rubrik

Stay Ready for PCI DSS with Sensitive Data Monitoring

Reduce Sensitive Data Exposure. Automate Consistent Processes with Policy-driven Simplicity.

Credit card fraud costs the payment card industry billions of dollars per year. The Payment Card Industry Data Security Standard (PCI DSS) was created to provide organizations that deal with credit cards with a standardized set of guidelines, controls, and best practices to defend against the threat. Failure to adhere to the PCI DSS can result in repeated monthly penalties[1], increased transaction fees, and loss of the ability to accept credit card payments.

To comply with PCI DSS, organizations must establish a policy, build and maintain a secure environment, and routinely undergo compliance audits. As well-meaning as PCI DSS compliance is intended to be, auditing and maintaining compliance is time consuming.

Implementing integrity controls can be technically challenging and auditing data can be quite daunting. Rubrik makes this simple. Sensitive Data Monitoring, a SaaS application, automates visibility into where regulated content is stored with data classification without any impact to production environments. The Rubrik Security Cloud platform already protects the data, Sensitive Data Monitoring gives visibility into that data.

ENHANCE VISIBILITY/ REVIEW ANYWHERE

On-prem or in the cloud. Protect and analyze.

SECURE CARDHOLDER DATA

Continuous scanning finds exposed data before a criminal does.

HELP PREPARE FOR AUDITS

Don’t get ready for audits. Stay ready for them.

MEET SENSITIVE DATA MONITORING: CLASSIFICATION TO HELP WITH PCI DSS

To begin using Sensitive Data Monitoring for PCI DSS automation, all a Rubrik customer has to do is turn it on and select a predefined template or customize one. Sensitive Data Monitoring begins to scan the Rubrik protected data in the background and flags matches for non-compliant data. Since production workloads are already being protected, the data to be analyzed exists within the Rubrik repository. Sensitive Data Monitoring sweeps through protected environments searching for defined patterns whether the data is on-premises, in a remote office, or in the cloud. This means no agents to install, no heavy scans on production workloads, and most importantly no heavy lifting for the IT staff. Sensitive Data Monitoring delivers automation of policy management and very fast time to value, and it keeps running in the background without constant intervention, upgrades, or hardware refreshes.

STREAMLINE SCANNING AND MONITORING

PCI DSS uses a layered approach of policy and control. Establishing a policy is always the first step in any information security effort, and enforcing and monitoring it is integral. Requirement 3.4, for instance, calls for an examination of removable media or secondary copies (like backup data) to be performed in order to validate that the encryption controls on the primary copies have been implemented. This is precisely how Sensitive Data Monitoring works. Rather than scanning production systems, Sensitive Data Monitoring examines the data in the Rubrik platform to identify and highlight patterns that match the defined policy.

[1] https://www.pcisecuritystandards.org/pci_security/why_security_matters

USE CASES

Enhance Visibility/Review Anywhere

Anywhere that cardholder data is stored is a location that must be secured, monitored, and reviewed, whether the data is on-premises or in the cloud. Stored data that is readable is a violation of DSS 3.4 through 3.4.1, but unless you are looking, you won't know about it. Sensitive Data Monitoring finds misplaced data or data that is copied temporarily to an accessible location and then forgotten about. If data is stored on servers or locations outside of defined secure zones, then Sensitive Data Monitoring will alert on policy deviations automatically based on the policies set.

Protect Against Blind Spots

Nothing invites an audit as quickly as a breach disclosure. This unexpected audit then introduces an unknown risk that something completely unrelated might be found. Investigators may very well clear the organization of any wrongdoing on the part of the breach, but then go on to find several previously unknown areas that do result in fines. The risk from unknown threats is reduced with Sensitive Data Monitoring since it scans in the background, analyzes the data and can find problem areas before they turn into trouble.

Continuously Assess the Security of Cardholder Data

Running vulnerability scans of systems is covered under DSS 11.2, but what if data is accidentally exposed or left unencrypted. Encryption is required under PCI DSS 3.5, and if source data is left unmasked and unencrypted in a defined zone then Sensitive Data Monitoring will find it automatically.

Remediate from Ransomware Attacks

DSS requirements 5 and 6 relate to vulnerability management and the need to protect against malware and ransomware. Data protected by Rubrik is stored in an immutable format which means you never have to worry about ransomware accessing and encrypting backups. Rubrik Anomaly Detection detects anomalous behavior and provides a workflow recovery that takes the guesswork out of remediating an attack. The Rubrik solutions for data governance enables continuous protection and rapid one-click recovery of workloads to get the facility back on its feet, meeting the requirement to have an adequate response to mitigate the effects of an attack in the event of an incident.

Reduce Disruption from Audits

Let's face it, audits are productivity killers. Time spent preparing for an audit is a pure waste of the IT team's effort. Weeks worth of resources spent scanning and preparing would be better spent on something more productive. When the QSA arrives, they will expect that everything is prepared and in place. Documented procedures for security as well as breach response are expected. Having Sensitive Data Monitoring background scan results available to serve as supporting evidence for the QSA demonstrates technical support for those policies.

Empower the Infrastructure & Operations Team

With Rubrik Security Cloud, your I&O team has the tools to regularly check for policy violations and remediate them on a more regular basis without the intrusiveness of scanning production systems and without the need for indexing. Rather than reactionary fire drills, they can set and forget, and if they need to introduce a new search pattern to the scans, it is easy to do.

Breach Response Plan in Place

Having a response plan for breaches is a requirement and being able to demonstrate and document that no negligence occurred is not simply a nice to have. Having the locations where cardholder data is stored and being prepared to run searches to investigate other locations will be part of the overall team effort during response. With Rubrik's ability to search data managed by Rubrik Cluster, you can quickly identify repositories of unencrypted cardholder data.

PCI DSS v4.0 Released: Managing Compliance Requirements

The PCI DSS has evolved since its initial release. Comments from the industry were incorporated, and PCI DSS v4.0 was finally released in 2022. Managing compliance requirements is an ongoing process, and having oversight of the entire environment is a key part of this effort. The 12 core requirements have not fundamentally changed, but additional guidance has been provided to promote security as a continuous process and to support additional methodologies to achieve security. Rubrik Sensitive Data Monitoring can help you manage your sensitive data exposure risk, thus staying compliant with the latest PCI-DSS v4.0 requirements.

WHAT OUR CUSTOMERS ARE SAYING

City of Sioux Falls

> “Data classification tasks that would have previously required expensive 3rd party auditors and multiple full-time engineers can now be completely automated. We drove over 90% operational savings by eliminating manual scripting and spreadsheet management, reducing time spent to complete hundreds of search queries from two weeks to just 1 hour. Not to mention, Sensitive Data Monitoring provides a platform to continuously monitor our sensitive data for high risk incidents, such as overexposed credit card numbers and social security numbers, seamlessly on our existing backup data without impacting production.”

Brandon Morris
Systems Administrator
City of Sioux Falls

University of Reading

> “Sensitive Data Monitoring allows us to easily prove PCI DSS compliance without risking fines, dedicating multiple resources and freeing up our employees for outcome-based value-add work. We can now automate sensitive data classification, such as credit card information, passport data, and other PII, to better understand our overall risk posture, assign data ownership, and comply with access requests, such as UK’s Freedom of Information Act. As a university, any compromise of student data can lead to damage to our students’ well-being and our organizations’ reputation.”

Kevin Mortimer
Infrastructure Services Manager
University of Reading

To learn more about Sensitive Data Monitoring and how it can help your organization automate their data governance requirements, please visit our website or contact your local sales person.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik is on a mission to secure the world’s data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.