

Hybrid Data Management Solutions



What is NewEvol Data Lake?

A next-gen data storage and analytics cybersecurity tool that is scalable, secure, and cost-effective. Designed to store large amounts of raw data in its native format – structured, semi-structured, & unstructured data, NewEvol Data Lake can collect and analyse petabytes of data with unbelievably fast processing time. This platform can retain your data without any limitations on volume and makes it easy to access the data for monitoring or threat hunting purposes.

WHY NEWEVOL DATA LAKE?

- > Store data at scale and gain data privacy
- > Quicker threat detection
- > More economical data analytics
- > Infinite Scalability: Expand architecture easily
- > Customize report as per need

KEY FEATURES

- > No data limit: can handle petabytes of data
- > Universal data ingestion
- > Highly scalable, centralized log storage
- > Guided search heads for query

KEY BENEFITS

- > Ingest all types of data without any limitations on the data types
- > Natural language querying for better and easy understanding of Analysts
- > Smooth scalability of architecture without any downtime or data loss

Store Data at Scale, Gain Privacy & Data Visibility

NO DATA LIMIT

NewEvol Data Lake is Hadoop-based architecture. NewEvol doesn't have a data cap or data limit. By retaining historical data in a distributed file system, the NewEvol Security Data Lake is an economical way to perform analytics without having to worry about the data volume as it can handle petabytes of data with incredibly fast processing time.

VERSATILE DATA INGESTION

You can ingest all types of data as there's no limitation on the data types. NewEvol is capable of handling all kinds of data types such as JSON, XML, PCAP, Syslog, and more. With multiple data ingestion types, NewEvol provides flexibility to the customers facing difficulties in the ingestion of unique types of logs.

HIGHLY SCALABLE

Built on Hadoop-based cluster architecture, NewEvol data lake provides easy and faster scalability of architecture without any downtime required as well as zero data loss, enabling customers to expand architecture without any trouble.

CONTACT US



1 Parklane Blvd, STE 729 E,
Dearborn, MI 48126



+1 (325) 515-4107



info@newevol.io



LOG COLLECTION



VISUALIZATION



REAL-TIME ANALYTICS

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

How It Works?

NewEvol Data Lake works in three phases

LOG COLLECTION & STORAGE

The process starts from log collection layer. In log collection layer, NewEvol collector collects logs from various devices. The collected logs are correlated and then sent to the centralized repository with 70% compression. In this data repository, data can be retained for years and makes analysts work easy to visualize & analyze data in depth.

DATA VISUALIZATION

Once the events get correlated, these data can be visualized on the NewEvol dashboards. From this console, Analyst can monitor the threat events captured on the pre-built dashboards. Users can also create a custom dashboard as per the need.

DATA ANALYTICS

Lastly, based on the detected threats, NewEvol data lake allows analysts to run analytics on threats to have in depth visualization of the alerts.

Infrastructure Requirement

The minimum hardware requirement to deploy the NewEvol platform is mentioned below. The hardware sizing may differ as per requirement.

SERVER	CORE	RAM	HDD	OS
Namenode 1	8	16 GB	500 GB	Ubuntu 16.04
Namenode 2	8	16 GB	500 GB	Ubuntu 16.04
Datanode	32	256 GB	2 TB	Ubuntu 16.04