

Anomaly Detection and Malicious User Prevention

Sotero's Real-Time Threat Detection and Prevention Capabilities



ANOMALY DETECTION TECHNOLOGY

Sotero's machine learning algorithms enable the analysis of each data access request and are able to review and categorize them based on their threat potential.

The Benefits Of Real-Time Anomaly Detection and Malicious User Prevention

Sotero offers organizations the ability to proactively detect malicious attempts to access, use and steal information. Sotero's machine learning algorithms enable the analysis of each data access request and are able to review and categorize them based on their threat potential. This analysis is done in real-time by a power self training ML model that enables threats to not only be detected but also stopped for execution. Sotero's anomaly detection technology enables organizations to have complete control over their data's privacy, compliance, auditability, and governance.

Each transaction adds to the history of learnings that will be used for analyzing the next set of transactions.

How It Works

Sotero's anomaly detection solution inspects every transaction that is submitted for execution. Each transaction, in addition to being logged, will be parsed into its separate components and the components are evaluated in the context of historical use of the data set. Each attribute that is a part of the transaction is assigned an anomaly score and a combined threat score is computed using weighted scores for all the attributes in the transaction.

The threat score is used to categorize transactions based on the score range. Score ranges are utilized to make decisions on the execution of the transaction, execution with a notification, or quarantining the transaction for further review and approval or disapproval. All decisions are then stored.

The transaction review, scoring, and decision engine is a major component of the Sotero encryption APIs. The logging and scoring framework works seamlessly in conjunction with the translation and encryption/decryption APIs with an autonomous service and asynchronous function.

The beauty of this approach is that each transaction adds to the history of learnings that will be used for analyzing the next set of transactions.

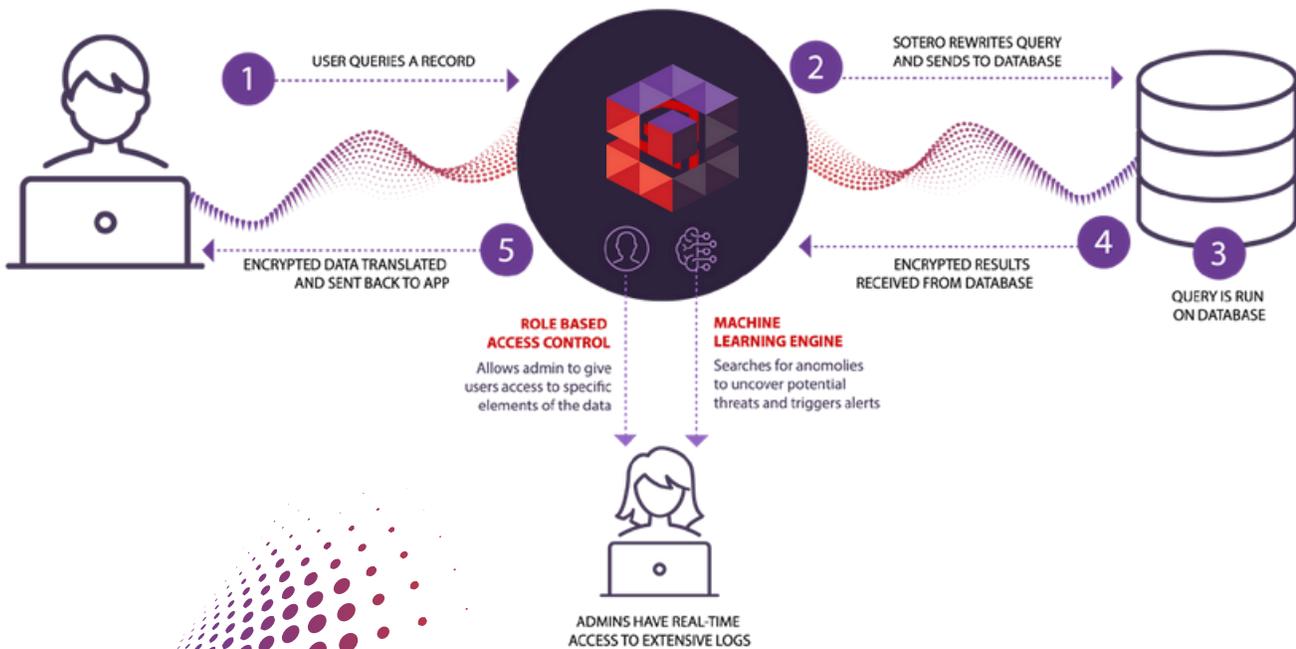
Management Console

The anomaly detection management console provides both administrative functions as well as serving as a repository of database activity that can be filtered by database or application, including in multi-tenant scenarios.

These include information such as:

- total transactions
- transaction by threat score range
- flagged transactions
- quarantined transactions

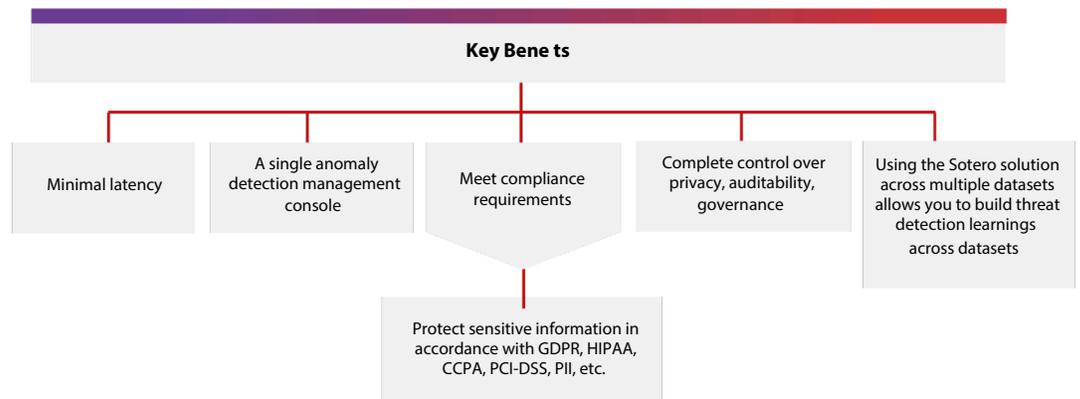
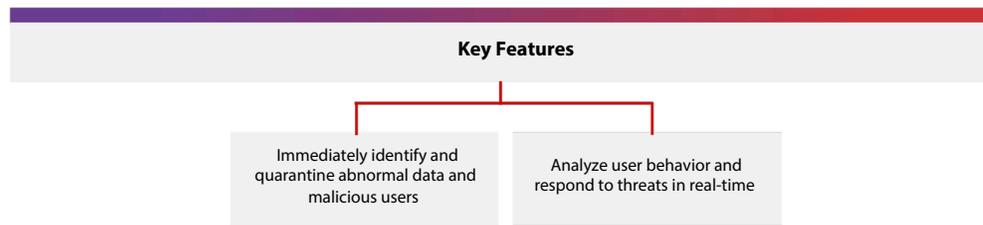
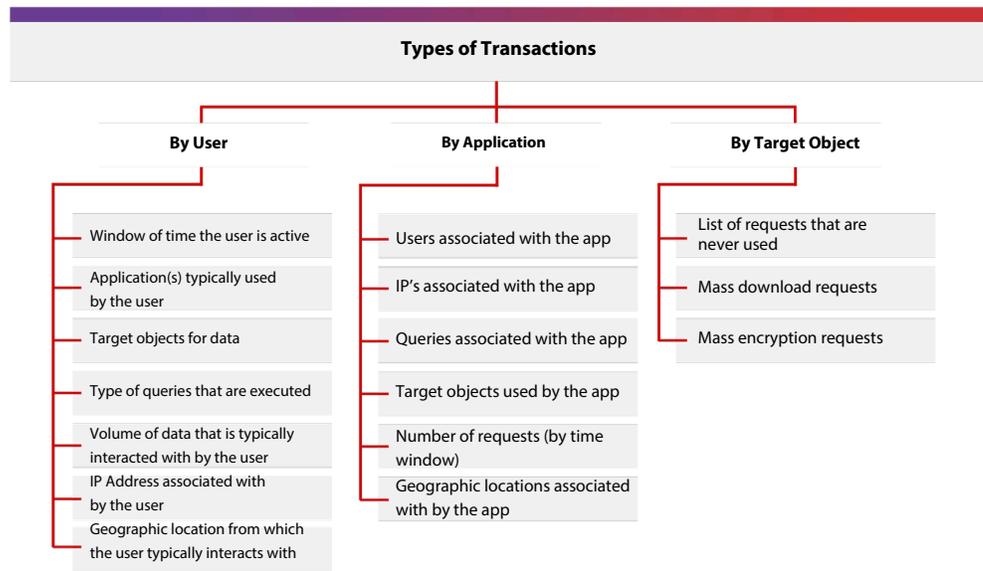
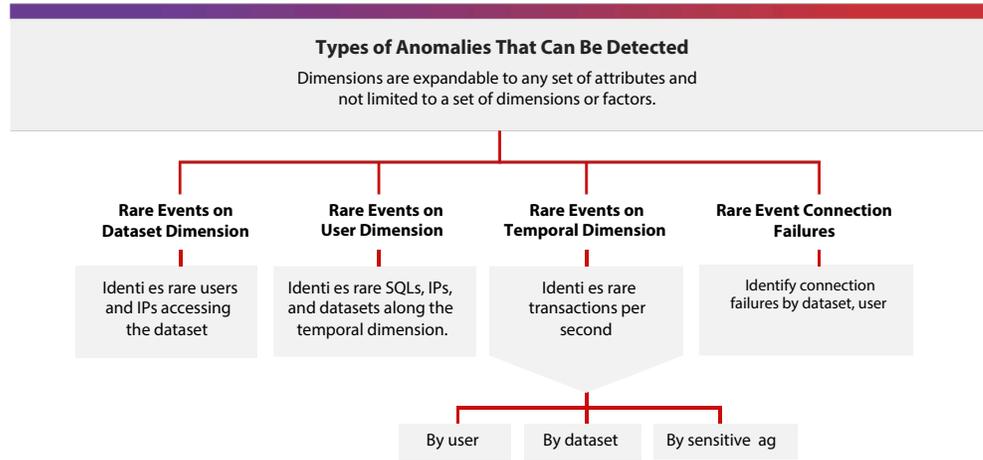
The management console allows the administrator to review transactions to either review or decline them.



The management console allows the administrator to review transactions to either review or decline them.

ANOMOLY DETECTION MANAGEMENT CONSOLE

The anomaly detection management console provides both administrative functions as well as serving as a repository of database activity that can be filtered by database or application, including in multi-tenant scenarios.





Key Features

- Immediately identify and quarantine abnormal data and malicious users
- Analyze user behavior and respond to threats in real-time

Key Benefits

- Minimal latency
- A single anomaly detection management console
- Meet compliance requirements
- Protect sensitive information in accordance with GDPR, HIPAA, CCPA, PCI-DSS, PII, etc.
- Complete control over privacy, auditability, governance
- Using the Sotero solution across multiple datasets allows you to build threat detection learnings across datasets

ABOUT SOTERO

Sotero is the global innovator and leader in next generation data security. Sotero's KeepEncrypt™ solutions secure your data by encrypting data at rest, in motion, and in-use with virtually no latency or impact on user experience. Securing data "in-use" enables our customers to realize higher returns and faster time-to-value from their data for mission-critical business use cases, including data analysis, data sharing, and product development. Sotero's data security solutions are used by mid-market and large enterprises around the globe in biotech research, financial services, software development, healthcare and other industries that rely on data for business innovation and competitive advantage.

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



1500 District Avenue
Burlington, MA 01803
www.soterosoft.com