Solution overview brochure

Protect your revenues

HPE CentralView Visual Analytics Dashboard

Hewlett Packard
Enterprise

Identify and stop fraud—quickly and effectively

The communications, media, and entertainment industry is susceptible to fraudulent activities—account takeover fraud, International Revenue Share Fraud (IRSF), content theft, PABX abuse, and interconnection fraud, which eats into your revenue and profits. And now, fraudsters are using more sophisticated technologies to perpetrate crimes. Even with existing fraud management systems in place, there could be weaknesses in your network that fraudsters could penetrate.

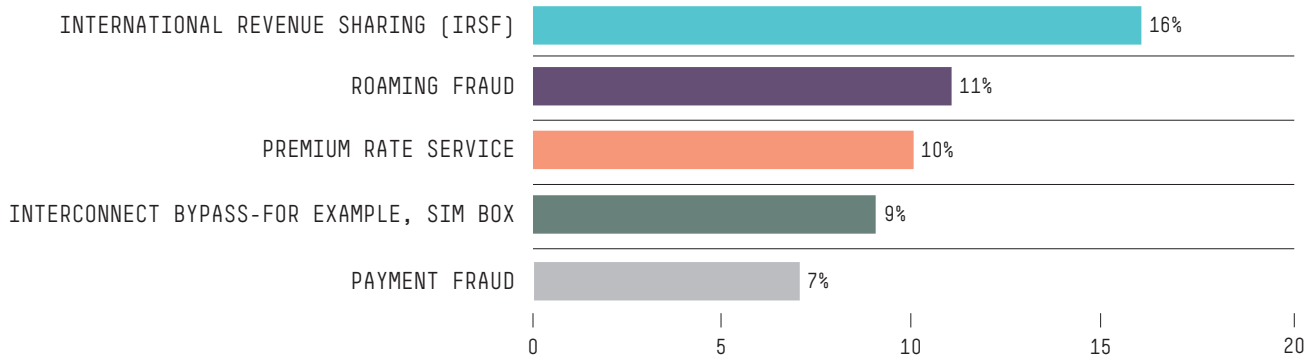
As a communications service provider, it's important to be in control of your network assets and know they're not being misused. Fraud management tools have made a significant difference in stopping and preventing losses. However, just as fraudsters are evolving, so must prevention tools.

To do this, fraud management tools should include intelligence capabilities, which enable companies to perform data mining for better risk management. For example, triggered functionality operational alarms—the current practice—analyze traffic data following a multidimensional analysis approach to see broader trends by grouping data into two or more categories, such as data dimensions and measurements.

Visual analytics is particularly helpful in fighting against fraud types that can be identified when looking at the concentration of calls having the same originating or destination number—such as:

- IRSF
- Interconnect bypass fraud
- Bonus recharge fraud
- Call-back fraud

Not surprisingly, these are consistently reported among the top fraud types globally, as shown in market studies and global surveys.



Source: CFCA 2013 Global Fraud Loss Survey

Figure 1. Survey: What do you view as the top five fraud types globally?

Now, by combining real-time monitoring with right-time visual analytics, operators and content providers can dramatically reduce fraudster threat to your hard-earned customers, systems, services, revenue, and brand image.

Get the right solution

Leveraging 20 years of Telco fraud management experience, we developed HPE Fraud Analytics—highlighted with the HPE CentralView Visual Analytics Dashboard, a platform that effectively helps carriers defend against ISRF, Wangiri/callback fraud, bypass fraud, and other risks.

HPE CentralView Visual Analytics Dashboard is part of the HPE Revenue Intelligence portfolio of tightly integrated, business-focused applications that quickly and accurately transform under-exploited data from disparate sources into competitive opportunities for revenue protection, customization, and generation.

It's based on the HPE Revenue Intelligence framework, and provides a set of ready-to-use modules and dashboards specifically designed for fraud analytics. On top of real-time data processing, which ensures timely creation of alarms and cases, Fraud Analytics provides advanced analysis techniques such as:

- Source Analysis
- Destination Analysis

Source Analysis

Source Analysis is a way to enhance near real-time detection and identify phone numbers that may be acting as bypass hubs for incoming interconnection, even if they belong to other national operators.

With the HPE CentralView Visual Analytics Dashboard, all incoming call records are aggregated by the originating number. Aggregates can be created on a daily basis or with higher frequency—such as three to four times a day—and highlight entries with the highest number of calls. The "top entries" identified are presented to analysts and can be used to trigger alarms/cases against specific thresholds.

Statistics are presented in a web-based dashboard, like in Figure 2, with tabular data on the top entries and graphical elements showing distribution and segmentation by area, operator, or time zone.

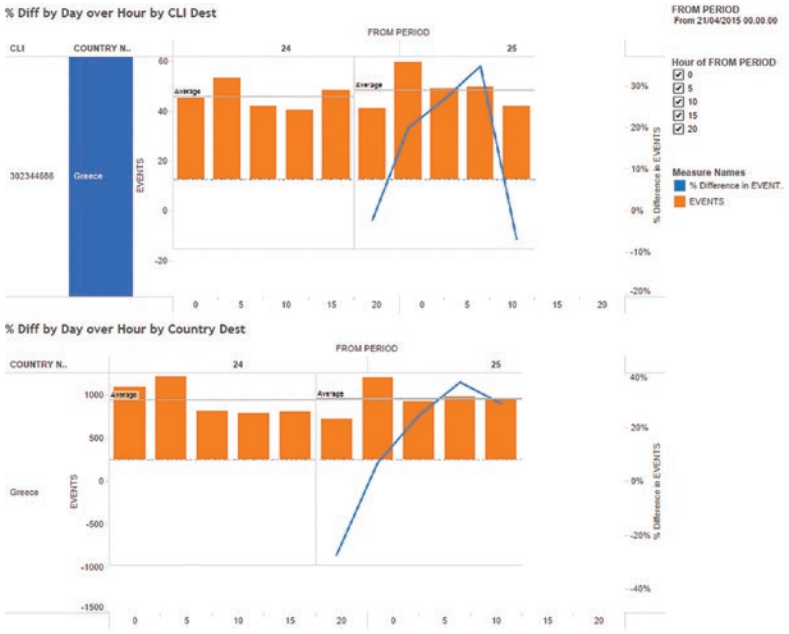


Figure 2. Source Analysis using HPE CentralView Visual Analytics Dashboard

Destination Analysis

The same principle used for Source Analysis can be adopted in a symmetrical way for outgoing traffic data. Called Destination Analysis, it's a detection technique aimed at highlighting the B numbers that are called the most by your own subscribers/lines.

B numbers are suspects of outgoing interconnection fraud and may be involved with IRSF cases.

The numbers are identified on an aggregation basis, which can be tuned according to specific needs. Presentation dashboards use graphical elements such as bubbles and graphs, as shown in Figure 3. They highlight the top entries and give a representation of their weight. Like with Source Analysis, it's also possible to segment findings by relevant criteria such as country of destination and time zone.

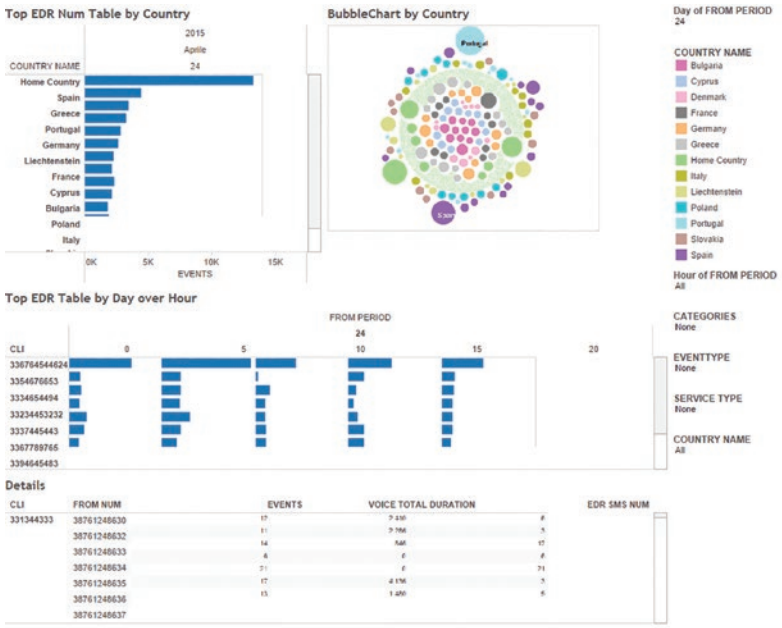


Figure 3. Destination Analysis histogram and bubble chart using HPE CentralView Visual Analytics Dashboard

Review Dashboard benefits

Build a strong defense with a quick return on investment—Deploy HPE CentralView Visual Analytics Dashboard with limited investment and a short implementation time to deliver a quick return on investments.

Slash fraud and reduce losses—Quickly identify threats so massive losses can be stopped from happening and the bottom line greatly improved.

Optimize interconnection management—Detect fraudulent bypasses and monitor trends in the volume of interconnections and support optimization.

Learn more at
hp.com/go/centralview

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA5-8560ENW, November 2015, Rev. 1