Runecast

How to ensure security compliance for PCI DSS

The Payment Card Industry Data Security Standard

BY KEV JOHNSON

Summary

What is PCI DSS?

- Who should be PCI DSS compliant?
- What are PCI DSS compliance requirements
- Twelve PCI DSS compliance requirements
- Major Pain Points
- The 3-Step Process

Simplify access, remediate & report

- Free up time & resources with automation
- How Runecast Analyzer can help
- PCI DSS Compliance checks in Runecast Analyzer
- A few facts about Runecast Analyzer

PCI Security Standards Council ®

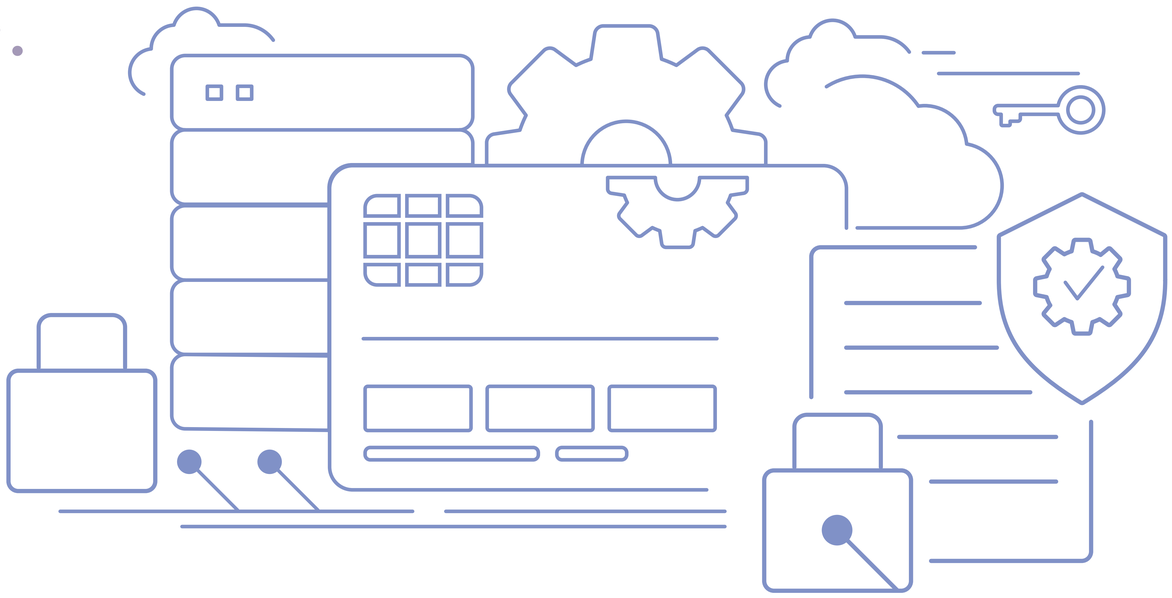
What is PCI DSS?

The **Payment Card Industry Data Security Standard** (PCI DSS) is an IT security standard for organizations that are involved in handling credit cards and their associated data. While administered by the Payment Card Industry Security Standards Council, the PCI Standard is mandated by the card brands, with the aim to tighten controls around cardholder data and reduce credit card fraud.

- **Guidelines for securely processing, storing, or transmitting payment card account data**
- **Maintained by the PCI Security Standards Council (PCI SSC)**
- **Established by leading payment card brands**

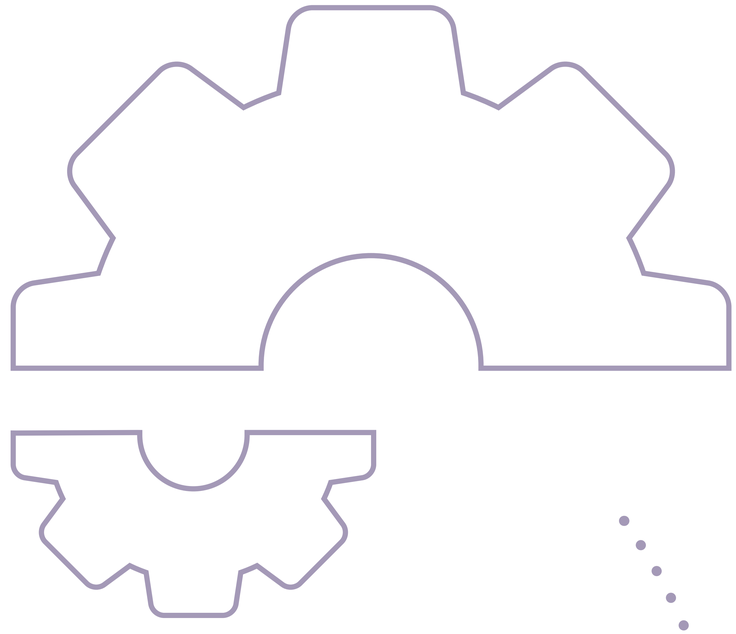
The PCI Security Standards Council is constantly working to monitor threats and improve the industry's means of dealing with them, through enhancements to PCI Security Standards and by the training of security professionals.

Who should be PCI DSS compliant?



The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

What are PCI DSS compliance requirements



For many IT departments – especially in the financial sector, greatly subject to PCI DSS regulations – security auditing and compliance are a continuous challenge due to the complexity of requirements.

PCI DSS comprises 12 compliance requirements for building and maintaining a secure network. Compliance validation occurs at regular intervals, performed by a certified assessor.

These 12 requirements are further broken down into additional groups known as control objectives, which cover a broad range of security processes for business continuity and consumer protection.

Twelve PCI DSS compliance requirements

Build and maintain a secure network	**1**	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	**3**	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**5**	Use and regularly update anti-virus software on all systems commonly affected by malware
	6	Develop and maintain secure systems and applications
Implement strong access control measures	**7**	Restrict access to cardholder data by business need-to-know
	8	Assign a unique ID to each person with computer access
	9	Restrict physical access to cardholder data
Regularly monitor and test networks	**10**	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an information security policy	**12**	Maintain a policy that addresses information security

Major Pain Points

One of the biggest challenges with PCI DSS is that security controls and their requirements do not specify any concrete capabilities and features of the associated products or services. Controls can seem vague and there is not much (if any) guidance on how to map a specific security control and requirement. For example, you need to make sure that you have encryption or firewall enabled and map that to a specific capability of your systems.

The 3-Step Process

3

Assess.

Identify cardholder data, take an inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities.

Remediate.

Fix vulnerabilities and eliminate the storage of cardholder data unless absolutely necessary.

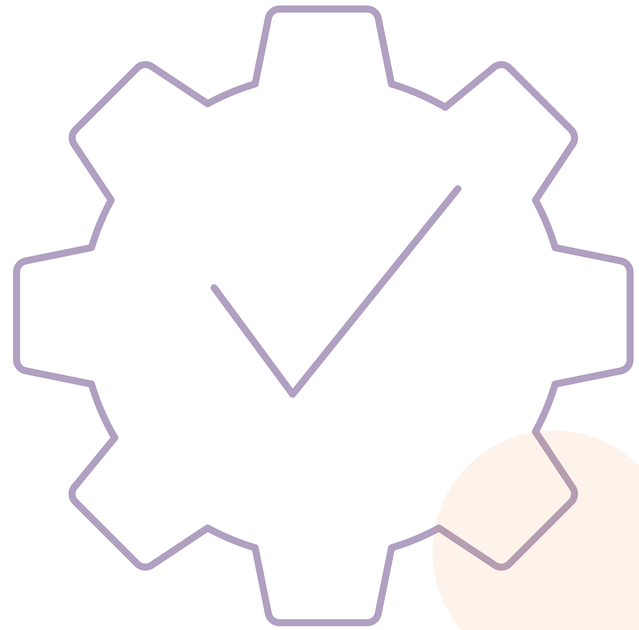
Report.

Compile and submit required reports to the appropriate acquiring bank and card brands.

Simplify access, remediate & report via automation (1/2)

Requirements for automated PCI DSS compliance

- Identification of non-compliances and vulnerabilities.
- Capability to customize checks where business risk posture requires higher standards than the baseline requirements.
- Coverage of both on-premises and cloud- based services.
- Continuous monitoring for PCI-DSS violations.
- Address Control ID and Milestone aspects of the standard.
- Provide historical analysis, with full reporting capabilities.
- Provide automation for remediation against PCI DSS controls.

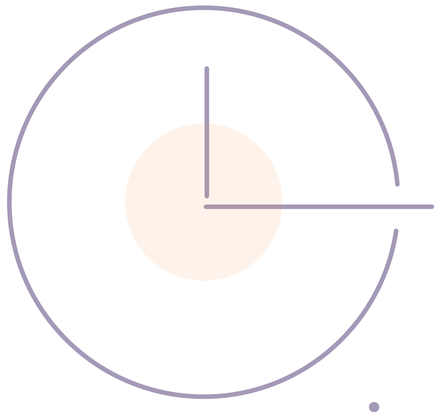


Simplify access, remediate & report via automation (2/2)

Requirements for automated PCI DSS compliance

- Coverage of vulnerability management and risk assessment.
- Support for the most up-to-date revision of the standard (3.2.1, released May, 2018).
- View specific and full content from the relevant control and context from the relevant requirement area for all non-compliance checks.
- Prioritize remediation actions according to PCI DSS security milestones.
- Provide a fully-justified view on how a specific automated check relates to a specific control in the standard, and (where applicable) where it relates to certain sub-sections of the control.
- Detailed technical descriptions that map the PCI standard to specific environments, including details for manual auditing and remediation.

Free up your time & resources with automation

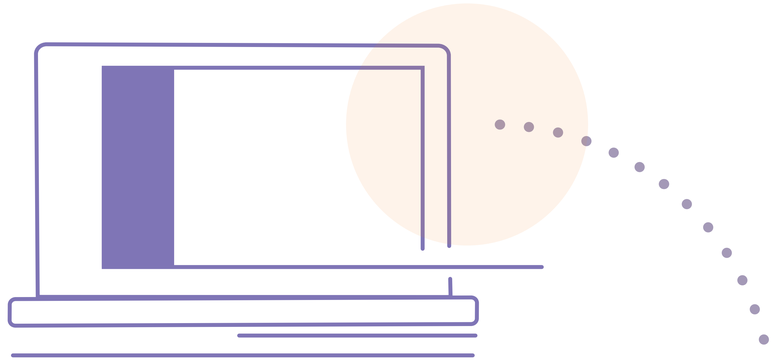


Stay on top of the latest security standards and best practices in the rapidly evolving environment (with no additional time investment for busy IT teams like yours).

Ensure excellent security compliance with the current size of your IT teams
Security audits are becoming increasingly frequent, your team doesn't need to reinvent the wheel before every single one of them. Rather build up on previous great work and spend time on more meaningful projects.

Failing an audit is not an option. Don't let the challenge of compliance eat your IT budget!

How Runecast Analyzer can help



Runecast Analyzer automates the process of checking VMware vSphere and NSX, as well as AWS native public cloud services for **compliance against PCI-DSS standards** – in total over 240 checks. Findings are mapped to each specific PCI-DSS issue ID, with each finding mapped back to the affected objects, giving you details on how to manually audit and remediate any non-compliances.

With Runecast Analyzer, you get year-round, **24/7 visibility into your audit compliance** posture. It allows you to get immediate visibility into risks and non-compliances inherent in your environment, allowing you to identify gaps between where you are and a fully compliant state, and also show as soon as any objects move out of compliance.

Runecast Analyzer **runs wherever you want to run it** - on AWS, Azure, Kubernetes or vSphere. More importantly, it keeps all of your data fully under your control, with no data sent to any third-party cloud services.

PCI DSS Compliance checks in Runecast Analyzer

The requirements and controls cited in the Runecast Analyzer profile are taken from the latest PCI DSS v3.2.1 (May 2018).

Runecast Analyzer uses the “Prioritized Approach” by which six security milestones are displayed that help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance.

The PCI DSS “Prioritized Approach” Milestones in Runecast Analyzer range from 1-6, with 1 being the highest priority and 6 being the lowest:

1 – Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised.	**4** – Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning and who is accessing your network and cardholder data environment.
2 – Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromises – the network or a wireless access point.	**5** – Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protections mechanisms for that stored data.
3 – Secure payment card applications. This milestone targets controls for applications, application processes, and application servers.	**6** – Finalize remaining compliance efforts and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

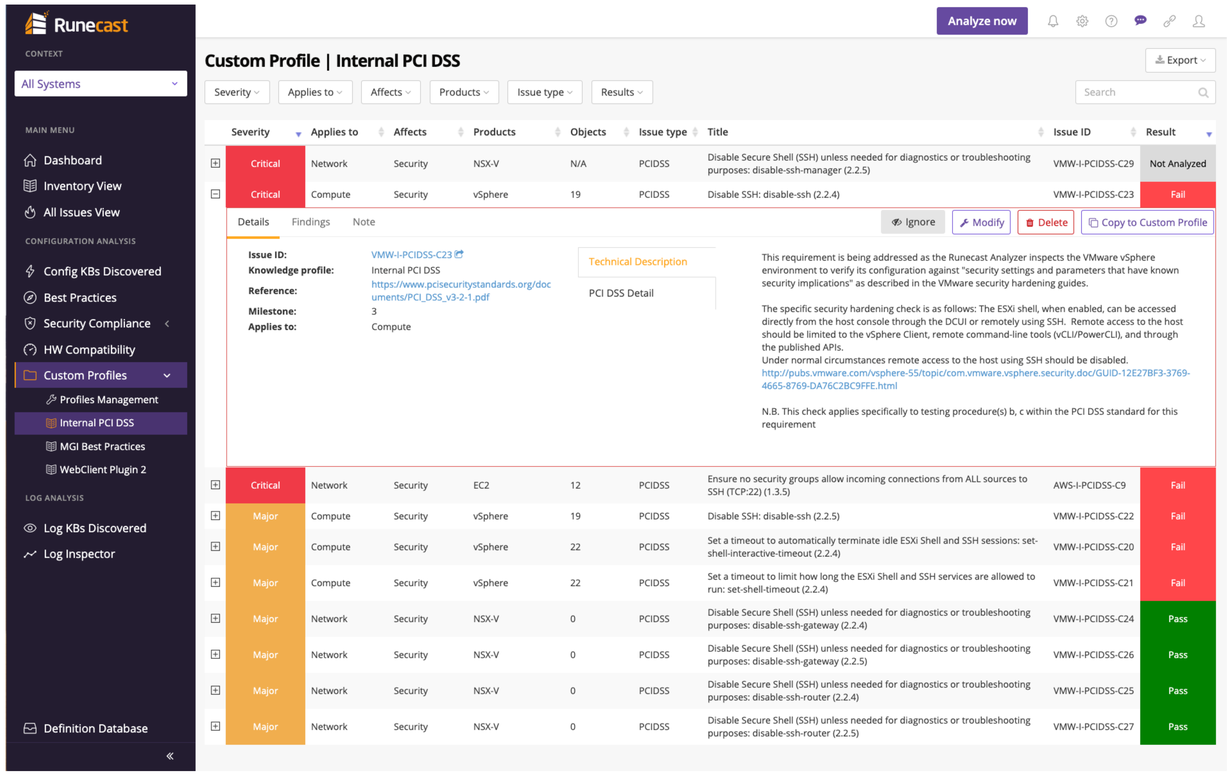
Every security check in Runecast Analyzer can either return a result of **Fail** or **Pass**. In cases where there is at least one object in your infrastructure that is not compliant with a specific security check, this check will be marked as **Fail**. A result of **Pass** means there are no objects failing for the specific check, but note that this does not mean you are fully compliant against the whole PCI DSS requirement or control.

Results of the PCI DSS compliance check are organized by severity: *Low, Medium, Major, Critical.*

Regardless of the original severity, some security rules may not be required for your organization's interpretation of the security policy. In Runecast Analyzer you can customize the displayed security checks by filtering those that are not required.

PCI DSS checks contain two types of rules (Customizable and Non-customizable). The main difference between them is that Customizable rules allow the user to change the parameters default values, used by the checks, to the desired ones.

Additional PCI DSS reports are available under the Export button. The Consolidated host report is offering a better overview of all the PCI DSS rules failed or passed for each vCenter, on Cluster and ESXI level.

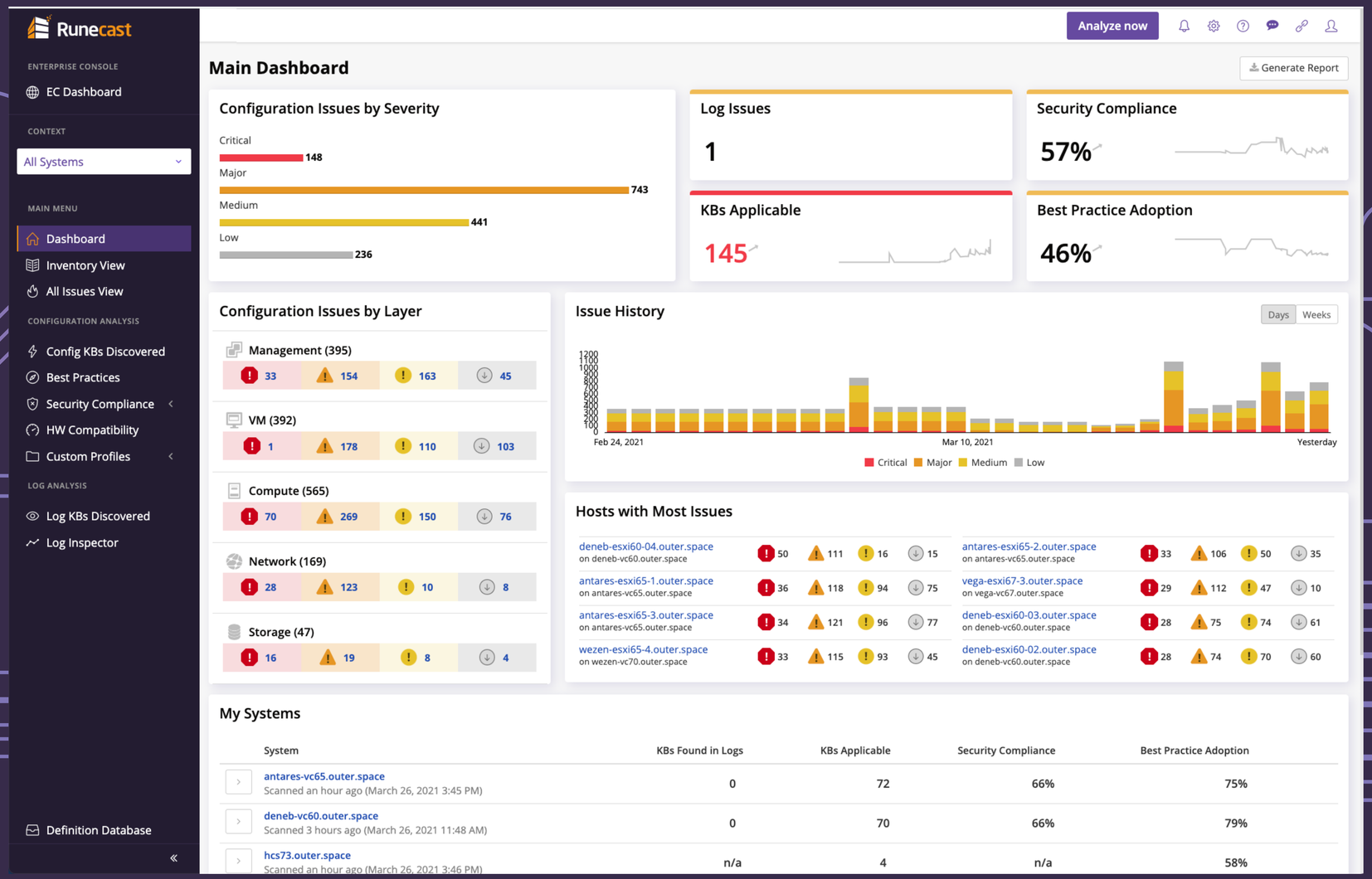


Optimize and Secure Your Hybrid Cloud

Gartner
COOL VENDOR 2020

A few facts about Runecast Analyzer

- Runecast Analyzer scans your environment on a user-defined schedule.
- If an issue is detected, you will be provided with resolution steps.
- Works securely on-premises
- Compliant with HIPAA, PCI DSS, STIG, NIST, CIS, and more.
- Updates weekly with the latest version of VMware's KB. For critical issues, Runecast releases updates within a few hours.
- Reduce delays in solving issues by up to 80%.
- Provides full visibility on first analysis, with actionable results in minutes



Companies who benefit from Runecast intelligence

SCANIA verizon Swedbank NYC HEALTH+ HOSPITALS avast Chevron

Discover all potential issues now!

Start your 14 day Runecast Analyzer free trial.

Get Runecast Analyzer for my environment

Want a quick product intro with our team?
Let us know at **roi@runecast.com.**

Runecast