



HOW LEPIDE IS HELPING PREVENT INSIDER THREATS

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

CASE STUDY

DISCOVERY

DETECTION

The Company had no ability to detect the symptoms of an insider threat due to lack of visibility.

RESPONSE

The Company had no way to automate the response in the event of an insider threat being detected.

NOISE

The Company had a lack of visibility over user behavior due to an over-reliance on noisy Windows Event Logs.

ACTION

DEPLOYMENT

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

SUPPORT

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

ALIGNMENT

Lepide set up the solution with the required reports, threat models, and dashboards configured for insider threats.

OUTCOME

Lepide enabled the Company to get complete visibility of en-masse encryption events, deviations in user behavior, permissions escalation and more. Lepide helped to deploy threat models that would automatically detect and react to the symptom of an insider threat. Lepide also helped the Company to reduce the risk of insider threats by identifying and addressing misconfigurations, open shares, stale data and inactive users. As a result, the Company chose to become a customer of Lepide, and with ongoing support, are able to demonstrate a reduced risk of insider threats.

[Launch Interactive Demo](#)