USE CASE

PCI-DSS 4.0

Securing Payment Card Information for Secure Transactions Globally

Challenge

- The Payment Card Industry Data Security Standard (PCI-DSS) 4.0 is an evolution of the industry rules that have been in place since 2006.
- Payment cards information remains a target for cybercriminals.
- A new customized approach to fulfilling PCI-DSS requirements offers greater flexibility to merchants and payment card processors to secure card data.
- An emphasis on risk-based approaches and assessments means that there’s more of a need to understand risks to sensitive authentication data and personal payment information.

What’s New in PCI-DSS 4.0

- Additional authentication controls, such as strict multi-factor authentication (MFA) requirements when accessing cardholder data.
- Updated password requirements, such as increasing password length requirements from eight to 12 characters.
- New requirements around shared, group, and generic accounts.
- Clearly defined roles and responsibilities for each requirement.
- New requirements to prevent and detect ongoing threats against the payment industry.
- A focus on security outcomes instead of prescriptive controls with the customized approach
- Emphasizing continuous security and monitoring to showcase compliance as an ongoing process, not solely an annual audit.
- More precise guidance on encrypted data management.
- More service provider responsibilities.
- Emphasizes that organizations maintain a documented description of the cryptographic architecture for a broad perspective on encryption, decryption, and key management processes.

Solution

- Sotero uses advanced machine-learning to discover data stored in the cloud and on-premises
- Sotero protection sits between end users and assets, allowing monitoring of cloud and on-premises infrastructure through a single portal
- Sotero protection is built in the cloud, scaling to meet the needs of the modern data-heavy enterprise
- Sotero threat detection creates an active defense for all data no matter where it’s stored
- Advanced AES-256 encryption at rest, in use, and in motion by default with customizable options.
- Sotero instantly quarantines any malicious attempts to modify data.
- With adjustable thresholds, Sotero empowers your organization to stop malware infections, detect insider threats, and secure critical payment card data.

Benefits

- Automated detection and advanced ML tracks usage, detecting anomalous behavior in real-time and stopping it.
- In-depth visibility integrates with existing SIEM or IaaS for a single pane of glass interface that provides a holistic view of your organization's information security
- Seamless integration with anomaly detection protects data without negatively affecting user experience
- Cloud deployment makes it easy to adopt, manage, and scale without expensive implementations
- Easy application integration with no server-side software and no code means that Sotero integrates quickly with your systems
- Encryption protects your unstructured data in the cloud, fulfilling the new PCI DSS emphasis on cloud data security

About Sotero

Sotero is the global innovator and leader in revolutionary data security. Sotero is a cloud-native data protection platform that protects ALL cloud data types, applications, and stores from catastrophic cyber attacks. Sotero protects your data in the cloud with no costly, time-consuming deployment or downtime. Advanced encryption and real-time machine learning techniques allow organizations to solve for insider and outsider threats while meeting compliance requirements with actionable audit logs. The platform enables fast deployments that enable data to be shared securely and used with confidence. With point and click set-up, Sotero’s data security platform is easy to deploy and manage with no impact on user experience. Organizations can now be protected in a matter of days, not weeks or months.