Identify and Prevent Voice Threats Before They Disrupt Your Business

Cyber threats against enterprises get an outsized amount of attention these days - for good reason. We constantly hear stories about the theft of confidential business data or the threat of exposing confidential data unless a ransom is paid. Of course, the counter to these threats is to invest in cybersecurity solutions that try to cover as many threats as possible in the most pragmatic way.

This solution brief will discuss the current state of voice security and options for best addressing the threat. One such option is Voice Threat Protection from Ribbon. As described below, it addresses these vulnerabilities with a systematic approach to voice security.

Background

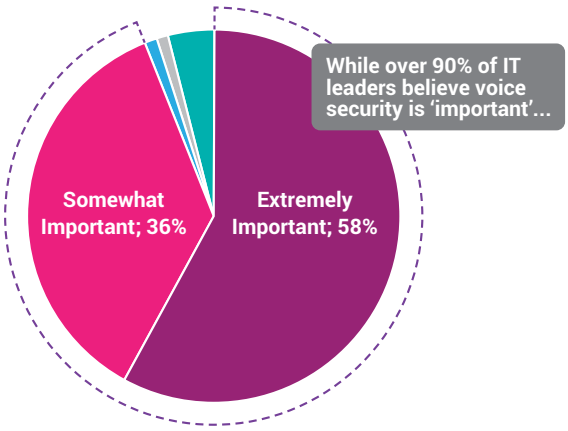
For the enterprise, there are many types of voice threats to address. A few of the better-known examples are:

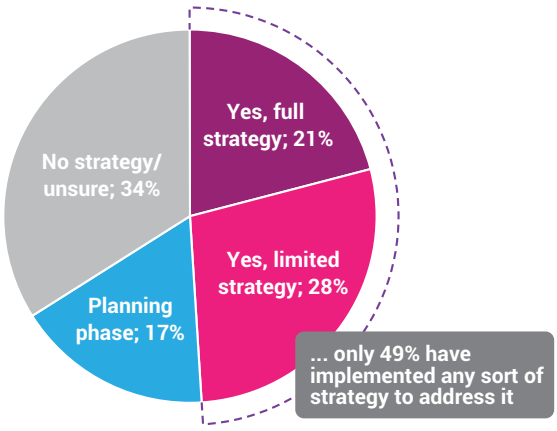
- Brute force attacks, using auto-dialer robocalling, to create *Telephony Denial of Service (TDoS)* attacks.
- High volume of *nuisance calls*, designed to disrupt normal operations by consuming enterprise UC or Contact Center resources and users or agents time.
- Hacking into VoIP systems to commit *premium rate toll fraud* or to impersonate remote agents to steal data.
- *Toll-free trafic pumping* where fake traffic is generated to an enterprise's toll free numbers, forcing them to pay for fraudulent traffic they do not want to terminate on their toll-free numbers.

The bottom line is that any enterprise using an IP PBX, IP-based Unified Communications and Collaboration services, or has an IP-based Contact Center is at risk for voice threats. It does not matter if these services are deployed within the enterprise premises or on a cloud domain, the threats remain the same.

Market Research Results

Market research firm Metrigy conducted their UC Management and Endpoints 2021-22 research study, with 400 enterprises across 18 industry verticals in August 2021. Included in this survey were questions addressing voice fraud. Two very important results came out of this data:





Source: Metrigy UC Management & Endpoints 2021-22 Research Study, Sept 2021

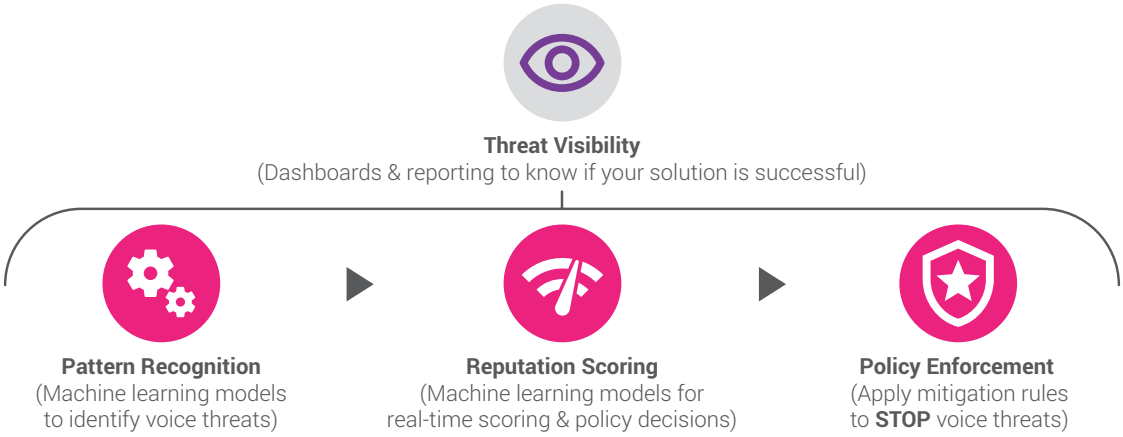
Clearly, a gap exists between the desire to implement voice security and its actual implementation.

But what can be done to stop bad actors who are attacking your voice network and services in real time? The answer is to invest in a voice threat prevention solution that is designed to address these threats and close down the attack vectors used by bad actors.

Voice Threat Prevention

A comprehensive voice threat prevention solution should have the following four key attributes:

1. Pattern Recognition – this automated function is based on machine learning models to identify voice threats.
2. Reputation Scoring – this automated function is based on machine learning models to provide real-time reputation scores and policy decisions for every call.
3. Policy Enforcement – applies real-time mitigation based on policy decisions to stop voice threats before they disrupt your business and potentially cause loss of confidential data or incur a financial loss.
4. Threat Visibility – provides dashboards and reporting for visibility.



Pattern Recognition

Pattern Recognition is based on machine learning models using enterprise network call data to detect both unknown and repeat threats by learning normative call traffic behavior. These models use a feedback loop to continuously learn to refine the accuracy of their pattern recognition, which enables non-normative activity to be flagged. By working directly with enterprise network call data, it is possible to identify potentially malicious calls and the bad actors that originate them. Think of this information as a digital fingerprint of the bad actor that is fed into a threat intelligence database.

Reputation Scoring

Reputation Scoring utilizes multi-dimensional input data to determine whether a call is likely malicious or not, outputting a score in real-time. Input data includes the digital fingerprint from the Pattern Recognition function and data from multiple 3rd party/national sources (such as crowd-sourced robocall databases or regulatory databases for "Do Not Originate" numbers). With real-time Reputation Scoring, an enterprise will be able to make the most accurate policy decision for how each call must be handled during call setup.

Policy Enforcement

Like the two functions above, this too must be automated. An effective Policy Enforcement function mitigates voice-based attacks before they disrupt legitimate voice calls or cause harm to an enterprise's business. The right place for policy enforcement is a session border controller (SBC) that is likely already in place for security and interworking of VoIP traffic associated with an IP-PBX, UC&C system, or IP-based Contact Center. Real time policy enforcement is possible whether the SBC is on the enterprise premises or deployed on a private or public cloud.

Threat Visibility

The first three functions described above are automated so real-time detection and mitigation of voice threats takes place rapidly enough to stop the bad actors. With automation comes the need for human oversight to know if your solution is succeeding and how well it is succeeding. For example,

- Are new threats being identified quickly enough?
- How complete is the voice threat mitigation?
- Where there are gaps and what needs to be addressed to plug those gaps?

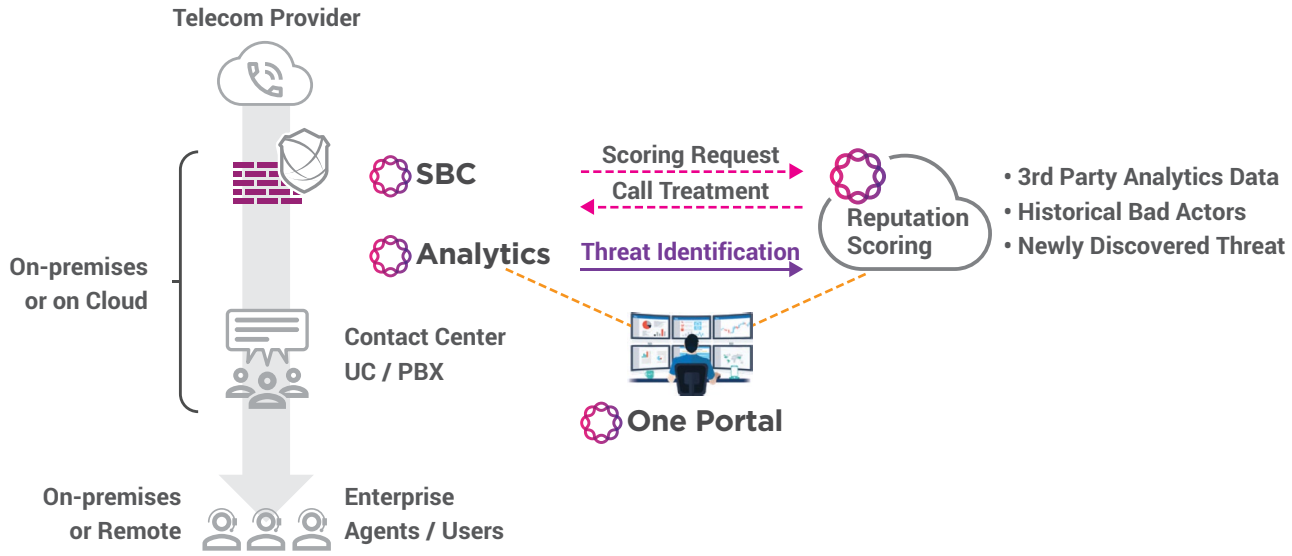
To do this an enterprise voice threat prevention solution needs to provide dashboards and reporting that cover high-level aggregate information as well as the ability to drill-down to per call details for investigation and troubleshooting.

Ribbon's Voice Threat Prevention Solution

Ribbon's solution combines the following to meet the 4 key attributes:

- Ribbon Analytics' FraudProtect application for pattern recognition and identification of potential bad actors and voice attacks.
- Ribbon's cloud-hosted Reputation Scoring service for real-time call scoring of each call attempt and policy decisions for call handling.
- Policy enforcement using Ribbon's Session Border Controller[1].
- Ribbon One Portal for common access to dashboard and reporting capabilities for threat visibility to know how well your solution is succeeding.

Here's how the solution would look from the enterprise point of view.



[1] Policy enforcement could be done by a 3rd party SBC, but with Ribbon, the enterprise will have a completely integrated solution.

Voice traffic, for IP PBX, UC&C or Contact Center services comes into, or leaves from, an enterprise domain on SIP trunks interconnected to a service provider. In the call path is the SBC. At the SBC, two functions are happening in parallel:

- For every incoming call or outgoing call attempt, the SBC will send a scoring request to Ribbon's cloud-hosted Reputation Scoring service.
- For completed calls, call detail records are forwarded to Ribbon Analytics to look for abnormalities versus normal traffic patterns. This is done to identify potential nuisance calls or voice fraud attacks and the bad actors that originate them. A digital fingerprint of a potential bad actor is forwarded to Ribbon's Reputation Scoring service to be incorporated into the Ribbon Threat Intelligence database.

Upon receiving a reputation scoring request, Ribbon's Reputation Scoring service will calculate one or more reputation scores using the data in the Ribbon Threat Intelligence database. These reputation scores are then used to determine the likelihood that a call is being made with, or without, malicious intent.

Based on the reputation score(s), a policy decision will be made on the call treatment (how to handle each call). The call treatment instruction will be sent in real-time to the SBC which will enact the call treatment, such as allowing good traffic to proceed, blocking a fraud attack, or route the call elsewhere for further call treatment if it falls into a gray area.

Finally, dashboards and reports ensure the solution is performing as expected and stopping voice threats before they damage your business.

Conclusion

Over the past 20+ years, Ribbon has amassed extensive knowledge and expertise about voice and VoIP services and intimately understands the nuances of what it takes to identify and prevent voice threats. By applying machine learning techniques to the problem, Ribbon provides enterprises with a comprehensive and continuous learning solution to protect your voice network and voice services from the many different types of security threats before they disrupts normal business, or even worse results in the exposure/loss of confidential data or financial loss.

Contact Us Contact us to learn more about Ribbon solutions.