USE CASE

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.

Sotero

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