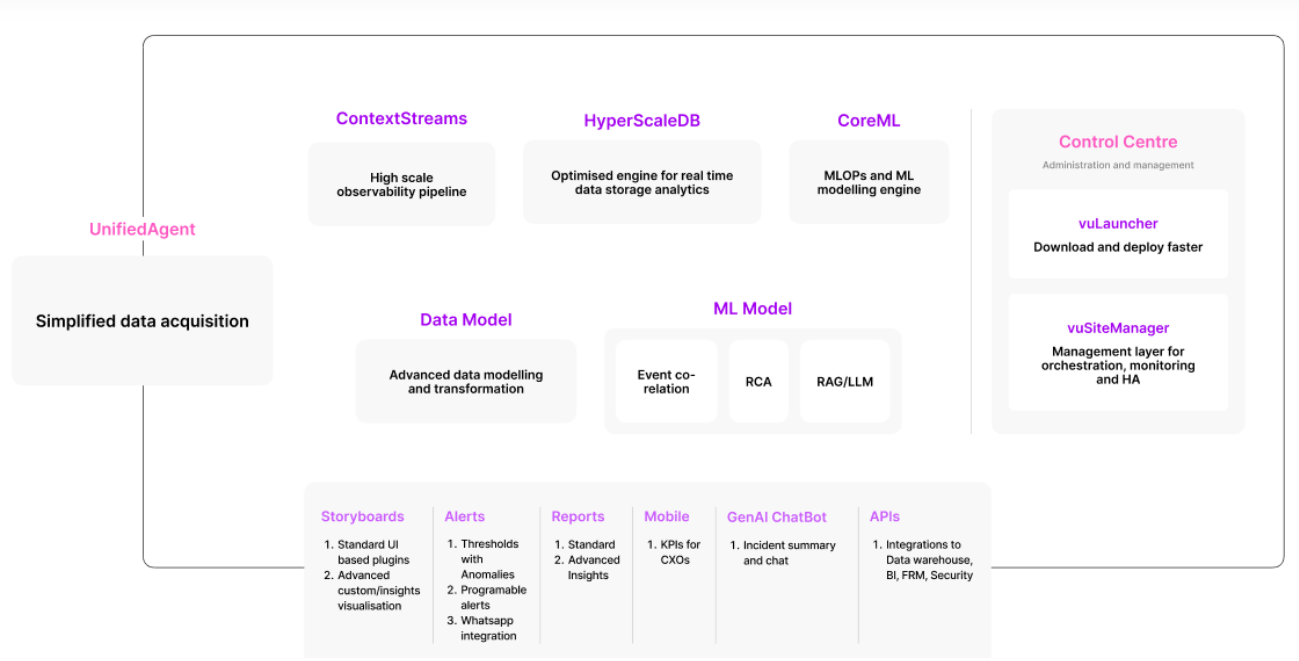
vuSmartMaps™

Log Analytics and Data Lake Functional Features

vuSmartMaps™ – Introduction

vuSmartMaps™ has been built ground up as a highly extensible Big Data /ML based platform that connects user experience, business transactions, infrastructure, and IT operations. The figure below shows the high-level view including the roadmap features:



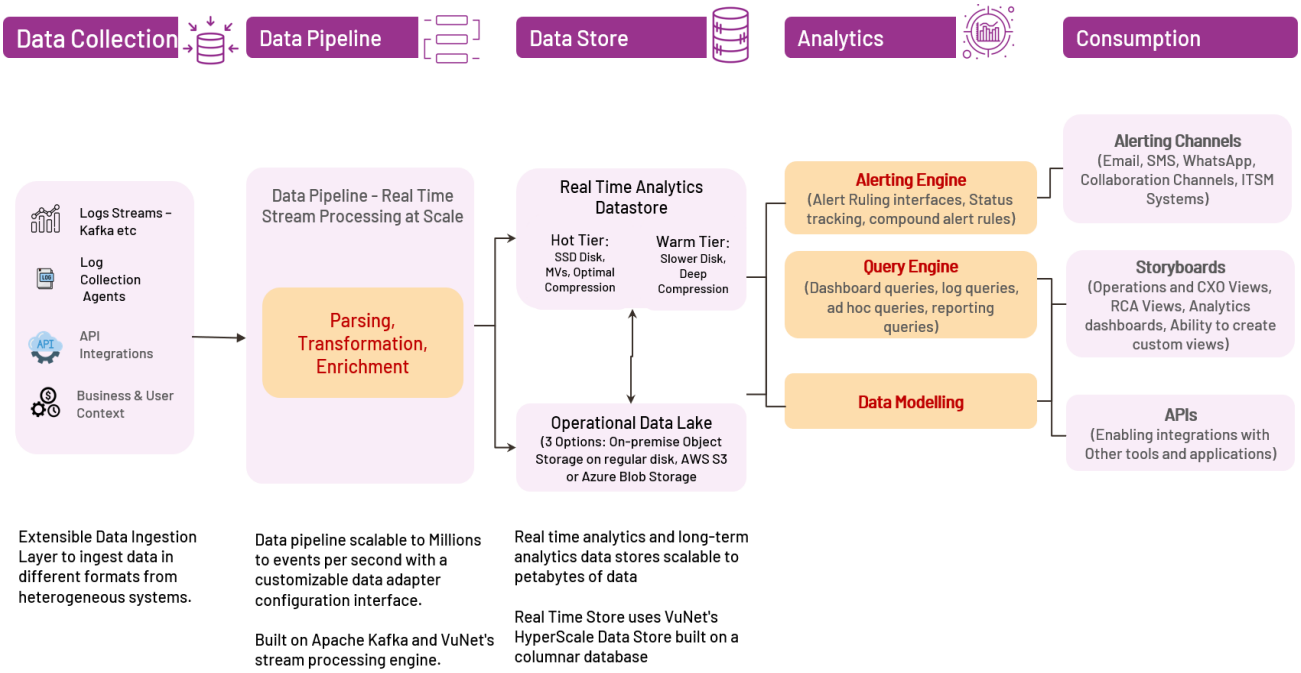
Key capabilities of vuSmartMaps™ for Observability are as follows:

- **Observability Pipeline for Ingestion, Handling, Enrichments and Routing** – vuSmartMaps ™ can ingest structured and unstructured data, events, metrics, and logs from many different data sources through its ContextStream Data pipeline. It natively supports 400+ data sources. vuSmartMapsTM collects performance data (Golden Signals) from all the touchpoints (Network, Server, Middleware, Application, Database, Storage) in the IT infrastructure. The ingested data is enriched, transformed and through the underlying transaction schema, made available for computation and visualization in the Data Model.
- **Hyperscale Data Store** – Data management layer based on composite architecture of columnar database supporting handling of large-scale data efficiently and effectively. Designed to meet the unique real analytics requirements of businesses, this data store framework enables optimized storage and sophisticated real-time data modeling and handling.

- **Data & Machine Learning Operations Layer** - All the ingested data is correlated, transformed, and enriched using vuMVA™ as a Multi-Vector Array. The data is stored in its proprietary Hyperscale data store which is also used to create an operational data lake. This enables creation of various machine learning and data analytics use cases including anomaly detection and user experience & application performance index.
- **Visualization Layer** – Pre-defined and canned storyboards and CXO dashboards that address the needs of executives and operations teams. Ability to customize and craft new storyboards, define role-based access and views.
- **Unified Visibility Across Distributed Deployment** – Platform supports ingestion, processing of data in each instance along with role-based access for users in each country, it also supports a common view across the instances.

Data Architecture

The following diagram provides an overview of vuLogX's architecture for log analytics. vuLogX is designed to handle high-scale log data ingestion, real-time processing, and advanced analytics, offering teams powerful insights into system and application logs. This architecture, structured into data collection, pipeline processing, storage, analytics, and consumption layers, supports the seamless flow of log data from diverse sources to actionable insights, ensuring organizations can monitor and troubleshoot efficiently across their infrastructure.



Functional Features

A detailed listing of features against the product modules and scope is summarized below –

vuSmartMaps ™ Core Central Platform	• Big Data cluster configuration and central platform – aggregation, correlation and visualization engine • Data pipeline and ingestion capability from diverse data sources, common data schema, data enrichment capabilities and alerting engine. • Integration to ITSM • Role Based Access • Reports
vuLogX – Log Aggregation and Analytics	• Ability to perform live searches, queries, and dashboard operations on the logs. • Additionally summarized metrics for KPIs, trends, patterns, and analytics • Capability for free text searches in logs to locate matching entries, view and download with searches conducted over specified time periods. • Availability of additional optional filters for refined searches, such as API, Transaction Type etc. • Ability to extract deeper fields of interest on transactions for business and operational KPIs

The detailed feature listing is provided below:

#	Feature	Description
1	**Data Ingestion**	
1.1	Source Integrations with IT components suing	Ingests data from multiple sources including network devices, applications, and databases.

	syslog, TCP, UDP Protocols	
1.2	Source Integrations with varied deployment workloads	Supports ingestion from diverse sources from on-premises or cloud (e.g., IoT devices, cloud platforms, hybrid workloads).
1.3	Data Formats	Supports a wide variety of log formats and protocols (e.g., JSON, Syslog, CSV, XML)
1.4	Device and App Support	Handles numerous data formats and protocols to accommodate diverse devices such as payment switch, ATM switch, Core Banking applications etc. without intrusive monitoring
1.5	Domain protocols	Supports various vertical (E.g. Banking) protocol logs for versatile data collection and analysis.
1.6	Agent /Agent Less based log collection	Includes features like secure transmission channels and data encryption, adhering to compliance standards.
1.7	No data loss	Capable of handling errors autonomously and can recover from operational failures without data loss.
1.8	Seamless Data Collection from New Devices	The Solution should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.
1.9	Source Integrations with IT components suing syslog, TCP, UDP Protocols	Ingests data from multiple sources including network devices, applications, and databases.
2	**Data Cleansing**	
2.1	Real-time/Dynamic Data Processing	Real-time data parsing and normalization for structured querying and analysis.

2.2	Enrichment & Contextualization	Enrich the ingested logs at real-time for further analysis. Customizable data enrichment during ingestion, enabling the addition of computed fields, tagging, and categorization to enhance log data context and relevance.
2.3	Data Deduplication	Implements deduplication processes to filter out redundant log entries and ensure that only unique and relevant data is stored, enhancing storage efficiency and data accuracy.
2.4	Log Reduction	Solution should support removing unnecessary log lines to reduce the overall size of the log at source or during processing.
3	**Data Storage**	
3.1	High Availability	Ensures zero message loss post ingestion and handles high-volume logging without performance degradation.
3.2	High Scalability	Supports horizontal scalability of data pipeline ensuring data integrity and continuous operation.
3.3	Configurable retention periods	Configurable retention policies enabling data lifecycle management from hot to cold storage based on age, size, or priority.
3.4	Security	Industry-standard encryption protocols for securing data at rest and in transit.
3.5	Data Compression (75%-85%)	Utilizes data compression techniques to reduce the size of log data, which helps in optimizing storage space and improving data retrieval times.
3.6	Object Storage Integration	Integrates with cold storage solutions such as Amazon S3to manage and archive older log data efficiently, optimizing cost and ensuring long-term retention of less frequently accessed logs.

4	Data Analysis	
4.1	Searching	Robust full-text search capabilities across stored data for quick incident response and root cause analysis.
4.2	VuNet Query Language Support	Ability to create easy and complex query using Standard Query Language for custom analysis
4.3	Pattern based Search	Powerful pattern-based search capabilities across all stored data for comprehensive log analysis and compliance reporting.
4.4	Data Derivation	Offers flexible and powerful data transformation capabilities for transforming raw data into actionable insights.
4.5	Pre-built Analytics	Provides several pre-built analytics (E.g. Frequently occurring errors, peak traffic hours) to derive operational insights and business intelligence.
4.6	Live Log	Provides live log monitoring to view log data as it is collected for immediate visibility into incoming logs.
4.7	Adjacent Logs	Enables users to expand their analysis by including log lines adjacent to those of interest for a broader understanding.
4.8	Creation of Log Clusters	Enables users to Choose multiple log tables at the same time and help them identify patterns, trends that helps them to troubleshoot faster.
4.9	Searching	Robust full-text search capabilities across stored data for quick incident response and root cause analysis.
5	**Data Reporting**	
5.1	Geo Map based Reporting & Visualization	Provides pre-built dashboards and customizable visualizations tailored for IT operations, support teams, and executive stakeholders.
5.2	Custom Reports	Unified query application for custom reports for both real-time and historical data analysis.
5.3	Report Exporting	Options to export reports in PDF, Excel and CSV

5.4	Reporting Formats	Seamless integration with reporting, alerts, and visualization tools for generating insights through pre-built dashboards and customizable visualizations for consistency and ease of use.
5.5	Role Based Access Control	Rich visualization tools including pre-built dashboards and customizable reports for various personas.
5.6	Notification via integration	Seamless integration into ITSM for alerting or collaboration channels for faster response.
5.7	Alert Notifications	Capable of sending alerts through emails, Slack channels, SMS, WhatsApp, and MS Teams
5.8	Automated Report Scheduling	Enables users to configure and automate the scheduling of reports, ensuring that reports are generated and delivered at specified intervals without manual effort.
5.9	Log-based Comparative Alerts using Anomaly Detection	Utilizes advanced algorithms and machine learning to identify unusual patterns and deviations in log data. This feature helps in proactively detecting potential issues or anomalies that require attention.
6	**Data Retention**	
6.1	Data Retention	Log retention is configured based on the pricing plans: Standard plans offer a 7-day retention period, while Enterprise and Pro plans provide longer retention periods.
6.2	Logs Archival	Logs older than the retention period based on event timestamps are automatically removed, and users can archive logs for extended retention.
6.3	Report Frequency & Retention	Configurable retention policies enabling data lifecycle management from hot to warm to cold storage based on age, size, or priority.

6.4	Log Rehydration from Object Storage	A process that allows organizations to retrieve and restore archived logs from long-term storage solutions, such as object storage, back into an active state for analysis and investigation. This feature is particularly valuable in scenarios where log data has been archived to reduce storage costs but needs to be accessed later for troubleshooting, compliance, or audit purposes.
6.5	Store logs for up to seven years in an active, hydrated, and enriched state.	This feature allows you to store logs for up to seven years in a state that is both active and enriched. Unlike traditional archival methods, where data is moved to cold storage and becomes less accessible, this feature keeps logs readily available ("hydrated") for immediate querying and analysis. Additionally, logs are enriched with relevant metadata and contextual information to enhance their usability over time
7	**Data Security**	
7.1	Domain protocols	Supports various banking protocol logs for versatile data collection and analysis.
7.2	Agent based log collection	Includes features like secure transmission channels and data encryption, adhering to compliance standards.
7.3	No data loss	Capable of handling errors autonomously and can recover from operational failures without data loss.
7.4	Logs obfuscation	Security practice is used to hide or mask sensitive information within logs before they are stored or transmitted. This process ensures that any potentially sensitive data, such as personal information, passwords, API keys, or other confidential details, is not exposed in log files, which could be accessed by unauthorized individuals.

7.5	Domain protocols	Supports various banking protocol logs for versatile data collection and analysis.
8	**Additional Functionalities**	
8.1	User Access Management	Provides robust features for managing user roles and permissions, ensuring that access to log data and analytics tools is controlled according to organizational policies and user needs.
8.2	API Access	Offers comprehensive API access for integrating with external systems, enabling programmatic access to log data, analytics, and reporting functions to support custom applications and automation.
8.3	Support	Provides a range of support options including technical assistance, troubleshooting, and problem resolution through various channels such as email, chat, and phone.
8.4	Log Forwarding	The Solution should support the sending of raw logs to third party products
8.5	Correlation of Logs with Telemetry	Correlation of logs with telemetry in Log Analytics provides a unified view of system behavior by linking log data with real-time telemetry metrics. This feature accelerates root cause analysis, enhances system visibility, and enables proactive issue detection.
9	**Integrations**	
9.1	Cloud based Integrations	AWS, Azure, Apache Cloudstack, Google Cloud, Salesforce Instantly ship and visualize logs from Amazon, Microsoft Azure, Google Cloud Platform, and other cloud-native technologies with out-of-the-box support for common data sources, enabling rapid deployment and insights within minutes.

9.2	Security Integrations	Cisco, Checkpoint, Palo Alto, Symantec, Juniper, Fortinet
9.3	Open Source Tools	Integrate with tools such as Fluentd, Fluent Bit, and Logstash
10	**Compliance**	
10.1	Audit compliance	Detailed logging of all data accesses and changes to support forensic investigations and compliance audits.