

Revolutionary Data Security

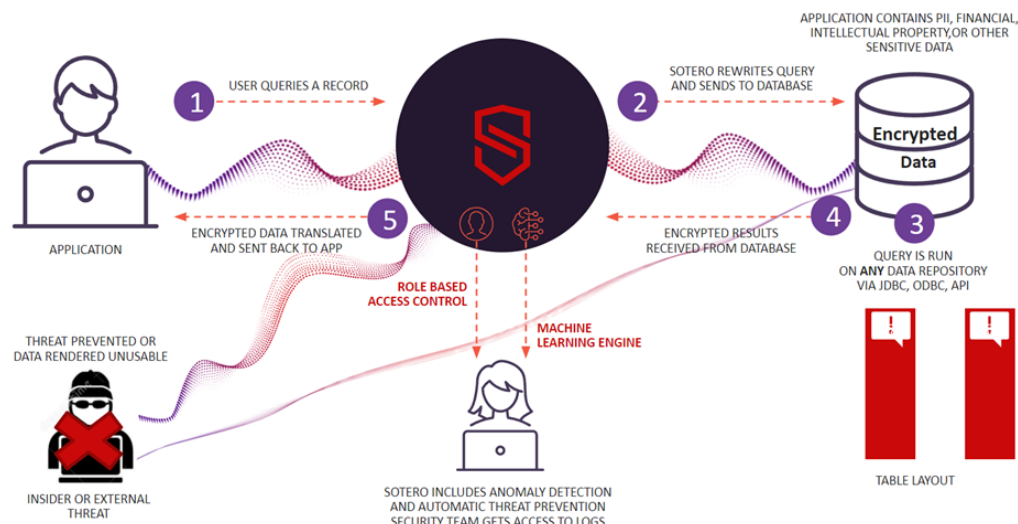
Protecting Data Anywhere All The Time

How is Your Data Protected?

Sotero reimagines security and privacy by providing a multi-layered approach to address the critical security gap of unencrypted data in use. It encrypts & protects the data through its entire lifecycle – at rest, in transit, and in use - and prevents active threats with real-time detection and automated quarantine of malicious access, giving you 360-degree data security. Sotero's multi-platform solution won't disrupt your users' experience and is easy to deploy and manage. With our lightning-fast encryption, and point and click set-up, you are up and running in a matter of days, not weeks or months.

Unleash The True Power Of Your Data With:

1. 360° data protection (in use, at rest, and in-transit)
2. End-to-end encryption from loading to query retrieval
3. Customer-owned encryption ensuring no external access to the encryption key
4. Embedded security at the data layer and privacy to minimize threats
5. Regulatory compliance – HIPAA, GDPR & CCPA
6. Granular privacy (Role and attribute-based access control)
7. Security at scale to match your growth



Protect

Encrypt query data and access it seamlessly

Sotero enables you to use your data fully – search & query – without ever decrypting. Results can also be safely accessed within the cloud with no additional software ever needed.

Detect

Identify suspicious access attempts in real-time

Sotero assigns every single transaction a Threat Score using a range of smart metrics. When a transaction exceeds the thresholds you set, Sotero will immediately notify you.

Defend

Instantly quarantine suspicious access requests

Sotero instantly quarantines any suspicious access request. Simply set your security thresholds and suspicious queries will be stopped before they ever run in the first place.

Why Sotero is Unique

Sotero's patented technology gives full protection and complete control of an organization's sensitive data in use, in motion, and at rest. This unique approach to data protection closes the security gap of data being decrypted while in use.

Features

- Cloud Deployment makes it easy to adopt, manage, and scale-up projects rapidly.
- Granular Access Setting puts you in control so you can allow/restrict access and choose selective encryption for fields, rows, or parts of a data set.
- Easy Application Integration with no server-side software and no coding required to rapidly integrate with your infrastructure.
- Scalability and High-speed performance minimize user experience impact, which is common with encrypted systems.
- Meet Compliance Mandates for HIPAA, GDPR, PCI-DSS, SOX, & more.
- Advanced Encrypt AES-256 encryption at rest, in use, and in motion by default with customizable options.
- In-depth Visibility integrating with existing SIEM or utilizing a single pane of glass interface for a holistic view of your organization's information security.

Sotero Benefits

- Share sensitive data rapidly and securely
- Meet customers' strict data security requirements
- Accelerate mission-critical use cases previously stalled by manual data workflows

Sotero Platform

The Sotero data security platform provides the security that organizations require to share sensitive data with downstream systems and third parties securely and at Scale.

The key is Sotero data in use encryption that keeps data encrypted while in transit to downstream systems or partners and, once there, data remains encrypted while it is being used. Data in use encryption ensures sensitive data is never left unsecured, regardless of lifecycle stage (at rest, in transit, or in use) and regardless of source or location (on-premises, in the cloud, or hybrid).

With Sotero, organizations now have the power to confidently allow internal collaborators, clients, and vendors to unlock the potential of your data without it ever being exposed. Businesses are no longer held back by data security concerns and manual workflows, enabling innovation and faster time-to-value from data while reducing the security team's cycles.