Regulatory Data Retention

Data logging to comply with telecommunication regulations

REGULATORY DATA RETENTION BENEFITS

- Minimizes storage costs with surgical data collection

- Creates structured data format for selection and storage based on contextually aware attributes

- Expedites locating specific data by filtering on specific database attributes

- Prevents unauthorized access to Personally Identifiable Information (PII) via obfuscation

MARKET OVERVIEW

Telecommunications regulators are defining data retention guidelines to ensure the safety and security of national infrastructure, requiring network operators around the world to retain specific customer data.

For safety, security, and law enforcement purposes, application-specific traffic data may be required to be logged and stored in the operator's big data system and made available if law enforcement departments acquire warrants. These regulations pose a number of challenges for operators, including storing only required data, minimizing overall the storage needs, securing the data, and extracting only the mandated data.

Traditional retention solutions struggle with the visibility required to retain only the required data and cause operators to invest in large storage for data that does not comply with the regulations. Many solutions also struggle with the scalability and flexibility to be able to grow with increasing demand and change with the regulatory landscape.

SOLUTION OVERVIEW

Sandvine's Regulatory Data Retention solution combines industry-leading network intelligence, unmatched granularity, and policy-enriched contextual awareness to deliver fine-grained control for data retention.

This fine-grained control minimizes the amount of mandatory data stored by the operator, reducing the storage cost and overhead for compliance with data retention regulations, while the correct data is captured.

The ANI Classification Engine uses machine learning and a frequently updated signature library to ensure accuracy for encrypted traffic. It also has the ability for operators to design custom signatures for regional-specific or niche applications.

Contextual Awareness

Data is stored with surgical precision to save storage and bandwidth cost, while simultaneously adhering to regulations. Specifically, data records can be enriched to include subscriber identification, application, location, service plan, and many other attributes that simplify the selection of data during a data retention request from law enforcement.

Logging and Real-Time Feeds

Statistics can be gathered on traffic passed, blocked, limited, or dropped, including volume, number of call attempts, quality of experience, and many other metrics that provide a closed-loop analysis of regulatory compliance.
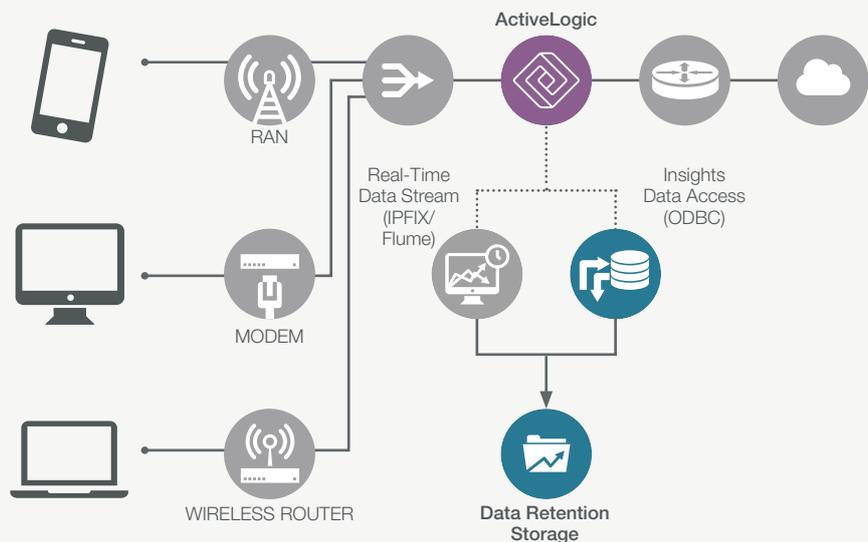
This data is:

• Fed in real-time, using industry standard formats like IPFIX or Flume, to data storage systems for archival and usage

• Collected from anywhere in the network – at the edge of the network, in the core, or at the peering point, depending on the goal of the data collection

• Accessed with the proper warrant information through a mediation portal

Sandvine's Regulatory Data Retention solution adheres to any regulatory requirement regarding capturing and storing data. Operators can confidently comply, with fine-grained accuracy and minimal storage costs.

Figure 1

Regulatory Data Retention Deployment

ActiveLogic

RAN

Real-Time Data Stream (IPFIX/ Flume)

Insights Data Access (ODBC)

MODEM

WIRELESS ROUTER

Data Retention Storage

SANDVINE

USA	EUROPE	CANADA	ASIA
2055 Junction Avenue	Svärdfiskgatan 4	408 Albert Street,	RMZ Ecoworld,
Suite Number 105	432 40 Varberg,	Waterloo,	Building-1, Ground Floor,
San Jose,	Halland	Ontario N2L 3V3,	East Wing Devarabeesanahalli,
CA, 95131	Sweden	Canada	Bellandur, Outer Ring Road,
USA	T. +46 340.48 38 00	T. +1 519.880.2600	Bangalore 560103, India
			T. +91 80677.43333

SANDVINE.COM