TECH BRIEF

Sotero Ransomware Protection

Securing all data from attacks

Ransomware Challenges

"Year over year, ransomware attacks increased by 13 percent, a jump greater than the past five years combined." (Verizon 2022 Data Breach Investigations Report). While this eye-popping fact is shocking, ransomware's increase isn't nearly as disturbing as its evolution.

Even as businesses evolved, so too have cybercriminals. Attackers are no longer satisfied with holding system functionality hostage. They have discovered that the data they once locked away on encrypted systems is an organization's most valuable asset. As a result, new sinister variations of ransomware attacks emerged.

Exfiltrating the data from target systems allows attackers to leverage its value by holding the data itself hostage in return for ransom. This increases the risk of data and intellectual property loss exponentially, combined with a ransomware attack's accompanying system outages and operational challenges.

Attackers are savvy enough to understand that organizations are often more willing to pay a ransom to keep attackers from making their sensitive data publicly available due to fines, penalties, and reputation loss. Now more than ever, it makes sense to focus the protection on the target. That target is your data.

What started with attackers compromising systems and locking them in an encrypted and unusable state until the victim met their ransom demands has morphed into a corporate enterprise with products, profit sharing, subscriptions, and technical support.

Evolving ransomware threats target end-user endpoints and shared storage, amplifying the impact of attacks well beyond a single user or narrow scope of systems. With organizations adopting the cloud en masse, sensitive data is rapidly moving outside of traditional perimeters. This places more high-value data at risk than ever before.

Ransomware Costs

Every 11 seconds, a new ransomware attack occurs, and with over 714 million ransomware attempted attacks in 2021, it's clear that the question is not if you will face a ransomware threat but when. Savvy businesses know this is a ticking timebomb, and being proactive is the best cyber defense. Ransomware attacks cost on average $5.3 million, and unprepared businesses lose around $8,500 per hour due to ransomware-induced downtime.

With so much on the line, how can organizations afford not to defend against ransomware proactively? How will your organization deal with ransomware threats against your cloud and on-premises infrastructure?

Legacy Solutions Miss the Mark

Existing ransomware prevention technology falls into either antivirus, endpoint detection, or endpoint detection and response solutions. Coupled with this, many vendors offer ransomware attack recovery and remediation services. These types of solutions detect a ransomware attack through a signature-based approach. However, this method does not guarantee that malware encrypting the disk will not result in some data loss. Instead, it broadly protects against all malware concerns.

Sotero

Sotero's Unique Approach

Sotero takes a different approach, utilizing a pattern or behavior-based detection. Using this approach, Sotero protects organizations against malware based on behavior such as disk and file access, not whether it has been seen before. Our patented technology and advanced machine learning (ML) capabilities allow us to look at patterns at the disk level, identifying threats as they develop. This approach prevents data theft and the corresponding extortion that follows. Sotero's approach is part of a comprehensive organizational disaster mitigation plan as it does not protect endpoints. Pattern-based recognition of ransomware attacks protects data while isolating the attack before it can spread.

Sotero ransomware protection covers your organization against all aspects of the ransomware attack process. It prevents your shared data from being encrypted and ensures that it cannot be stolen and used against you at a later time.

Sotero ransomware protection extends the existing protections granted by the Sotero Data Security Fabric. With Sotero, your organization can defend its data throughout its entire lifecycle, at rest, in transit, and in use.

Sotero ransomware protection places your organization in control of protecting your data. With complete ownership of encryption keys, your organization can ensure total privacy, even if the external hosting is compromised.

Sotero quickly and efficiently integrates into existing and on-premises infrastructure as a cloud-native solution. This design allows organizations to rapidly implement and protect their entire organization, eliminating lengthy onboarding processes of other data protection solutions.

- Extends ransomware protection into the cloud
- Protects data at scale without degradation of performance
- Defense against ransomware data theft
- Seamless integration with existing cloud deployments
- Active monitoring of ransomware attacks to protect data before it is compromised
- Provides in-depth visibility for administrators into file utilization and modification
- Layers over existing encryption solutions, taking advantage of the proprietary machine learning model to rapidly identify patterns

Ransomware Protection Features / Benefits

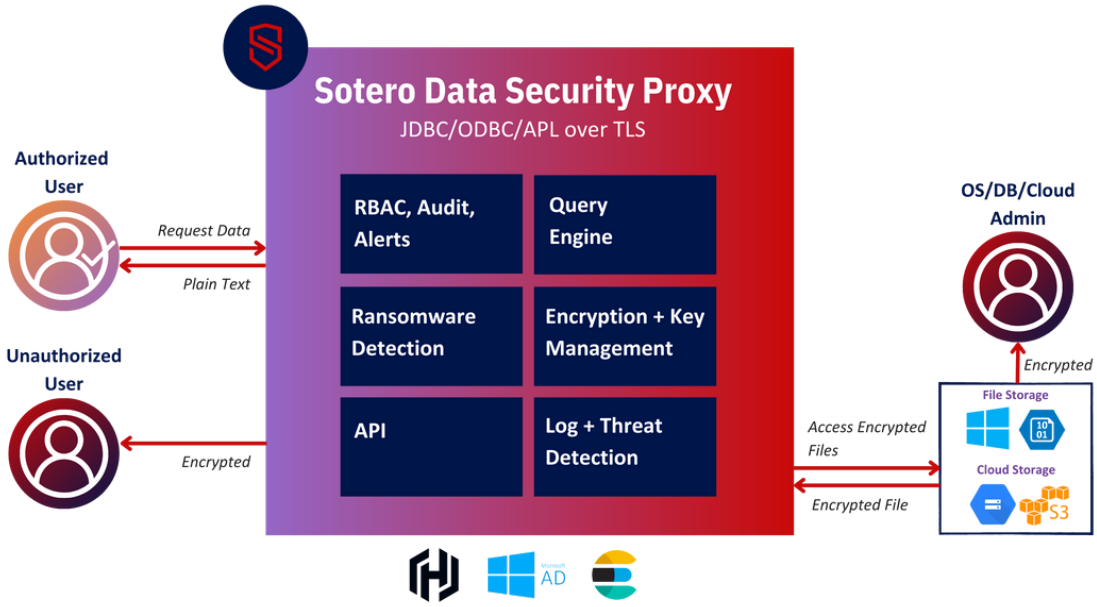
1. No impact on end-user experience
2. Stores files in their encrypted form on the backend file server
3. Enforces RBAC and allows only privileged users to view the file contents in their encrypted form
4. Real-time detection using ML models to immediately block a ransomware attack and notifies stakeholders - thereby minimizing damage and risk
5. Ability to detect and isolate an attack as it starts to keep it from infecting the rest of the organization
6. In-depth visibility with ransomware view exposing IP where the attacker originated, user, and list of impacted files for immediate, targeted recovery
7. Integrates with
    a. Existing SIEMs
    b. Enterprise DLAP systems

Sotero

Sotero's File Protection

Sotero's ransomware is a part of Sotero's File Protection, which is a scalable platform offering:

- Network share/cloud storage protection
  - Protects critical data stored on network file shares and cloud storage using encryption
  - Enforces role-based access privileges. Only privileged users can view the file contents in their decrypted state
  - Logs all user activity by exposing it through an audit dashboard
  - Delivers full lifecycle encryption – at rest, in transit, and in use



Architecture

The Sotero architecture allows organizations to rapidly onboard the Sotero Ransomware Solution. Sotero Ransomware solution is designed with a Cloud-first approach to integrate into existing infrastructure seamlessly.

Sotero architecture leverages containerization to streamline implementation. All application components are dockerized, and all docker images are published onto the docker hub.

With Sotero, organizations can be fully operating in a matter of days rather than weeks.

Step-By-Step Walkthrough

Sotero's Data Protection sits between client devices and their cloud storage. It analyzes all file access and modifications made to the storage.

Using advanced ML analytics, Sotero checks for ransomware indicators such as disk utilization in real-time. This information goes beyond traditional signature-based solutions as it allows the detection of Zero-day ransomware.

Once ransomware or any malicious activity has been detected, alerts are issued to interested stakeholders allowing further escalation and investigation into the incident.

Sotero tracks in-depth information on all access requests to fuel machine learning models and increase algorithmic accuracy. Using the Ransomware View, teams can investigate incidents to determine the full scope of an infection — based on IP address, user information, and all affected files.

Using this information, investigators can track back to the source of the infection to eradicate all traces of the malware from the infected endpoint, preventing future infections.

About Sotero

Sotero is the global innovator and leader in revolutionary data security. As a cloud-native ransomware protection-as-a-service platform, Sotero protects ALL cloud data types, applications, and stores from catastrophic cyber attacks. Sotero protects your data in the cloud with no costly, time-consuming deployment or downtime. Advanced encryption and real-time machine learning techniques allow organizations to solve for insider and outsider threats while meeting compliance requirements with actionable audit logs. The platform enables fast deployments that enable data to be shared securely and used with confidence. With point and click set-up, Sotero's data security platform is easy to deploy and manage with no impact on user experience. Organizations can now be protected in a matter of days, not weeks or months.

Schedule a demo today to learn more.

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