Over the past year, the retail industry has been the victim of numerous high-profile data breaches. As long as retailers continue to hold valuable credit card data that can be quickly converted into cash, they will continue to be the target of attackers.

Retailers also need to balance the demands of securing their environment with the compliance requirements of the Payment Card Industry Data Security Standards (PCI DSS).

How a retail data breach happens

The initial compromise often involves straightforward attack methods, e.g. leveraging default credentials, a web app vulnerability, or phishing. The purpose is to gain access to the network without raising alarms.

After the attacker has established a foothold, they will study the environment and build custom malware. This is deployed on all point-of-sale (POS) systems in phases and used to harvest and exfiltrate magnetic strip data from credit cards without detection.

Once the attacker possesses the data, they will try to sell it as quickly as possible in underground forums before the breach is detected. This is used to manufacture fake cards for criminal operations.

Security challenges faced by retailers

- A motivated, organized and nimble adversary targeting highly valuable credit card data
- Complex and distributed IT infrastructure with legacy and difficult to patch systems
- Custom malware targeting POS systems becoming easier and cheaper to build and adapt
- Overwhelming number of alerts resulting in failing to spot genuine indicators of compromise
- New version of PCI DSS requiring various changes to security and compliance programs

Reduce risk of a breach

Vulnerabilities in POS and other retail systems provide an access point for attackers to establish a foothold. Security teams need to proactively find and quickly fix weaknesses in their network to reduce the attack surface.

Rapid7 threat exposure management solutions can help you:

- Identify and prioritize the risk of vulnerabilities, misconfigurations and controls across your network
- Simulate attacks on your network to uncover weaknesses and test effectiveness of security controls
- Automatically audit your network for PCI compliance and generate reports from built-in templates
“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.”

Nick Sorgio
Assistant Vice President, Bob’s Stores

---

**Accelerate security improvement**

As a popular attack target, retailers need a comprehensive security program aligned to business goals, industry best practices and PCI compliance requirements. Security programs should drive continuous improvement to stay ahead of threats.

**Rapid7 security advisory services can help you:**

- Perform a gap analysis of your program against a security maturity model and industry best practices
- Develop strategic and tactical roadmaps, including a prioritized set of security initiatives
- Create executive scorecards to measure security improvement and risk reduction over time

**Find the attacks you’re missing**

It takes on average 209 days to discover an intrusion (Mandiant 2014 Threat Report). During this time, attackers are harvesting and exfiltrating credit card data for fraud. It’s not enough to just prevent attacks, retailers need to continuously monitor their network to quickly detect compromise and minimize damage.

**Rapid7 incident detection and response solutions can help you:**

- Detect attacks using compromised credentials, user impersonations and lateral network movement.
- Investigate and respond to incidents with an interactive timeline and full access to user activity data
- Integrate with existing monitoring solutions to improve alert quality with intruder behavior analytics

**Simplify PCI compliance**

Rapid7 is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council, authorizing us to help you achieve compliance with PCI DSS.

**Rapid7 can help you:**

- Perform quarterly internal and external vulnerability scans
- Audit systems against industry-accepted hardening standards
- Perform internal and external penetration tests
- Monitor user access to cardholder data and restricted network zones
- Identify gaps in your security program against PCI DSS

Learn more about how Rapid7 can help with PCI DSS at [www.rapid7.com](http://www.rapid7.com)