WHITE PAPER

Sotero Data-In-Use Encryption

Use and Share Data In Its Encrypted State with the Sotero Data Security Platform

Sotero

Keep data encrypted while it is at rest, in transit, and in use.

Key Takeaways

1. Traditional encryption protects data only when data is at rest (disk encryption) or in transit via secure communication methods such as SSL and TLS. These shortfalls leave companies with significant vulnerabilities when the data is in use by on-premise or cloud applications.
2. Sotero Data-In-Use Encryption takes a new approach that ensures that sensitive data is never left unsecured, regardless of lifecycle stage (at rest, in transit, or in use), and regardless of source or location (on premise, cloud, or hybrid).
3. Data-in-use encryption secures data, without requiring any modifications to applications, and the database or network in which the data resides.
4. Data in-use encryption is being employed by companies in industries with critical data protection requirements, such as financial services, banking, pharma, healthcare and others..
5. Companies that have employed data-in-use encryption have realized several benefits, including data monetization, secure collaboration and data sharing and reduced product development costs.

The Next Generation of Data Encryption

A breakthrough approach that ensures that sensitive data is always secure, wherever it resides.

Though encryption is the most effective way to reduce the probability of a security breach, traditional encryption carries a major hurdle – it protects data only when data is at rest (disk encryption) or in transit via secure communication methods such as SSL and TLS.1 These shortfalls leave companies with significant vulnerabilities when the data is in use by on-premise or cloud applications.

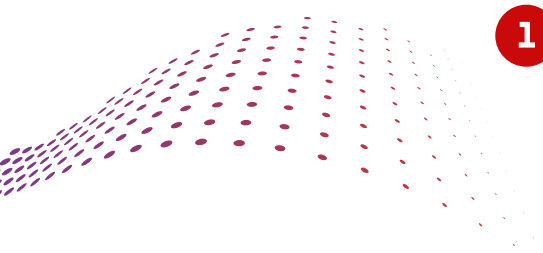
Additionally, as companies rely more heavily on cloud environments, they face even greater risks. By giving control of the data to cloud providers, organizations face significant vulnerabilities because the cloud providers may not encrypt data securely. Even when they do secure the data, cloud providers often have access to the data and the encryption keys.

The good news is the emergence of Sotero Data In-Use Encryption.

Data in-use encryption is a groundbreaking approach that ensures that sensitive data is never left unsecured, regardless of lifecycle stage (at rest, in transit, or in use), regardless of source, or location (on premise, cloud, or hybrid). These capabilities set in motion a new world for using, sharing, and monetizing data, securely and with confidence.

The Shortfalls Of Traditional Encryption

Although encryption offers a range of benefits, traditional encryption technologies still have several 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 that 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, these approaches do 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, 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.

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

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

2 Cloud infrastructure and applications often put 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 customers to provide their own cybersecurity and do not enforce it, leaving cloud applications vulnerable, unless the organization has a highly sophisticated security management program.[2]
- 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 back-end servers that hold sensitive data. Lack of control at endpoints enables attackers to access sensitive data, even if it is encrypted. 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.[3]

Now let's take a look at how In-Use Encryption eliminates these vulnerabilities.

[2] ibid
[3] 2019 SANS Survey on Next-Generation Endpoint Risks and Protections, 2019

Data-In-Use Encryption Eliminates These Vulnerabilities

Data-in-use encryption is an innovative, holistic approach that secures data throughout the entire data lifecycle by securing the data itself, not just the application, database, or network in which it resides.

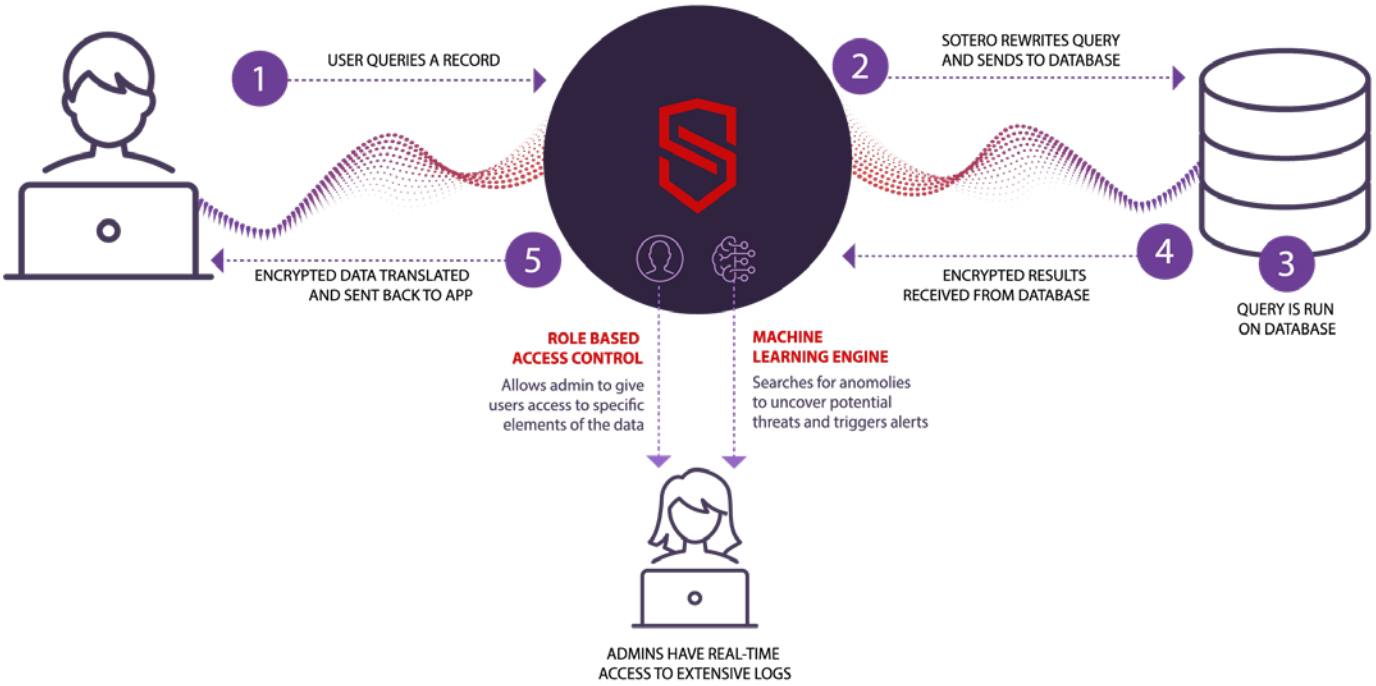
Data-in-use-encryption has the following unique advantages over traditional security approaches:

1. **All sensitive data is encrypted wherever it resides**, including all data fields in all applications, adhering to the AES-256 standard. This includes heterogeneous applications, such as ODBC, RDBMS, and JDBC databases, and applications deployed on premise, in a private cloud, or in a public cloud. Whether it is structured, semi-structured, or unstructured, data remains encrypted all the time, anywhere.

2. **Data is encrypted throughout the entire data life cycle** (at rest, in transit, and in use). Because data in use 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.

How In-Use Encryption Works



Software as a Service (SaaS) and Infrastructure as a Service (IaaS) solutions that reside in the public cloud typically introduce two key vulnerabilities.

- Cloud providers require their customers to provide their own cybersecurity for their data and do not enforce that security, leaving cloud applications much less protected unless the organization has a highly sophisticated security management program.
- Data in the cloud is accessible to the database administrators of the cloud applications or infrastructure via direct access to the database.

Modern data encryption solutions can fully protect your data from both intruders and your cloud service provider by encrypting all your sensitive data across the entire data lifecycle, ensuring that applications and partners interact only with encrypted data, and giving you control over the key.

Restricts Access to keys. The client/entity that generates and owns the data should keep the key so they are the only ones who can access the key. This means that cloud service providers or database administrators have no way to unlock the unencrypted data.

The Advantages Of In-Use Encryption

The multi-layered approach to data security employed by data-in-use encryption empowers organizations to safely use, share, and monetize data, leading to several advantages compared to traditional security approaches:

Employ Better Security

Data-in-use encryption eliminates a major security gap in which attackers gain direct access to a data store and steal your data. Sensitive data that is traditionally accessed in this manner is now encrypted through the entire lifecycle – at rest, in transit, and in use – and wherever it resides.

Encrypt And Control Cloud Data

Data stored in cloud-based SaaS applications or IaaS can now be encrypted, enabling you to store sensitive data in the cloud. Data security and access to the data is completely controlled by you.

Achieve Secure Business Collaboration

Your organization can securely share data with business partners, collaborators, and other enterprises. Data that you choose to share can be encrypted, and access rights can be limited to people with whom you want to share the data.

Adhere To Data Privacy And Security Regulations

The encryption and user access controls help you to protect sensitive information, including PII, in accordance with regulations such as GDPR, HIPAA, CCPA, and PCI-DDS.

Reduce Security Product Costs

In-Use Encryption provides universal protection for all your data stores, eliminating the need to purchase encryption licenses for specific databases.

Reduce development costs

You can now encrypt data for cloud use without the burden or spending countless development cycles.

Organizations Are Benefiting from Data-In-Use Encryption

Sotero Data-In-Use Encryption is used by companies today in industries with critical data protection requirements, such as financial services, banking, pharma, healthcare and others. Data-in-use encryption benefits any company that collects, uses, and shares sensitive data, including PII data:

- **Organizations that house data in the cloud** for broader use and analysis. Examples: online retailers, online banks, and online stock trading platforms.
- **Service and software providers** that wish to secure their data more effectively, 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 must comply with international data regulations** while keeping 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.

Where To Go From Here

The Sotero data security platform with data-in-use encryption is used by companies the world over to secure sensitive data throughout the data lifecycle, wherever that data resides. With the Sotero platform, businesses are operating with confidence that their sensitive data is secure, while reducing the strain on the company's security team, not to mention the financial and brand risk of data breaches.

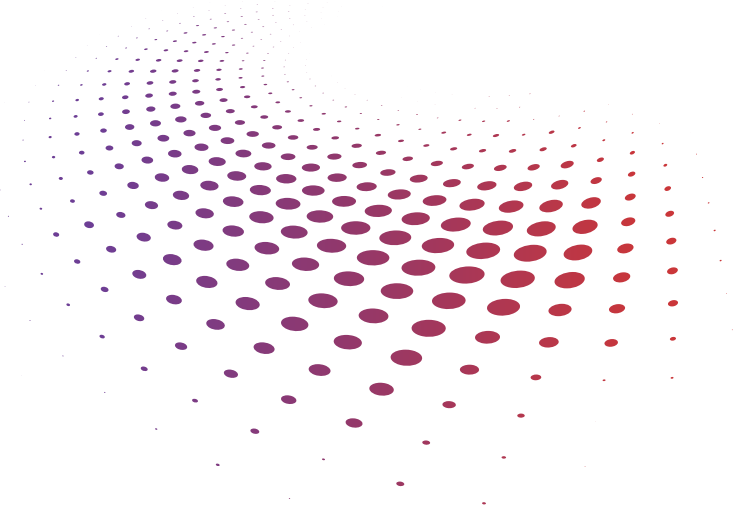
Click here to request information about the Sotero platform, or to schedule a product demo. https://info.soterosoft.com/contact-us

ABOUT SOTERO

Sotero is the global innovator and leader in revolutionary data security. Sotero's data security platform provides a single pane of glass that enables our customers with a way to protect data anytime, anywhere, regardless of data store, integration mechanisms, and user tools. The platform is able to control, access, operate, and use data to extract information that drives organizations' business outcomes and innovation.

Sotero provides organizations with a scalable and flexible data security fabric that migrates and moves data securely, in all its instances in an interconnected world. Organizations gain complete control over their data privacy, compliance, audibility and governance for use cases ranging from securing data at the edge, IoT devices and streaming data, and moving data securely to downstream systems.

→ Learn more at www.soterosoft.com



Sotero

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