks numbers against police databases and alerts law enforcement when matches occur. Redflex video is also valid evidence for court proceedings.

The heart of the Redflex solution is high-end database that receives and processes all traffic video through secure connections. The system identifies violations and, with client approval, generates tickets and mails them to violators. Because Redflex passes financial transactions to processing institutions, its systems must pass SAS 70 audits and comply with data protection standards such as Payment Card Industry Data Security Standard (PCI DSS) to avoid fines. The data center also includes a range of standard business applications on a mix of Windows and Unix servers.

Situation: Undermanaged Security

When Eric Nooden joined Redflex as Information Security Specialist, he found many out-of-date server operating systems. Because system stability was a priority with Redflex proprietary solutions, no one wanted to risk outages. “The systems administrators were nervous about patching servers,” says Nooden. “They were afraid of breaking them.”

The Redflex team did have multilayer security in place, with firewalls, anti-virus software, and other technologies. “They had security tools without a security person,” says Nooden. “No one had time to manage security.” The undermanaged security posture was more reactive than proactive, and Nooden joined Redflex to change that.

Solution: Rapid 7 Nexpose Enterprise Edition

Among the solutions Nooden inherited were vulnerability-scanning systems from three vendors. One of these systems was a Rapid7 Nexpose Enterprise Edition appliance. Nooden put it to work, performing a system-wide scan across all databases, Web servers, network components, and user computers. The Nexpose appliance scans for more than 14,000 vulnerabilities and performs about 54,500 checks to locate and identify threats and assess their risk to the environment. Integration with Metasploit provides remote scan control, exploit identification, and automated exploitation functionality. The scan report uses SANS guidelines to rank



About Rapid7

Rapid7 is the leading provider of unified vulnerability management and penetration testing solutions, delivering actionable intelligence about an organization's entire IT environment. Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their [network security](#), [Web application security](#) and [database security](#) strategies.

Recognized as the fastest growing vulnerability management company in the U.S. by *Inc. Magazine*, Rapid7 helps leading organizations such as Liz Claiborne, the United States Postal Service, Carnegie Mellon University and Red Bull to mitigate risk and maintain compliance for regulations such as PCI, HIPAA, FISMA, SOX and NERC. Rapid7 also manages the [Metasploit Project](#), the leading open-source penetration testing platform with the world's largest database of public, tested exploits. To obtain a free download of Nexpose or Metasploit, please visit <http://www.rapid7.com/resources/free-downloads.jsp>.

For more information, visit www.rapid7.com.

potential vulnerabilities according to severity, helping Nooden to prioritize tasks. The report also includes step-by-step procedures for effective remediation.

Initial Nexpose scans found default passwords in many devices, especially in the network, identified easily exploitable vulnerabilities in unpatched server operating systems, and gave step-by-step plans to quickly address them.

Nooden says the Nexpose user interface is highly intuitive and the reports are comprehensive. "It's so straightforward, I didn't need any formal training," he says. But he hired a Rapid7 Professional Services consultant to teach him how to fine-tune configurations to look for specific information. Nooden uses Nexpose to scan critical systems daily and others weekly or monthly. He relies upon the information in scan reports to issue change requests with the appropriate server, network, and desktop administrators and track when vulnerabilities are fixed. Rapid7 Technical Support resolves his questions quickly, often within a few minutes.

Results: Proactive Security Posture

Of its three vulnerability-scanning solutions, Redflex only renewed its license for Rapid7 Nexpose. Says Nooden, "Nexpose catches stuff others won't. It's shown no false-positives." A baseline scan with another product "gave me peanuts in comparison."

Rapid7 Nexpose Enterprise Edition provides detailed information that assisted the Redflex staff with a database upgrade project that increased the security posture of proprietary systems without compromising stability. It helps prove compliance with financial standards and regulations. Nooden plans to use Nexpose to pre-scan servers before they go online.

Like many security professionals, Nooden measures success by his ability to sleep well at night, without worries or phone calls. Rapid7 Nexpose helped him achieve that. Moreover, jokes Nooden, "It shows that I'm doing something."