SECURONIX™

SOLUTION BRIEF

Oracle Cloud Infrastructure Security Monitoring

Oracle Cloud Infrastructure (OCI) is emerging as the platform many enterprises are choosing as their public cloud. But as usage grows, so does the potential for attack. As with most public clouds, OCI provides built-in security for traditional attacks such as malware and denial of service. However, OCI is vulnerable to insider threats such as credential compromise and data exfiltration.

As network control moves, the focus of security operations pivots from prevention-centric tools, such as firewalls and endpoint solutions, towards detection-centric solutions, such as SIEM and UEBA.

Utilizing advanced analytics for insider threat detection and strong security integrations, Securonix provides complete security for Oracle Cloud Infrastructure environments.

Securonix and Oracle Cloud Infrastructure

Securonix integrates along the entire OCI infrastructure lifecycle, enabling SOC analysts to detect threats quickly.

In order to gain quick access to OCI security events, Securonix has a direct integration with the Oracle CASB Cloud Service Pub/Sub, enabling the collection and analysis of logs across various OCI components. Securonix also integrates with several other OCI data touchpoints, including governance and audit events, performance monitoring events and several other key OCI services.

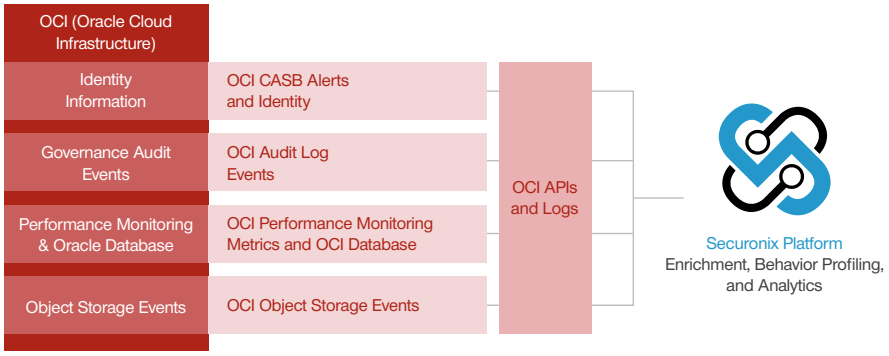

Figure 1: Securonix Integrates with the Oracle Cloud Infrastructure Products Shown Above

OCI CASB and Performance Monitoring Integration

By integrating with the Oracle CASB Service, Securonix monitors actions taken within the complete suite of Oracle services, such as analytics, identity, and cloud databases. This enables comprehensive visibility across your Oracle Cloud Infrastructure.

Securonix also integrates with Oracle Cloud Performance Monitoring in order to observe changes to provisioned resources such as virtual machines and networks. Event ingestion from these sources is critical for identifying threats such as anomalous service usage or account behavior, unauthorized or unusual cloud resource usage, and cloud access from unusual geographic locations – all possible indicators of cloud compromise.

Solution Benefits

- Gain full visibility into Oracle Cloud products including performance monitoring, governance and audit, identity, and OCI database and object storage.
- Fast detection and response using streamlined, direct API integration with Oracle Cloud.
- Decrease mean-time-to-response time using enriched data combined with additional context for accurate threat modeling.
- Visualize activities and changes in your OCI infrastructure with out-of-the-box dashboards and reports that are customizable.
- Protect multi-cloud environments with a single solution.

Securonix Threat Modelling Goes Further To Detect Advanced Attacks Such as Cryptojacking

Most attacks today are not detectable using a single security event. Sophisticated attackers use several steps to accomplish their goal, which creates alerts that need to be examined together as a series in order to identify the threat. Securonix threat models stitches together indicators of compromise (IOC) across data sources in order to detect such advanced attacks.

For example, in order to detect a cryptojacking attack, a combination of IOCs may include:

- A suspicious console login found in the OCI console logs.
- A related permission elevation found in the Oracle Identity logs
- A spike in start instances on OCI, or rare start instances found in the Oracle Cloud Performance Monitoring logs.
- Event logging being disabled in the Oracle CASB logs.

These IOCs are shown within Securonix in a threat chain view, allowing analysts to investigate threats mapped to the different attack stages corresponding to the MITRE ATT&CK framework.

Conclusion

Securonix provides capabilities beyond simple log aggregation. Using multiple enterprise services and data touchpoints, Securonix creates comprehensive protection for Oracle Cloud Infrastructure. The Securonix solution ingests data from relevant data sources in order to provide accurate threat detection through correlation and analytics. Securonix also supports fast search and hunting capabilities using stored data and is capable of scaling to meet the volume of demand, no matter how large your OCI usage.

Identifying threat context by intelligently enriching threat data together with relevant contextual information is essential in order to identify advanced threats. Coupled with behavior analytics, Securonix provides a platform that not only identifies advanced threats, but also recommends remediation actions.

A modern cloud infrastructure requires cloud native security that can handle the scale, speed, and accessibility required. Securonix provides multiple integrations for broad coverage of Oracle Cloud Infrastructure offerings, in a mature solution. It provides you with single pane of glass visibility across your entire environment.

The Securonix platform delivers all these needs, and more. As an industry leader recognized by Gartner, Securonix is an ideal solution for keeping your Oracle Cloud Infrastructure secure.

Key Use Cases

- Unauthorized access such as a login from a rare IP or geolocation, a spike in failed logins, a land speed anomaly, or a malicious IP.
- OCI configuration anomalies such as a spike in instance creation or deletion, suspicious admin activities, or unusual app engine requests.
- Suspicious OCI Identity Management activity such as suspicious user creation, admin privilege changes, password policy changes, or rare privileged activity.
- Anomalous API connections including from a rare IP or geolocation, or a malicious IP address.
- Suspicious OCI virtual network traffic including port scans or connections on anomalous ports.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000