Ribbon Analytics - FraudProtect

ribbon

Unified Communications fraud continues to cost carriers and enterprises tens of billions of dollars per year. Bad actors typically commit telecom fraud for financial gains. In order to meet their objectives, bad actors often cover a broad set of call scenarios – from IP-PBX hacking, to subscription fraud, to Wangiri (one ring and cut) and other use cases. With the variety and inherent complexities of SIP and VoIP protocols, UC environments will benefit greatly from the added value of behavioral analytics and anomaly detection to deter or eliminate the various types of fraud attacks.

Built for both carriers and enterprises, the FraudProtect analytics application provides you with the insight and tools needed to identify and stop the UC fraud in your network. FraudProtect will help you by identifying repetitive calling patterns and flagging them as anomalous activity. This is done in real-time based on destination detection and other KPIs. As more fraudulent calls are made, they are quickly identified and terminated, thus mitigating the potential for expensive toll charges.

Identifying Fraudulent Behaviors

Most UC fraud activities are traced to a few behaviors in calling destination and traffic patterns. Identifying the patterns can be as simple as noting the destination or as complex requiring historical analysis of traffic. The fraud can happen on a single subscriber, a business trunk, or by redirecting millions of users unknowingly.

The most successful attacks tailor the fraud to mimic actual user or network behavior. This allows them to go unnoticed for the most amount of time and generate significant cost to the unsuspecting organization. Bad actor attacks may be focused on specific traffic flows (region by incoming calls), specific trunk groups, or targeted subscriber numbers.

To combat these bad actors, a fraud mitigation solution needs to be able to quickly identify anomalous behavior whether it is simple or complex. It needs to be able to adapt and train itself to the organization's calling patterns and be customized to the traffic and network it is protecting.

FraudProtect gives you valuable insights and mitigation policies by using network behavioral analytics and customizable incident detectors to stop fraud before the bad actor(s) can do any damage.

Network Behavioral Analytics

FraudProtect models various baselines of the UC network behavior to establish a characteristic "normal" activity. Once a baseline is created the application monitors your communication network activity for anomalies and deviations from the established baseline. These anomalies are identified, graded as to the likelihood that these incidents are fraudulent, and reported to you for mitigation.

The FraudProtect behavioral model, shown in Figure 1, allows to you create a baseline model that includes the variations of network activity such as working vs non-working hours as well adapting to changes due to things such as business growth or seasonal activity. FraudProtect online learning adapts the behavioral model to reflect the current "normal" baseline to avoid false positives.

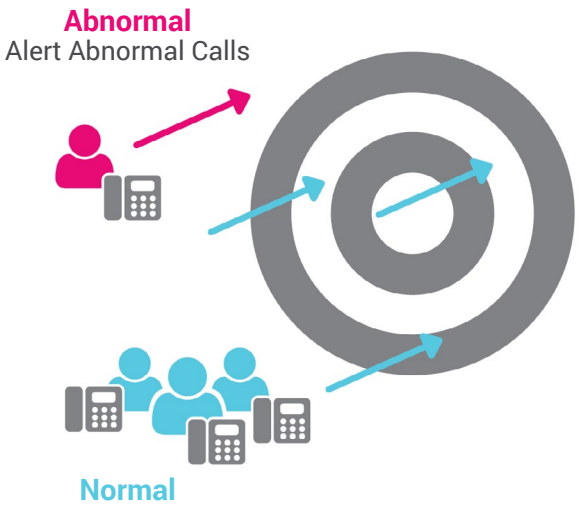

Figure 1. FraudProtect behavioral model

Subscriber (or Caller #):
The subscriber monitor tracks the behavior of individual subscribers in the network. A behavior model is trained and maintained for each network subscriber. The model tracks metrics such as call attempts, call duration, calling number, called number, types of calls (Local, Long Distance, International) during working hours as well as non-working hours. When a subscriber's activity exceeds thresholds of normal behavior, a threat incident is raised resulting in the subscriber being blocked from using network resources. This enables network administrators to find single or groups of phone numbers trying to misuse the system.

Trunk Groups:
The trunk group monitor tracks the activity of trunk groups (ingress/egress/both directions). Like the Subscriber monitor, the trunk group behavioral model is trained and maintained for each trunk group. When a trunk group exceeds thresholds of normal behavior, a threat incident is raised indicating incident. This enables network administrators to find changes in trunk group behavior and stop calls to high rate or premium numbers, which accumulate large toll bills.

Targets (or Called #):
The target monitor tracks the activity of called numbers in the network. To manage the vast numbers of called numbers accessible from a network they are grouped by a configurable number of prefix digits. Like the Subscriber monitor, the target behavioral model is trained and maintained for each called number grouping. When a called number group exceeds thresholds of normal behavior, a threat incident is raised indicating the top offending called numbers in the group resulting in these number(s) being blocked from further calling. This enables network administrators to find changes in call destinations and stop calls to high rate or premium numbers, which accumulate large toll bills.

Subscriber Protect

Subscriber Protect helps prevent fraud scenarios that target subscribers on a service provider's network. Fraud scenarios such as number spoofing and denial of service are aimed at subscribers but can also have negative financial or legal impacts to the service provider. Subscriber Protect alerts service providers to anomalous behaviors that are typically associated with fraud scenarios.

Subscriber Protect detects following Fraud Scenarios:
- Spoofing of individual numbers
- Calling number Denial of Service
- Use of autodialers
- Neighbor spoofing

Subscriber Protect applies in following fraud scenarios:

Spoofing of individual numbers:
Phishing attempts or autodialing campaigns are often unsuccessful because the call recipients simply ignore calls from unidentifiable numbers. Fraudulent parties may therefore mask their caller ID to make it look like their calls are coming from a legitimate or well-known number, such as a service provider, bank, or well-advertised business. Subscriber Protect can detect potential spoofing of individual calling numbers.

Called number Denial of Service:
In this type of fraud, the perpetrator sends a continuous stream of call attempts to a specific user, in the hopes the user will stop answering, miss legitimate calls, or eventually stop service altogether. Subscriber Protect can detect anomalous call patterns to individual subscribers.

Use of autodialers:
Many service providers prohibit the use of autodialers on the network. Subscriber Protect can detect non-human dialing volume and behavior.

Neighbor spoofing:
Bulk call fraud schemes (such as phishing attempts or autodialing campaigns) are often unsuccessful because the call recipients simply don't answer calls from foreign or unidentifiable numbers. Fraudulent parties may therefore mask their caller ID to make it look like their calls are coming from a local number. Subscriber Protect can detect anomalies among calling number prefixes, which may indicate neighbor spoofing.

Subscriber Protect is a set of anomaly detectors. Figure 2 explains, how each detector learns what the "normal" traffic patterns are for different time periods throughout the week, and then automatically detects and flags traffic that is outside those normal patterns.

Interval	Baseline (number of calls)	Observed	Outcome
Friday 4:01-5:00pm	37-51	47	✓ Within expected range
Friday 5:01-6:00pm	4-6	32	⚠ Outside expected range
Saturday 9:01-10:00am	1-3	4	✓ Slightly outside range but within sensitiviety level
Saturday 10:01-11:00am	2-5	18	⚠ Outside expected range

Figure 2. Anomalous Detector

When anomalous behavior is detected, Subscriber Protect raises an incident. Ribbon Fraud Protect application with Subscriber Protect can be configured to perform the following next steps:
- Send email or text notifications to system users so they can manually investigate
- Send reports to external systems, such as Ribbon's Identity Hub or a third-party application
- Perform a mitigation, for example, block a calling number

Incident Detectors
For an additional layer of fraud detection, the FraudProtect application has a powerful customizable toolset called "incident detectors". There are two types of Incident Detectors seeded and customer defined. Seeded Incident Detectors are predefine by Ribbon and focus on targeted fraud characteristics. Customer defined Incident Detectors can be defined by the customer based upon the specific network deployment. Shown in Figure 2, this capability allows you to create specific fraud detectors modeled to your specific requirements to flag undesired activities within your network.

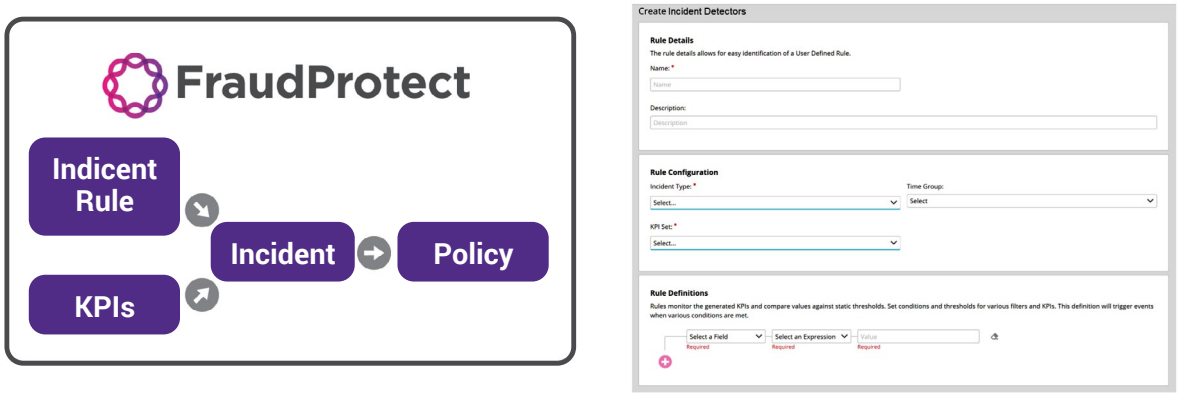

Figure 3. Incident Detectors

The incident detector functionality provides you with the following controls for granular fraud monitoring of your network:

- **Customizable Incidents** - define system behavior based upon your network. Set the level of risk with sensitivity controls
- **KPI sets** (Key Performance Indicators) - track/monitor metrics from any data source or derived metric
- **Incident rules** - set triggers flagging activities based upon changes in metrics or a period, values, or rate
- **Policy** - create alerts/mitigation scripts to control the network behavior as a reaction to the incident

FraudProtect is the leading telecom fraud solution that utilizes both network behavioral analytics and incident detectors to allow you to monitor a spectrum of activities identifying and stopping fraud within your UC network.

Ribbon Analytics Platform

FraudProtect leverages Ribbon big data analytics platform to respond to real-time communications security and network quality incidents faster, more intelligently, and more efficiently. From fast-path content ingestion, to reporting, to API capabilities, the Protect platform is built for scalability, reliability, and performance while allowing the you to fully comply with privacy policies.

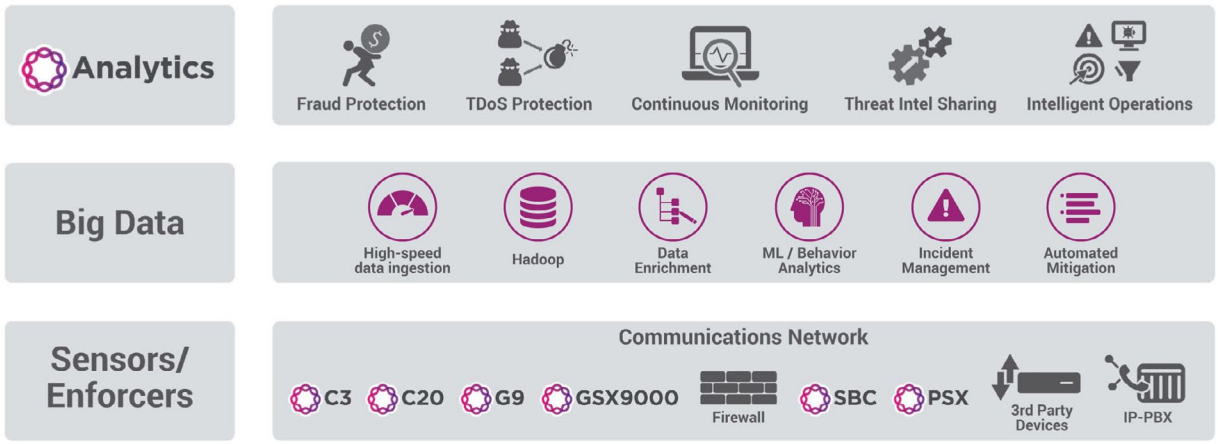

Figure 4. Ribbon Analytics Platform

With Ribbon Analytics platform, you have ready access to the data that enables smart decision-making using out of the box analytics applications. With Ribbon, you are empowered to take a proactive competitive stance in a dynamic industry that is continuously updating content and services to meet the innovations of the latest apps, devices, connections, and technologies.

Contact Us Contact us to learn more about Ribbon solutions.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.