

Secure PII Anywhere, All the Time

With Sotero's Intelligent Data Security Fabric

PII Data Security Challenges

Collaboration

Sharing information across organizations drives innovation. With collaboration comes the risk of disseminating PII. Third parties and remote workers may not have the same controls protecting their endpoints creating gaps for an attack.

Data Availability

Overreactions to protecting PII often result in restricting data availability to the point it is unusable. Organizations need to be able to effectively use their data without getting bogged down in drawn-out access requests.

Compliance Regulations

PII data is highly regulated and failures to adhere to compliance can result in hefty penalties including fines, jail time, or damage to company reputation.

“As a cloud-based platform in healthcare, data security to secure PHI is a key aspect of our commitments to our clients. Sotero enables us to meet those commitments and exceed them. The ability to keep PHI secure during use is a key differentiator.”

~ Murali Menon / Founder/CTO — ClinicalBox

Data-Centric Security



Data is Most Vulnerable In Use

We hear a lot about protecting data at rest or in transit but that leaves a critical security gap. If you're not protecting sensitive data like PII while it's in use then you are leaving a hole for cyberattackers & insider threats.

Customer PII is the Costliest Type of Record Lost or Stolen in Breaches

IBM noted customer PII cost an average of \$180 per lost or stolen record in 2021. In 2020, customer PII cost \$150 per lost or stolen record, representing an increase of 20%. That cost continues to rise.

Data is the Target — Protect the Target

Simple effective data protection is the solution. Sotero is a holistic data protection solution, simplifying multiple tools into one easy-to-manage data security platform.

Unencrypted PII is Vulnerable. PII in Use is Unencrypted.

Our patented Sotero KeepEncrypt™ technology solves this gap in protection. Only Sotero keeps your data secure at all stages of its lifecycle. Because data in use remains encrypted, even when a system breach occurs, data loss is prevented.

At rest, in transit, and in use — when we say all, we mean all.

**People Are
Worth \$1,285**

*According to
the Dark Web Index

Data thieves do it for the money. The most profitable cyberattacks target data. Whether it be ransomware or insider data theft with the intent to sell it on the Dark Web, data is the juiciest target.



Data In Use Encryption Advantages

Data In Use Encryption Above & Beyond

Sotero ensures data remains encrypted everywhere. Using strong AES-256 standards, structured, semi-structured, and unstructured data is protected regardless of location.

We Close the Data In Use Security Gap

PII is encrypted throughout its lifecycle and loss is prevented, even in the event of a breach because data remains encrypted.

Role-based access controls (RBAC) allow you to restrict access to data. Granular field-level control protects data from unauthorized access, even from cloud providers or database administrators who don't need to read the data.

Sotero Keeps You In Control

Take control of data stored in cloud-based SaaS or IaaS with encryption. PII and all access to it is completely in your control.

- Share data securely and rapidly with internal collaborators, partners, and downstream systems.
- Address production use cases more rapidly by encrypting data throughout the lifecycle.
- Onboard new vendors, partners, and customers rapidly and securely.
- Store data in the cloud with confidence that it is secure at all times.

Enable a higher level of data security by securing sensitive data while in use.

Sotero's Revolutionary Technology

Data In Use Encryption

Unlike traditional encryption solutions that only protect it at rest or in transit, Sotero also protects it in use, eliminating gaps in protection.

Real-Time Anomaly Detection

Sotero detects anomalies at the data level, protecting PII by leveraging machine learning (ML). The ML engine recognizes and blocks intruders in real-time before unauthorized access is granted and a breach occurs.

Data Security Inheritance

Security products, applications, and data assets added to the security fabric automatically inherit security and single-pane governance of the platform.

Plug-and-Play Interoperability

With Sotero there is no need to modify or customize your applications to work with Sotero, adding assets to the security fabric integrates capabilities without any code changes or customization.

Secure Third-Party Data Management

Share sensitive data with third parties securely and at scale. Sotero's data in use encryption protects data throughout its lifecycle no matter if it resides on-premise, in the cloud, or in a hybrid environment.

Cloud Data Security

Sotero lets you manage your own encryption keys in the cloud, keeping PII protected so even the cloud service provider cannot access it.

ABOUT SOTERO

Sotero is the global innovator and leader in revolutionary data security. Sotero's data security platform provides a single pane of glass that enables our customers with a way to protect data anytime, anywhere, regardless of data store, integration mechanisms, and user tools. The platform is able to control, access, operate, and use data to extract information that drives organizations' business outcomes and innovation.

Sotero provides organizations with a scalable and flexible data security fabric that migrates and moves data securely, in all its instances in an interconnected world. Organizations gain complete control over their data privacy, compliance, audibility and governance for use cases ranging from securing data at the edge, IoT devices and streaming data, and moving data securely to downstream systems.

→ Learn more at www.soterosoft.com



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