ORACLE DATA SHEET

Oracle Enterprise Telephony Fraud Monitor

Oracle Enterprise Telephony Fraud Monitor is a self-learning, scalable solution to help enterprises and Managed Service Providers (MSP) detect phone fraud and prevent it before damage is done.

ORACLE COMMUNICATIONS

NEW FEATURES

- Real-time traffic-spike fraud monitoring
- Dynamic rules
- Import blacklisted destinations
- Customizable actions
- Alerting and Network Policies to block, throttle or redirect
- Supports automated policy update

FRAUD DETECTIONS

- International Premium Rate Service Numbers(IPRS)
- Call Pumping
- Telephony Denial of Service (TDoS)

Overview

To identify fraudulent calls, Oracle Enterprise Telephony Fraud Monitor builds on end-to-end correlated, network-wide session model, then analyzes the model to determine user behavior and compare it with the individual learned behavioral patterns. The session model is built from data generated from probes throughout the network. The probes collect real-time information about all users, customers, trunks, and IP addresses. Based on this passive monitoring system, the solution is undetectable by potential attackers and imposes no performance burden on the network.

Fraud incidents can be identified and alerted within a matter of minutes. Enterprises can leverage these alerts to disable users, trunks, and subscribers on their Session Border Controllers (SBCs), application servers, core network elements, or provisioning servers. Other responses to fraud cases include redirecting users to systems like voicemail or rate limiting the amount of traffic.

Easy Deployment and Integration

There is no need to deploy new or additional network elements in the path of the calls; Oracle Enterprise Telephony Fraud Monitor can extend existing infrastructures to efficiently detect and prevent phone hacking and toll fraud. Existing Oracle Communications SBCs can serve as embedded probes, eliminating the need for additional network equipment. Because Oracle Enterprise Telephony Fraud Monitor probes are passive, they do not add any potential for service quality degradation or impose any risk of negative impact on network availability. Oracle Enterprise Telephony Fraud Monitor comes with a set of predefined rules available for immediate use. If needed, the predefined rules may be extended and customized. Fraud can be detected by triggering a single rule or a combination of multiple rules, such as when several fraud metrics combine to indicate a previously unseen fraud incident.

Fraud Detection

Oracle Enterprise Telephony Fraud Monitor includes three major functions—passive monitoring of all subscribers/IP addresses, identification of their behavioral patterns, and assignment of scores and thresholds to trigger fraud risk alerts.

- **Monitoring**: Real-time traffic is monitored for sudden increases or spikes. An alert or trigger is generated when a spike is detected. Reports may be visually displayed for each spike via a web-based interface.
- **Traffic Analysis**: Oracle Enterprise Telephony Fraud Monitor automatically learns traffic patterns to destinations over time. It uses rules to calculate values from multiple metrics such as number of concurrent calls, aggregate call duration and calls per second, enabling a more accurate assessment of the situation. The self-learning feature saves time by combining the gathered values into a score for each user and for each user group, with no per-user configuration required. If needed, exceptions can be configured on a per-user basis.
- **Score Assignments and Threshold**: Scores are applied when thresholds are exceeded based on flexible rules. If scores are calculated that exceed predetermined thresholds, alarms are generated warning of fraud risks. Any deviation from the pattern indicates that the network is facing could be a fraud attack. However, relying on just one metric can result in false alerts. Oracle Enterprise Telephony Fraud Monitor uses rules to calculate values from multiple metrics, enabling a more accurate assessment of the situation. It comes with a set of predefined rules available for immediate use and offers the ability to extend the predefined rules with customized sets of rules:
  - **Metrics:** Oracle Enterprise Telephony Fraud Monitor comes with a library of metrics to measure the basic attributes of subscriber behaviors, for example, minutes spoken, , concurrent calls, calls per second.

ORACLE

- **Rules:** The rules are used to determine what call behavior is considered fraudulent and at what severity, according to a rating system. A rule can make use of any number of metrics.
- **Score:** The score is the accumulation of the values and is used to determine whether or not a destination has surpassed a threshold.
- **Threshold:** Surpassing a defined threshold causes an alarm to be raised. Thresholds can either be static values or be dependent on a key performance indicator (KPI). The most-powerful thresholds are fully automatic and depend on deviations from previous behavioral patterns.

 Blacklists: Blacklists may be loaded manually and will invoke triggers on known fraudulent destinations.

Fraud Prevention

There are countless ways to start an attack, such as hacking into an enterprise's IP private branch exchange (PBX) or voicemail system, using standard passwords on web graphical user interfaces (GUIs) of VoIP phones, or abusing leaks in enterprise voicemail systems.

 Agnostic Attack: Oracle Enterprise Telephony Fraud Monitor looks at the one thing all attacks have in common—the deviation of the current behavior from the user's normal behavioral pattern. This enables the software to both cover the current attack scenarios and detect future ones.

 Real-time Prevention: The real-time data capture of user behavior enables better, faster identification and prevention of fraudulent behavior. The entire process, from detecting an attack to stopping it, is shortened to just a few minutes—or immediately, as with blacklisting. The system keeps a dynamic list of destinations that have recently been sources of attacks in any of the connected networks. If the corresponding blacklist feature is enabled, then attacks can be stopped immediately.

 Real-time Alerts: When Oracle Enterprise Telephony Fraud Monitor calculates scores beyond safe thresholds, it provides immediate alerting in case of known fraud scenarios. It also generates an automatic alert if call patterns do not match the pattern of the corresponding user or user group, and a critical threshold has been reached.

Summary

Oracle Enterprise Telephony Fraud Monitor is a self-learning, scalable solution that helps enterprises detect fraud and prevent it before damage is done. The software system is easy to deploy and can fully integrate with existing infrastructure. Oracle Enterprise Telephony Fraud Monitor monitors all calls in the VoIP network, performs real-time analysis of user behavior, and learns the behavioral patterns of each individual user and user group. Using predefined or customized rules from multiple metrics, it identifies deviations in user behavior and stops fraud attacks efficiently and effectively. For more information, go to www.oracle.com/industries/communcations

ORACLE

CONTACT US

For more information about [insert product name], visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services