TOLLRING SCAM PROTECT

Monitor, detect and trace scam calls with Tollring Scam Protect. Reduce your risk, protect your network and your customers, and meet your regulatory obligations.

Take control of your call traffic

Scam calling is on the rise, and accounts for a significant proportion of all call traffic. The methodologies and technologies employed by scammers are broad and ever-more sophisticated, and pressure is mounting from customers and regulators to mitigate the problem.

Tollring Scam Protect is a cloud-based solution designed to drastically minimise service providers' risk from scam call traffic. By detecting, reporting and alerting on call traffic that shares the characteristics present within scam calling, you can better understand your exposure, enhance your own rules and tolerance thresholds, and ultimately take action on your own terms.

Benefits to Service Providers

- Agnostic, CDR-based solution ensures seamless compatibility with cloud-based voice platforms.
- Scalable, with the ability to monitor millions of endpoints.
- Delivered securely via the cloud.
- Easy to set up and start receiving customised reports from day one.
- Increase customer confidence, satisfaction and retention.

Parameter-driven intelligence

Scam Protect uses comprehensive behaviour profiling based on the latest scam calling intelligence to provide insight into the call traffic on your network. Intuitive graphical dashboards of incidents and activity provide a view on most active A-party, scam call parameters and trunk groups.

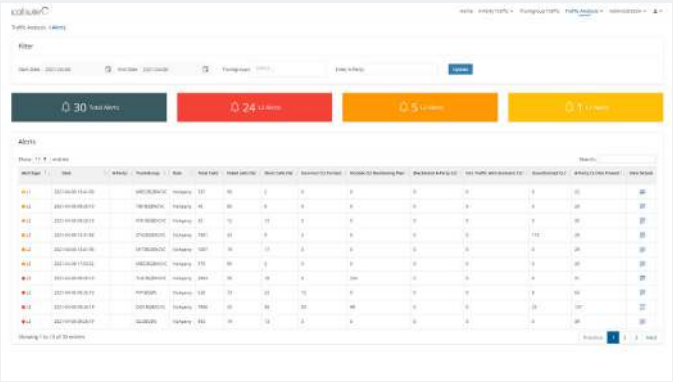
Traffic-monitoring parameters include:

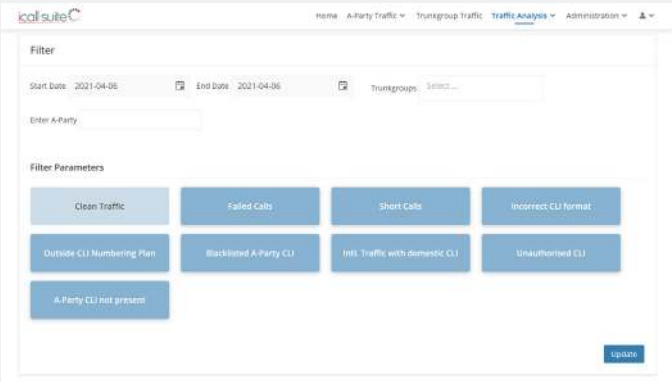
- Failed calls
- Short calls
- Calls outside of CLI numbering plan
- Blacklisted A-party
- A-party CLI not present
- Unauthorised CLI
- Incorrect CLI format
- International traffic mismatch with domestic CLI

These parameters facilitate detection of wide-ranging scam call approaches such as Wangiri, robocalling and CLI spoofing.

Deep-dive reporting with flexible filtering gives revenue assurance teams the tools they need to explore key incidents. Detailed call view dashboards provide call times and durations, a-party and b-party, trunk group and scam parameters.

All reports can be exported for further analysis and action.





Powered by TOLLRING

e. sales@tollring.com w. www.tollringprotect.com

TOLLRING PROTECT

TOLLRING SCAM PROTECT

Continually monitor your call traffic, from anywhere

Advanced, multi-level alerting provides service providers with a view on incidents by severity. Alerts can also be based on parameter rule breaches, trunk groups, A-party and date. The alert dashboard provides a simple view of the alerts triggered by call traffic.

Whether you need to use the solution to take swift action or simply to conduct periodic reviews, you can configure email alert recipients to meet your needs and to your own customisable schedule.

Meet regulatory reporting obligations

Scam Protect makes it easy to demonstrate compliance in line with regulatory obligations. Use the system to investigate singular, impactful incidents or recurring problems, to conduct advanced traffic analysis searches, sorting and filter by date/date range, trunk group or A-party. In addition, you can download scam call details and/or perpetrators to inform authorities whilst reassuring customers that you are taking a stand against scam calling.

Essential toolkit for revenue protection teams

Owing to its platform-agnostic architecture and intuitive interfaces, Tollring Protect is easy to set up and manage. With customisable thresholds and rules across domains and traffic types, it gives you full visibility of your call traffic and any exposure to scam calling.

Features in Detail	
Cloud SaaS application, accessible via any browser	Scalable scam call monitoring on hosted voice platforms
	Data refresh in 10 to 30 minutes, dependent on platform
Scam traffic parameter-driven analytics	Graphical dashboards of incident alerts and scam activity analytics Dashboard reporting by most active A-Party, scam call parameter or trunk group
	Traffic monitoring by scam parameter; failed calls, short calls, outside CLI numbering plan, blacklisted A-party CLI, A-party CLI not present, unauthorised CLI, incorrect CLI format and international traffic with domestic CLI
	Dashboard reporting by most active A-party, scam call parameter or trunk group
	Detailed call view dashboard, showing A-party, B-party, trunk group, call time and duration, filterable by scam traffic parameter
	Export call view dashboard report (PDF or CSV), or email with a subject to specified email address (To, CC or BCC)
Advanced alerting on detection of scam activity	Alert dashboard reporting by alert level (1, 2, 3), parameter rule breached, trunk group, A-party and date
	Alert settings to define email address(es) by alert and notification schedule (1, 4 or 24 hourly)
	Option to resend or forward alert notification
Advanced search and filtering to refine results to your needs	Sortable columns and filtering by date / date range, trunk group or A-party
	Advanced traffic analysis search facility to refine analysis by date / date range, trunk group, A-party or scam traffic parameter thresholds
Administrator access for customisation of application settings and user management	User administration including option to restrict user to view traffic on selected trunk groups
	Rule customisation across domain (A-party, trunk group or both) and traffic type (all, international or domestic) using rule parameter thresholds
	Automated and manual administration of trunk groups by name and traffic type
	Blacklist customisation (Blacklisted A-party CLI)
	Whitelisted traffic parameters to deactivate monitoring on traffic falling within parameter thresholds