HOW LEPIDE IS HELPING PREVENT RANSOMWARE

Our client is a hospital based in the USA. We have happily accommodated their request for anonymity.

CASE STUDY

DISCOVERY

WINDOWS

The Company were overly-reliant on Windows Event Logs which meant a lack of visibility over user behavior.

VISIBILTY

The Company had no ability to detect the symptoms of a ransomware attack should the worst happen.

RESPONSE

The Company had no way to automate their threat response in the event of a ransomware attack.

ACTION

DEPLOYMENT

The Company chose to deploy Lepide Data Security platform and undergo a complimentary risk assessment.

VISIBILTY

The Lepide support team did all the heavy lifting configuring the solution to the Company's exact requirements.

RESPONSE

Lepide set up the solution with the required reports, threat models, and dashboards configured to detect and responds to ransomware.

OUTCOME

Lepide were able to provide the Company with complete visibility of en-masse encryption events, deviations in user behavior, permissions escalation and more. Lepide helped the Company to deploy threat models to automatically detect and react to ransomware attacks in progress on their File Servers and in their M365 hybrid environment. Lepide were able to demonstrate a reduced risk of ransomware attacks by identifying and addressing misconfigurations, open shares, stale data and inactive users.

Launch Interactive Demo