| SOLUTION BRIEF

PCI Compliance

Make PCI compliance business-as-usual

Because payment card information is one of the most appealing targets for attackers, protecting payment card transactions and cardholder data (CHD) is crucial. The breach or theft of cardholder data affects the entire payment card ecosystem. Customers suddenly lose trust in merchants or financial institutions. Merchants and financial institutions lose credibility—and in turn business—and are also subject to numerous financial liabilities.

A Requirement, Not a Recommendation

The Payment Card Industry Data Security Standard (PCI DSS) provides organizations that process payment card data with a baseline standard of technical and operational security requirements that are designed to protect cardholder data from breaches and theft. The payment brands themselves require adherence to the PCI DSS standards for service providers and merchants, regardless of size.

PCI security standards impact virtually every company involved with credit card processing, including merchants, financial institutions, point-of-sale vendors, and hardware/software developers involved in processing payments.

It's About Good Security, Not Just Passing an Audit

Many companies take a minimalist approach to PCI by treating the process as a once-a-year project. However, major breaches have made companies take PCI and overall IT security more seriously.

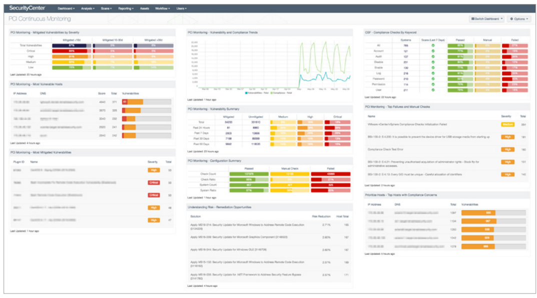
As many companies have discovered the hard way, taking a bare minimum approach to achieving a PCI-compliant status only demonstrates that an organization meets the requirements of PCI DSS at a given moment in time.

According to the 2016 Verizon Data Breach Investigations Report, when it comes to breach trends, "89% of breaches had a financial or espionage motive," and "the time to compromise is almost days or less, if not minutes or less." Organizations responsible for securing cardholder data must shift from the mindset of passing a point-in-time audit to year-round continuous compliance and effective security.

Continuously Assess PCI Compliance

The ability to continuously analyze and monitor both the systems and applications within your cardholder data environment (CDE), as well as the traffic going into and out of your CDE, is critical for protecting payment card data.

Tenable has a comprehensive security solution that provides the continuous visibility, critical context and actionable intelligence you need to monitor the technical controls that PCI requires, year-round. The continuous monitoring, centralized intelligence and purpose-built PCI compliance dashboards and Assurance Report Cards (ARCs) help Service Providers and Merchants monitor ongoing compliance with the PCI DSS.


SecurityCenter
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Users
PCI Continuous Monitoring
Switch Dashboard
Options
PCI Monitoring - Mitigated Vulnerabilities by Severity
PCI Monitoring - Vulnerability and Compliance Trends
CSF - Compliance Checks By Keyword
PCI Monitoring - Most Vulnerable Hosts
PCI Monitoring - Vulnerability Summary
PCI Monitoring - Top Failures and Manual Checks
PCI Monitoring - Most Mitigated Vulnerabilities
PCI Monitoring - Configuration Summary
Understanding Risk - Remediation Opportunities
Prioritize Hosts - Top Hosts with Compliance Concerns

Obtain visibility into the vulnerability and configuration status of your network by monitoring critical PCI DSS controls

SecurityCenter Continuous View™ (SecurityCenter CV™) covers more than 75% of PCI DSS technical controls, while satisfying both centralized logging and monitoring requirements (10.5-10.6) as well as internal scanning requirements (11.2).

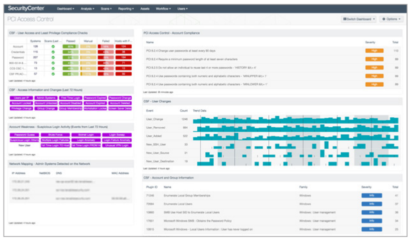
Proactively Monitor and Maintain Your PCI Compliance Posture with SecurityCenter Continuous View®

- **Broad coverage** - Continuous monitoring of more than 75% of PCI DSS technical controls provides a comprehensive, near real-time view into the status of your PCI DSS compliance posture.
- **Continuous visibility** - Unique combination of active scanning, agent scanning, intelligent connectors, continuous listening and host data monitoring help you quickly identify when you are drifting out of compliance so you can take immediate action.
- **Centralized view** - Identify threats and avoid data leakage by monitoring all devices within your cardholder data environment (CDE), including physical, virtual, mobile, and cloud, as well as traffic going into and out of the CDE.
- **Streamlined assessment** - Automated baseline creation, anomaly detection and continuous monitoring, as well as purpose-built PCI DSS Assurance Report Cards (ARCs), dashboards, and reports make it easy for you to track and efficiently manage your entire PCI DSS security program from a central location.

Automate Collection and Review of Host Activity Data

One of the biggest challenges with PCI compliance is meeting PCI DSS Requirement 10, which requires centralized logging and daily review of all access to cardholder data and other host activity from all in-scope systems.

SecurityCenter CV facilitates and automates daily host data collection and review by securely collecting, normalizing, aggregating and storing host data. It provides extensive host data reporting and analysis tools, and also can proactively monitor systems in the CDE to ensure that they are properly configured to capture host data.

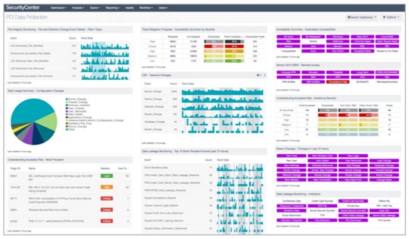


Monitor access control measures to ensure adherence to PCI requirements

SecurityCenter CV provides the capabilities needed to meet specific PCI logging and monitoring requirements as specified in Section 10 of the PCI DSS. For organizations that already have a SIEM, the logging and monitoring data collected by SecurityCenter CV can flow into the SIEM and the organization's incident response program.

Identify Threats to Card Data in Near Real Time

With SecurityCenter CV, identify point-of-sale malware, unauthorized access, and other malicious activities with near real-time monitoring and log review. Quickly detect the presence of malware or other unauthorized programs running in your environment.

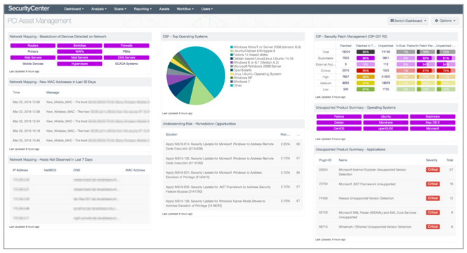


Assess compliance with PCI cardholder data protection requirements

Maintain Compliance Between Assessments

In order to effectively defend the organization from all threats – internal and external – security teams must implement PCI DSS security efforts into their "business-as-usual" activities. According to the Verizon 2015 PCI Compliance Report, of those companies that passed their annual assessment, 80 percent failed a subsequent interim assessment. This shows how quickly organizations drift out of compliance, and increasing the risk of a data breach due to the false sense of security that comes from having passed an annual assessment. PCI Compliance is a continuous evaluation process, not a once a year audit event.

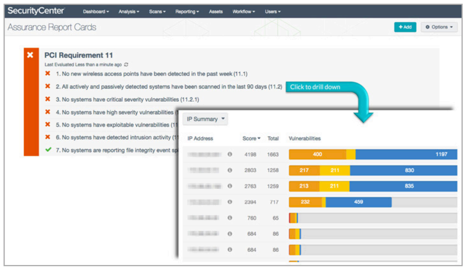
SecurityCenter CV centralized intelligence and monitoring helps you establish and maintain an ongoing PCI compliance posture over time, enabling you to monitor the effectiveness of your PCI compliance security processes and controls on an ongoing basis, and demonstrate that your organization adheres to the PCI DSS "business as usual" (BAU) standard (PCI DSS v3.1 standard, page 13) as a part of your overall security strategy.



Monitor "business as usual" security efforts in real-time

Measure PCI Compliance Program Effectiveness

Tenable PCI ARCs enable security teams to measure and communicate the status of their security program investments within the context of their PCI compliance program by using business terms IT security leaders and the business understand. Each ARC maps to one of the main PCI DSS requirements, so executives can quickly grasp the relationship between IT security team efforts, investments, policies and the organization's current PCI compliance posture.



Assurance Report Cards

PCI Requirement 11

Last Evaluated Less than a minute ago

✗ 1. No new wireless access points have been detected in the past week (11.1)

✗ 2. All actively and passively detected systems have been scanned in the last 90 days (11.2)

✗ 3. No systems have critical severity vulnerabilities (11.2.1)

✗ 4. No systems have high severity vulnerabilities

✗ 5. No systems have exploitable vulnerabilities (1

✗ 6. No systems have detected intrusion activity (1

✓ 7. No systems are reporting file integrity event sp

IP Address	Score	Total	Vulnerabilities
[redacted]	4198	1663	400 1197
[redacted]	2803	1258	217 211 830
[redacted]	2763	1259	213 211 835
[redacted]	2394	717	232 459
[redacted]	760	65	
[redacted]	684	86	
[redacted]	684	86	

ARCs provide snapshots of PCI security efforts using language business executives can understand

About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

tenable™

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