tenable

SOLUTION BRIEF

ADDRESSING PCI DSS WITH TENABLE.IO

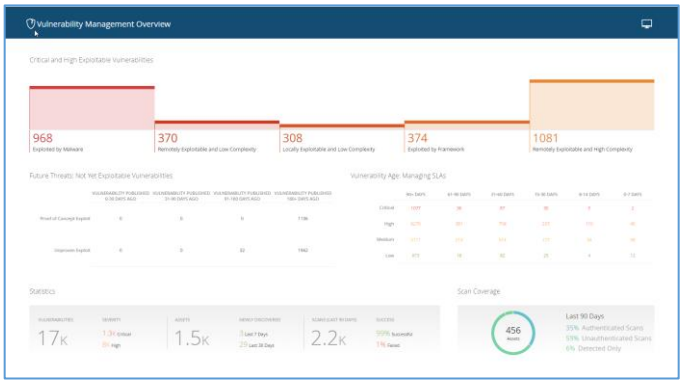
PCI COMPLIANCE

Because payment card information is one of the most appealing theft targets for attackers, protecting payment card transactions and cardholder data (CHD) is critical. A breach of cardholder data affects the entire payment card ecosystem. Merchants, processors, acquirers, issuers and service providers lose credibility – and in turn lose business – and are also subject to financial liabilities. More importantly, customers may lose trust in merchants or financial institutions.

INTERNAL VULNERABILITY SCANNING

PCI DSS 6.1 requires you to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk rating to newly discovered vulnerabilities. Additionally, PCI DSS 11.2.1 requires you to perform quarterly internal vulnerability scans.

Tenable.io Vulnerability Management is continually updated with the latest vulnerability information and quickly scans your cardholder data environment for known vulnerabilities. Tenable.io VM uses CVSS scoring to rate vulnerability risk so you can identify those that are “high-risk” and prioritize remediation accordingly. Additionally, it can re-scan your environment to help you confirm vulnerabilities were resolved per your policy.

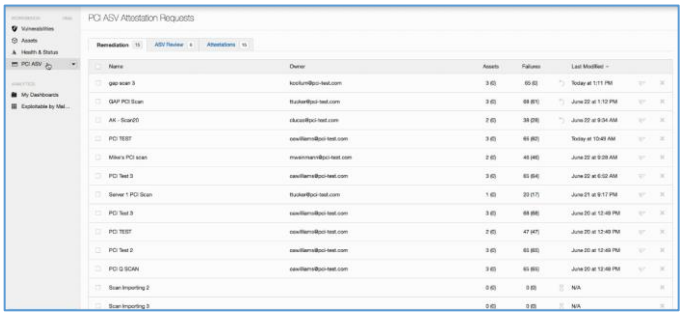


Quickly identify highest priority vulnerabilities

EXTERNAL VULNERABILITY SCANNING

PCI DSS 11.2.2 requires that an Approved Scanning Vendor (ASV) performs quarterly external vulnerability scans.

Tenable.io PCI ASV, an add-on to Tenable.io VM, streamlines the quarterly external vulnerability scan submission and dispute resolution process. With pre-configured scan templates and an efficient process, you can quickly run scans, submit attestation requests and resolve disputes.



Efficiently manage your quarterly PCI ASV scanning

KEY BENEFITS

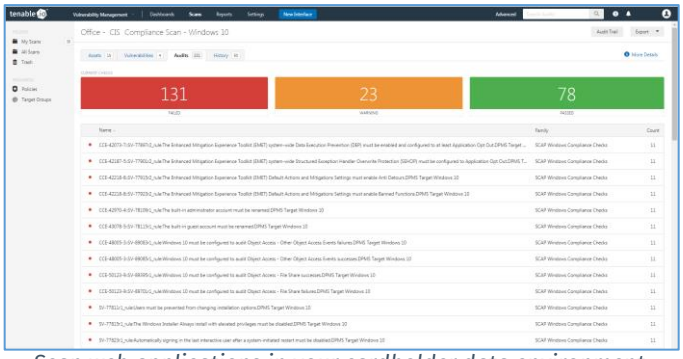
- ***Security, not just compliance -*** PCI compliance is critical, but realistically, it probably is not your entire job. More likely, it is only one of your many challenges. You have plenty of other servers, endpoints, and network devices to protect – not to mention cloud assets and possible operational technology assets. Tenable’s PCI solution is part of the Tenable.io cyber exposure platform that helps you secure all of your assets, including those in scope for PCI.
- ***Operations made easy -*** You need to focus on security, not on administering security tools. Tenable.io, a cloud-based solution, lightens your load. It is maintained by Tenable, and it comes with our 99.9% uptime Service Level Agreement.
- ***Future Growth -*** Do not get stuck at a dead end with a solution that won’t grow with you. Tenable.io supports modern assets, such as cloud, mobile, containers, and operational technology. It also will support your needs for scalability and integrating with your other security tools.

SOLUTION BRIEF

CONFIGURATION COMPLIANCE

PCI DSS 2.2 requires that you develop configuration standards for all system components. Cardholder Data Environment system components may include in-scope servers, endpoints, firewalls, routers, and databases. The configuration standards for Cardholder Data Environment components may be based on industry-accepted hardening standards, such as Center for Internet Security (CIS) benchmarks.

Tenable.io™ Vulnerability Management includes configuration audit policies for all popular versions of servers, endpoints, firewalls, routers, and databases so you can audit configuration standard compliance. For example, you can determine if anti-virus is installed and set to be active on boot, if only necessary services and protocols are enabled, and if all system clocks are using time-synchronization technology.

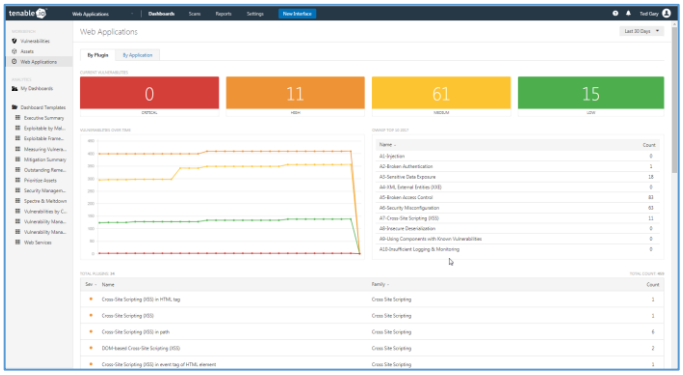


Scan web applications in your cardholder data environment

WEB APPLICATION SCANNING

If your cardholder data environment includes public-facing web applications, PCI DSS 6.6 requires you to address new threats and vulnerabilities to ensure these applications are protected against known attacks.

Tenable.io Web Application Scanning delivers safe and automated vulnerability scanning for your in-scope web applications. It helps you identify and address the specific vulnerability types included in Requirement 6.5 so you can rapidly assess your web applications without heavy manual effort. Tenable.io Web Application Scanning provides high detection rates with minimal false positives, ensuring you understand the true risks in your web applications.



Identify misconfigurations with compliance scans

TENABLE.IO – A MODERN VULNERABILITY PLATFORM

Built on the leading Nessus® technology, Tenable.io™ brings clarity to your security and compliance posture through a fresh, asset-based approach that accurately tracks your resources and vulnerabilities, while accommodating dynamic assets like cloud and containers. Tenable.io maximizes visibility and insight and effectively prioritizes your vulnerabilities, while seamlessly integrating into your environment.

The platform includes unlimited Nessus data sensors for active and agent-based scanning and passive traffic listening. In addition, Tenable.io includes an API and SDK for those who want to automate the sharing of Tenable.io capabilities and vulnerability data, or build on the Tenable.io platform. Built on the Tenable.io platform are a growing number of applications that solve today's toughest security challenges, including vulnerability management, container security and web application scanning – making it easy to start with one application and upgrade to others as requirements grow. This combination of applications, data sensors and automation provides maximum coverage and continuous visibility into assets and vulnerabilities – so you can take better-informed action to protect what matters most.

TRAINING

Tenable offers training for those who are new to using Tenable.io and want the knowledge and skills to maximize use of the product, as well as advanced topics for seasoned users. Courses are available on-demand via www.Tenable.com

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