Sotero

Data In Use Encryption Is Better For Protecting PII

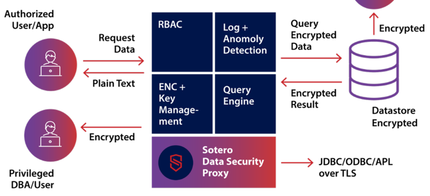
Here's Why

1 Collaboration is a Risk

A certain amount of data sharing is essential for productivity and innovation, but protecting sensitive information like PII is challenging. Third parties and remote workers rarely have their endpoints secured which creates gaps and increases risk.

2 Data Is Most Vulnerable In Use

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.



3

Data in use encryption, allows PII to be worked with outside of the organization for research, analysis, or day-to-day tasks without compromising the security of PII. Sotero sits between the user and the data store deciding what data the user has rights to and managing the query behind the scenes so the analysis can happen without disseminating the critical data.

The Numbers

294 million

The number of people affected by the data breaches in 2021*

*Source: Identity Theft Resource Center's annual report

$2 = Social Security numbers (SSN)	**$14-199** = payment services
$1 = medical records, more for complete records	**$100** = driver's licenses
$17-65 = credit card w/ CVV	**$17-65** = avg for passports*

*Source: Dark Web Price Index 2021

"Encrypting data, particularly for cloud data platforms, is a powerful way to secure sensitive data at rest, but has traditionally been a very high effort task to accomplish.

Sotero has found the solution by building a product to do the hardest parts.

Customers can now seamlessly encrypt data which remains encrypted in use for cloud use cases without the burden of spending countless development cycles. This technology is a game changer."

Andrew Lance, Founder and Principal - Sidechain Security

5 Advantages

of Sotero Data Security Fabric with Data In Use Encryption for PII

Protect PII Anywhere, All the Time 1	No matter how your data is structured or stored, PII can remain encrypted and controlled even when in use.
Detect Threats 2	The use of machine learning to proactively protect PII by detecting and blocking threats in real-time, stopping attacks before a breach occurs.
Control the Cloud 3	Ensures that PII is protected from insider threats. Keep PII out of the hands of administrators, even in a cloud environment where your cloud provider has privileged access.
Standardize Data-First Security 4	Apply the same security practices and governance to all new and existing solutions to make sure there are no gaps in your implementation.
Simple Effective Protection 5	Rapidly onboard new data stores and applications to protect PII immediately without long and complicated configurations.