



# Revolutionary Ransomware Protection

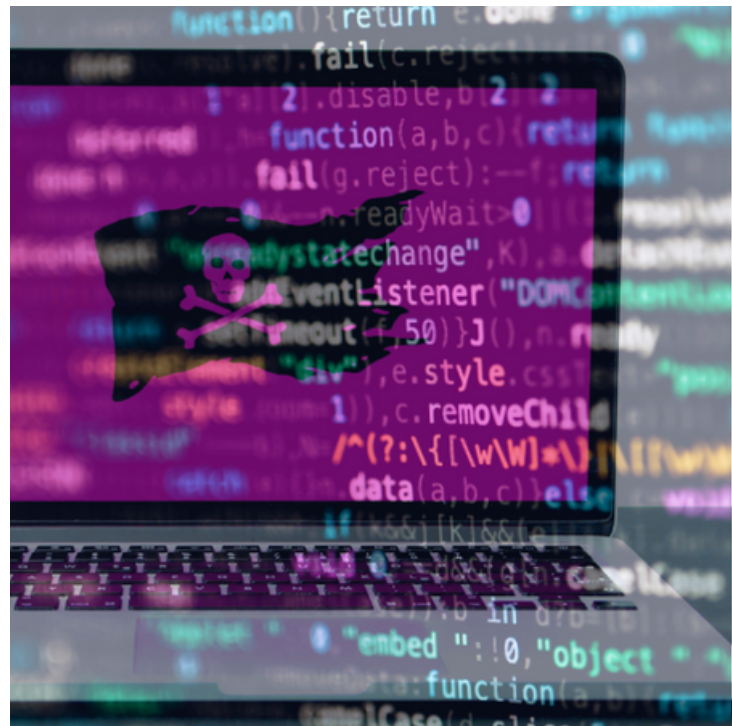
Protecting Data Anywhere  
All The Time

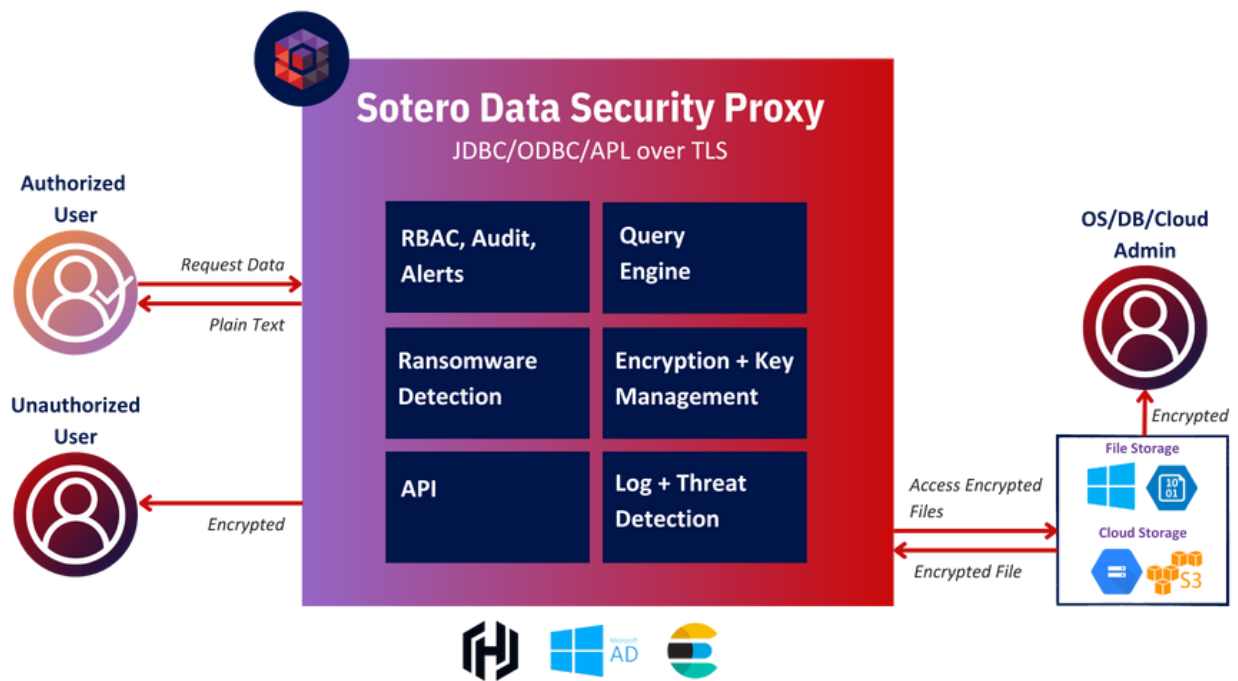
## Are you ready for Ransomware?

Ransomware infections continue to be a bane to business, with attacks evolving to include data theft and extortion that even extends to unstructured data stored in the Cloud. Sotero reimagines ransomware protection to create a multi-layered approach to address this security threat. Sotero encrypts and protects data to prevent ransomware and attackers from stealing data. Then, with powerful ML technology, Sotero can determine when file access and modification indicate ransomware in real-time. Once this behavior is detected, our platform can rapidly block access, stopping attackers before they can lockdown or steal your data.

## Defend your data with:

1. Machine Learning powered ransomware detection
2. Automated controls to stop attacks
3. 360° data protection (in use, at rest, and in-transport)
4. End-to-end encryption from loading to query retrieval
5. Embedded data security and privacy to minimize threats
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 encryption protects your unstructured data in the cloud from ransomware preventing theft and extortion attacks that are frequently combined with most modern ransomware infections.

## Detect

*Identify malicious access attempts in real-time*

Sotero tracks and classifies how legitimate users access and modify files. Using advanced ML, Sotero is able to identify ransomware behavior from legitimate users.

## Defend

*Instantly quarantine Malicious usage*

Sotero instantly quarantines any malicious attempts to modify data. With adjustable thresholds, Sotero empowers your organization to stop ransomware infections.

### Our Ransomware Protection Is Unique

Unlike legacy ransomware protection that relies on signatures of previously discovered threats, Sotero detects based on behavior. Sotero will detect new strains of ransomware based on how they interact with files and data, not because they have been seen before.

### Sotero Benefits

- Share sensitive data rapidly and securely at scale without performance degradation
- Meet customers' strict data security requirements
- Accelerate mission-critical use cases previously stalled by manual data workflows

## Features

- Automated Detection advanced ML tracks usage, detecting ransomware in real-time and stopping it.
- 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.
- Advanced Encrypt AES-256 encryption at rest, in use, and in motion by default with customizable options.
- 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.

## Sotero Platform

The Sotero data security platform provides holistic data security to defend against ransomware and 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). Encryption prevents data theft from attackers and ransomware, helping meet compliance regulations and avoid costly fines and lawsuits.

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.