CASE STUDY

Enabling a National Telecommunications Provider with Data Protection at Scale

Customer Profile

A leading national telecommunications company in Mexico is one of Latin America’s largest cellular communications providers, with investments in telecommunications across the American continent.

It provides wireless communication services to 90% of Mexico’s population, covering over 63% of the country’s geographical area. This enterprise boasts an estimated 77.2% share of the Mexican wireless market, serving over 77.2 million subscribers.

The provider’s success can be attributed to its strong structure and specialization, as well as the commitment of its employees to effectively and consistently meet the wireless communication needs of its customers.

> *"Unlike other vendors in the data security market, Sotero scales with our client's needs, its REST API expands its platform's usability to non-coders."*
>
> ***~ Jaime R. Michel Juárez - AppTec*** *(reseller)*

Customer Challenge

The leading telco provider came to Sotero with two challenges. The first challenge focused on managing access to consumer data to drive revenue analytics. Part of the telco provider’s dilemma was ensuring the provider’s distributors did not misuse renewal subscription data, which is leveraged to secure renewals. If distributors were to get access to renewal data, they, in turn, would obtain renewal subscription commissions, costing the telco provider massive losses in revenue.

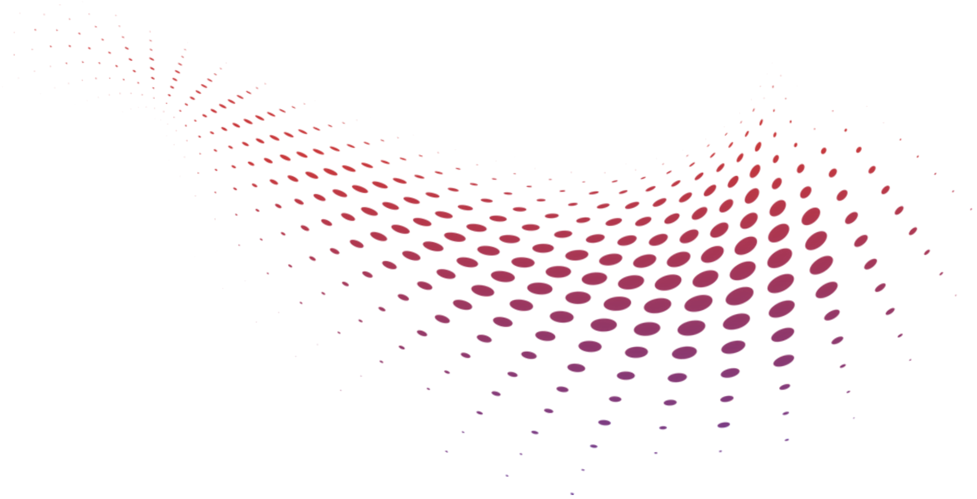
Adding to the challenge is the massive subscriber base of which 15 million customers in a single market, generate 1.2 petabytes of data which pools into a single data lake or data warehouse. Existing processes could not manage access for privileged users over such a large volume of data.

The second challenge focused on meeting compliance mandates. In the main data warehouse, over 40 billion records accumulated annually containing sensitive elements, specifically PII data, that were not protected. Meeting compliance required the telco provider to safeguard all inbound international call logs. These logs existed as structured data, which grew by an average of 300 million data points daily.

Results

- Users could securely access the data necessary to complete their jobs without the risk of exposure to data that could be misused.
- Existing data sets were protected from theft and misuse using encryption and access controls that scaled as data accumulated, creating a hardened foundation for their organization.
- The telco provider generated evidence of continuous compliance through logs and the audit dashboard, indicating all data access requests by applications and users.
- The telco provider had the confidence that it was protected against internal and external threat actors directly accessing data, as it remained encrypted throughout its lifecycle, rendering it useless to attackers.
- The telco provider can grow future application integrations with Sotero as Sotero’s REST API allows even non-coders to utilize the power of Sotero.

> **The client is now able to generate evidence of continuous compliance through logs and the audit dashboard...**



Solution

Using Sotero’s UI, the telco provider created a unique data set, identifying which tables had sensitive elements and defining encryption types for selected PII elements. The encryption process was completed using Sotero’s REST API through the GUI interface, bulk encrypting the data stored in YellowBrick without impacting the end-user experience.

Using the Sotero interface, the organization could define explicit access controls across tables and fields using Role-based Access Controls (RBAC). With this configuration, permissions could be applied to groups of people, simplifying management and delivering on the need for restricted access.

To meet compliance mandates of protecting all data, the telco provider used Sotero and its seamless integration with Denodo and other query tools. The telco provider could run queries against encrypted data without modifying their front-end interface through this integration.

By integrating seamlessly as part of the data flow, Sotero simplified the integration process. It eliminated the timely task of re-coding applications and allowed users to continue using the same applications without the need for re-training. From the user’s point of view and how they interact with the data, the experience was identical.

In addition to updating access controls and securing the data, Sotero delivered additional functionality through its real-time anomaly detection capabilities. Sotero continuously monitors data utilization on an individual basis, creating unique behavioral models. If deviations in behavior occur, such as changing location, accessing at irregular hours, or adjustments in data accessed, alerts are generated. This allowed teams to investigate if a threat exists, such as an outside attacker, insider threat, or stolen credentials.

About Sotero

Sotero offers a comprehensive data security platform that protects data against a broad range of malware threats beyond ransomware, and against insider risk. With minimal latency and zero impact on user experience, Sotero's patented technology secures data "in-use," empowering customers to stay ahead of the competition, innovate, and defend against evolving threat actors.

Standing out from the competition, Sotero’s solution is the only technology capable of not only detecting zero-day attacks - threats exploiting previously unknown vulnerabilities - but also automatically blocks them to give you a proactive defense against evolving threats.