Ribbon Security Analytics Overview

Ribbon Analytics empower you to respond to cyberattacks, fraud and network operational issues on your real-time communications (RTC) network efficiently and more intelligently. Ribbon Analytics is a virtualized solution that quickly and easily integrates with your existing RTC network investments. Ribbon Analytics platform receives information from various network elements – such as Ribbon SBCs and other 3rd party communication network devices. This information is parsed and analyzed for various RTC security breaches and service quality issues.

The Ribbon Analytics application portfolio allows you to view end to end call flows, diagnose service quality issues as well as make automated security enforcement decisions based on quantitative real-time communications (RTC) network information. Using the Ribbon Analytics platform, these decisions can then be pushed to any "enforcer" anywhere in the network. Figure 1 below shows the Ribbon Analytics architecture and how this solution provides a single, centralized view of the end to end network which is critical in RTC cybersecurity threat detection, fraud management and network operations.
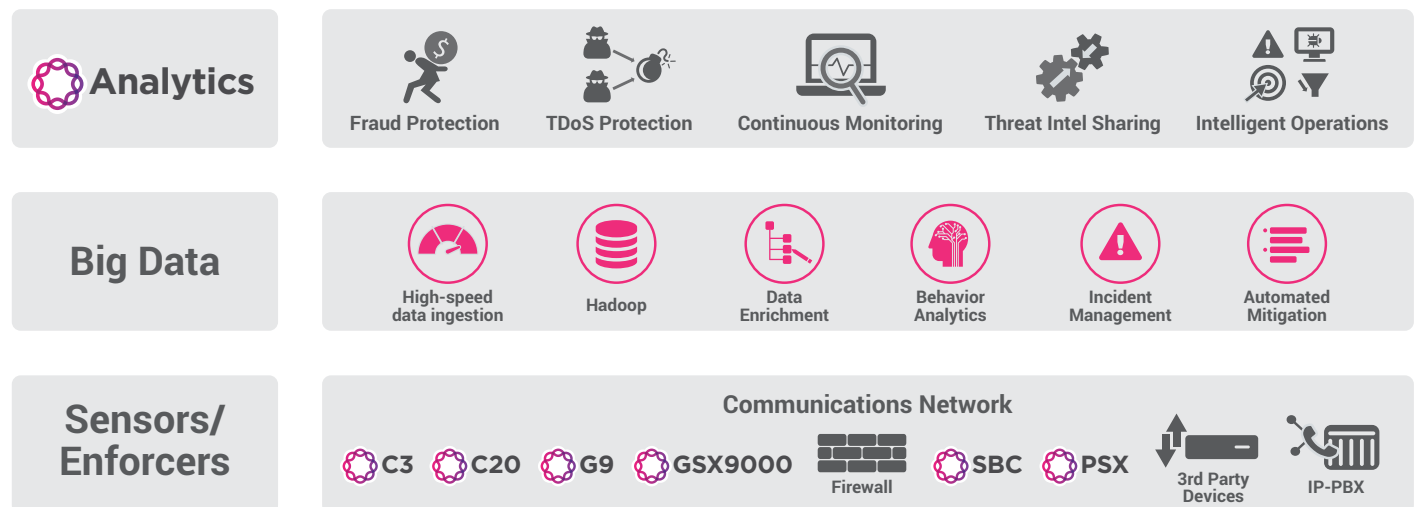

Figure 1. Ribbon Analytics Architecture

Benefits

- **RTC Security:** Detect bad actors trying to infiltrate your RTC network and close the security aperture in your entire network by disseminating security policies across network "enforcers" such as SBCs and firewalls
- **Intelligent Operations:** Proactive analytics are designed to improve user experience and reduce operational costs. IT staff gain a composite view of voice quality and network performance as it changes. Your overall quality of experience will be improved by having a holistic view of your communications network operations.
- **Faster Resolution:** Reduce network administrator time trying to isolate quality and security issues across disparate communication elements. The Ribbon Protect platform correlates network-wide KPIs and events for maximum efficiency. Easily troubleshoot call quality issues with end-to-end SIP ladder Diagrams.
- **Network Tool Consolidation:** Reduce the various number of management tools used to detect RTC Security and quality of experience issues from many to one. With a probe-less data capture methodology, you will reduce complexity and OPEX/CAPEX costs.

Ribbon Analytics Applications

NetProtect

Completely protecting the RTC network starts with a deep understanding of attack vectors targeting SIP. Ribbon Communications, a leader in SIP security, has the solutions capable of identifying the specific threats targeting SIP traffic in RTC networks.

Today, the challenge is how to further secure SIP-based traffic. Mitigating bad actor infiltration, rogue endpoints generating DoS attacks and other network incursions using SIP are just some of the new attack vectors that need to be addressed.

Ribbon's NETProtect identifies these attacks and distributes threat intelligence policies across the communications network so you can close the network-wide security aperture exposed by RTC traffic. Distributed security policies between your SBCs and 3rd-party devices such as next-gen firewalls allows you to stop bad actors at the edge of the network. It also enables your organization to have a more effective and holistic security methodology across the converged (data and communication) network.

TDOSProtect

Protect your real-time communications from unwanted calls coming into your network that might appear to be valid but can tie up communication applications such as IVRs or PBX trunks with long call duration times. Ribbon TDoSProtect uses advanced algorithms and machine learning techniques to detect and mitigate these attacks. Advanced policies are applied at the edge of the network to siphon out these unwanted, disruptive calls from your communications networks and applications.

FraudProtect

Many bad actors locate and enter real-time communication networks in order to fraudulently call out to premium rate services or infiltrate RTC network elements and launch an International Revenue Share Fraud (ISRF) attacks which cumulatively defrauds unsuspecting organizations out of billions of dollars per year. Ribbon FraudProtect baselines your network calling patterns and seeks out repetitive calling patterns to anomalous places. Those known fraudulent or suspicious calls are flagged based on destination detection and other fraud scanning methods. As more fraudulent calls are made they are quickly identified and terminated, thus mitigating any expensive telecom charges.

RoboProtect

Keep your communication free of calls coming through from various numbers that are "known" fraudulent or nuisance calls. Many times these calls come from a computerized auto-dialer to deliver a pre-recorded message, as if from a robot. Ribbon RoboProtect uses advanced databases to quickly identify the source of the robocall and apply policies to the edge of the network to stop these calls before they disrupt your employees or customers.

> **Rapid discovery, rapid review, rapid resolution...so your mission-critical communications remain secure and available.**

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.

Contact Us Contact us to learn more about Ribbon solutions.