Ribbon Analytics - RoboProtect

Stop unsolicited phone calls

People and businesses continue to be bombarded with nuisance calls (robocalls) — and from all indications, the problem is getting worse. In March 2019, there were an estimated 5.23 billion robocalls or more than 2000 robocalls per second. This is madness! Despite laws preventing misuse from automated out-bound dialers, the algorithms used to make these calls are non-discriminate. So how do you keep your communication free of calls that come through as various numbers that are "known" fraudulent or nuisance calls?

RoboProtect, part of Ribbon Analytics suite of Security applications, uses advanced algorithms to quickly match calls to databases to identify the call as a robocall and apply policies to the edge of the network to stop these calls before they disrupt your employees or customers. RoboProtect will enable you to stop those unsolicited and spoofed phone calls.

How it works

RoboProtect provides detection and mitigation from automated out-bound dialers, telemarketers or other un-solicited callers. RoboProtect uses 3rd party databases such as the publicly available FCC complaints database or other commercially available databases for detecting nuisance calls.
Figure 1 below shows the Ribbon Analytics RoboProtect application.

These third party databases are imported into the Ribbon Protect platform, then queried based on known traffic patterns identified in the communications network. If the "Calling Number" exceeds a configurable call rate, RoboProtect will raise a threat event and push mitigation policies, such as blacklisting of those nuisance calls, down to the SBCs and PSXs in the network to stop that particular traffic.

RoboProtect benefits:

• Integration with 3rd party robocalling databases

• Automated system wide remediation

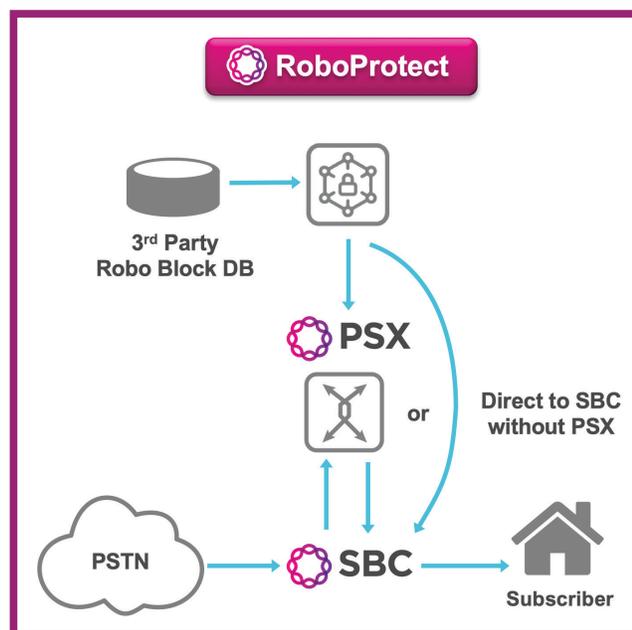• SBC and/or PSX policy enforcement to stop unwanted calls

Figure 1. Preventing robocalls

Ribbon Protect Platform

RoboProtect leverages Ribbon Protect, a big data analytics platform, to respond to real-time communications security and network quality incidents faster, more intelligently, and more efficiently.

The heart of the Protect platform is its UC anomaly detection and policy mitigation capability. The anomaly detection module collects and analyzes data across the entire communications network that is then made available to Ribbon Analytics applications. With customer-defined policy management functionality, detected anomalies generate alerts (e.g. SMS, email) and can be mitigated with actions to the appropriate network elements in real-time.

www.rbbn.com