

“Nexpose helped us become more secure and smarter about how we do things.”

Monica Beckworth
Manager, IT Security and Compliance
Stein Mart

Stein Mart relies upon Rapid7 Nexpose Enterprise Edition to scan its IT infrastructure for vulnerabilities

Headquartered in Jacksonville, Florida, Stein Mart (www.steinmart.com) is a nationwide retailer of fashion merchandise, with service and presentation of a better department or specialty store, at prices up to 60 percent below department store prices. With more than 260 U.S. stores in 30 states, Stein Mart’s assortment of merchandise features current-season, moderate-to-better fashion apparel for women and men, along with accessories, shoes, and home fashions.

As a retailer, Stein Mart must comply with the Payment Card Industry Data Security Standard (PCI DSS) to protect financial transactions on its store and corporate servers and Web site. A data breach would trigger an expensive PCI audit and fines, and importantly would also compromise customer trust and damage its reputation, possibly impacting future sales.

Challenge: Analyze Security Posture

As Stein Mart extended its IT infrastructure, it developed a security framework to protect it. But it lacked a comprehensive system for scanning and analyzing its security posture. The IT security team initially experimented with freeware that gathered and consolidated security data.

“Our biggest problem was taking all the consolidated data and doing something with it,” says Monica Beckworth, manager of IT Security and Compliance at Stein Mart. Stein Mart needed a better way to analyze the data, so that they could understand the risks and vulnerabilities in their current security posture and remediate them.

Along with Security Audit Analyst Ambar Batista, Beckworth determined that Stein Mart needed an easy-to-use vulnerability and analysis solution with the following capabilities:

- Scan, consolidate, and analyze data across a multivendor, multiplatform IT infrastructure, scanning server operating systems and applications, databases, Web servers, and network elements
- Schedule scans on a regular basis to help establish a proactive security posture
- Create comprehensive reports that rank specific risks and vulnerabilities by criticality to enable the team to prioritize remediation tasks

- Suggest remediation steps and provide links to learn more about vulnerabilities
- Interact with an existing third-party trouble-ticketing system
- Support remote scanning at every store

Solution: Rapid7 Nexpose Enterprise Edition

After evaluating vulnerability scanning products from several vendors, Beckworth and Batista chose Rapid7 Nexpose Enterprise Edition software. It can be configured to automatically scan for more than 14,000 vulnerabilities and perform more than 54,500 checks across Web applications, databases, networks, server operating systems, and other software products. It locates and identifies threats, assesses and ranks their risk to the environment, and offers step-by-step remediation plans. It has a PCI template to track vulnerabilities specific to compliance. It supports remote scanning and offers an API for integration with other IT management systems such as a ticketing system.

Currently, Stein Mart uses Nexpose to scan network devices, data center servers, and Web applications.

“We were able to set up, configure and scan almost immediately. The transition to Nexpose produced the results that we needed right away,” says Beckworth. “It’s easy to run the scans. It’s easy to run the reports.”

Results: Better Teamwork, Tighter Security

Batista uses information in Nexpose reports to address risks with server managers and network administrators. “If I see a critical or urgent vulnerability on the report, that tells me I need to get it resolved as soon as possible,” she says. “It helps with remediation: the links the report provides enable me to do research prior to presenting it to the team and assists the team in understanding the vulnerability and pursuing resolution.”

The use of Rapid7 Nexpose has positively impacted the performance of the entire IT staff, six teams in all.

“Nexpose has made it easier to get buy-in from all of the teams,” says Beckworth, “because they’ve become more accountable. It’s really fostered more team involvement. We’ve made better relationships with other IT teams. We work on it together, so we get things done faster.”

The Security team also uses Nexpose to pre-scan new data center and Web servers before they go online. The successful integration of Nexpose into security management also improved Stein Mart’s patching process such as scheduling the testing and application of server OS patches from Microsoft.

Batista enjoys a “great” relationship with Rapid7 support personnel and the product upgrade process. “They go above and beyond to help me out. They really try to find out from their customers what



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.

we want. Every time an upgrade comes out, it gives me something that I can really use, not just something that someone thinks I could use."

Next Steps: Extend and Deepen Scans

Beckworth and Batista plan to extend their use of Rapid7 Nexpose in several directions.

First, with the help of Rapid7 Professional Services, they plan to leverage the Nexpose API interface to automate information exchange with their trouble-ticketing system for thorough problem tracking and resolution.

They want to extend scans to include databases, which the tool already supports.

They plan to install client software at all 260-plus Stein Mart stores to automate remote scans. Until now Batista has been scanning stores remotely through a laptop that is configured with Nexpose software and shipped from store to store. A store manager plugs the laptop into the store network. Batista then configures the engine for the store's network and schedules the scan from her console in the central data center.

Both Beckworth and Batista would recommend Rapid7 Nexpose without hesitation. "There's a lot of value for the price," says Beckworth.

"I've been very impressed with the product. Any beginner would be able to use it and understand it," says Batista.

"But, it has all the bells and whistles you need," adds Beckworth. "Nexpose helped us become more secure and smarter about how we do things."