Lepide

Datasheet

NYDFS

NYDFS

The NYDFS Cybersecurity Regulation is “designed to promote the protection of customer information as well as the information technology systems of regulated entities.” What this essentially amounts to, is a requirement for a risk assessment to be conducted and used to implement a proactive and sophisticated security strategy. Security strategies should be set up in three stages; detection, prevention and response.

The NYDFS Cybersecurity Regulation focuses on financial services companies in the State of New York. Covered entities include but are not limited to banks, insurance companies, mortgage brokers, lenders and credit unions. There are some notable exceptions to the covered entities. If your company has fewer than 10 employees, turns over less than $5,000,000 in gross annual revenue or ahs less than $10,000,000 in year-end total assets, then you may be exempt.

How Lepide Helps

Implementing a Cybersecurity Program (Section 500.02)

Lepide can help you develop a data protection program that focuses on protecting PII within your environment. Using Lepide, you can identify and classify PII, determine who has access to it (and spot excessive permissions), analyze user behavior and report and alert on anomalies/ threats.

Generate an Audit Trail (Section 500.06)

Lepide provides users with a single platform to manage risk and implement data protection strategies. Built in reports enable you to search through an audit trail of events to investigate breaches. These reports provide key audit data, including who, what, when and where information, in an easy-to-read format.

Data Access Governance (Section 500.07)

With Lepide, you can identify which users have access to PII so that you can maintain appropriate access rights. Ongoing analysis helps you to spot changes to permissions that may affect your least privilege position. You can even spot which users have excessive permissions so that you can revoke them.

Run Regular Risk Assessments (Section (500.09)

The Lepide Risk Assessment dashboard gives you an overview of the critical areas of risk in your environment. Information on the amount of PII you store, who has access to it and what users are doing with it is all displayed on one intuitive dashboard. Lepide can also provide a completely free, turnkey risk assessment report that highlights current active threats in your critical environment.

Monitoring Data interactions and Incident Response (Sections 500.14 and 500.16)

Lepide actively monitors user behavior, including file copies, deletes, moves, renames, modifications and more. Unusual or unwanted modifications can trigger a real time alert to ensure the CISO has visibility over current threats. Lepide can also help you respond to active threats in your organization by automatically triggering a script on alert. Scripts can be used to stop a ransomware attack, isolate a particular user or server and mitigate the damages of an attack in process.