Lepide

Mapping the Lepide Data Security Platform to **NIST 800-171**

NIST 800-171

The NIST Framework Core is essentially a list of activities that you should be undertaking to improve your cybersecurity posture, organized into categories. The way the Core is written is using inclusive, non-technical language designed to be communicated easily across departments.

It's broken down into five main functions, each of which we will go through here in a bit of detail to give you an idea of how you can apply them to your cybersecurity strategy.

Identify Where Sensitive Data is and Who Privileged Users Are

First thing you need to do is to determine where your biggest areas of risk are. These areas of risk generally come down to your most sensitive data and your privileges users. Identify where your data containing personally identifiable information, financial information, corporate secrets and other sensitive content resides. This may require the use of a data discovery and classification tool or, if you are reliant on Windows File Server, you may be able to do this through the native File Classification Infrastructure.

Once you have determined where sensitive data is, you should know which users and groups have access to it. It would also be wise to identify any factors in your environment that could be putting your data at risk, such as large numbers of stale users creating a large potential attack surface.

Protect Your Sensitive Data by Being Proactive

Take the first steps to improving your data security based on the identification phase. Limit access to your most sensitive data by adopting a policy of least privilege. Review all of the privileged users you identified; do all of them need elevated access rights?

If you have identified open shares take steps to remove them. If you identified a large number of users with passwords set to never expire, then ensure you revise your policy on password rotation. If you identified a large number of inactive users, take steps to reduce them if possible. There are many proactive steps you can take to improve your data security simply based on the identification function of the NIST Framework.

Detect Anomalous User Behavior

Once you have started being proactive, this function is all about keeping up a continuous effort to detect unusual activity surrounding your data. Many user and entity behavior analytics solutions provide a feature known as anomaly spotting where, using a predefined learning period, they determine what is normal behavior and alert on abnormal activity.

You should also be able to detect when changes to permissions occur that could affect your most sensitive data. Make sure that you maintain that policy of least privilege by identifying and reversing unnecessary or unwanted permission changes.

If you are able to identify and receive real time alerts on whenever a suspicious change occurs to a file containing sensitive data or the surrounding permissions, you are well placed to deal with a potential security threat. To do this, you should define an incident response plan that details the exact steps you should take should you detect something that requires action.

Respond to Suspicious Changes

If you have created a detailed incident response plan, as stated in the previous Function, then you should be well placed to quickly respond to any potentially harmful changes. This response may be to revoke privileges, shut down a computer or server or simply reverse an unwanted change to a file or folder.

Recover and Learn

Have a plan in place to recover should the worst happen. Importantly, this Function focuses mainly on learning how to improve your overall cybersecurity posture and inter-departmental communication by taking lessons from security incidents. Data security is an ongoing, continuous and constantly evolving process that requires constant vigilance from all departments.

Mapping Lepide to NIST 800-171

Key Activity	Control Text	Technology Alignment
Access Control	3.1.1 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). 3.1.2 - Limit information system access to the types of transactions and functions that authorized users are permitted to execute. 3.1.3 - Control the flow of CUI in accordance with approved authorizations. 3.1.4 - Separate the duties of individuals to reduce the risk of malevolent activity without collusion. 3.1.5 - Employ the principle of least privilege, including for specific security functions and privileged accounts. 3.1.6 - Use non-privileged accounts or roles when accessing non-security functions. 3.1.7 - Prevent non-privileged users from executing privileged functions and audit the execution of such functions. 3.1.12 - Monitor and control remote access sessions. 3.1.22 - Control information posted or processed on publicly accessible information systems. 3.8.2 - Limit access to CUI on information system media to authorized users.“	Lepide Identify (Data Discovery and Classification) Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics)
Logging, Monitoring and Alerting	3.3.1 - Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. 3.3.2 - Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Key Activity	HIPAA Specific Control Area	Technology Alignment
Logging, Monitoring and Alerting (continued)	3.3.4 - Alert in the event of an audit process failure. 3.3.5 - Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. 3.3.6 - Provide audit reduction and report generation to support on-demand analysis and reporting. 3.3.9 - Limit management of audit functionality to a subset of privileged users. 3.14.1 - Identify, report, and correct information and information system flaws in a timely manner. 3.14.3 - Monitor information system security alerts and advisories and take appropriate actions in response. 3.14.7 - Identify unauthorized use of the information system Protect audit information and audit tools from unauthorized access, modification, and deletion..	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Systems Security	3.4.3 - Track, review, approve/disapprove, and audit changes to information systems. 3.4.6 - Employ the principle of least functionality by configuring the information system to provide only essential capabilities. 3.13.2 - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. 3.13.3 - Separate user functionality from information system management functionality. 3.13.4 - Prevent unauthorized and unintended information transfer via shared system resources. Mark media with necessary CUI markings and distribution limitations.	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Key Activity	HIPAA Specific Control Area	Technology Alignment
Incident Response	3.6.2 - Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Risk Analysis and Management	3.11.1 - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI. 3.12.3 - Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Lepide Identify (Data Discovery and Classification) Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Lepide Data Security Platform

Core Capabilities

Lepide Identify

(Data Discovery and Classification)

- Discover and classify data in real-time.
- Tag data.
- Data valuation.
- Identify data most at risk.

Lepide Trust

(Access Governance)

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Change permissions.

Lepide Insight

(User and Entity Behavior Analytics)

- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

Lepide Detect

(Threat Detection and Response)

- Detect threats in real-time.
- Baseline/profile employee behaviour.
- Identify anomalous employee behaviour.
- Alert and respond to threats in real-time.

Start a free trial

Get a demo

Get a free risk assessment