Oracle Communications Security Shield Cloud

Capitalizing on adaptive intelligence and dynamic risk assessment, the Oracle Communications Security Shield Cloud delivers a 360° view of your network's telecom traffic, validates every call, and automatically enforces policy-based call handling - including the killing of malicious calls, all in real-time.

ALWAYS-ON, COMMUNICATIONS SECURITY

Today's cyber-criminals are targeting the communications infrastructure of enterprises like never before and succeeding well beyond most executives' perceptions. These adversaries are now dominated by nation-states and organized crime who have strong incentives and unlimited resources to attack your communication networks. Using new and ever more innovative hacking techniques, they are aided by the enterprise's attack surface constantly shifting. Further, today's legacy systems rely on historical knowledge and rigid rules, which drives heighten volumes of false-positive alerts for an already overloaded security staff to sift through. And, with every breach, these criminals can cost your business impaired productivity, heighten operational risks, reputational damage, and for SMBs - even financial ruin.

The Oracle Communications Security Shield Cloud (OCSS Cloud) service evaluates calls crossing an enterprise's network edge, detects malicious call signatures and behaviors, and produces a risk assessment for each call, all in real-time. Guided by this risk assessment, it uses policy-based actions to then automatically control the call's resolution, aligning the call's handling with an enterprise's own perspective towards risk.

OCSS Cloud's dashboard provides a 360° view of your telephony traffic and any risks, the mitigation of threats, and all actionable insights enabling smarter investigations. Its automated control capability performs a dynamic risk assessment for every call, validates the caller's identity, and performs threat signature and anomaly behavior detection to spot bad actors. Its real-time enforcement function automates the threat mitigation by leveraging the Oracle Enterprise Session Border Controller.

OCSS Cloud's capabilities protect enterprises from telecom-based threats, such as theft of service, harassment calls and account takeover. Leveraging Oracle Cloud's

Key Features

- 360° visibility of real-time communications traffic
- Dynamic Risk Assessment of every communication for call validation
- Advanced AI/ML including:
  - Behavioral Analytics
  - Threat Signature Detection
  - Anomaly Detection
- Always-on, Automated Threat Detection and Mitigation
- Leverages Oracle Cloud's AI, Analytic and Security capabilities

Key Business Benefits

- Protects real-time communication services, with actionable insights to automatically mitigate risks
- Validates your callers

  Addresses telephony-based-threats such as:
  - Account Takeover Fraud
  - Nuisance Calling (Caller-ID Spoofing)
  - Toll Fraud
  - Toll Free Traffic Pumping
  - Telephony Denial of Service (TDoS)
- Provides a comprehensive, intuitive view of your real-time communications traffic
- Provides analytics for more efficient incident management
- Requires minimal time for set-up and learning (training)

analytical, machine-learning (ML) and security capabilities prevents the high level of false-positive alerts suffered by existing historical solutions, and enables your highly skilled security staff to focus on keeping your core business safe.

360° VISIBILITY

The Oracle Communications Security Shield Cloud provides real-time visibility of your communications traffic through an intuitive, comprehensive, 360° dashboard. The business analytics information provides actionable insights as attacks or anomalies occur, enabling quick investigations and remedies while attacks are still in progress. The dashboard provides information on traffic metrics and patterns, on threat occurrences and their sources, and on the reputation score distribution for calls, as well as documenting all of the actions taken for identified threats.

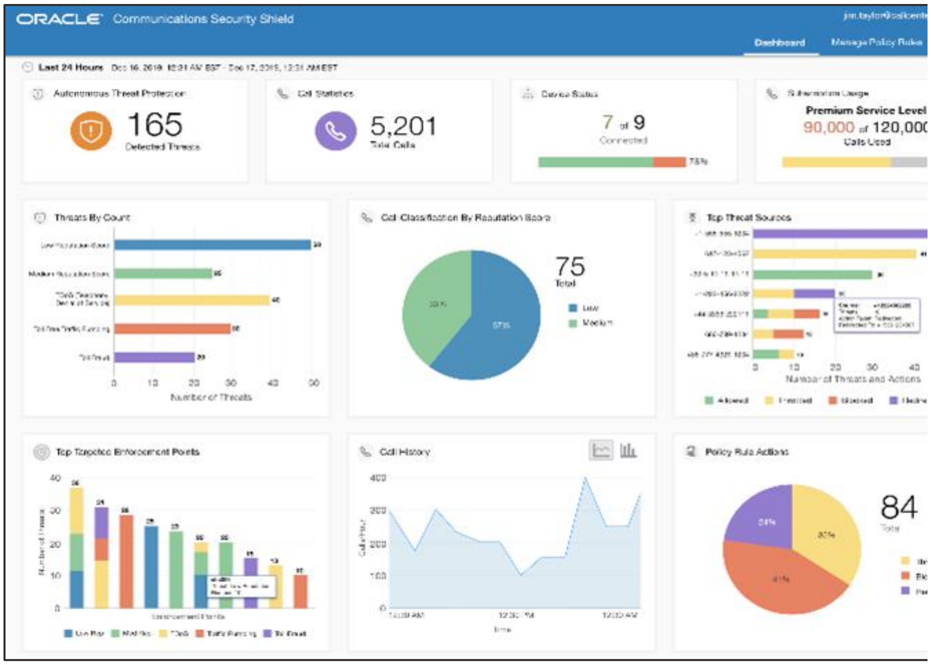

Figure 1 - Oracle Communications Security Shield Cloud Dashboard

DYNAMIC RISK ASSESSMENT

Communications traffic is secured through real-time risk assessment leveraging adaptive intelligence and advanced AI/ML analytics. This assessment verifies the identity of the caller and called party, and determines the risk they pose to your business or infrastructure by identifying fraudulent calls and spoofing. OCSS Cloud uses Behavioral Threat Analytics (using anomalous traffic behavior patterns, such as call from/to suspicious number ranges), Threat Signature Detection (using known traffic patterns), and Anomaly Detection Methods (using multivariate statistical analysis), and may leverage real-time phone number intelligence. Together, they enable a data-driven Dynamic Risk Assessment (“Reputation Score”) to be generated for each call, and your enterprise can select which policies apply for each class of reputation score, so that all subsequent call handling aligns with your business’s risk policies.

The advanced detection methods supersede (static) rule-based mechanisms of legacy or knowledge-based authentication (KBAs) systems. KBA systems are especially susceptible to breaches because adversaries can compile a ‘profile’ through phishing/pharming and information available on the dark web. OCSS Cloud’s advance detection methods rely, in part, on historical and real-time data, which

Related Enterprise Communication Products

The following products support Oracle Communications Security Shield Cloud:

- Oracle Enterprise Session Border Controller
- Oracle Enterprise Communications Broker
- Oracle Communications Interactive Session Recorder

provides sound actionable insights, and helps to avoid the massive volume of false-positive alerts that legacy solutions may generate. This allows your IT security staff to focus on real issues more central to your core business.

REAL-TIME ENFORCEMENT

The Oracle Communications Security Shield Cloud's policy-based enforcement capability enables enterprises to configure how to mitigate calls with unacceptable risk scores. This ensures that the handling of each call aligns with the enterprise's own risk tolerance guidelines. Options for mitigating attacks include:

- Blocking calls during call set-up;
- Redirecting calls to an investigator or a call recording server; and
- Terminating live calls.

The actual enforcement actions are executed by the Oracle Enterprise Session Border Controller. For inbound calls, OCSS Cloud provides the ability to generate notifications to your call agents.

An overview of all enforcement actions is provided by the OCSS Cloud's dashboard for diagnostic visualization.

SUMMARY

With the Oracle Communications Security Shield Cloud, Oracle provides a unique real-time offering that capitalizes on Oracle Cloud's advanced analytical methodologies, AI/ML capabilities and security features. The objective of protecting your communication infrastructure and services is to increase your productivity, reduce your operational risks, reduce "alert fatigue." and time wasted by your IT security staff, maintain your band's loyalty, and to protect your bottom-line.

It encompasses separate yet symbiotic functionalities, including a 360° dashboard for data visualization; adaptive intelligence and analytics for dynamic risk assessment; and real-time enforcement to ensure threats do not develop into network or service breaches. In doing so, OCSS Cloud addresses many of the communication infrastructure and service security threats by providing an always-on, real-time communications security solution to protect your network from cyber-criminals.

CONNECT WITH US

To learn more, visit: oracle.com/security-shield

To request follow-up, visit: Contact Us
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle-communications

facebook.com/oraclecommunications

twitter.com/oraclecomms

Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle Corporation.