SOLUTION BRIEF

tenable

Tenable for Retail

Continuously Monitor and Assess PCI Security Maintain Consumer Confidence

The retail industry has been the target of some of the highest-profile data breaches in recent years. With a deeply embedded and highly dispersed infrastructure comprised of thousands of brick-andmortar stores and ecommerce websites, many retail brands are household names. Data thefts in this sector garner immediate and relentless attention. Consumer personal identity and financial information promises enticing rewards for hackers, who employ savvy schemes to steal and monetize these lucrative data assets for maximum profitability. Nefarious attacks that compromise confidential customer data are on the rise, and retailers are increasingly vulnerable to advanced targeted attacks like DDoS and ransomware.

> Retailers worldwide are attacked more than any other industry.
> 2017 Global Threat Intelligence Report

Every online and instore retail merchant, point-of-sale vendor and service provider that accepts, processes, stores or transmits credit, debit or gift card data must demonstrate compliance with Payment Card Industry Data Security Standard (PCI DSS) operational controls and technical requirements designed to protect transactions and cardholder data from malicious activity and theft.

Adopting best practices to neutralize cyberthreats, vigilantly protect consumer data across channels, secure payment card transactions and ensure compliance are crucial priorities for today's retail sector.

Solutions

- Tenable.io
- Tenable.sc
- Nessus Network Monitor

Key Benefits

- Payment Data Security
- Consumer Confidence
- Continuous Compliance
- Comprehensive Visibility
- Reduced Risk

Key Challenges

Merchants must protect customer privacy and relationships by continuously building and maintaining trust. Retailers are expected to prevent data theft and fraud while simultaneously offering customized shopping experiences. The technology innovations that enable highly personalized services are outpacing the industry's ability to protect consumer information.

DATA SECURITY

Cybercriminals hunt for infrastructure misconfigurations to gain access to vulnerable point-of-sale (POS) systems and servers, from which they steal the data stored in payment card magnetic strips. When consumer data is compromised, retailers risk major impacts to the bottom line, brand integrity and business continuity.

> Nearly one in three retailers has suffered revenue losses as a result of a cyberattack.
> 3 Trends Shaping Retail Cybersecurity in 2017

PCI COMPLIANCE

While PCI compliance is a key driver for the retail sector, diligent cybersecurity practices go well beyond baseline regulatory requirements, leveraging modern technology solutions for comprehensive visibility and proactive remediation of real-time vulnerabilities.

> 74% of IT professionals said their companies are only partially PCI DSS compliant.
> **Global Study on the State of Payment Data Security** (Ponemon Institute).

LEGACY SYSTEMS

The outdated architectures that often support hybrid retail environments typically lack adequate defenses, luring hackers to exploit irresistible security gaps. When new technologies are integrated into aging infrastructures without proper security protections, the attack surface expands, making data breaches harder to detect.

The credit card industry remains reliant on decades-old technology. While the chip cards introduced a few years ago provide unique codes for transactions, they still feature cardholder names, account numbers and expiration dates in full view for all to see. There's minimal protection against fraudulent use of lost or stolen cards. In addition, POS systems that store payment data on-prem instead of in the cloud can be hacked by malicious perpetrators.

MODERN TECHNOLOGIES

The innovative technologies that enhance customer experience can also jeopardize security. The machine learning systems that analyze purchasing patterns across channels to deliver personalization simultaneously open attack vectors while customizing the shopping experience. Also, as IoT innovations like smart shelves, RFID merchandise trackers and perishable goods sensors gain momentum, more DDoS attacks are expected to target these unprotected devices

Solutions Overview

Tenable, a PCI Approved Scanning Vendor (ASV), delivers cybersecurity solutions that empower retailers to rigorously protect customer information and maintain PCI compliance. Our vulnerability management and analytics tools and technologies enable merchants to gain full visibility and continuously monitor security and compliance posture; evaluate vulnerabilities across the ecosystem; measure and analyze effectiveness of security mechanisms; and understand, prioritize and mitigate risk.

The Tenable cybersecurity solutions portfolio for retail includes cloud-based and on-prem vulnerability management platforms:

TENABLE.IO

Manage risk on the modern attack surface. Tenable.io enables realtime discovery of every modern asset across all digital computing environments. Live discovery allows healthcare organizations to accurately assess, analyze and prioritize constantly evolving vulnerabilities across the entire ecosystem of partner providers. Bring clarity to security posture with an asset-based approach to security that provides maximum coverage in a dynamic landscape.

TENABLE.SC

Continuously discover, assess, improve and report on every aspect of network security and compliance, encompassing all on-prem, virtual, cloud and mobile devices, systems and technologies.

NESSUS NETWORK MONITOR

The retail environment is home to many IoT devices that cannot be actively scanned without operational interruption. At the same time, merchants require automated discovery of all devices on the network, as well as the ability to continuously monitor traffic without disrupting critical operations.

Gain complete visibility of device security and overall network status with a combination of active and passive scanning. Deploy Nessus Network Monitor to passively scan for vulnerabilities in network-connected IoT devices. Passive scanning avoids the need to take critical payment systems offline for assessment.

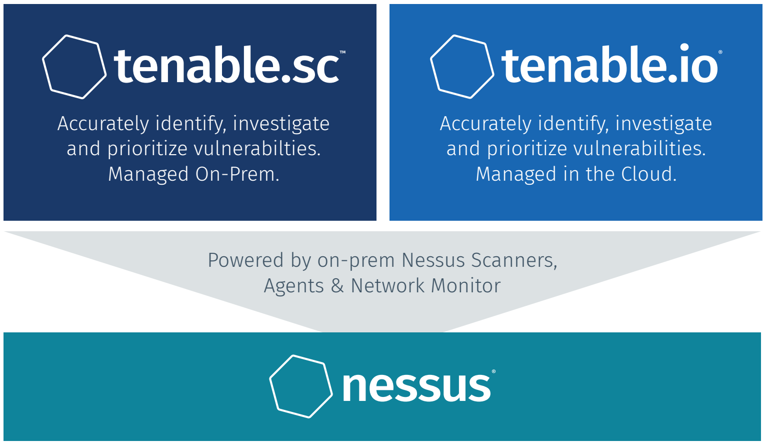
COMPREHENSIVE SOLUTIONS FROM TENABLE

Vulnerability Management

- Enterprise Management
- Live Asset Discovery
- Reporting
- Integrations & API
- Agents
- Passive Monitoring

Vulnerability Assessment

- Comprehensive, high-performance scanning
- Extensive configuration auditing



tenable.sc™

Accurately identify, investigate and prioritize vulnerabilties. Managed On-Prem.

tenable.io®

Accurately identify, investigate and prioritize vulnerabilities. Managed in the Cloud.

Powered by on-prem Nessus Scanners, Agents & Network Monitor

nessus®

RETAIL PORTFOLIO FEATURES AND CAPABILITIES

- Gain complete visibility of digital assets across the retail environment.
- Analyze all on-prem, mobile and cloud systems, devices, applications and operating systems across the cardholder data environment to rapidly and accurately identify potential threats and prioritize risk remediation.
- Quickly detect malware and unauthorized software.
- Discover system changes, anomalous behavior and suspicious activity across transaction servers.
- Continuously monitor, assess, demonstrate, validate, report and maintain adherence to all PCI security and technical control standards.
- Perform all PCI required internal and external vulnerability scans of cardholder data and retail locations.
- Get a unified view of PCI compliance status.
- Evaluate PCI compliance program effectiveness.
- Use active and passive scanning, intelligent connectors, and host data monitoring to quickly identify potential noncompliance and take immediate action.
- Rely on purpose-built PCI DSS Assurance Report Cards, dashboards, and comprehensive reporting tools to track and manage PCI security from a single pane of glass.
- Measure and communicate PCI compliance status to executives in business terms; demonstrate the impact of security investments.

Benefits

Tenable solutions deliver the following benefits to retail organizations:

PAYMENT DATA SECURITY

Get the actionable intelligence required to secure customer data across retail channels. Detect emerging threats, and protect personal identity and payment card information.

CONSUMER CONFIDENCE

Vigilantly protect customer data to maintain and strengthen brand loyalty, industry leadership and competitive advantage.

CONTINUOUS COMPLIANCE

Automatically assess security posture across the retail environment. Pinpoint nonconformance issues and maintain adherence to all PCI DSS regulatory requirements.

COMPREHENSIVE VISIBILITY

Gain a real-time view of vulnerabilities and potential threats across the retail environment.

REDUCED RISK

Continuously monitor, identify and assess security weaknesses and potential attack vectors in payment card systems.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**