

# Fraud Guard



**Fraud Guard** protects your organisation against misuse and abuse of your voice services, tailored to your business' needs. Easy to deploy and run, comprehensive monitoring and reporting capabilities give you flexible management control of your voice costs.

## Overview

Installed on your server and seamlessly integrated with your voice switch, Proteus Fraud Guard is a wallboard application that monitors your voice infrastructure 24 hours a day to provide the solution to a host of fraud activities.

This comprehensive and detailed fraud protection will monitor call data records and automatically alert you if an infringement takes place.

## Executive Highlights

### Fraud Alerts

Proteus Fraud Guard uses the latest IP technology. It examines call detail records, continuously checking against system and custom trigger points, and sends alerts to defined recipients such as network security managers.

### Control Costs and Usage

Proteus Fraud Guard allows you to set limits for costs, for individuals, departments and cost centres, and receive notification as those limits are approached or breached.

### Improve customer service and voice network response

Unlike traditional call management solutions, which are typically reactive and provide post event reporting, Proteus Fraud Guard offers high-quality, real-time, graphical monitoring of activities such as network status, incoming calls summaries, outbound calls and your network status.



## Features

## Benefits

Multi-user, telecom event server

Suitable for any size of organisation

Browser interface

Familiar interface – easy to use, deployed quickly

Multi-browser display for high quality graphics (suitable for wallboard type display unit)

Suitable for single person management through to management control centre environments

Secure user login, tied to an access policy

Allows layered access definable by the user

Each access policy template is used to restrict what a user can view

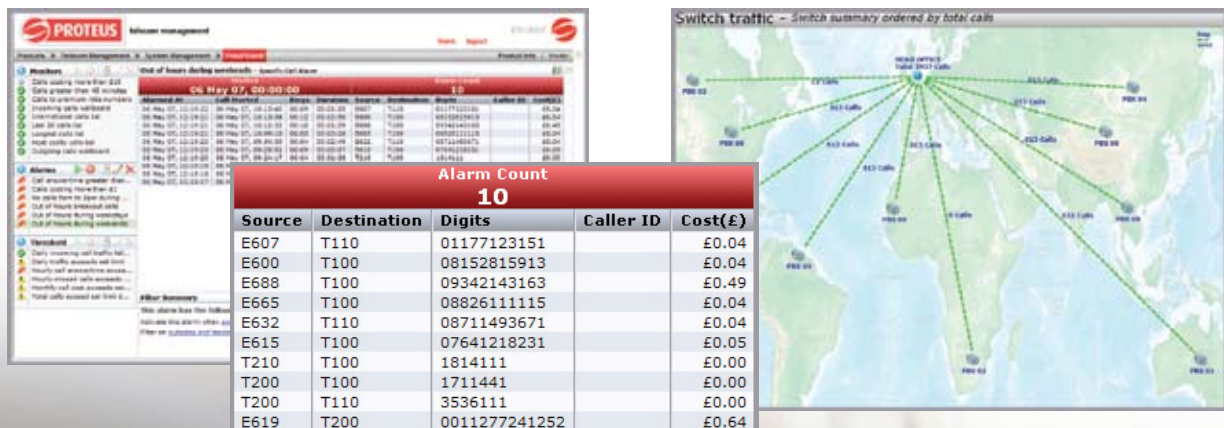
Can be tailored to suit specific organisation policy requirements

Users have their own filters, views and alarms

Analysis can be user defined for maximum results

Instant alarms are raised to local users on screen or remotely via email or other customer specific types, e.g. SMS

You decide who, when and how alerts are managed



## Fraud activities identified

- DISA (Direct Inward System Access)
- Call forwarding, voicemail and auto-attendant (Dial Through Fraud)
- Calls to the maintenance port
- Calls to unexpected destinations
- Calls during company holidays or out-of-hours
- Large numbers of short duration incoming calls (war dialling)
- Network breakout (trunk to trunk calls)
- Calls exceeding particular thresholds (cost, duration, volume)

## Application Benefits

- Immediate, proactive warning of potential fraud
- Improve and actively monitor your operator and support desk response times
- Reduce costs by identifying expensive, long distance premium rate and personal calls as soon as they happen
- Action emergency calls as soon as they happen
- Identify missed calls by CLI to improve customer satisfaction or missed sales opportunities
- Provide up-to-the minute billing projections to control costs
- Confirm that your switches are functioning correctly