HOW SOTERO WORKS

Sotero Data Protection

Technical Platform Overview

SOTERO DATA PROTECTION PLATFORM

PROXY
Used to ensure the data is protected.

VAULT
Contains access management and attribute-based controls.

ML ENGINE
Detects and protects against any unauthorized attempts at retreiving data.

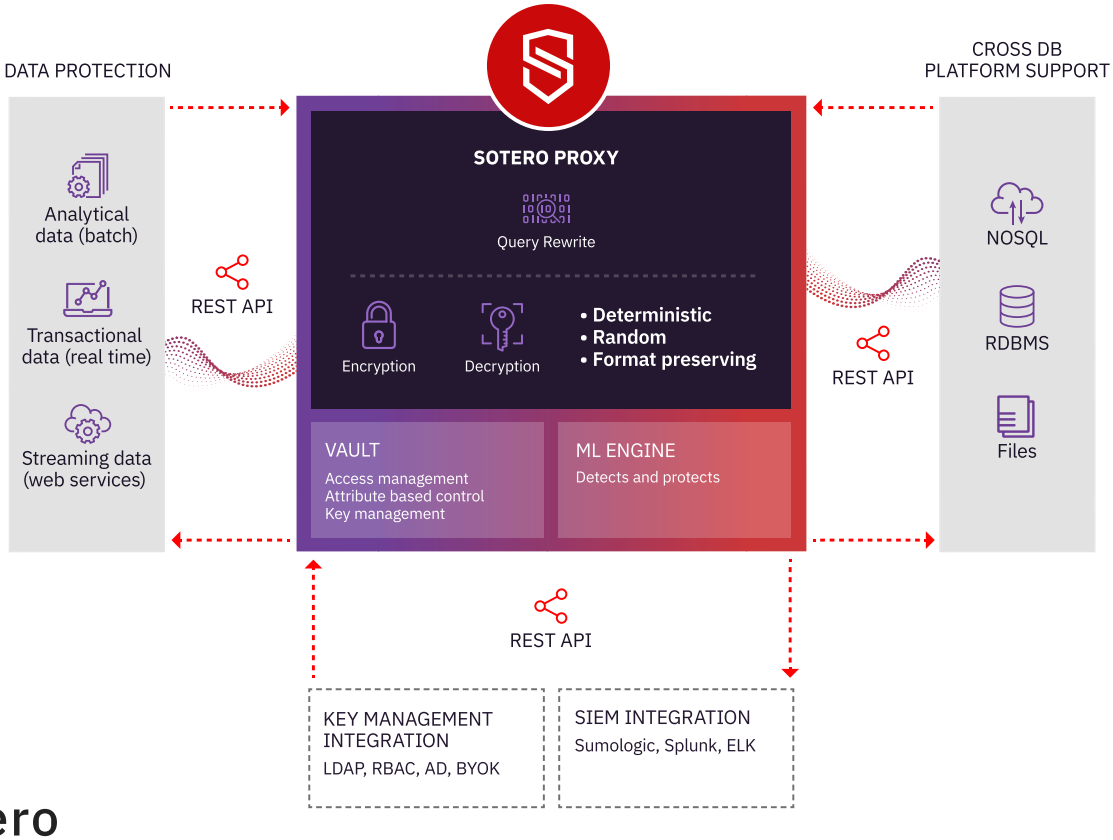
Sotero protects all data, at all field levels, and across all databases. It protects data wherever it's located—on premises or in a cloud—providing secure access for data transfer, analysis, and sharing.

Because of Sotero's unique technology, businesses can confidently protect data in use without performance degradation. The platform provides universal protection while allowing granular levels of control.

Here's a look at the technology that makes these functions possible.

Sotero Proxy, Vault and Machine Learning (ML) Engine

The Sotero data protection platform consists of three modules: the **Sotero Proxy** (the key module, used to ensure the data is protected), the **Sotero Vault** (containing access management and attribute-based controls), and the **Sotero ML Engine** (which detects and protects against any unauthorized attempts at retrieving data).



Sotero

Sotero Proxy

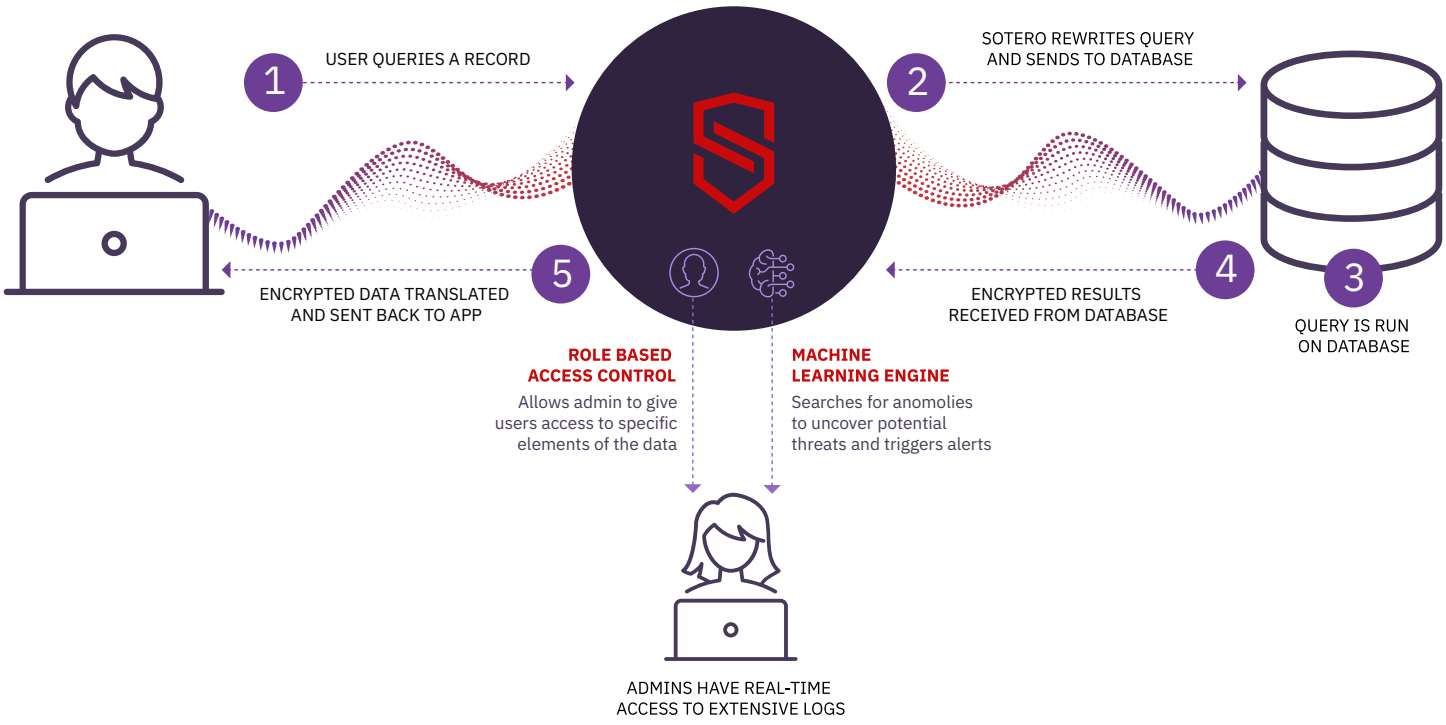
The Sotero Proxy ensures that sensitive data is encrypted, even when in use by applications. It provides decrypted data for authorized queries from your application users. The Proxy uses three levels of encryption: deterministic, random, and format-preserving.

Each Sotero customer has a dedicated Proxy, which the customer configures with a graphical setup tool to establish permissions on accessing data. A customer can select tables and columns containing data that needs to be encrypted, establish user roles and access controls, and configure communications between the Proxy and applications and databases.

After the initial setup, when an application queries the database the query is routed to the Sotero Proxy. It does so using a driver that connects the application to the proxy's REST API or application connector.

The Proxy processes the query. For data requests, it fetches encrypted data from the database. The Proxy then evaluates the user's access rights and sends unencrypted results back to privileged users. Users without the proper privileges would receive encrypted data in response to a query. Queries from unauthorized users will not be completed. For data inserts/updates, it validates the user credentials and, if they are valid, the Proxy encrypts the new data, sends it to the database, and logs the data changes. Data flows between the Sotero proxy and the applications/databases in messages secured by SSL encryption.

REST APIs give programmatic access to the components in the Proxy module, allowing application developers to embed Sotero into applications that work with sensitive data and to configure the Sotero platform with programmatic calls instead of using the platform's graphical setup tool.



Sotero Checks Access Privileges Before Responding to Application Queries

Sotero

Sotero Vault

The Sotero Vault is a highly secure key management service that uses TLS access control and multiple layers of AES-256 keys to encrypt the data. The Vault holds the data encryption keys (DEKs) used to encrypt the data as well as a master key (or key encryption key, KEK), which is used to encrypt the DEKs themselves. The DEKs are symmetric keys, meaning the same key is used to encrypt and decrypt the data.

If Sotero is deployed on your premises, you will receive a Key Generator utility that enables you to create the keys and store them in your private Sotero Vault. In this scenario, Sotero will never see or access your keys.

If you are using Sotero in the Sotero cloud, you will receive a dedicated namespace within the common Vault, which acts as a vault within a vault. The Sotero team will run the Key Generator utility on your behalf. DEKs are typically created so that there is one for an entire organization. However, if an extra layer of security is required, separate DEKs can be generated for each field. To further protect the encryption key, you have the ability to change the DEK, which will require re-encrypting all sensitive data with the new DEK, or to rotate, or change, the KEK.

> **The platform can be deployed on your premises, in a private cloud, or in the Sotero cloud, a multi-tenant cloud environment.**

Sotero ML Engine

The Sotero ML Engine detects and protects your data from unauthorized use and prevents attacks in real time. The ML Engine evaluates each incoming query against historical patterns of use and can immediately stop a suspicious query before the data is released to the user. The ML Engine can stop an attacker who gains access to the system or an authorized user of the system who behaves in a suspicious manner.

Where the Sotero Platform Resides

The Sotero Data Protection Platform can be deployed on your premises, in a private cloud, or in the Sotero cloud, which is a multi-tenant cloud environment. Regardless of its physical location, the platform logically sits between your application and your data store, encrypting data in your data stores, validating requests for accessing data, and decrypting data for authorized requests.

Learn More

For more information on the Sotero Data Protection Platform, schedule a product demo at www.soterosoft.com.

Sotero

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