Oracle Communications Security Shield Cloud

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

Always-on communications security

Today's cybercriminals are targeting the communications infrastructure of enterprises like never before and succeeding well beyond most executives' perceptions. As workforces became remote, cybercriminals besieged workers and businesses with increasingly sophisticated attacks like robocalling, shellshock, caller-ID spoofing, denial-of-service (DoS) attacks, impersonation, and artificial traffic. The impact was so profound that the World Economic Forum in its Global Risks Report 2021 ranked cyberattacks and data fraud in the top three of "most worrisome" trends for companies globally, and in the United States, the FBI reported a record-breaking 791,790 cybercrime complaints, a 69-percent increase from the previous year.

Communications-based threats, such as theft of service, harassment calls, and account takeover disruptions can seriously harm your brand and cause significant financial damage. Further, today's legacy systems rely on historical knowledge and rigid rules, which drives heightened volumes of false-positive alerts for an already overloaded security staff to sift through.

Oracle Communications Security Shield Cloud (OCSS) 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 and all pre-answer. OCSSC provides observability of your telephony traffic, type of calls, risks, and actionable insights enabling smarter investigations.

It leverages machine learning-based (ML) behavioral analytics to look behind the incoming phone number and tracks actual call behavior indicative of spam activity, malicious activity and intent. OCSS generates a risk assessment score that provides an easy-to-understand classification. Using the results from ML-based behavioral analytics, OCSS provides information on intent of a call (for example: probable scam or fraud call, a likely robocall, or probable telemarketing call, etc.)

Guided by the risk assessment, call filters can be enabled that determine how you want to treat calls. User controlled call filters allow aligning the call's handling with an enterprise's own tolerance for risk.

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

With unwanted and unwelcome calls filtered out, or at least flagged, you can avoid costs by reducing time wasted on answering these calls. Moreover, with higher risk calls identification, you can save on verifying or authenticating users by only sending higher risk callers to an advanced verification process and low risk callers to an expedited process. OCSSC's capabilities protect enterprises from telecom-based threats, such as theft of service, harassment calls and account takeover.

Observability

The Oracle Communications Security Shield Cloud provides real-time visibility of your communications traffic through an intuitive, comprehensive, 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.

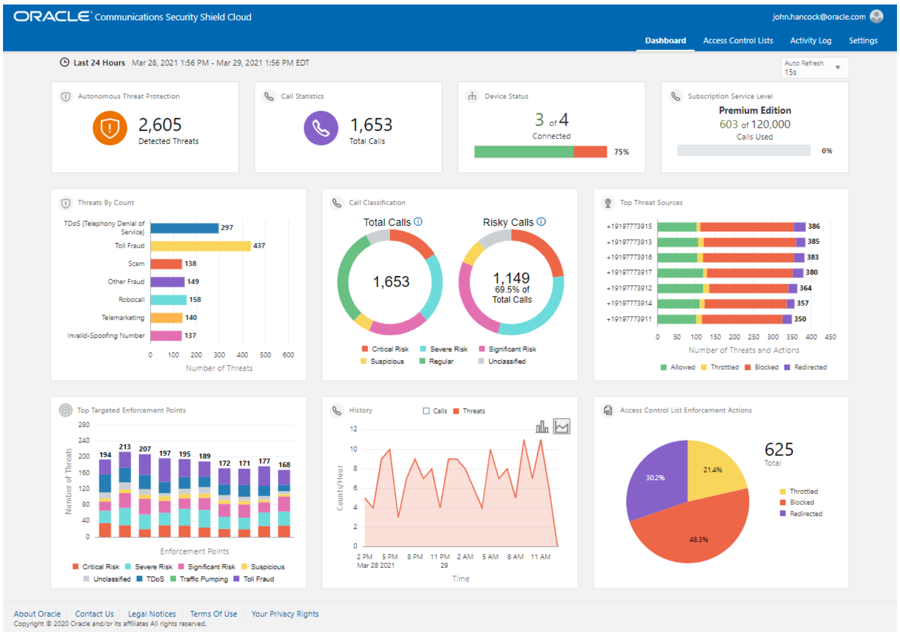

Figure 1. Oracle Communications Security Shield Cloud Dashboard.

Dynamic risk assessment

Communications traffic is secured through real-time risk assessment leveraging ML analytics. This assessment verifies the identity of the caller and called party, the type of call and determines the risk they pose to your business or infrastructure. A data-driven Dynamic Risk Assessment ("Reputation Score") is 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 provides sound actionable insights, and helps to avoid the massive volume of false-positive alerts that legacy solutions may

Key business benefits

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

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, specific type of calls (so-called no value calls like robocalls) as well as generic access control lists for allowing or blocking calls to enter or leave your network. 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 setup
- Redirecting calls to an investigator or a call recording server
- Terminating live calls
- Rate limiting calls to a specific calls per second limit

The enforcement actions are executed by the Oracle Enterprise Session Border Controller or Oracle Session Router.

Summary

With OCSS, Oracle provides a unique real-time communications security solution that capitalizes on Oracle Cloud's advanced analytical methodologies, AI/ML capabilities and security features. OCSS provides always-on, real-time communications security to protect your network from cybercriminals.

The objective of protecting your communication infrastructure and services is to increase your productivity, reduce your operational risks, improve productivity of your security staff, maintain your brand's loyalty, and protect your bottom-line.

Oracle can provide you with a risk assessment of your environment based on your unique inputs. Ask your Oracle representative how you can experience the benefits of OCSS.

Related Oracle Communication products

- Oracle Enterprise Session Border Controller
- Oracle Enterprise Communications Broker
- Oracle Communications Session Router

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle