WHITE PAPER

360° Data Security:

The Unique Value of the Sotero Platform

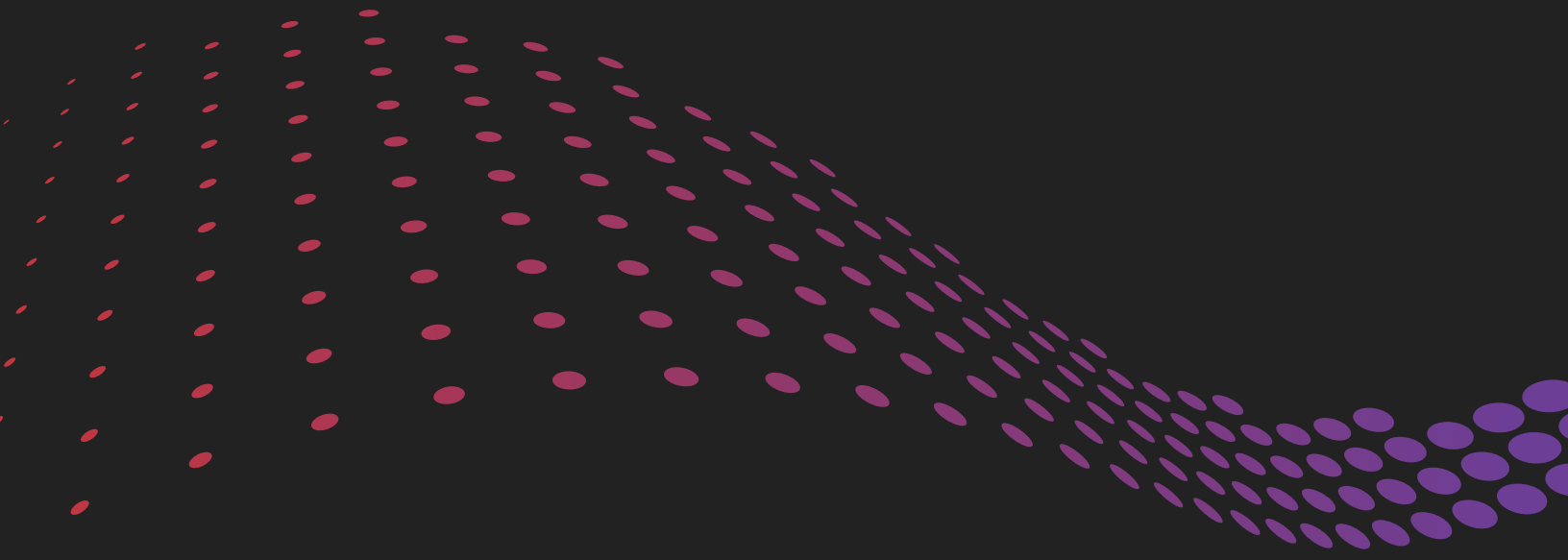
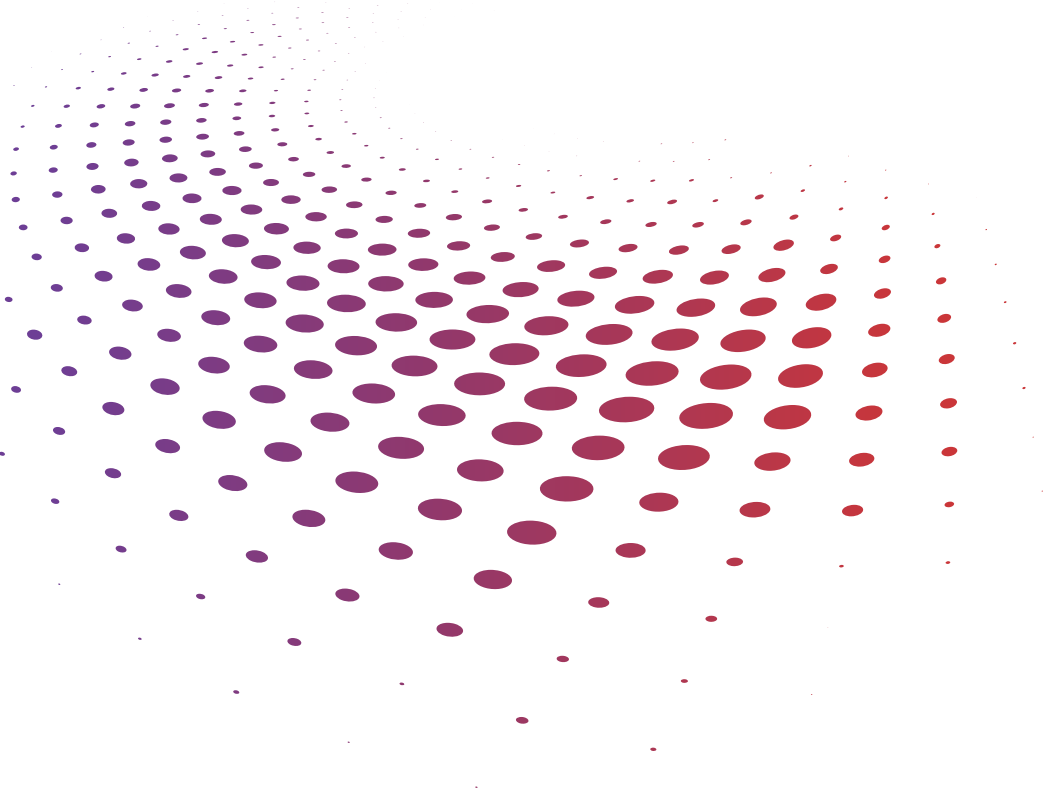
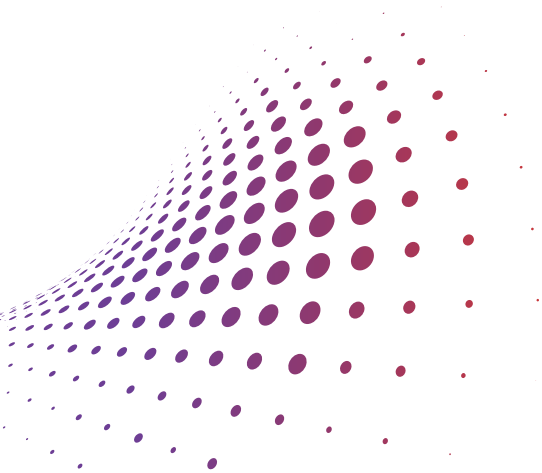


Table of Contents





98% of sensitive records exposed in 2019 data breaches were the result of unauthorized access, hacking/intrusion, or accidental web/ internet exposure.

– IDENTITY THEFT RESOURCE CENTER

Introduction

Companies spend billions of dollars annually to secure their infrastructure and data, yet data breaches routinely occur even when network security and user validation is in place. A single breach can cost millions of dollars to detect, respond, and recover. It can also affect the long-term viability of your business as securing personal data becomes an important, global issue. In fact, in a recent global survey, 85% of consumers said they wish there were more companies they could trust with their data.[1]

Encryption has proven to be the most effective way to lower the impact of a security breach, but traditional encryption helps only when data is at rest (disk encryption) or in transit via secure communication methods such as SSL and TLS.[2] That leaves companies with significant vulnerabilities when the data is used by on-premise or cloud applications. Additionally, as companies rely more heavily on cloud environments, including SaaS and IaaS products, they face even greater risks. By giving control of the data to cloud providers, they face vulnerabilities because the cloud providers may not encrypt data securely. Even when they do secure the data, the cloud providers have access to the data and the encryption keys.

The Sotero Data Security Platform takes a new approach to protecting data that ensures sensitive data is never left unsecured. Sotero easily secures all your data, regardless of source, location (on-premise, cloud, or hybrid) or lifecycle stage (at rest, in transit, or in use). Sotero can be seamlessly deployed and used, enabling your business to operate smoothly and securely and giving you the confidence to use, share, and monetize data.

This paper is intended for security, product, and business teams that want to better protect their sensitive data. We will explain how the Sotero Data Security Platform works, how easily Sotero can be deployed and operated, and the advantages organizations have gained from using the platform.

[1] PwC Consumer Intelligence Series, Trusted Tech survey, 2020

[2] Cost of a Data Breach Report, Ponemon Institute and IBM Security, 2019

In the U.S.
alone, more than

1,400

data breaches
occurred in 2019.

— Identity Theft Resource Center

WHY SECURING DATA IS INCREASINGLY DIFFICULT

Clearly securing data is not easy. In the past, it was easier because there were fewer applications and data was often siloed and more easily protected. Today, however, data is at the core of nearly every business –healthcare, financial services, software, pharmaceuticals, retail, and education.

Companies' competitive differentiation, collaboration with partners, and customer trust depends on their ability to use, share, and monetize data securely. They use an increasing array of specialized software, systems, and access devices/endpoints (e.g., mobile phones and IoT devices) to unlock the value of their data and make their business operate efficiently. Data flows more freely in this environment, both inside and outside the company. It's typically stored in many places, including on-premise databases and applications, software as a service (SaaS) applications hosted in a public cloud, and cloud infrastructure as a service (IaaS) systems.

More systems result in more attack points, higher complexity, and higher risk. This is reflected in the ITRCs data, which shows that 98% of sensitive records exposed in 2019 data breaches were the result of unauthorized access, hacking/intrusion, or accidental web/internet exposure.[4]

Traditional Encryption, Cloud Migrations, and Endpoints Put Sensitive Data at Risk

Data is the life blood of most organizations. Data is used to improve critical business metrics in all industries, such as the sales results, customer satisfaction, the efficiency of manufacturing processes, and the quality of healthcare. It's safe to say that every enterprise has sensitive data, such as customer data, personally identifiable information (PII), employee data, financial information, or transaction information. Today, securing that information is not simply a good business practice, it is increasingly a mandate by a government order, such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR), or an industry standard, such as Payment Card Industry – Data Security Standards (PCI-DSS). Yet according to the Identity Theft Resource Center (ITRC), in the U.S. alone more than 1,400 data breaches occurred in 2019, resulting in the exposure of more than 164 million sensitive records and another 705 million non-sensitive records.[3]

The Sotero platform addresses four major areas of vulnerability that are underlying factors in data breaches:

1. Encryption doesn't protect data in use – Companies that encrypt their sensitive data often conclude their data is completely protected, but that is incorrect. Traditional encryption consists only of:

- disk encryption, which protects data only when it is at rest on the disk, and
- encrypted communication links, such as those powered by SSL and TSL encryption, which encrypt data only when it is in transit from one system to another.

While valuable, this encryption does not cover one of the major vulnerabilities that companies face today: an attacker obtaining unauthorized, direct access to the database. Access can be gained by several methods, including phishing attacks, misconfigured databases, or custom software programs that impersonate valid applications requesting data. Once a system is breached in this way, the attacker can write queries to access and/or steal all the underlying data. The database operating system will fetch the data from the disk, unencrypt the data and send query results back to the attacker in plain text.

Disk encryption also does not prevent unauthorized access from those that are charged with administering the database, whether those people are employees or third-party consultants. For example, encrypted data on the disk does not prevent a database administrator from querying the database to get unencrypted data and, thereby, reviewing or stealing data they do not need to access.

[3] Identity Theft Resource Center, 2019 End-of-Year Data Breach Report

[4] ibid.

"Encryption of data at rest provides little protection against intrusions in which a hacker gains remote privileged access to a running server in which the passphrase has already been entered."

– NOAM ARZT AND MICHAEL BERRY, HLN CONSULTING

As database products have matured they have begun to offer ways to better protect unauthorized access to data, such as Always Encrypted for Microsoft SQL Server and Transparent Data Encryption for Oracle. Even if such native tools were available for each and every SaaS application, IaaS product, and on-premise application or database, using disparate native solutions and replicating those solutions at each instance would make it unmanageable and risky for most companies.

2. Cloud applications and infrastructure often put your data at risk – As companies shift more of their sensitive data to the cloud, they introduce more potential cracks in their security program. Specifically, SaaS applications and IaaS that reside in a public cloud introduce the following vulnerabilities:

- Cloud providers require their customers to provide their own cybersecurity and do not enforce it, leaving cloud applications less protected, unless the organization has a highly sophisticated security management program.[5]
- Data in the cloud is accessible to the database administrators of the cloud applications or infrastructure via direct access to the database.
- If data in the cloud is encrypted by the cloud or application provider, the provider still holds the encryption keys and can access the data in the database.

3. Endpoints such as mobile applications, point of sale systems, and IoT devices may not be secure – Attacks often start at endpoints, such as workstations or printers, which are often left unsecured, and then proceed to backend servers that hold sensitive data. A recent survey of security professionals indicated that employee-owned mobile phones and laptops and IoT devices/sensors are susceptible to attack and are the least likely to be covered by security management programs. In that same survey, 28% of survey respondents confirmed that attackers had accessed endpoints.[6] Lack of control at endpoints enables attackers to access sensitive data, even if it is encrypted.

4. Endpoints such as mobile applications, point of sale systems, and IoT devices may not be secure – Anomaly detection systems have two limitations. First, they are usually deployed at the firewall or network level, not the data access level. This prevents them from detecting data requests that are benign at the access level but still malicious at the data level. Second, log file and user behavior analysis tools, such as Splunk, do not operate in real time. They can help organizations discover hacking/intrusion and unauthorized access as part of a forensic investigation, but they do not enable a company to interrupt and prevent unauthorized access in real-time.

[5] ibid.

[6] 2019 SANS Survey on Next-Generation Endpoint Risks and Protections, 2019

Sotero Leaves No Data Unsecured Throughout the Entire Data Life Cycle

The Sotero Data Protection Platform takes a new, holistic approach to data protection by securing the data itself, not just the application, database, or network in which it resides. This system has the following unique advantages over traditional security approaches:

1. All sensitive data is encrypted. All sensitive data, including all data fields in all applications, is secured with the platform's KeepEncrypt™ encryption component, which adheres to the AES-256 standard. This includes heterogeneous applications, such as ODBC, RDBMS, and JDBC databases, and applications deployed on your premises, in a private cloud, or in a public cloud.

2. Data is encrypted throughout the entire data life cycle (at rest, in transit, and in use). Because data in use is remains encrypted, even when a system breach occurs, data loss is prevented.

3. Access to unencrypted data is controlled. Role-based access controls allow you to control which users can see which data and specify data access at a granular (field) level. This protects data from unauthorized access even from database administrators at your company or at your cloud provider who have direct access to the system, but do not need to view the underlying data.

4. Governance is provided through a centralized, simple platform. The system allows you to manage data security for all your data stores from a single platform and using a single method. This simplifies and improves the success of a security management program.

5. Anomalies are detected and responded to in real time. The platform not only encrypts the underlying data, but analyzes data requests in real time and stops suspicious requests.

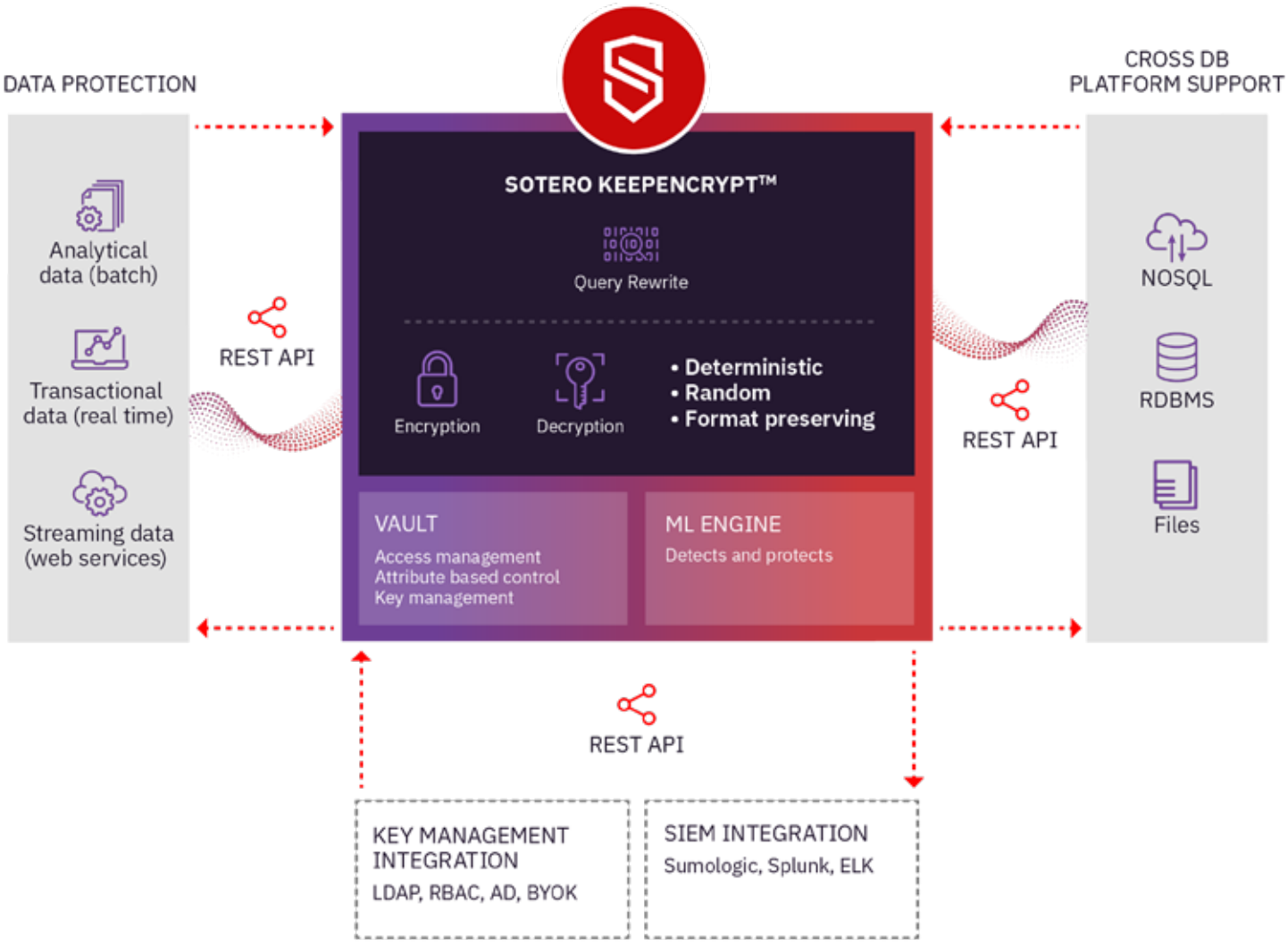
6. The Sotero platform complements existing security systems. The Sotero platform can work alongside your existing security information and event management (SIEM) systems, enhancing them with additional protections to reduce breaches and data loss.

How It Works

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

Sotero KeepEncrypt™, Vault and Machine Learning (ML) Engine

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



Sotero KeepEncrypt

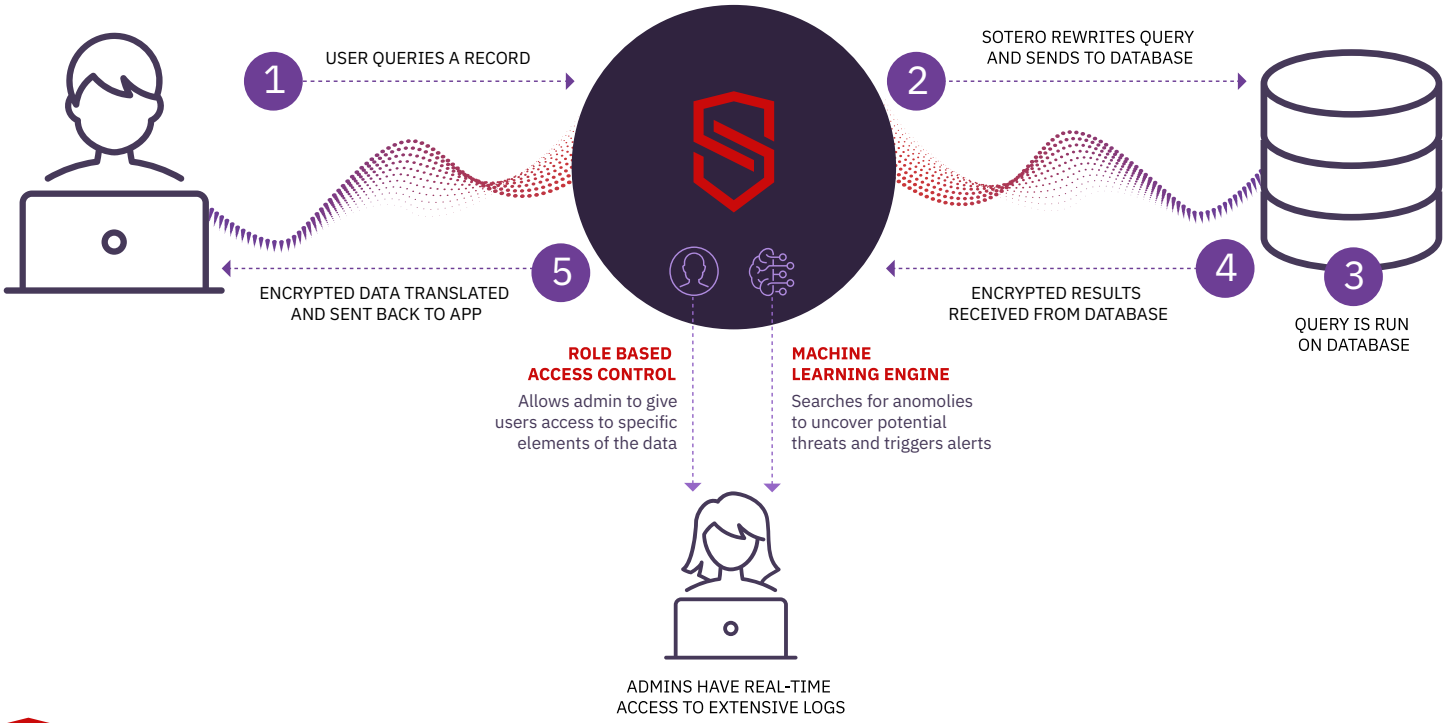
The **Sotero KeepEncrypt** component ensures that sensitive data is encrypted, even when in use by applications. It provides decrypted data for authorized queries from your application users. KeepEncrypt uses three levels of encryption: deterministic, random, and format-preserving.

Each Sotero customer has a dedicated KeepEncrypt component, 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 KeepEncrypt and applications and databases.

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

KeepEncrypt processes the query. For data requests, it fetches encrypted data from the database. KeepEncrypt 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, KeepEncrypt encrypts the new data, sends it to the database, and logs the data changes. Data flows between Sotero KeepEncrypt and the applications/databases in messages secured by SSL encryption.

Sotero Checks Access Privileges Before Responding to Application Queries



REST APIs give programmatic access to the components in the KeepEncrypt component, 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 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.

Sotero ML Engine

The **Sotero ML Engine** component 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.

"Sotero has found the solution [for the large effort needed to encrypt data, particularly cloud data] by building a product to do the hardest parts. Customers can now seamlessly encrypt data that remains encrypted during use for cloud use cases without the burden of spending countless development cycles. This technology is a game changer."

– ANDREW LANCE,
FOUNDER AND PRINCPAL –
SIDECHAIN SECURITY
(A CRYPTOGRAPHIC TECHNOLOGY
CONSULTANCY)

Advantages to Using Sotero

Sotero's multi-layered approach to data security empowers organizations to safely use, share, and monetize data. The Sotero approach to data security provides the following advantages to organizations compared to traditional security approaches:

- **Encrypted data in use** – Sotero closes a major security gap where attackers gain direct access to a data store and steal your data. Sensitive data accessed in this way would now be encrypted. Sotero covers data through the entire life cycle – at rest, in transit, and in use.
- **Universal deployment** – Sotero can be deployed on premises, in the cloud, in a VPC, or in a fully SaaS platform.
- **Encrypted and controlled cloud data** – Data stored in cloud-based SaaS applications or IaaS can be encrypted. Access to the data is controlled by you. With Sotero, you can confidently put sensitive data in the cloud.
- **Restricted data access for DBAs** – User privileges can prevent internal and external DBAs, including cloud administrators, from viewing unencrypted data. DBAs directly accessing the data store will see encrypted data.
- **Secure business collaboration** – Data shared with business partners, collaborators, and other enterprises can be encrypted and access rights limited to people with whom you want to share data.
- **Simplified and scalable security management** – Data in all your on-premise and cloud applications and data stores can be secured by Sotero. This gives you a single protection method and a centralized management platform, eliminating the need to deploy multiple native security products and allowing you to scale your security management program.
- **Instant detection and reaction to threats** – Even with encryption and controlled access, threats can come from internal actors or from attackers that gain access to system passwords. Sotero analyzes user behavior and responds in real time to stop suspicious behavior.
- **Improved data governance** – Sotero logs every query, allowing you to understand and better control your data usage.
- **Adherence to data privacy and security regulations** – The encryption and user access controls from Sotero help you to protect sensitive information, including PII, in accordance with regulations such as GDPR, HIPAA, CCPA, and PCI-DDS.
- **Reduced security product costs** – Sotero provides universal protection for all your data stores, eliminating the need to purchase encryption licenses for specific databases.

Deploying and Using Sotero's Data Protection Platform Is Simple, Seamless, and Scalable

The advantages of the Sotero platform are within reach of any organization that needs to secure sensitive information. The platform has the following characteristics that allow it to mesh seamlessly with existing infrastructures and business processes:

- **Simple deployment** – Sotero is deployed by installing the KeepEncrypt, Vault, and ML Engine components either on-premise, in a private cloud, or in the Sotero cloud. Then, using a graphical setup tool, Sotero KeepEncrypt is configured, including the communication links to applications/databases, encryption, and user/role privileges. Unlike other security products, there is no need to change the applications and no need to install additional agents on the network. When configuring the encryption, the setup tool will allow you to graphically select which tables and columns you would like to encrypt, select the encryption type (e.g., DET), and encrypt the data via a bulk encryption process. At the end of the encryption process, the sensitive data in the original database will be replaced with encrypted data. Deployment time depends on how much data is encrypted, but for most organizations the Sotero Data Protection Platform can be deployed in just a few hours.
- **Seamless operation** – Sotero is deployed and operated without disrupting your business. Applications are not changed in the deployment process so users do not need to change how they interact with those applications.
- **High performance** – Routing queries and data through Sotero KeepEncrypt adds a lag of 1-2% on overall roundtrips, but desired performance levels can be reached by simply adding extra Sotero processing nodes.
- **Scalable** – As your data scales, Sotero scales as well and does not require additional maintenance. For example, when sensitive data is added or updated through an application interface (e.g., sales person enters new prospect information into the CRM), Sotero automatically encrypts and stores the data without intervention from the administrator.
- **Reliable and resilient** – Sotero can be deployed in high resiliency configurations with failover and redundant systems to eliminate single points of failure for mission critical operations.

Who Benefits from Sotero's Approach?

Sotero benefits any company that collects, uses, and shares sensitive data, including PII data. By securing sensitive data, Sotero enables the business to operate with confidence, reduces the strain on the company's security team, and reduces the financial and brand risk of data breaches. This includes organizations such as:

- companies that house data in the cloud for broader use and analysis. Examples: online retailers, online banks, and online stock trading platforms.
- service providers/software providers that want to better secure their data, as well as use that superior security as a selling point for customers. Examples: SaaS providers, cloud infrastructure providers, and outsourced HR service providers.
- companies that need to comply with international data regulations while keeping data storage more streamlined. Examples: multinational financial services companies and online retailers with international customers.
- companies that share data or collaborate with suppliers and other business partners. Examples: contract research organizations in the pharmaceutical industry and manufacturers with international suppliers.

Real-World Results

Data Collaboration in Healthcare Research

Summary of use case

As part of testing a new drug, a pharmaceutical company collects patient data, including disease marker and PII data, from hospitals and sends the data to a contract research company for analysis. Sotero encrypts the sensitive data as it leaves the hospital or the research company. The research company completes the analysis without providing unnecessary access to sensitive data.

"As a cloud-based platform in healthcare, we know that 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

Compliance in Financial Services

Summary of use case

A financial services company located in Europe wants to move EU customer data to the U.S. for processing by a third party. To maintain compliance with the GDPR regulation, the data has to be encrypted. Sotero enables them to transports the data to the U.S. in encrypted form and perform queries in the database in the U.S. without violating GDPR. Sotero only allows people in the EU with appropriate privileges to view the unencrypted data.

"Our partnership with Sotero has allowed Axis to provide a complete GDPR solution for our clients. With Sotero, we can address production use cases and provide users with a consolidated reporting environment while allowing data sharing with external entities. We see Sotero as a solution for many previously challenging use cases in the future."

– MICHAEL LOGAN,
CEO – AXIS TECHNOLOGY, LLC

Differentiating Feature for Software Platforms

Summary of use case

A health benefits provider wants to use the services of a cloud-based healthcare analytics provider, but isn't comfortable sending claims data from their premises to the cloud for analysis. Sotero provides the healthcare analytics provider a secure data solution that assures the customer that its data will be protected. The benefits provider securely moves data from its on-premise system to the cloud so it can be analyzed. The health care analytics provider wins a new customer.

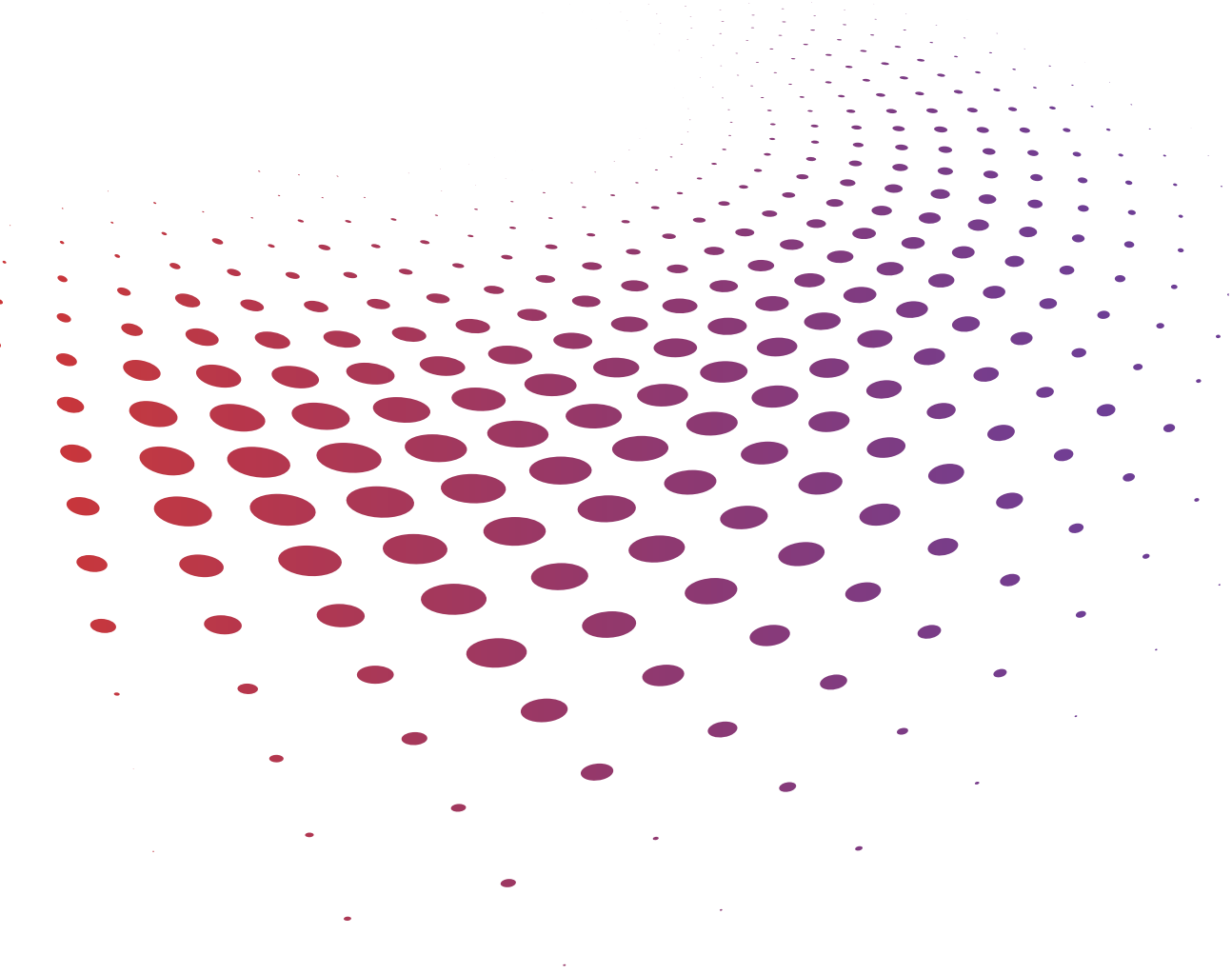
"Sotero enables me to provide my customers with data security and privacy. It helps in attracting new customers and frees me to focus my efforts on expanding my products and capabilities."

– RAVIKIRAN DHARMAVARAM,
CEO – EXAFLUENCE

Conclusion

By providing greater encryption capabilities, granular user/role access controls, and real-time anomaly detection, the Sotero Data Protection Platform is changing how security and product teams view their data. The platform's unique focus on increasing security of the data itself, including capabilities to protect data in use and data in cloud environments, is enabling businesses to operate more securely and with less risk should a breach occur. Sotero is giving its customers the confidence to use their data to the fullest, earn the trust of customers, and differentiate themselves from their competitors.

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