


## Compliant by the speed of light

Telecom Data Retention solution xDR





The story for telecom operators and Internet service providers is known: they are requested to retain call and internet records, email logs and subscriber data for a period between twelve months to 3 years. They have to respond promptly to authorized inquiries by law enforcement agencies without undue delay and report the retained data. Meaning, that they need to make an additional investment in support systems that enable them to comply with these data retention laws.

Clearly, it is not sufficient to simply extend the retention period of billing records as the laws and regulations require additional details and demand strongest data protection. Depending on the size and type of operator, we're discussing millions to billions of records to be retained every day and operators must be prepared to respond to hundreds to thousands of inquiries per day.

At Uni Systems, we decided to address these needs and challenges with the introduction of a purpose-built solution for telecom data retention: our **xDR Data Retention Solution**. This system is based on the technology of the world-leading centralized logging and analytics platform, the Elasticsearch engine, combined with Uni Systems' great experience and expertise in the SIEM domain and telco data retention systems.

## The challenges

- Store millions to billions of records per day of data collected from various sources in the network;
- Serve hundreds to thousands of inquiries by law enforcement agencies per day;
- Respond to authorized requests without undue delay;
- Apply high security standards to protect sensitive subscriber data and details about the inquiries;
- Be prepared for network evolution and service changes.

## The solution

Uni Systems xDR Data Retention has been designed to enable fast and secure access to retained data by authorized agencies. It enables network operators and Internet service providers to easily comply with recent telecom regulations for data retention.

Key features:

- Collects communications data (CDR, IPDR) and correlates subscriber and location based data from any telecommunications network;
- Retains large amounts of data in a powerful and secure data base;
- Provides very fast search and analytics in billions of data records;
- Automates request processing and reports search results;
- Enforce policies using layered security features to prevent unauthorized access, or altering the data by ensuring data immutability;
- Support concurrent search requests which are limited only by the available hardware resources;
- Provides a secure search REST API for spawning search requests either from the GUI, CLI or Web Browser.

## The benefits

**Cost-efficiency | Reliability**

**Search speed | Role based access control**

Extreme flexibility for loading and reporting against xDR data, as complete programs written in any programming language can be used during data ingestions or/and during data reporting accordingly, to allow integrations, correlations with external systems and business logic additions. The core of the solution is Elasticsearch an open-source, RESTful, distributed search and analytics engine, categorized by Gartner as SIEM alternative with proven indexing and searching performance.

## Seamless System Integration

Rather than replacing existing equipment, Uni Systems xDR has been optimized for seamless integration with existing data retention infrastructures, thereby, enabling business continuity during infrastructure migration.

There are three main subsystems that do the job seamlessly:

### Collection Subsystem

Data generated by networks nodes can be loaded into Uni Systems xDR internal database at a very high speed, while the system simultaneously supports multiple xDR sources. The collection engine forms a data pipeline where the output of each processing element is the input of the next one.

### Reporting Subsystem

Reporting subsystem is based on UniCase GUI as well as a number of business reports that utilize solution's search REST API.

### Storing Subsystem

Storing subsystem uses a structure called an inverted index, which is designed to allow very fast full-text searches. It is distributed by design and is built to scale. For xDR time data analytics use case, time-based indices and a tiered architecture with 3 different types of nodes (Master, Hot-Node and Warm-Node), are used.

## Other Features

### MONITORING

- Enables easily monitoring of all the solution components.
- Support monitoring through throttling the collection agents.

### ALERTING

- Identify changes in sensitive data.
- Pick from many alerting options with built-in integrations.
- Stores a complete history of all alert executions for easy tracking.

### ADMINISTRATION

- Visualize and explore raw data from authorized users for admin and debugging purposes.

### ACCESS CONTROL

- Give access to the right people and protect from unauthorized users and unintentional modification.
- Grant the IT/Ops team the ability to monitor infrastructure health without being able to see or modify the data. Alternatively, give a specific team read-only access to specific data, but deny access to other data.
- With support for multitenancy, you can grant users access to specific databases.

### ENCRYPTION

- Protect data - credit card numbers, email addresses, accounts - as it travels within the infrastructure.
- With SSL/TLS encryption, node-to-node, HTTP, and transport client traffic are secured. IP filtering also prevents unapproved hosts from joining or communicating with the infrastructure.
- If encryption is required at rest, then transparent disk encryption at the OS level can be optionally applied.

### AUDITING

- The audit log features allows easily maintenance of a complete record of all system and user activity. Filter of the activity is permitted to only the logs needed or all of the activity.
- It allows staying compliant with internal security policies and regulations like HIPAA, PCI DSS, FIS-MA, ISO, and GDPR. Logging the audit data back to the solution for easy searching and analyzing later is also available.

## Why Uni Systems

Uni Systems is a long-standing strategic partner to financial institutions, public organizations, telecom operators, enterprises and institutions in the European region, providing integrated solutions and value added services. The Company's portfolio of solutions includes comprehensive network consulting services based on the expertise and know-how of its highly skilled network engineers and an overall team of 800+ IT professionals, who can assist you to utilize and expand your network infrastructure and accelerate your business value.

