

Datasheet

September, 2020

# Omega Core Audit <sup>TM</sup>

For Oracle Database, with built-in SIEM integration



Access control, audit monitoring and protection in real time

## Key Features & Benefits

- Access Control
- Standard Auditing
- Real-Time Protection for DDL and DML commands
- Protection from DBA
- Change Control
- Duty Separation
- Security Events Trail
- Policy-based evaluation
- Multi-factor authorization
- Application & environment context authorization
- Issue Tracking
- Security Management
- Out-of-box, software-only
- SIEM integration



Omega Core Audit is a software security solution created to help customers approach the complex and difficult security challenges in Oracle Database Systems - protecting against outsider and/or insider threats, unauthorized access, and enforcing duty separation in meeting regulatory compliance requirements, external or internal.

Omega Core Audit implements strong practices of Access Control, Continuous Auditing and Real-Time Protection, providing clear visibility and control into database activity, including privileged accounts, like DBA-s, thus leading to a safer and more secure information system.

These are top requirements for database owners looking to protect sensitive business or privacy related data of customers, employees and partners, thus conforming to best security compliance standards and recommendations.

Omega Core Audit can be virtually used by any organization that uses Oracle Database and it is looking to implement database information security compliance standards, best industry practices and strong internal security controls.

The type of out-of-box, software-only solution, allows for quick implementation without interfering with existing functionalities and needs no additional software licenses or devices.

## Introducing Omega Core Audit

Omega Core Audit is an out-of-box, software-only solution. It is a full back-end solution that is installed in minutes and easily managed by its applicative interface. The solution enhances the Oracle native security features with state-of-art and value-added programming and automation. It brings easiness to its users letting them focus only on the conceptual security tasks, without concentrating on complex technical security configurations, made easy and plainly presented to them via its rich user interface.

Security applied at the core - from within the database - ensures same rigid level of compliance from all possible connection directions, applications, users or devices and offers immediate auditing and protection action before user's actions or transactions. It also requires no (or very minimal, industry recommended) changes in existing security configurations.

Omega Core Audit approaches Access Control, Auditing and Protection security requirements by implementing a policy-rule-condition evaluation model and multi-factorial authorization. Auditing and Real-Time Protection are triggered by defining Protection Areas and applying authorization rules.

## Controlling privileged accounts

Database privileged accounts, DBA-s, Application Owners and Batch Accounts also represent the most common “door” for attacks. This can lead to unauthorized access and information compromising. Omega Core Audit restricts privileged accounts and DBA-s from accessing and modifying application data and also from manipulating the database beyond their regular duties, although they might have (and usually do) the necessary privileges.

## Separation of Duty

Omega Core Audit separates duties of normal database management from those related to audit, security and compliance. Furthermore it comes with four out-of-box predefined roles: Auditor, Account Manager, Security Analyst and Administrator for full functionalities.

## Database Auditing and Protection for Compliance made easy

Omega Core Audit relieves the information owners and system administrators from the complex tasks of performing auditing and protection tasks that can take long and periodic hours to develop, setup, maintain and report. Omega Core Audit ensures an answer to the classical questions – Who/What/How/When/Where in regard to users’ activity in the system. To best meet compliance requirements you need to control access, audit and protect data from unauthorized access and also have an effective and accurate reporting.

### Omega Core Audit main components and features:

- **Access Control** Establishes database perimeter defense by applying mandatory access control to all connections to the database. No users, including highly privileged accounts and DBAs, can log on to the database without complying with the predefined access policies.
- **Standard Auditing** Audits the system for user activity, user statements and operations on system objects, thus enforcing security controls and meeting regulatory compliance.
- **Real-Time Protection** Real-time protection on top of fine-grained auditing for data access and changes (DML commands, SELECT included); Change management control for structural changes (DDL commands) and system events with object source code history.
- **Policy-based evaluation** Complex and difficult tasks of auditing and protection are presented to the user into a policy-rule-condition evaluation hierarchic model, according to specific modules. Conditions are evaluated based on operand values, trust level or logical expressions.
- **Multi-factor authorization by environment and application context** Multiple factor like user, hostname, IP address, program name, client identifier, other data like and dozens more, offer multiple combinations of user environment authorization. Row and column authorization achieves the same for application context.
- **Unified Security Events Trail** A single unified trail for security events that captures audit trails from different sources offers benefits in visualization, management and provides a better look into the monitored database activity.
- **SIEM integration** Supports Splunk SIEM - enhanced support through Omega Core Audit App for Splunk! Opened to all SIEMs/Log Management Systems supporting records ingest via TCP or pull by Oracle query.

### Contact us

For more information about Omega Core Audit please visit [www.dataplus-al.com](http://www.dataplus-al.com), or contact us at:

### DATAPLUS

Tirana, Albania

Street Address: Bul. Zog I, P. “Edicom”, 8F.

E-Mail: [info@dataplus-al.com](mailto:info@dataplus-al.com)

Cel: +355 68 2061664

Tel: +355 42419275

Copyright © 2007-2020 DATAPLUS. All rights reserved. Omega Core Audit is registered at US Copyrights Office and is protected by US and international copyright laws. Omega Core Audit and the DATAPLUS logo are trademarks of DATAPLUS. All other trademarks are the property of their respective owners.