

Cloud Data Security

A Many organizations are reluctant to move data to the cloud due to several security vulnerabilities:

- Cloud providers require you to provide your own cybersecurity, they do not enforce your cybersecurity initiatives.
- Data in the cloud is accessible to database administrators of the cloud applications or infrastructure in plain text, leaving all your sensitive elements vulnerable.
- If data in the cloud is encrypted by the cloud or application provider, the cloud provider holds the encryption keys, again leaving a security gap.

Organizations are now able to eliminate these obstacles to leveraging the cloud with the Sotero data security platform. With Sotero, organizations are now completely in control of cloud data protection through these breakthrough capabilities:

- Data in motion encryption that secures data while in migration from legacy systems to the cloud.
- Cloud-native data security that keeps data encrypted at all times – even while it's being used.
- Encryption key management where only you, not the cloud services provider, own and has access to the encryption keys.

The Benefits

1. Data in motion encryption secures data while in transit to the cloud.
2. Cloud-native data security keeps data encrypted at all times – even while it's being used.
3. Encryption key management where only you, not the cloud services provider, own the encryption keys.



Data Analysis in Pharma and Healthcare

A lingering challenge for pharmaceutical and healthcare companies is the inability to make clinical trial data available securely to downstream systems in a timely manner for relevant analysis. This data is highly time-sensitive, therefore it's critical to move the data as quickly as possible. However, due to the strict security requirements of patient-level data, organizations are forced to transfer the data manually, which reduces the value of the data and delays the drug development cycle.

Pharma and healthcare organizations are overcoming this challenge with secure data sharing enabled by the Sotero data security platform. Sotero data in use encryption secures the data while it is in motion and in use. Role-based access controls ensure that only privileged users may access the data – those without access privileges only see encrypted data.

These capabilities now enable pharmaceutical and healthcare organizations to reap the benefits of sharing information among teams, while allowing for scalable cloud computing, and threat prevention analytics without sacrificing security. Organizations can quickly and easily integrate the Sotero platform into GxP regulated environments rather than enduring numerous testing and validation cycles.

The Benefits

1. Provide rapid access to data without the risk of exposing sensitive, patient-level information.
2. Meet the security and privacy requirements related to the storage and use of patient-level data in both production and downstream systems.
3. Accelerate the data's time-to-value from months to hours, powering faster development.
4. Organizations can quickly and easily integrate Sotero's technology into their GxP regulated environments rather than going through cycles of testing and validation.



Data at the Edge

As organizations are no longer restricted with having applications work through centralized data stores, but can instead move to a framework where data is located at the edge, there are a range of emerging security and privacy challenges. One of the major challenges is that traditional data security solutions protect data only when it is stored in a centralized location.

The Sotero data security platform employs an extensible data security fabric that protects data wherever it resides. With Sotero, organizations can now enable secure storage, use and analysis of data at the edge with limitless integrations, OS-independent libraries, a secure streaming network, and asymmetric keys for data/application pairs.

Sotero enables organizations to process high volumes of IoT data in a timely fashion at next to no latency by enabling a production framework that supports multi-petabyte analytic warehouses without impacting privacy at scale. The Sotero platform provides a secure data sharing model where multiple parties can co-mingle their data and operate analytics without either party having the need to decrypt the data.

The Benefits

1. Replace numerous security point solutions with a centralized platform for managing all data assets wherever they reside.
2. Protect data at its source, eliminating the need to migrate data to a centralized location, saving you time and money.
3. Focus on moving information and insights as opposed to moving data, because the data is secured at the source.



Data Compliance – GDPR, CASL, CCPA, PHI, PII, HIPAA

Whether you are looking to anonymize and securely store EU data in the U.S. while remaining GDPR compliant, or looking to ensure compliance with PHI, PII, or HIPAA, Sotero's data security platform ensures your data is secure and compliant – regardless of where it is located.

The Sotero platform provides an intelligent data security fabric that enables organizations to keep data encrypted throughout its lifecycle (in use, in transit, at rest) from one centralized platform. Your organization can now secure data from the moment that it is loaded into your platform, to the time that it's extracted out of that platform for additional use – without the data ever being exposed. Role-based access controls (RBAC) ensure that only those with privileges may access the data.

The Benefits

1. Keep data encrypted and secure at all times, regardless of where it is located.
2. Become, and remain, compliant by ensuring your data is secure literally anytime, anywhere.
3. Eliminate the need to deploy solutions in multiple geographic locations to keep data secure, to minimize development and support costs.



Ransomware Protection

To date, organizations have only been able to take a reactive approach to ransomware protection. With the Sotero data security platform, organizations can now take a proactive approach to protecting from ransomware attacks before they occur.

The Sotero data security platform provides two significant advances that enable organizations to detect and prevent cyber-attacks, ransomware attacks and other potentially malicious behavior.

1. Anomaly Detection at the Data Level

Anomaly detection solutions are typically deployed at the network or firewall level. This prevents threat actors from detecting data requests that appear non-threatening at the access level, but are malicious at the data level. It is data that we must protect first and foremost as it's often the most valuable asset of an organization.

The Sotero Platform provides anomaly detection at the data level, to protect the actual assets that are the targets of malicious actors – the data. Granular access settings enable you to allow or restrict access and choose selective encryption for fields, rows, or parts of a dataset. Even if an attacker is able to break into the network, he or she is likely unable to get past the data level.

2. Machine Learning

The Sotero platform employs a machine learning (ML) engine that recognizes and blocks intruders in real time, before unauthorized access is granted and a breach occurs. Pattern protection algorithms enable the system to continually learn with every signal or event.

The Benefits

1. Prevent external processes or threats from anyone without the right privileges having the ability to encrypt data.
2. Get real-time alerts of any malicious behavior while it is being stopped in its tracks.
3. Get point-in-time snapshots of your data assets in the case malicious activity is detected to recover data assets in the event a master file has been impacted.



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

Security Ecosystem Consolidation

IT security organizations continue to struggle with managing countless security point solutions and disparate management platforms. With the Sotero data security platform, organizations are no longer required to deploy multiple products to protect each data asset or storage platform.

The Sotero platform employs a technology agnostic data security fabric that replaces platform-specific data security products with one centralized data security fabric. Simply add an application or data asset to the fabric and it automatically inherits all of Sotero's data security capabilities without any code changes or customization. You get plug-and-play interoperability without the need to modify or customize your applications.

With Sotero, you can move from a fragmented, complex data security stack to one unified data security fabric that provides 360° management of your entire data security ecosystem. You're no longer forced to go to point solutions to know who is accessing your data. You get governance, auditability, visibility, and 100% control via a single pane. You are now empowered to manage your entire data security ecosystem through a centralized platform for a simpler, more cost-effective approach to data security.

The Benefits

1. Manage your entire data security ecosystem from a single pane of glass.
2. Eliminate the need to deploy multiple native security products.
3. Easily scale your security management program.



Third-Party Data Management

The ability to share data securely and rapidly is key to unlocking data's real value. Sharing data in a secure manner is no easy feat because there has been no means for organizations to keep data encrypted and secure while it is being shared with and used by third parties.

The Sotero data security platform is helping organizations overcome this barrier by enabling them to rapidly share sensitive data with downstream systems and third parties securely and at scale, to keep business moving forward.

The foundation to secure data sharing is Sotero's data in use encryption, a patented data security breakthrough 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 premise, in the cloud, or hybrid).

In addition, role-based access controls (RBAC) ensure that only privileged users may access the data – those without access privileges only see encrypted data.

The Sotero platform allows data to be co-mingled, matched, and shared without the need to send plain text data into an environment. In addition, high volume, multi-tenancy data can be processed quickly and with ease with unprecedented high performance.

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, enabling innovation and faster time-to-value from data while reducing an organization's business unit cycles.

The Benefits

1. Share sensitive data securely with vendors, downstream systems, and internal collaborators.
2. Acquire and retain customers, by being able to meet their strict data security requirements.
3. Improve speed and efficiency of mission-critical use cases as that were previously stalled by manual data workflows.



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