

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
- A few facts about Runecast Analyzer





• PCI DSS Compliance checks in Runecast Analyzer





where the second $\mathsf{P}(\mathsf{I}|\mathsf{D}\mathsf{S}\mathsf{S}\mathsf{Z})$



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.

- payment card account data
- 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.



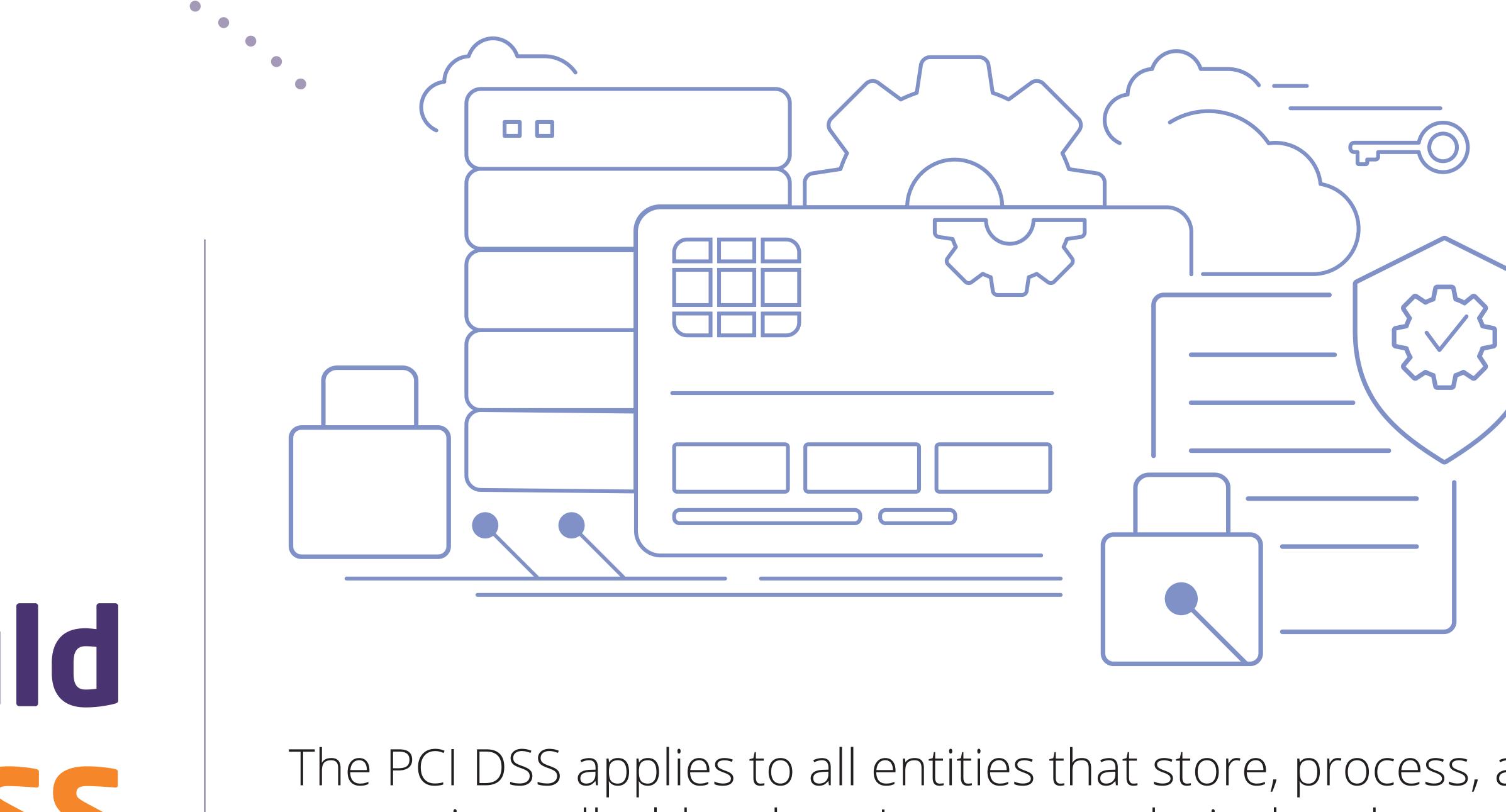
Guidelines for securely processing, storing, or transmitting

Maintained by the PCI Security Standards Council (PCI SSC)



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.

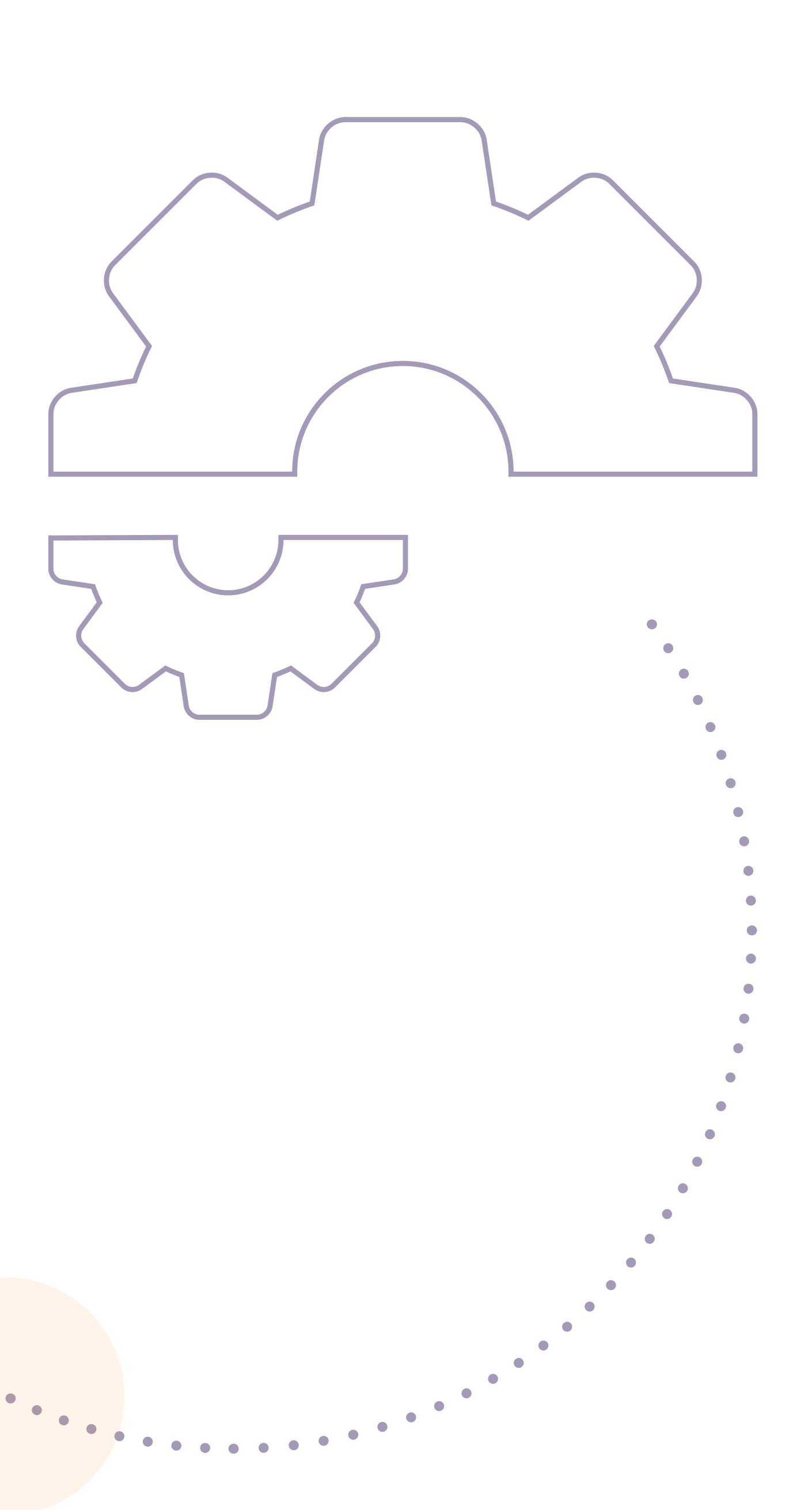
PCI DSS comprises 12 compliance requirements for building and maintaining a secure network. Compliance validation occurs at regular intervals, performed by a certified assessor.

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



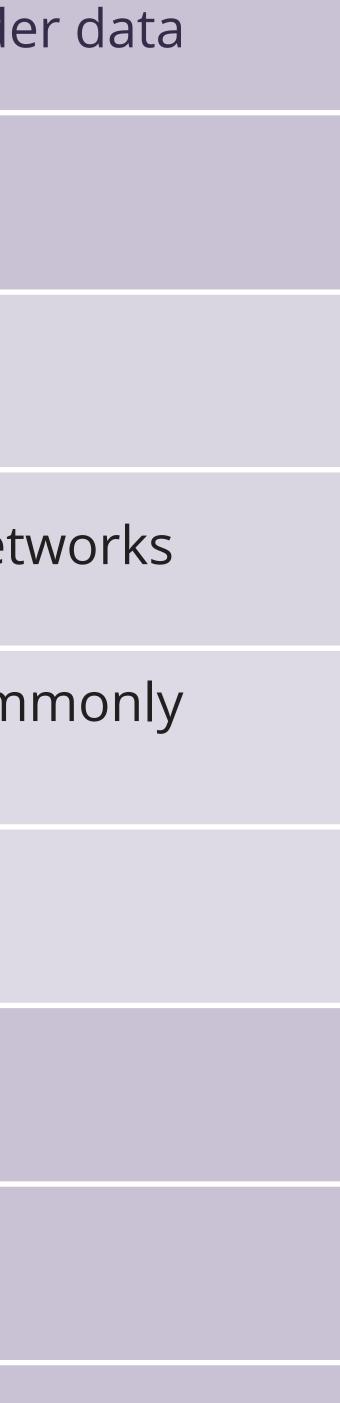


Runecast What is PCI DSS?

	1	Install and mai
n a secure network	2	Do not use ven and other secu
ect cardholder data	3	Protect stored
cu carunoiuer uata	4	Encrypt transm
a a como o te ma como	5	Use and regula affected by ma
nagement program	6	Develop and m
	7	Restrict access
s control measures	8	Assign a unique
	9	Restrict physica
	10	Track and mon
and test networks	11	Regularly test s
tion security policy	12	Maintain a poli



- intain a firewall configuration to protect cardholder data
- ndor-supplied defaults for system passwords urity parameters
- cardholder data
- nission of cardholder data across open, public networks
- arly update anti-virus software on all systems commonly alware
- naintain secure systems and applications
- to cardholder data by business need-to-know
- IN ID to each person with computer access
- cal access to cardholder data
- nitor all access to network resources and cardholder data
- security systems and processes
- licy that addresses information security



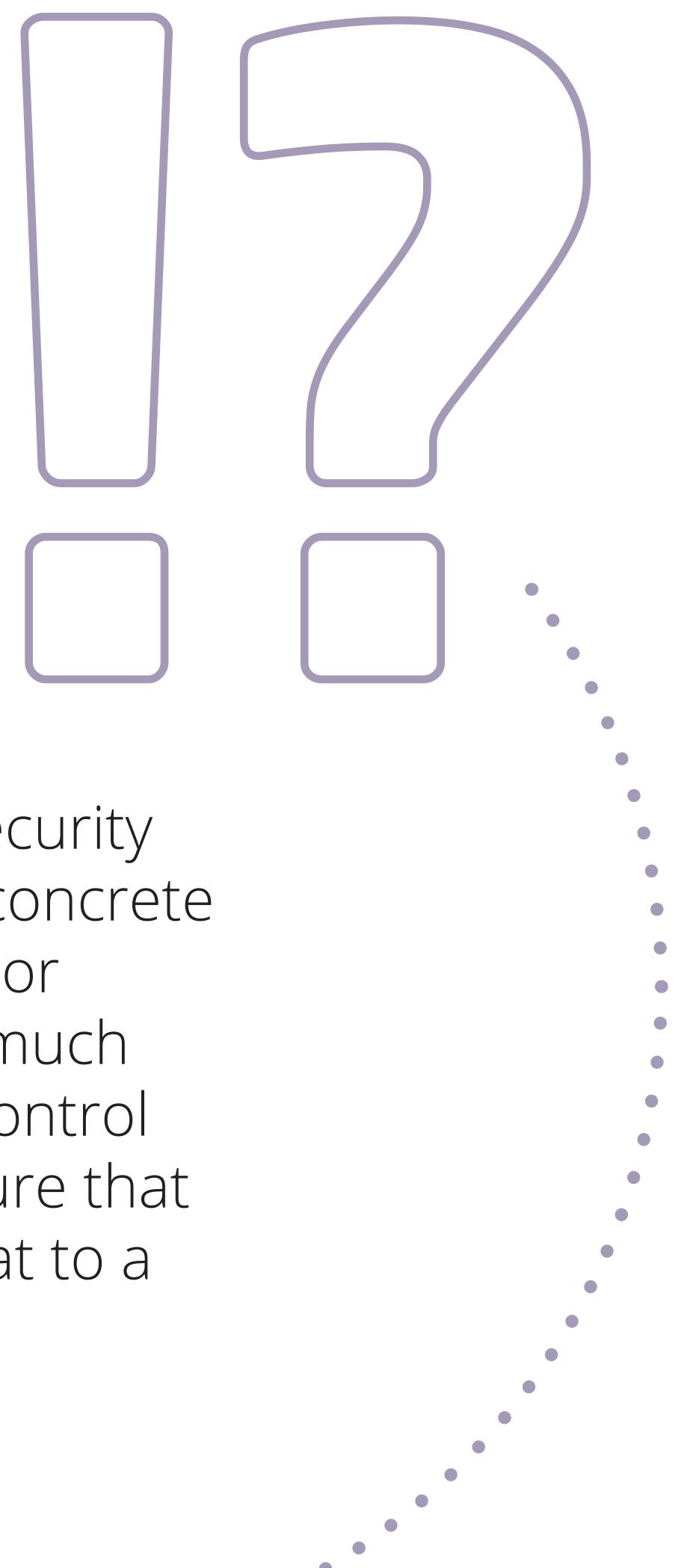


Pain Points



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 B-Step Process



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



Runecast What is PCI DSS?

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.

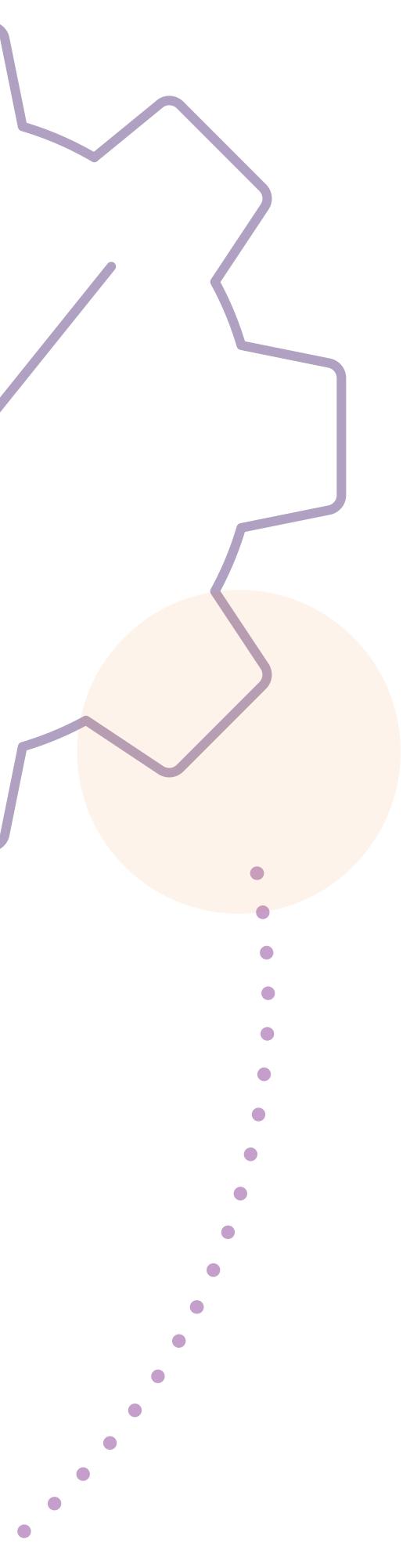
Continuous monitoring for PCI-DSS violations.

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







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.



What is PCI DSS?

Coverage of vulnerability management and risk assessment.

Support for the most up-to-date revision of the standard (3.2.1, released May, 2018).



Free up your time & resources with automation

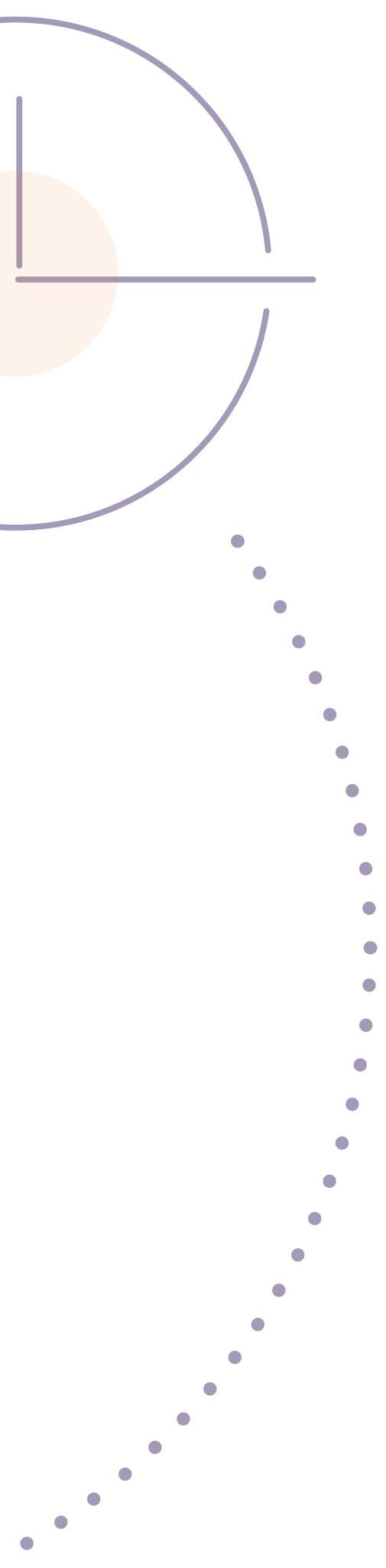
Stay on top of the latest security standards and best practices in the rapidly evolving environment (with no additional time investment for busy IT teams like yours).

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.

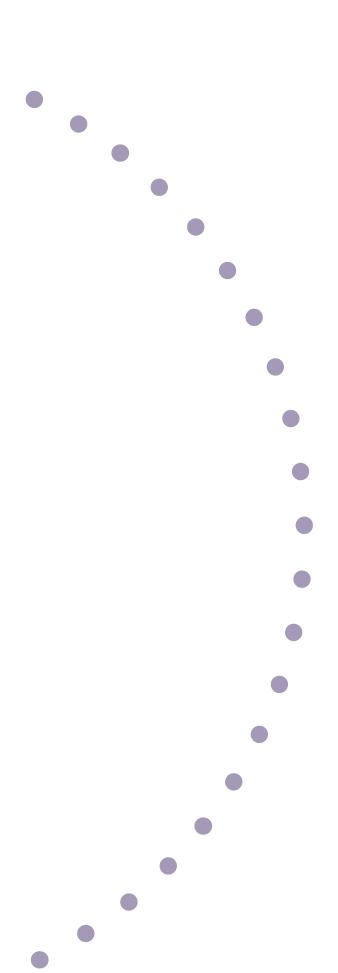
With Runecast Analyzer, you get year-round, **24/7 visibility into your audit** compliance posture. It allows you to get immediate visibility into risks and noncompliances inherent in your environment, allowing you to identify gaps between where you are and a fully compliant state, and also show as soon 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 This milestone targets a key area of r compromised.

2 – Protect the perimeter, internal, ar milestone targets controls for points - the network or a wireless access pc

3 – Secure payment card applications for applications, application processe



What is PCI DSS?

data and limit data retention. risk for entities that have been	4 – Monitor milestone a concerning environmer
nd wireless networks. This s of access to most compromises oint.	5 – Protect s have analyz must store protections
s. This milestone targets controls es, and application servers.	6 – Finalize are in place requiremen and process



r and control access to your systems. Controls for this allow you to detect the who, what, when, and how and who is accessing your network and cardholder data

stored cardholder data. For those organizations that zed their business processes and determined that they Primary Account Numbers, Milestone Five targets key mechanisms for that stored data.

remaining compliance efforts and ensure all controls The intent of Milestone Six is to complete PCI DSS nts and finalize all remaining related policies, procedures, ses 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.

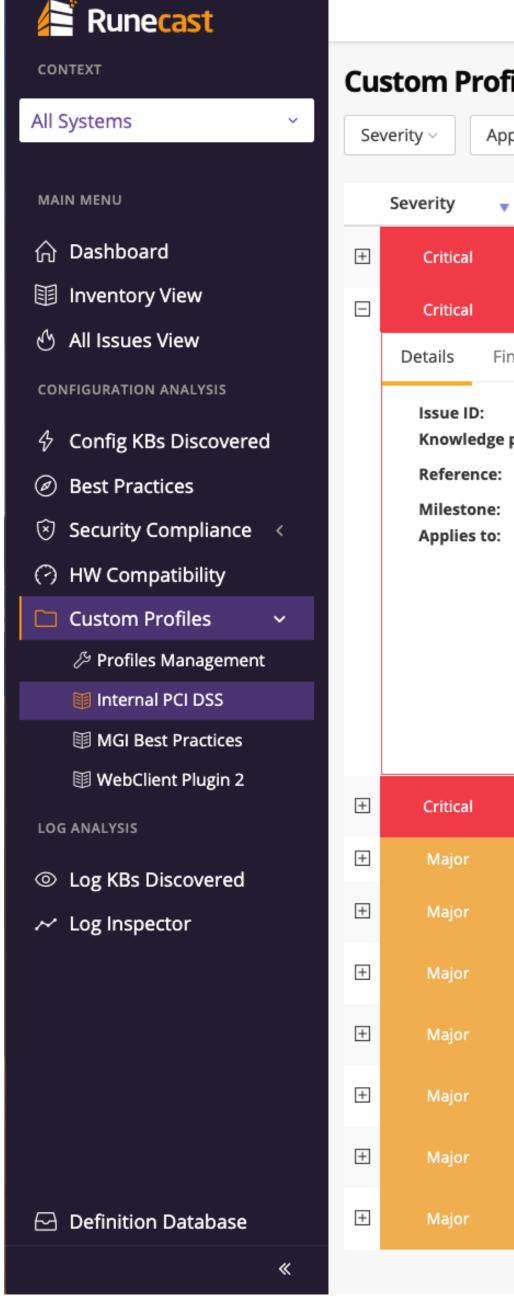
Regardless of the original severity, some security rules may not be required for your organization's interpretation of the security policy. In Runecast Analyzer you can customize the displayed security checks by filtering those that are not required.

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.



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





ile Inte	ernal PCI DS	S								📥 Export
plies to \vee	Affects ~ Pro	oducts ~ Issue typ	e ~ Re	esults ~					Search	(
Applies to	Affects	Products	Objects	🔶 Issue type 🌲	Title			🕴 Issue	e ID 🍦	Result
Network	Security	NSX-V	N/A	PCIDSS	Disable Secure Shell (SSH) unless needed fo purposes: disable-ssh-manager (2.2.5)	or diagnostics	or troubleshoot	ting VMW	-I-PCIDSS-C29	Not Analyze
Compute	Security	vSphere	19	PCIDSS	Disable SSH: disable-ssh (2.2.4)			VMW	-I-PCIDSS-C23	Fail
ndings No	ote					ø Ignore	🗲 Modify	🛍 Delete	🗇 Copy to	Custom Profi
profile:	VMW-I-PCIDSS-C23 Internal PCI DSS https://www.pcised uments/PCI_DSS_v 3 Compute	curitystandards.org/doc		nical Description	This requirement is being add environment to verify its config security implications" as descr The specific security hardening directly from the host console	guration again ribed in the VM g check is as fo	st "security sett ware security h lows: The ESXi	ings and para ardening guid shell, when er	meters that ha les. nabled, can be	ave known accessed
	compute				should be limited to the vSphe the published APIs. Under normal circumstances r http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specific requirement	remote access nere-55/topic/c ml	to the host usir om.vmware.vsp	ng SSH should ohere.security.	be disabled. .doc/GUID-12E	27BF3-3769-
Network	Security	EC2	12	PCIDSS	should be limited to the vSphe the published APIs. Under normal circumstances r http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specific	remote access here-55/topic/c ml cally to testing	to the host usir om.vmware.vsp procedure(s) b,	ng SSH should ohere.security. , c within the P	be disabled. .doc/GUID-12E	27BF3-3769-
Network Compute		EC2 vSphere	12 19	PCIDSS PCIDSS	should be limited to the vSphe the published APIs. Under normal circumstances r http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specific requirement	remote access here-55/topic/c ml cally to testing	to the host usir om.vmware.vsp procedure(s) b,	to AWS-	be disabled. .doc/GUID-12E2	27BF3-3769-
	Security				should be limited to the vSphe the published APIs. Under normal circumstances r http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specific requirement Ensure no security groups allow incoming of SSH (TCP:22) (1.3.5)	remote access here-55/topic/c ml cally to testing	to the host usir om.vmware.vsp procedure(s) b,	to AWS- VMW	be disabled. doc/GUID-12E2 PCI DSS standar	27BF3-3769- rd for this Fail
Compute	Security	vSphere	19	PCIDSS	should be limited to the vSpher the published APIs. Under normal circumstances r http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specific requirement Ensure no security groups allow incoming of SSH (TCP:22) (1.3.5) Disable SSH: disable-ssh (2.2.5) Set a timeout to automatically terminate id	remote access here-55/topic/c ml cally to testing connections fro	to the host usir om.vmware.vsp procedure(s) b, om ALL sources	to AWS- vMW	be disabled. doc/GUID-12E2 PCI DSS standar	27BF3-3769- rd for this Fail Fail
Compute Compute	Security Security Security	vSphere vSphere	19 22	PCIDSS	 should be limited to the vSphere the published APIs. Under normal circumstances in http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specified requirement Ensure no security groups allow incoming of SSH (TCP:22) (1.3.5) Disable SSH: disable-ssh (2.2.5) Set a timeout to automatically terminate id shell-interactive-timeout (2.2.4) Set a timeout to limit how long the ESXi Shere 	remote access here-55/topic/c ml cally to testing connections fro lle ESXi Shell ar ell and SSH ser	to the host usir om.vmware.vsp procedure(s) b, om ALL sources nd SSH sessions	to AWS- vMW stoet to VMW	be disabled. doc/GUID-12E2 PCI DSS standar I-PCIDSS-C9 -I-PCIDSS-C22	27BF3-3769- rd for this Fail Fail Fail
Compute Compute Compute	Security Security Security Security	vSphere vSphere vSphere	19 22 22	PCIDSS PCIDSS PCIDSS	 should be limited to the vSphere the published APIs. Under normal circumstances in http://pubs.vmware.com/vsph 4665-8769-DA76C2BC9FFE.htm N.B. This check applies specified requirement Ensure no security groups allow incoming of SSH (TCP:22) (1.3.5) Disable SSH: disable-ssh (2.2.5) Set a timeout to automatically terminate id shell-interactive-timeout (2.2.4) Set a timeout to limit how long the ESXi Sherun: set-shell-timeout (2.2.4) Disable Secure Shell (SSH) unless needed for the secure Shell (SSH) (SSH)	remote access here-55/topic/c ml cally to testing connections fro lle ESXi Shell ar ell and SSH ser or diagnostics	to the host usir om.vmware.vsp procedure(s) b, om ALL sources nd SSH sessions vices are allowe or troubleshoot	to AWS- vmw ed to vmw	be disabled. doc/GUID-12E2 PCI DSS standar I-PCIDSS-C9 -I-PCIDSS-C20 -I-PCIDSS-C21	27BF3-3769- rd for this Fail Fail Fail Fail
Compute Compute Compute Network	Security Security Security Security Security	vSphere vSphere vSphere NSX-V	19 22 22 0	PCIDSS PCIDSS PCIDSS PCIDSS	 should be limited to the vSphere the published APIs. Under normal circumstances re http://pubs.vmware.com/vsphe/4665-8769-DA76C2BC9FFE.htm N.B. This check applies specified requirement Ensure no security groups allow incoming of SSH (TCP:22) (1.3.5) Disable SSH: disable-ssh (2.2.5) Set a timeout to automatically terminate id shell-interactive-timeout (2.2.4) Set a timeout to limit how long the ESXi Sherun: set-shell-timeout (2.2.4) Disable Secure Shell (SSH) unless needed for purposes: disable-ssh-gateway (2.2.4) Disable Secure Shell (SSH) unless needed for purposes: disable-ssh-gateway (2.2.4) 	remote access here-55/topic/c ml cally to testing connections fro lle ESXi Shell ar ell and SSH ser or diagnostics or diagnostics	to the host usir om.vmware.vsp procedure(s) b, om ALL sources nd SSH sessions vices are allowe or troubleshoot	ang SSH should ohere.security. c within the P to AWS- VMW cod to VMW ting VMW	be disabled. doc/GUID-12E2 CI DSS standar I-PCIDSS-C9 -I-PCIDSS-C20 -I-PCIDSS-C21 -I-PCIDSS-C21	27BF3-3769- rd for this Fail Fail Fail Fail Pass Pass





Optimize and Secure Your Hybrid Cloud

Gartner

COOL VENDOR 2020



A few facts about Runecast Analyzer

- Works securely on-premises
- Runecast releases updates within a few hours.
- Reduce delays in solving issues by up to 80%.





• Runecast Analyzer scans your environment on a user-defined schedule. If an issue is detected, you will be provided with resolution steps.

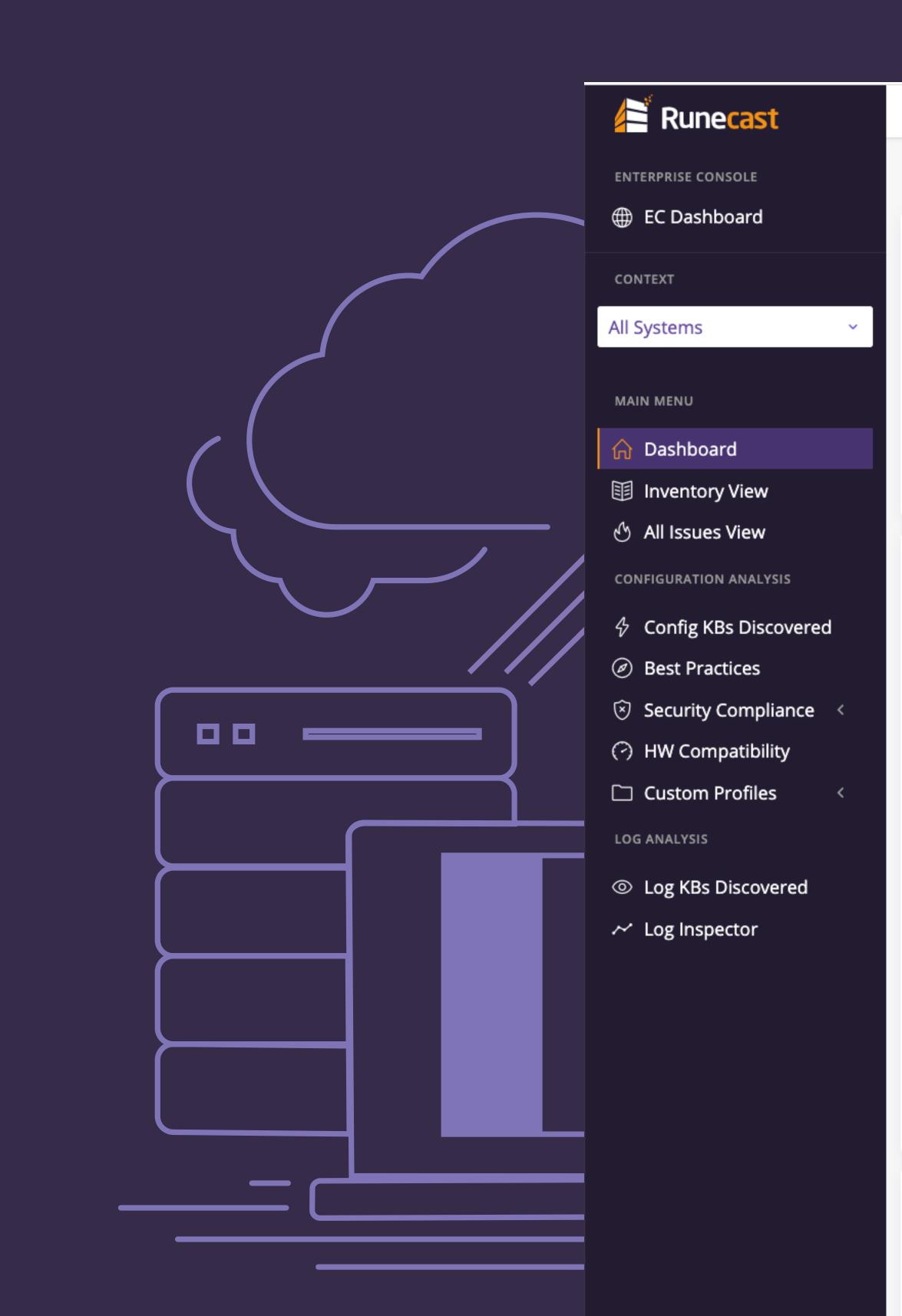
Compliant with HIPAA, PCI DSS, STIG, NIST, CIS, and more.

• Updates weekly with the latest version of VMware's KB. For critical issues,

• Provides full visibility on first analysis, with actionable results in minutes



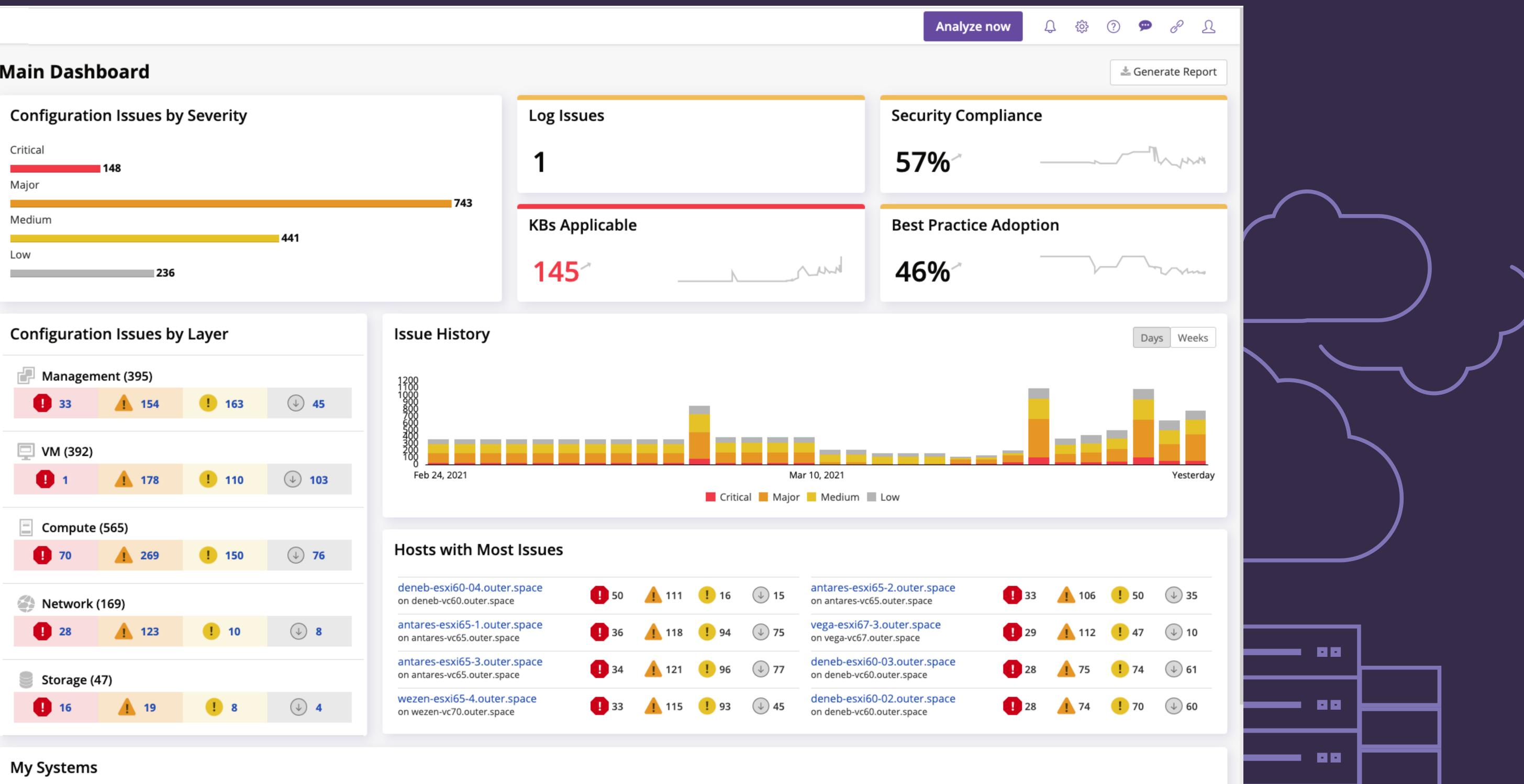
14

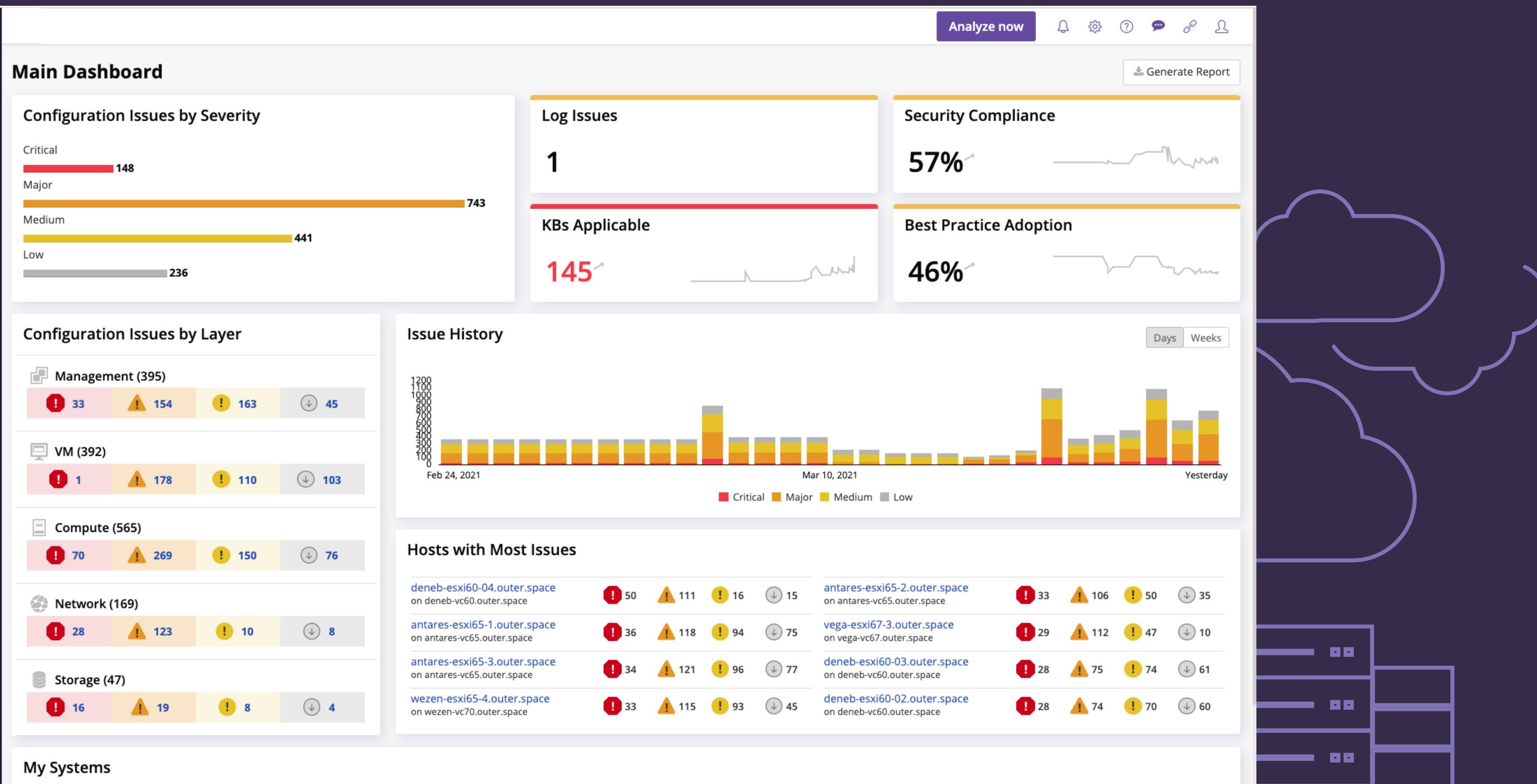


🖂 Definition Database









Network (169)		deneb-esxi60-04.outer.space on deneb-vc60.outer.space	! 50	111	! 16	J 15	antares-esxi65-2.outer.space on antares-vc65.outer.space	! 33	106	. 50	4 35
! 28 ! 123 ! 10	⇒ 8	antares-esxi65-1.outer.space on antares-vc65.outer.space	936	118	94	4 75	vega-esxi67-3.outer.space on vega-vc67.outer.space	! 29	112	. 47	↓ 10
Storage (47)		antares-esxi65-3.outer.space on antares-vc65.outer.space	! 34	121	96	17	deneb-esxi60-03.outer.space on deneb-vc60.outer.space	! 28	75	! 74	 ↓ 61
! 16 ! 8	↓ 4	wezen-esxi65-4.outer.space on wezen-vc70.outer.space	! 33	115	93	45	deneb-esxi60-02.outer.space on deneb-vc60.outer.space	! 28	1 74	. 70	(↓ 60
ly Systems											
System		KBs Found in Logs		KBs Ap	plicable		Security Compliance	Best Pra	ctice Adopt	ion	
	PM)	KBs Found in Logs		KBs Ap	plicable 72		Security Compliance 66%	Best Pra		ion 5%	
System				KBs Ap				Best Pra	7		

Companies who benefit from Runecast intelligence











- 88







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.