USE CASE

Vormetric Integration

From Protecting Data Sometimes to Anywhere All The Time

Overview

Vormetric is a similar data protection solution focusing on data at rest and data discovery to deliver data protection. This leaves a significant gap in the execution where data in use is not adequately protected. Not only will it become unencrypted in use, but also, there are no controls automating oversight for utilization. Vormetric relies upon an audit log collection that requires manual analysis. Without this coverage, the organization can become a victim of both external and insider threats without any awareness of a compromise occurring.

Challenge

- Vormetric offers similar data at rest and data in-motion functionality to Sotero
- Vormetric solution is not cloud-based and requires a separate hardware device on-premises for Hardware Security Models (HSM) and as a key manager.
- Vormetric requires agents on all servers
- Customers have trouble determining why they would replace Vormetric with Sotero and need to understand the Sotero Value added
- Unlike Sotero, Vormetric has operating system dependencies that require upgrades and maintenance and temporary outages to support them
- Vormetric is database dependent and does not apply to unstructured data such as Word documents, Excel files, or PDF documents
- Data protection by Vormetric is database specific and does not offer seamless and transparent protection across all database engines like Sotero does
- Vormetric has a limited protection scope and does not offer protection to shared data as they are specifically targeted to the database or file system they operate in
- Vormetric is less feature rich, not offering functionality of auditing and access control, instead relying on other products to fill in the gap
- In RDS environments Vormetric doesn't have access to the database servers and hence cannot support RDS Instances
- Vormetric tokenization solution limits the usability of the data

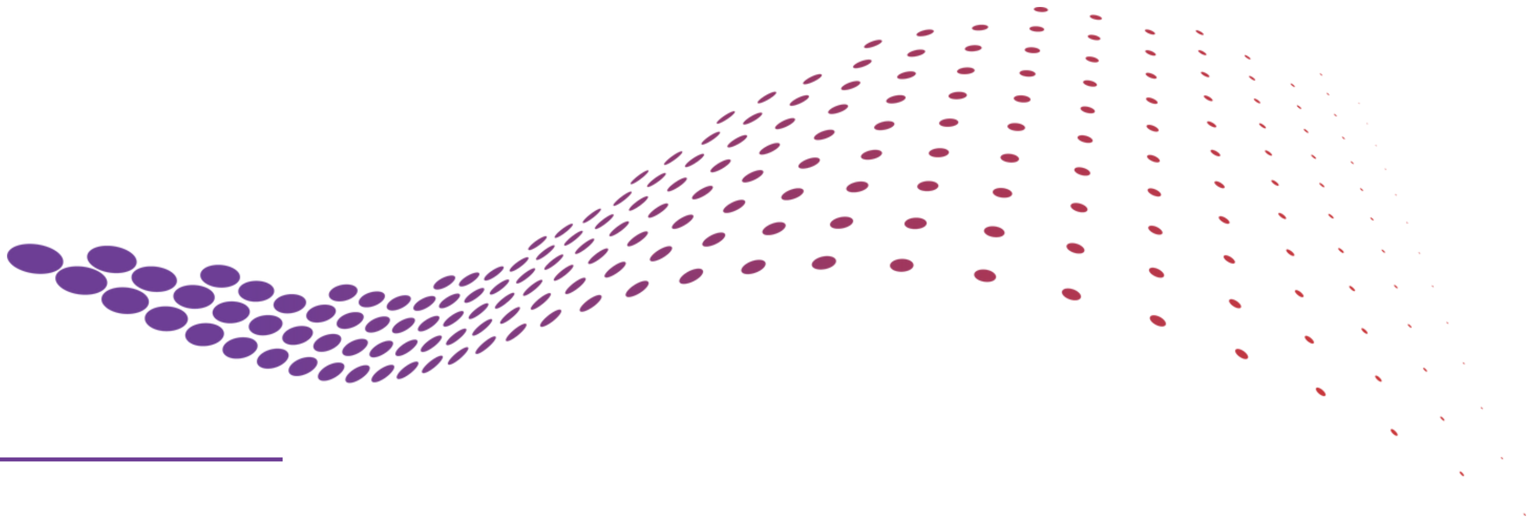
Sotero
99 S. Bedford Street, Suite 106
Burlington, MA 01803
www.soterosoft.com

Solution

- Sotero can be used in tandem with Vormetric for on-premises to fill in missing capabilities of encryption of data in-use
- Sotero can be used in lieu of Vormetric for cloud deployments, filling in the gap in service Vormetric does not offer
- Sotero also uses real-time threat detection to identify high-risk access attempts to data that Vormetric does not
- Sotero in tandem with Vormetric helps protect the enterprise from cloud-based ransomware threats on shared storage

Benefits

- Sotero is easy to implement in the cloud allowing current Vormetric users to rapidly onboard in days rather than weeks while running in tandem with Vormetric
- Vormetric access logging is augmented by Sotero threat detection to provide actionable insights into inappropriate utilization
- Sotero encryption in-use closes the gap for data-lifecycle encryption creating a fully secure infrastructure
- Sotero threat detection closes the gap on the SureDrop functionality, allowing identification of risky access attempts for shared data
- Sotero expands beyond basic encryption offered by Vormetric to include Ransomware protection.



About Sotero

The Sotero Data Security Platform provides a centralized way to encrypt and protect data through its entire lifecycle – at rest, in transit, and in use. With real-time detection and automated quarantine of malicious access, Sotero also prevents active threats, giving you 360-degree data security without disrupting the user experience. With our lightning-fast encryption and our point and click set-up, Sotero's solution is easy to deploy and manage, ensuring you are protected in a matter of days, not weeks or months

Schedule a demo today to learn how Sotero complements and enhances Vormetric.