WHITE PAPER

In-Use Encryption Technology

Next Generation Encryption That Enables Organizations To Use Data Securely In Its Encrypted State

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. In-Use Encryption is the next generation of encryption. It 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). In-Use Encryption secures data, without requiring any modifications to applications, and the database or network in which the data resides.

3. In-Use Encryption is used today by companies in industries with critical data protection requirements, such as financial services, banking, pharma, healthcare and others.

4. The advantages provided by In-Use Encryption enable organizations to safely collect, use, and share data, leading to several benefits for organizations.

5. Companies that have employed In-Use Encryption have realized several benefits, including data monetization, secure collaboration and reduced product development costs.

Encryption – The Next Generation

In-Use Encryption is the next generation of encryption. It takes a new approach that ensures that sensitive data is never left unsecured.

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 for companies is the emergence of In-Use Encryption.

In-Use Encryption is the next generation of encryption. It takes a new 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 come with 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]

4 Anomaly detection systems have limitations.

Anomaly detection systems have two limitations. First, they are usually deployed at the firewall or network level, rather than at 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.

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

In-Use Encryption Eliminates These Vulnerabilities

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. This advanced encryption technology is used today by companies in industries with critical data protection requirements, such as financial services, banking, pharma, healthcare and others.

In-Use Encryption has the following unique advantages over traditional security approaches:

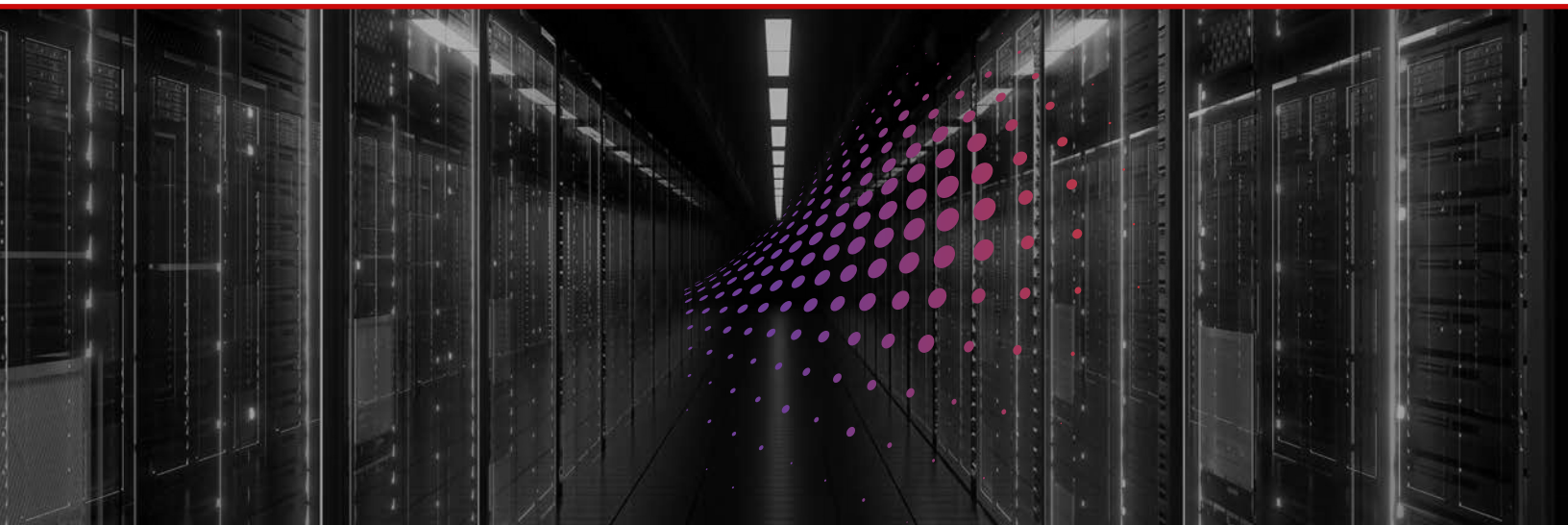
1. **All sensitive data is encrypted**, including all data fields in all applications, adhering to the AES-256 standard. This includes heterogeneous applications, such as ODBC, RDBMS, and JDBC databases, and applications deployed on premise, in a private cloud, or in a public cloud.

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.

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 uses a single method.

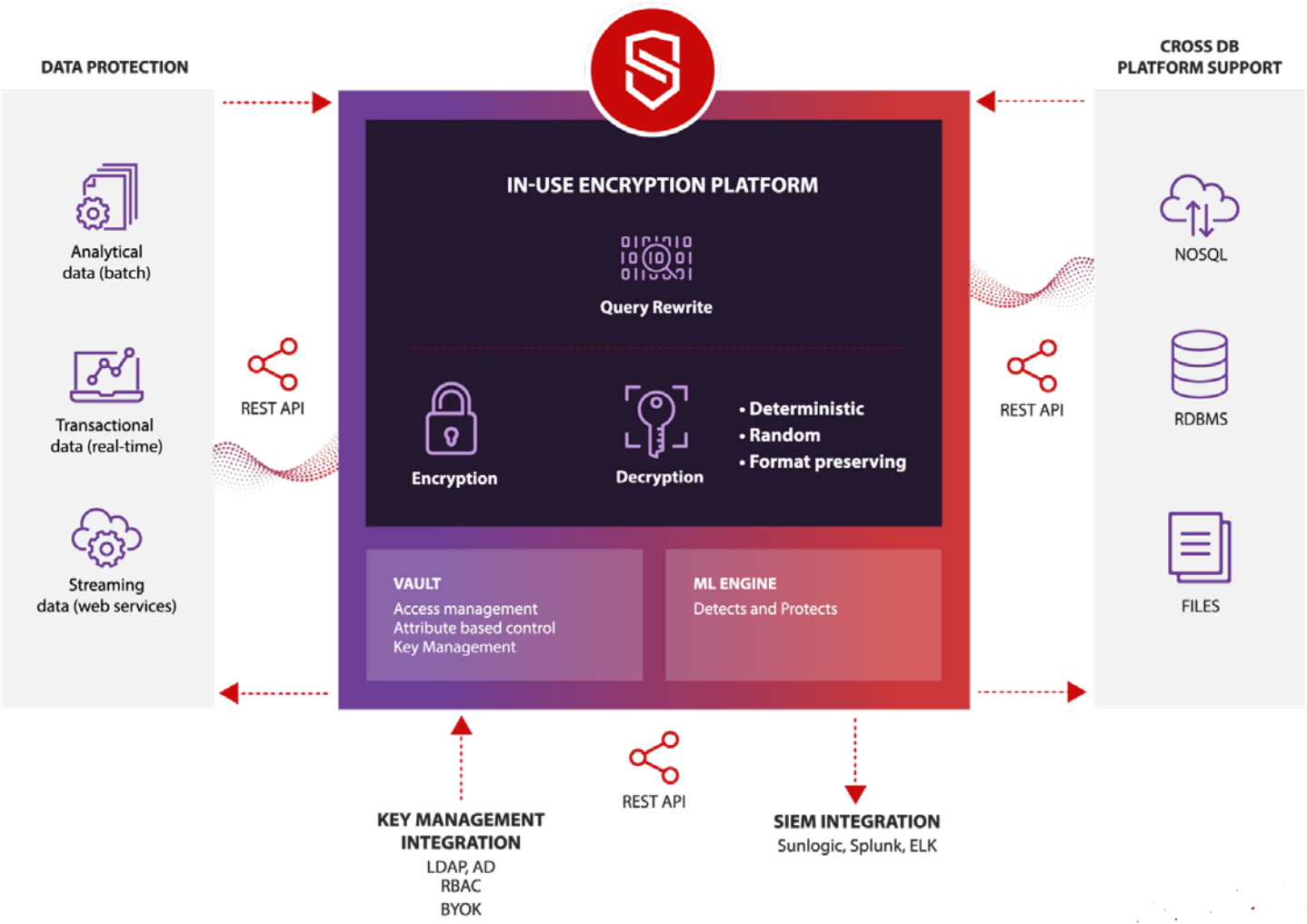
5. **Anomalies are detected and responded to in real time**. In-Use Encryption not only encrypts the underlying data, but analyzes data requests in real-time and blocks suspicious requests.



How In-Use Encryption Works

In-Use Encryption consists of three components:

1. Data Protection
2. Access Management
3. Breach Detection ML Engine



Whether the platform resides on premise or in the cloud, 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.

Data Protection Component

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

This component processes a query by fetching 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.

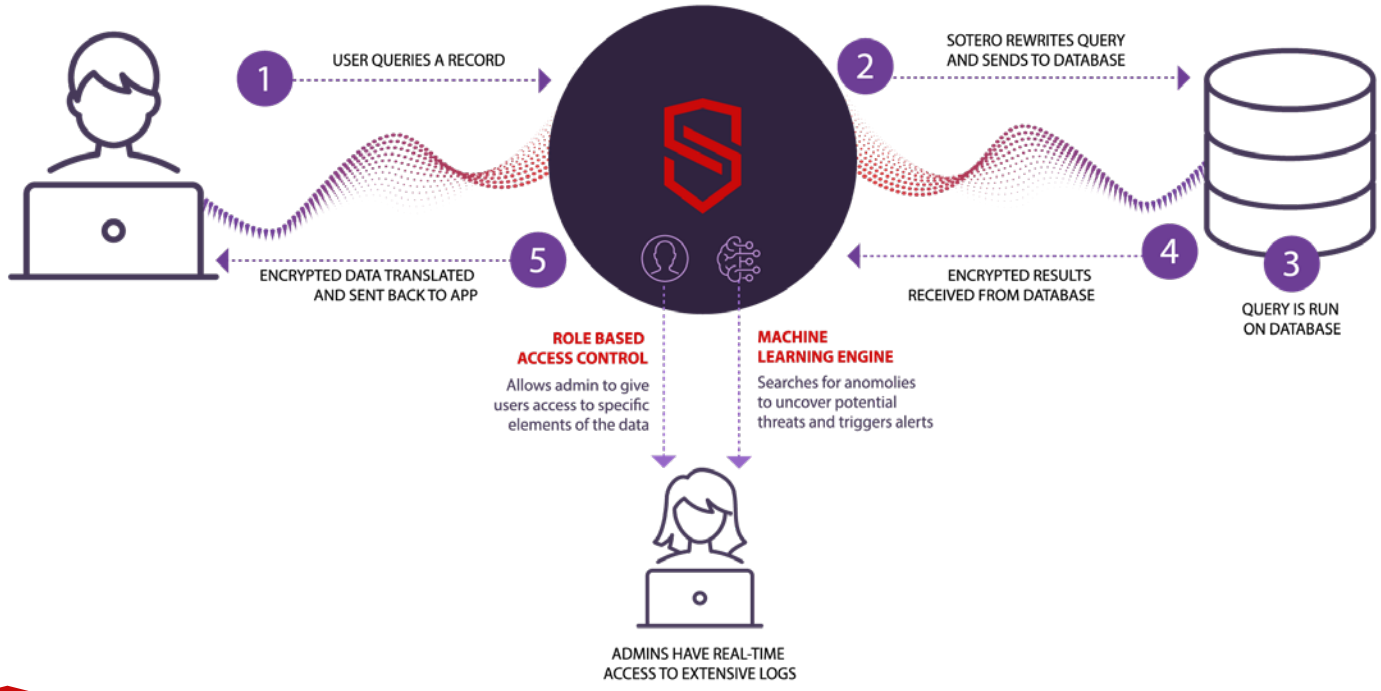
Access Management Component

This is a secure key management service that uses TLS access control and multiple layers of AES-256 keys to encrypt the data. It is essentially a vault that 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.

Breach Detection ML Engine

This component detects and protects 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.

HOW IN-USE ENCRYPTION WORKS



The Advantages Of In-Use Encryption

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

Encrypt Data In Use

This breakthrough capability closes a major security gap where 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 life cycle – at rest, in transit, and in use.

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. Access to the data is completely controlled by you.

Achieve Secure Business Collaboration

You 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.

Simplify And Scale Security Management

Data in all your on-premise and cloud applications and data stores is secure. 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 yoursecurity management program.

Detect And React To Threats In Real-Time

With traditional encryption and access control, threats can still come from internal actors or from attackers that gain access to system passwords. In-Use Encryption analyzes user behavior and responds in real time to identify and stop suspicious behavior.

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.

Companies That Benefit from In-Use Encryption

In-Use Encryption benefits any company that collects, uses, and shares sensitive data, including PII data:

- **Companies 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

As the pioneer in In-Use Encryption, Sotero's In-Use Encryption platform is 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 "in-use encryption," the next generation of encryption technology. Sotero's data security solutions are used by companies around the world to realize more value from their data by encrypting that data even when it is in use or in motion – regardless of location. This enables organizations to achieve faster time-to-value from their data for a range of mission-critical business use cases, from data analysis to data sharing to product development.

Sotero's data security solutions are used by mid-market to 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.

→ Learn more at www.soterosoft.com

Sotero

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