RAPID7

PCI DSS Compliance Case Study

Rapid7 Nexpose Enhances PCI Compliance and Overall Network Security for Bob's Stores

About Bob's Stores

In 2008, Bob's Stores was looking to broaden its security tools in order to meet new PCI compliance standards. Specifically, with requirement 11 of the PCI DSS in mind, which called for regular tests of security systems and processes through internal and external scans, Bob's IT department began researching how other vulnerability management vendors could help Bob's meet these standards and protect customer data.

Nick Sorgio, Assistant Vice President, technology manager at Bob's who is responsible for information security and oversees a cross-functional team IT team that handles the entire technology infrastructure, describes the situation they faced in 2007. "With the new PCI requirements, especially for scanning, there was a lot of pressure on retailers to quickly meet compliance standards. At that time, we had no vulnerability management system in place that would help with those mandates and determining a vulnerability management tool that would easily help us get there became a top business priority."

BOB'S STORES

Client
Bob's Stores

Industry
Retail

Website
www.bobstores.com

Challenge: PCI DSS Compliance

To address this crucial compliance need, Bob's completed a full assessment of every vulnerability management vendor in the market – ultimately leading the Company to Rapid7. During the evaluation process, Bob's was immediately impressed by Rapid7's ability to identify vulnerabilities across networks, operating systems, databases, Web applications and a wide-range of system platforms. To meet Bob's specific PCI needs, Rapid7 Nexpose provided vulnerability assessment scanning and monitoring capabilities that met the required PCI data security standards, while also providing sound vulnerability management practices as part of a comprehensive security program. In addition, Nexpose delivered audience-based PCI reporting, including PCI audit reports with detailed step-by-step instructions for vulnerability remediation and automated compliance.

"We took a look at every possible vulnerability management company out there, and Rapid7 was by far above-and-beyond the others," said Sorgio. "Rapid7 truly looks at everything, and that completeness was something we didn't see anywhere else. This made it an easy decision for our IT team."

Case Study Highlights

Challenge

When a host of new PCI DSS requirements came in to place, Bob's Stores needed to make sure they could meet these compliance standards efficiently and with confidence.

Solution

Rapid7 Nexpose provided vulnerability assessment scanning and monitoring capabilities that met the required PCI data security standards, while also providing sound vulnerability management practices as part of a comprehensive security program.

Solution: Time-Saving Scanning Automation

Working with Nexpose, the IT team at Bob's quickly realized its endless potential. Like many companies today, Bob's IT department doesn't have the endless budget or staff necessary to manage an infrastructure in an easy, cost-effective and secure fashion; however, Nexpose easily fit into a time-saving process that required little change or additional employee resources. This saved Sorgio countless hours of having to run various tools on individual devices and, instead, allowed him to scan and view all of the servers at once.

> *"We took a look at every possible vulnerability management company out there, and Rapid7 was by far above-and-beyond the others."*
>
> **Nick Sorgio**
> Assistant Vice President
> Bob's Stores

"Nexpose just made our lives easier," recalled Sorgio. "It was incredibly easy to set up the system and get started scanning across the board. The automated scans and detailed reporting features are great and better than anything else we have seen, especially for compliance. We thought we had a good handle on our patch management, but the second we started with Nexpose and receiving scan results, we were actually surprised to see how much more detailed and helpful Nexpose results were. Without that type of in-depth knowledge, the majority of companies are unable to truly see where they actually stand in their security management."

In addition to relying on Nexpose for vulnerability scanning, Bob's IT department turns to Rapid7 as its PCI partner. Rapid7 experts are always on hand to help the IT team understand the PCI requirements and provide analysis of the results. "Our questions are always about taking a deeper dive into understanding the vulnerabilities that Nexpose finds; never about the usability of the product," Sorgio said. "For example, the PCI Council requires scan vendors to address vulnerabilities in a particular way, determining both vulnerable and potentially vulnerable risks, and this can be difficult to understand sometimes. Rapid7 has almost become our PCI partner, taking the time to work with us and prioritize our compliance risks."

Future Plans

Once Bob's got started using Nexpose and Rapid7 experts as a strategy for compliance, the team quickly realized the value that comprehensive vulnerability management can bring beyond the original PCI requirements.

"In the retail world, people automatically protect the things that are of the most value, such as customer cardholder data," said Sorgio. "However, with Nexpose we quickly learned that vulnerabilities can be the biggest risk and weakness in most corporations, and that it's the places that aren't as well-guarded that get overlooked and become a gateway into even the most secure systems." As a result, Bob's recently just implemented enough IP addresses to scan their entire environment soup to nuts – a 50% increase in the Nexpose licenses that they previously used.   Bob's also began using Metasploit, the open source penetration testing framework with the world's largest database of public, tested exploits, several months ago to meet the penetration testing requirements of PCI compliance and plan to continue this in the future as well.

"We saw the value that Nexpose provides with its scans and the risk of not using it across the board was just too high," said Sorgio. "As does anyone responsible for security, I have to consistently consider what the biggest risks our company faces are and with vulnerability management at the top of the list increasing our work with Rapid7 was a no-brainer."

Sorgio sums up his assessment of Rapid7 Nexpose this way, "Our experience with Rapid7 has taught us that a good vulnerability management program is the foundation of a successful, strong security program and it really all builds out from there.   Rapid7 has easily become one of my favorite vendors to work with and they are the cornerstone of our security program."