

Robocall mitigation methods

Blacklists

use blacklists to mitigate robocalls with specific attributes, including:

- Calling telephone numbers or prefixes
- Calling SPIDs (OCNs) that are not me
- Calling locations, e.g., states/provinces/regions that are not yours
- Calling countries that are not yours
- IP addresses that I have identified as robocallers
- User agents that I customers do not use, but robocallers do use.

When a call is identified by a blacklisted attribute, you can either block the call or divert it to a CAPTCHA gateway for Interactive-Voice-Response screening. I can review blacklisted call origination reports to investigate the underlying causes.

I can use Shield for robocall mitigation that screen calls at origination for calling numbers that are **invalid, high-risk**, or appear on **Do Not Originate** lists.

I can set policies by groups, subscribers and numbers to control the handling of such calls. For example, these calls can be blocked, diverted, or reported.

Reputation

I can perform a reputation lookup on calling numbers at origination for robocall mitigation. This lookup returns a reputation score from 0 to 100. The higher the number, the worse the reputation.

If your customer has a calling number with a poor reputation, you may find that they are a victim of number spoofing. We can help you repair the reputation of their number with reputation analytics companies, or you may wish to issue them a different number.

Dynamic traffic analysis

I can use real time dynamic traffic analysis, called SIP Analytics, to detect and mitigate robocalls at origination. SIP Analytics monitors all originated calls by source over a rolling 60-minute window. It compares cumulative call count by source within this window with thresholds that trigger a response to a robocalling event.

SIP Analytics is self-learning. Thresholds are based upon call history and are updated dynamically in real time. A legitimate high-volume caller would therefore acquire a higher threshold, while a residential consumer

would typically acquire a lower threshold. Default thresholds are used for a new source until it accumulates sufficient history to enable calculation of dynamic thresholds.

When a cumulative call count for a specific source breaches a threshold, calls from that source can either be blocked or diverted. In either case, I can investigate to determine whether the caller was originating unlawful robocalls.

Call Detail Record (CDR) analysis

I can collect CDRs from I network equipment and review them with NexOSS for robocall mitigation. You can develop reports to look for unexpected high call volume, short call duration, call hang ups by called party and so forth. If you find suspicious call activity, then I can investigate.