opentext™ | Cybersecurity

Product Flyer

Scaling Big Data Security for Telcos

Telecommunications service providers (Telcos) capture massive volumes of data that can provide valuable insights to better serve customers, improve products and optimize operations. But keeping sensitive data secure and private for use in analytics is a major challenge. Using data at scale while lowering risk requires protection that scales with the data.

"We had vast amounts of data with standalone implementations of security across pockets of data environments. So the problem was, "how do we scale security at a speed to support the growth of the business?" Taking that challenge and converting it to opportunity, is where SecureData came in. We want to drive security from a business POV; create a roadmap for the business to use data freely across the enterprise–we all know the data is protected so the business can use and share data as needed. We've doubled our size in a few years and transformed the industry."

Head of Applications and Data Security
Mobile Operator

While value creation from data lakes is increasingly in demand, adoption barriers include reliable security and data governance, with fear of privacy breach from data exposure in Hadoop and analytics applications. More data sources, and user and application access, increase risk that discourages potential business opportunities.

Data Is the Center of the Telecom Business and Where Value Is Created

With massive volumes of messages and data records pouring in around the clock, telecommunications service providers (telcos) are implementing data lakes to capture real-time traffic combined with historic data.

Telcos are streaming, feeding, and storing sensitive data including IMEI, IMSI, tower data, and CPNI that must be protected. For example, a network of 100 million customers may generate more than 35 billion CDRs (Call Detail Records) per day[1], which if compromised, can lead to loss of customer confidence and regulatory penalties. There is much at stake if no clear data protection strategy is in place.

The value of mining big data analytics combined with extreme data growth is driving data lake adoption. Competition is tightening in the telco sector, with commoditization of traditional services and disruption from over-the-top (OTT) players. Margins and revenues per user are falling for some companies.[2] Knowing precisely where to offer new services, promotions, and network upgrades for greater speed and throughput is essential to customer retention and competitive advantage. Big data technologies such as Hadoop, Teradata, and Vertica enable insights to optimize the business and customer service, and improve network operations and performance.

Locked-Down Data Protection vs. Open Usability of Data

There's a potential organizational conflict between creating new value with open access to data vs. securing data in a locked-down, unusable mode. Hadoop insecurity combined with high data sensitivity concerns may constrain access to data lakes to keep telcos from using big data to its full potential when risk is assessed by security and compliance teams.

By design, a data lake is hard to secure. Hadoop poses many unique challenges—including the automatic replication of data across a highly distributed environment. More data sources, user and application access, data sharing and processing, all increase the risk of data loss through insider theft, data mishandling, or the weak security of a third party partner during collaboration.

1. Source: **www.rcrwireless.com/20141014/big-data-analytics/telco-case-study-vodafone-argyle-data-tag6**
2. Source: **www.strategyand.pwc.com/trend/2017-telecommunications-industry-trends**

There are traditional IT security controls that should be put in place, such as perimeter protection, and monitoring user and network activity. But system-centric controls are unreliable, even impractical, given the need for data access and use across the extended enterprise. The drive for insights and a return on investment cannot be achieved by locking down access to just a few data scientists, in silos, with static controls in place.

Data Protection and Risk Reduction

Efforts to update regulations for personal privacy protection are underway in several countries and regions. The European Union (EU), has introduced the General Data Protection Regulation (GDPR), to strengthen data protection efforts for all residents, and to ease the regulatory environment for international trade by offering a uniform regulation. When telcos process data of individuals who are in the EU when their personal data is collected, this regulation applies—no matter where the telco is located globally.

The GDPR recommends pseudonymization and encryption as mechanisms that can be used to protect personal data. Pseudonymization is a term for various techniques for data de-identification when the pseudonym or surrogate data can be used in business processes. Field-level encryption and tokenization are both methods of pseudonymization.

The Solution: Embed Protection into the Data Using Hyper Format-Preserving Encryption (FPE)

Augmenting infrastructure system and perimeter controls with protection embedded into the data is essential to scale protection, while mitigating risk exposure, in order to securely enable analytics.

Using data safely at scale calls for de-identifying data as close as possible to its source before ingestion into data lakes to eliminate gaps in protection, masking the sensitive data elements with usable, yet de-identified surrogate values that maintain format, behavior, and meaning. Voltage SecureData Enterprise by OpenText Hyper FPE makes this possible, preserving characteristics of the original data, including numbers, symbols, letters, numeric relationships, and referential integrity across distributed data sets.

Voltage SecureData Enterprise for Hadoop and IoT provides maximum data protection with next generation Hyper FPE, the only NIST-recommended FIPS-validated FPE protection available based on the FF1 standard. The Voltage SecureData Enterprise platform also provides Voltage SecureData Enterprise with Hyper Secure Stateless Tokenization (SST) for high-performance tokenization of payment card data subject to PCI DSS compliance.

The protected form of the data can be used in applications, analytic engines, data transfers and data stores, while being readily and securely re-identified for those specific applications and users that truly require access. Yet, in the event of a data breach, the protected data yields nothing of value, avoiding the penalties and costs that would otherwise have been triggered.

Protecting Sensitive Data in the Data Lake

Customers deploy Voltage SecureData Enterprise with Hyper FPE and SST technologies with their Hadoop framework using pre-built solutions for Apache NiFi, Sqoop, Spark, Flume, Storm/Kafka, MapReduce and Hive. Templates can be quickly expanded to integrate with other technologies in the Hadoop stack. User-defined functions (UDFs) enable data protection agents to be deployed natively in Teradata and Vertica.

Voltage SecureData Enterprise for NiFi allows telco analysts to graphically design and easily manage large-scale data flows, including CPNI and cell tower data, by inserting encryption at the intelligent IoT edge to protect data before it moves into the Hadoop data lake.

Customer Case Study: A Major Telecoms Carrier with Global Operations

Primary Use Case: Personal data protection

Ecosystem Scope: Big data, mission critical IT, cloud, enterprise and mobile

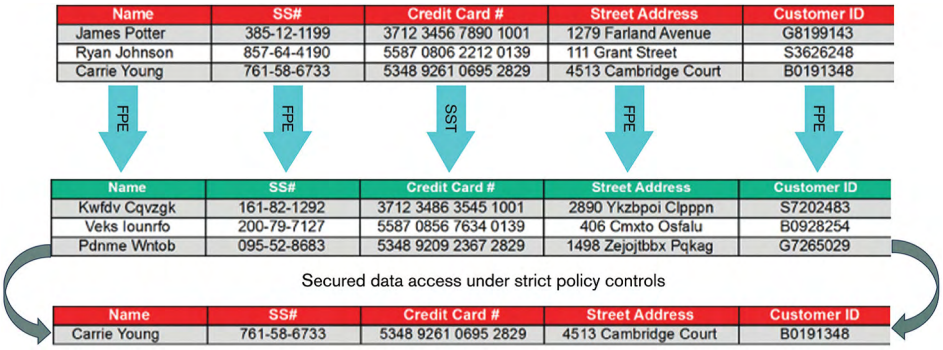

Figure 1. Data protection with Hyper FPE and Hyper SST replaces original values to maintain data usability while lowering risk.

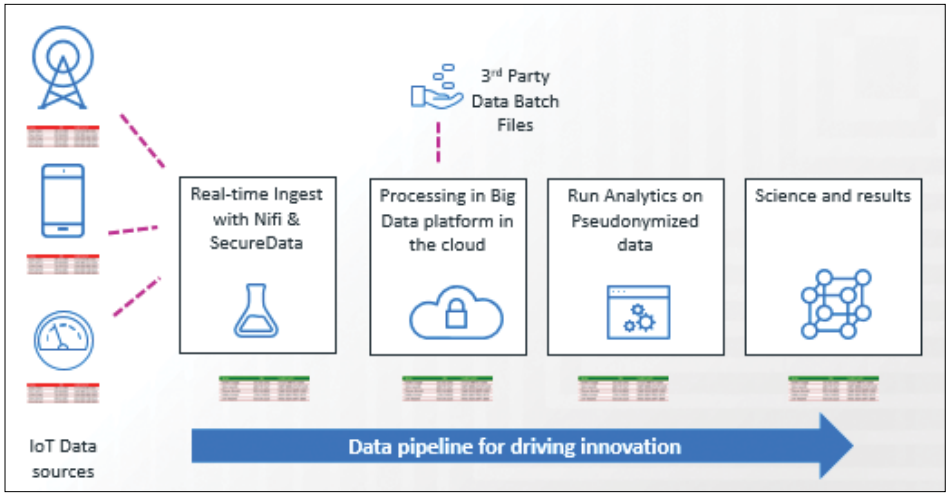

Figure 2. Pseudonymize billions of records for analysis at the edge to reduce risk of data exposure and eliminate gaps in protection

A large multi-country telco runs back-bone infrastructure that delivers services to over 300 million consumers. With the rise in threats from criminal and nation-state sponsored cyber-attacks, and government mandates to protect critical infrastructure, the company embarked on a new mission. The goal was to ensure that all sensitive data would be protected wherever it moves across all systems, applications and services.

Today, that top-down vision is achieved with petabytes of data secured across 26 data types, thousands of applications, in the data lake and cloud workloads. Voltage SecureData Enterprise technology is the new standard at the company. The deployment protects data for billions of transactions and mobile devices, while enabling IoT strategies to capture new market segments, and sustain growth and innovation.

Safely Unleash the Power of Big Data

Voltage SecureData Enterprise with Hyper FPE and SST enables Telcos to:

- Extract value safely with analytics from protected data in Hadoop data lakes
- Comply with GDPR and other data protection regulations, such as PCI DSS
- Expand to AWS or Azure to spin up flexible workloads for cloud elasticity advantages
- Deploy data protection from ingestion at the source and throughout its end-to-end lifecycle

The risk of improper data exposure to applications and users, and increased regulatory pressure, need not hold back the innovation that enables telcos to operate competitively, with new insights available.

Voltage SecureData Enterprise addresses data risks by applying data-centric security that protects data at rest, in motion and in use—allowing data to scale for analytics and persisting protection during migration to hybrid IT. Voltage SecureData Enterprise enables platform-agnostic, non-disruptive, data protection at hyper scale for billions of daily transactions used in analytics to safely increase access to data.

Find out how to unleash big data for analytics insights to more users and applications for increased business value creation.

Learn more at
www.microfocus.com/sdhadoop

Connect with Us
www.opentext.com

"We use big data and machine learning to discover patterns in customer and transactional data. Speed is crucial to us. SecureData allows us to encrypt the data as we take it out of our source systems and before it ever hits our big data systems so there's never a time when the data is unencrypted. With Voltage FPE we can use our existing skillsets, knowledge base and schema to pull our data into big data, encrypt the data and have people be effective right away. Using SecureData we can do more and more innovation. It's invaluable to us."

VP Platform Engineering and Shared Services
Technology Company

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.