Oracle Communications Fraud Monitor

Oracle Communications Fraud Monitor is a self-learning, scalable solution to help network operators detect phone fraud and prevent it before damage is done. It is part of the Oracle Communications Session Monitor Family of Products, an end-to-end network visibility and monitoring software system that increases the return on investment (ROI) of Long Term Evolution (LTE), IP Multimedia Subsystem (IMS), and Voice over IP (VoIP) deployments, and provides an unprecedented view of the network for both operations management and in-depth troubleshooting.

Overview

Oracle Communications Session Monitor Family of Products allows enterprises and service providers to quickly and securely migrate to Internet Protocol (IP) networks, reduce operational costs, generate additional revenue, prevent voice fraud, and minimize churn. Oracle Communications Session Monitor Family of Products is a proven, carrier-grade solution for enterprise networks and fixed and mobile service providers with more than 100 deployments globally, including many tier-1 service providers.

To identify fraudulent calls, Oracle Communications Fraud Monitor builds on end-to-end correlated, network-wide application-layer data to perform a real-time analysis of user behavior and compare it with the individual behavioral patterns that are automatically learned by the system for each subscriber. Passive, software-based Oracle Communications Fraud Monitor probes are deployed throughout the network, and Oracle is embedding Oracle Communications Fraud Monitor probes into its network session delivery and control infrastructure portfolio to allow network operators to optimize their IP communications networks while reducing network cost and complexity. 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 are identified and alerted within a matter of minutes, potentially even while the sessions are being set up. Network operators 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 (for example, to a voicemail system) or rate limiting the amount of traffic. Utilizing Oracle Communications Session Monitor Family of Products, network operators can further analyze and document the attack vector, install appropriate detection methods, and prevent future similar attacks.
Oracle Communications Session Monitor Family of Products are a robust network intelligence solution that helps service providers and enterprises to improve productivity and efficiency by providing a high-level overview of what is actually happening in their networks. Using Oracle Communications Session Monitor Family of Products with Oracle’s network session delivery and control infrastructure products allows service providers and enterprises to get the most out of their IP communications networks with unique, real-time management capabilities. Network operators can move beyond individual element management and benefit from real-time, network-wide visibility into multi-vendor IP communications networks.

**Related Products**
- Oracle Communications Operations Monitor
- Oracle Communications Control Plane Monitor
- Oracle Enterprise Operations Monitor
- Oracle Communications Fraud Monitor
- Oracle Communications Session Border Controller

**Easy Deployment and Integration**

There is no need to deploy new or additional network elements in the path of the calls; Oracle Communications 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 through a simple software upgrade, eliminating the need for additional network equipment. Because Oracle Communications 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.

**No Configuration Needed**

Oracle Communications Fraud Monitor comes with a set of predefined rules available for immediate use. If needed, it is also possible to extend the existing configuration with customized sets of rules. 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.

**Collaborative Blacklisting**

Fraudsters don’t limit themselves to individual networks, but often try to abuse multiple international networks at the same time. The Oracle Communications Fraud Monitor system allows an automated and manual update of the blacklisting information, including IP addresses, phone numbers, and Session Initiation Protocol (SIP) user agents used for fraud. This information originates from verified fraud cases and allows for fast and accurate alerting even if a new fraud scenario has not been seen in the monitored network.

**Figure 1: Oracle Communications Fraud Monitor**

Oracle Communications Fraud Monitor has an easy-to-use, web-based interface for simplifying configuration, management, monitoring, and operations. The lower chart shows the red baseline closely matching the current traffic, while the score information in the upper chart reflects peaks that far exceed usual points awarded and indicate blacklist triggering due to a fraud incident.

**Self-Learning Solution**

Oracle Communications Fraud Monitor monitors all calls in the VoIP network and learns the behavioral patterns of each subscriber over time. It uses rules to calculate values from multiple metrics such as number of concurrent calls, time-based traffic patterns, unusual source IP addresses, or call destinations, 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.

**Attack Agnostic**

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. Oracle Communications 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.

**Stopping Fraud As It Happens**

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 subscribers 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.

**Unique Approach to Stopping Fraud**

Unlike competitive products, Oracle Communications Fraud Monitor takes into consideration calls that have not yet finished, which allows prevention of fraud while it is in progress, rather than having to wait for call detail records (CDRs) to be rewritten or billing cycles to finish.

**Further Prevention of Fraud Attacks**

When Oracle Communications Fraud Monitor calculates scores beyond safe thresholds, it provides immediate alerting in case of known fraud scenarios.

**Easy to Use**

Oracle Communications Fraud Monitor 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. With Oracle Communications Session Monitor Suite, fraud incidents can be analyzed in depth utilizing call history, message flow diagrams, PDF reports, and packet capture (PCAP) file exports.

**How Oracle Communications Fraud Monitor Works**

Oracle Communications 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**: All subscribers/IP addresses in the entire network are monitored, and reports can be visually displayed for each one via the web-based interface.
- **Behavioral Analysis**: Oracle Communications Fraud Monitor automatically learns behavioral patterns of all subscribers and IP addresses over time.
- **Score Assignments and Threshold**: Scores are applied to all calls and to all
subscribers and IP addresses based on flexible rules. If scores are calculated that exceed predetermined thresholds, alarms are generated warning of fraud risks.

**Scoring**

Any deviation from the user’s behavioral pattern indicates that the network is facing a fraud attack. However, relying on just one metric can result in false alerts. Oracle Communications Fraud Monitor uses rules to calculate values from multiple metrics, enabling a more accurate assessment of the situation. It combines these values into a score for each subscriber. 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 Communications Fraud Monitor comes with a library of metrics to measure the basic attributes of subscriber behaviors, for example, minutes spoken, time of day, concurrent calls, unusual call destinations, and unusual source IP addresses.
- **Values**: The values are the result of the weightings attributed to each rule. Values are provided for the current moment and as an average for every hour.
- **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 user 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.

**Summary**

Oracle Communications Fraud Monitor is a self-learning, scalable solution that helps service providers and 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 Communications 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.

**Contact Us**

For more information about Oracle Communications Fraud Monitor, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.