Whitepaper

September, 2020

Omega Core Audit ™

For Oracle Database, with built-in SIEM integration

Access control, audit monitoring and protection in real time

Introduction

The database is usually the central point of enterprise's most valuable informational assets, data on customers, partners, transactions, financial and much more. With the arrival of the information age, millions of such records owned by the company are being confronted with an ever increasing number of attacks from insider and/or outsider sources who are trying to gain unauthorized access to steal, destroy, compromise or retrieve industrial espionage data. Database security is one of the top concerning priorities of the information owners that needs to comply with more internal and external regulatory compliance practices and standards that require stronger information security controls.

The database remains today one of the less protected point of the enterprise's information, which traditionally has been focused mostly in protecting perimeter networks, or operating systems which do indeed create some barriers, but which are few effective against insider threats, especially from privileged account holders, who not only are within the internal network, but by nature of their jobs may access information bypassing application security, or own a high security clearance on it. Furthermore the traditional network and OS protection has been modeled with the concept in mind of the once "isolated" database within the internal network, but due to their increasing business services and interfaces, today's databases are much more open toward the external networks and internet, and the number and sophistication level of the attacks has since then increased.

In all of the recent studies performed by the authoritative bodies of the field, inside breaches account for more than 50% of data breaches, usually with higher impact than breaches from outside.

The Challenge

Implementation of stronger information security controls requires implementation of stronger database security measures, mainly access control, audit, protection and accurate reporting. While many third party solutions do have built-in application security, these measures are effective only when the database is accessed through the application, thus not accounting for many other types of connections.

Native security features offer enough details and capabilities to fulfill compliance requirements, but their development, implementation, maintenance and reporting represents a considerable and delicate amount of work that requires time and human resources involved in a continuous process. Audit trail purging and management is something to be taken cared too. A policy-rule based implementation would be needed for proper formalization of the security controls in levels higher then simply technical. A full set of effective and accurate data visualizations must be in place. And the delivery of records to external log systems and SIEMs for central and safe storage and better alerting and monitoring is another best practice, and in some industries, a requirement too.

Consolidating, enhancing and formalizing the native features into a fully automated solution are further steps in this challenge.

Introducing Omega Core Audit

Omega Core Audit is an out-of-box, software-only security and compliance solution for Oracle databases. 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 does not interfere with existing functionalities and also requires no (or very minimal, industry recommended) changes in existing security configurations.

Omega Core Audit enhances and automates the database native security features by state-of-art programming of these the security processes into software modules representing main compliance requirements like Access Control, Auditing and Real-Time Protection, all integrated into a central solution.

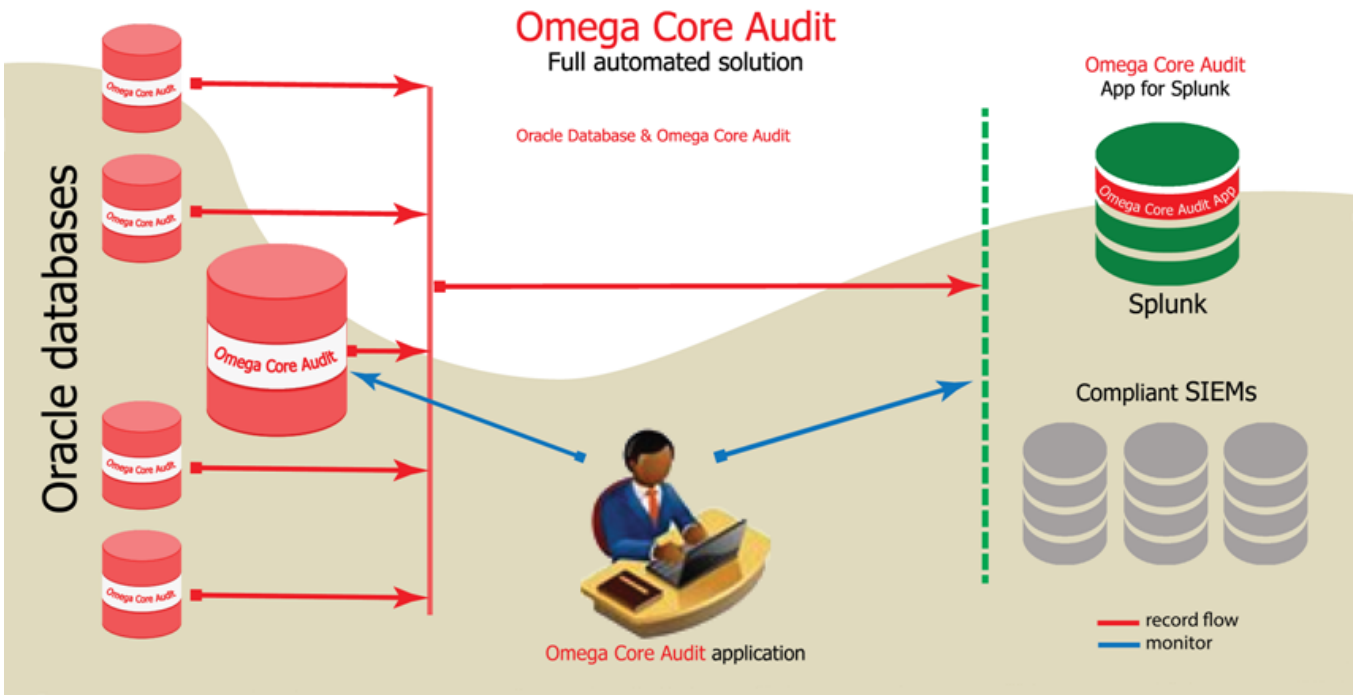
Security controls can be implemented as policy-based evaluation, implemented as a policy-rule-condition schema. Multi-factor authorization of user & environment values context is exercised in real-time. The approach brings flexibility and easiness in implementing security controls.

Flexible unified Security Events searching, data export capabilities in common formats like Text /XLS/XML and a set of dynamic reports ensure analytical capabilities to security information events and a clear picture of activity inside the database.

Omega Core Audit Architecture

The Omega Core Audit solution has three main components:

- **Omega Core Audit Engine**: An Oracle PL/SQL software package containing core audit and protection logic, Back-End installed into the target database under the SYS schema and running with its privileges.
- **Omega Core Audit Repository**: An Oracle Schema Repository containing all system configurations and audit events, Back-End installed into the target database.
- **Omega Core Audit Application**: A Windows-based client desktop Application, connecting to the target database and interacting with the Engine and Repository.



The system implements audit and protection in four modules:

- 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 DDL Change management control for structural changes (DDL commands) and system events with object source code history.
- Real-Time Protection DML Real-time protection on top of fine-grained auditing for data access and changes (DML commands, SELECT included).

Although a fully autonomous solution regarding Oracle Database Security, Omega Core Audit has built-in support for, and features compatibility to all common SIEM and Log Management Systems.

Highlighted: Splunk

Controlling privileged accounts

Database privileged accounts - DBA-s, Application Owners and Batch Accounts are present in all database systems enabling administrators to perform their daily duties like performance tuning, backup and recovery, space management, user management, replication and patching. These privileged accounts in the same time are the main target of intruders and or insider abusers, because of their special rights into the database. Compromise of these accounts leads to unauthorized access and information breach.
Thus enforcing controls on privileged accounts is a top requirement of all main compliance standards, best practices and internal security policies.

Omega Core Audit restricts privileged accounts from accessing and modifying application data and also from manipulating the database beyond their regular duties, even if they have (and many do) the necessary privileges that permit so. Access Control, Audit and Real-Time Protection features are exercised on the high privileged accounts too, DBA included.

Separation of Duty

Duty Separation is also one of the most important security configuration and top list in regulatory compliance requirements. Same person must not be DBA, Security Officer or Auditor at the same time; the functionalities and responsibilities assigned to organization's human resources must be clearly distinct.

Omega Core Audit separates duties of normal database management from those related to audit, security and compliance, running the later inside its core. After the install you can further harden the system by revoking a few audit privileges from privileged accounts and roles. Thus the DBA's, Application Owners, Batch Accounts, Backup Operators, Space Administrators and more, can continue exercising their normal duties, but without interfering with issues of security and auditing.

Inside its domain, Omega Core Audit addresses separation of duty and responsibilities by its four out-of-box roles that perform the following:

- Administrator - Full functionalities.
- Account Manager - Accounts, Profiles, Roles and Privileges.
- Auditor - Access Control, Standard Audit and Real-Time Protection.
- Security Analyst - Security Analyst, overall monitoring.

Unified Security Events Trail

A single unified Security Events trail that integrates events from different source modules offers benefits in visualization, management and provides a better look into the monitored database activity. It also simplifies record management and optionally the transportation of records to external log collection systems (SIEMs).

Security Events are visualized and searched in summary and record level by the Omega Core Audit application.

Key features & benefits

- Access Control, mandatory authorization of the database logon process
- Continuous Audit Monitoring, highly detailed, up to the full SQL text and SQL bind parameters
- Real-Time Protection for structural (DDL commands) and data (DML commands) changes
- Protection from highly privileged accounts and DBAs
- Duty Separation and out-of-box Roles for system's main components
- Unified Security Events Trail
- Secured Protection Areas
- Change Control, full object source history before and after audited/protected event
- Policy-based evaluation
- Multi-factorial authorization
- Row value and column authorization
- User & environment context authorization in real time
- Middle-tier Application Level Auditing and Protection by CLIENT_IDENTIFIER
- Mapping of standard audit trails with audit settings (statement/privilege and object)
- Automatic management of audit trail records
- Issue tracking module to mark and classify Security Events
- Security Management, made easy for batch operations handling multiple commands
- Full back-end solution - ensuring protection from all directions
- Out-of-box, Software-only solution
- Transparent implementation - no (or tiny, industry recommended) change of existing setup
- Detailed dynamic reporting
- SIEM Integration

Access Control

The increasing number of threats and breaches require stronger security controls on systems access. By its default installation Oracle, like most of the commercial database systems, is opened for access by whoever gives a right username/password. This creates possibilities for abusers who do not have to fight for "perimeter-breaching" as a first step for their malicious actions.

The Access Control module enforces the necessary security controls to counter these threats and establishes a reliable system access authorization. It implements a special protection layer that supersedes standard user logon privileges. The logon process is evaluated on the access control policies, access is mandatory, users will log into the database only after complying with at least one policy. Non-compliant connections will be rejected in real time and not allowed to open a session to the database.

The Access Control module is enforced even on highly privileged accounts and DBA-s. Multi-factor user authorization permits logon only on successful combination of user & environment context values, be those hosts, terminals, IP addresses, program used, machine, user, time and many more.

Access control trails provide details on user's logon activity into the system

Distinguished features:

- High-speed processing – tested in systems with thousand connections per minute.
- Real-Time Monitoring and Response.
- Protection from highly privileged users and DBA-s.
- Automatic Trail Management.
- Silent (Learning mode) for non-disruptive implementation.

Standard Audit

Compliance standards, security policies and auditory procedures require preservation and documentation of system activity to enforce user correctness and responsibility against their actions. Proper collection and availability of audit records is top requirement of every compliance approach. Auditing helps refraining non-correct user behavior and protects against informational abusing and misusage.

The Standard Audit module ensures answers to the classical questions – Who/What/How/When/Where in regard to user's activity in the system. It operates on top of Oracle native features, is easily configured and graphically enables a complex set of auditing commands via the interface. Auditing consists on:

- Auditing of Statements & System Privileges – identifies actions made possible by system-wide granted privileges like SELECT TABLE, INSERT ANY TABLE, CREATE SESSION, EXECUTE ANY PROCEDURE and so on.
- Auditing on Object Level – identifies action performed versus an application or database object, let us say we are interested in tracing every SELECT, INSERT, DELETE, UPDATE into the ACCOUNTS table, made by any user.

Automatic standard audit trails management relieves the administrator from tasks of administering the audit records.

Audit is enforced is enforced even on highly privileged accounts and DBA-s. Full SQL command and bind variables are displayed.

Distinguished features:

- Statement & System Privileges Auditing.
- Object Privileges Auditing.
- Real-Time monitoring.
- Effective on highly privileged users and DBA-s.
- Mapping of audit trails with audit settings (statement/privilege and object).
- Automatic Trail Management.

Real-Time Protection (DML and DDL)

Today auditing only is simply not enough anymore; implementation of information protection is also a top requirement for information security compliance. Security controls must be in place to automatically reverse unauthorized actions and/or prevent unauthorized user access to sensitive information.

The Real-Time Protection module proactively defends and monitors the database against unauthorized actions in real time. It implements a special protection layer that supersedes user security privileges, the user's action is evaluated on the real-time protection policies, action will be completed successfully only if complying with the organization's policies, otherwise it will be rolled back.

The Real-Time Protection module configures the kind and level of protection to be applied in different areas/objects in regard to object type and/or system commands that may be applied on it. Protection Areas defines areas to be protected by combining owner, object type, object name and user action.

It covers the whole range from Data Manipulation Language (DML Commands) like SELECT, INSERT, DELETE, UPDATE, …., to Data Definition Language (DDL Commands) like ALTER, CREATE, DROP, …, etc.

The Real-Time Protection module can prevent highly privileged accounts and DBA-s from accessing and/or modifying application data, or applying structure modification using their powerful privileges.

Multi-factor user authorization can permit user actions only on successful combination of user & environment context values, be those hosts, terminals, IP addresses, program used, machine, user, time and many more.

These preventive controls help reduce the potential impact of a data breach which might lead to unwanted consequences for the institution. Omega Core Audit Real-Time Protection can be used to protect an entire application or a specific set of tables within an application, providing highly flexible and adaptable security enforcement.

Distinguished features:

- Structural (DDL) Protection
- Data (DML) Protection
- Real-Time Monitoring and Response
- Protection from highly privileged users and DBA-s
- Silent (Learning mode) for non-disruptive implementation.
- Middle-tier Application Level Auditing & Protection - enables Auditing and Protection in application user level in case of systems that access the database with a single logon account.
- Change Management / Source Code History
- Automatic Trail Management

Security Administration

Omega Core Audit comes with a set of Security Management functionalities enabling the Account Manager to easily and quickly complete his tasks.
The application interface offers coverage in handling of the following:

Distinguished features:

- Users, Roles and profiles management.
- System and Object Privileges management.
- Multiple batch-style commands for quick multiple management.

Policy-based evaluation and multi-factor authorization

Omega Core Audit for Oracle implements a flexible mechanism for authorizing access to database, application structure and data. It combines a policy-based evaluation system with a multi-factor authorization by environment context and application (row and column) context. This structure of policy-rule-condition is applied in the Access Control, Standard Audit and Real-Time Protection DDL and DML modules.

Policies are compounded by rules. They (like rules and conditions) evaluate to true/false. Different options for evaluating a policy based on its rules can be used, kind of Any True/All True/Formula. Rules in themselves are compounded by conditions. They too have similar evaluation options like Policies and are evaluated versus their conditions evaluation results.
Conditions are evaluated based on:

- Factor validation by operation codes - like =, >, <>, like, between, in……, etc, versus operands values, i.e. user & environment real-time values like host, terminal, IP address, program used, machine, user, time and many more.
- Minimum Trust Level - required matched with different predefined factor identities assigned with trust levels
- Validate expression - where a function returning Boolean can be used at will

Distinguished features:

- Policy-based Evaluation
- Multi-Factorial user & environment context evaluation
- Different methods of factor evaluation - Operand, Trust Level, Validate Expression
- Different options of policy and rule evaluation - Any True, All True, Logical Formula
- Cache - for performance optimizing
- Debug Logging on policy, rule and condition evaluation
- User Policy Appliance - All, Apply, Exclude

SIEM and Log Management Systems integration

Omega Core Audit's open structure allows and enables automatic delivery of audited events to SIEMs and Log Management Systems that support records ingest through one of:

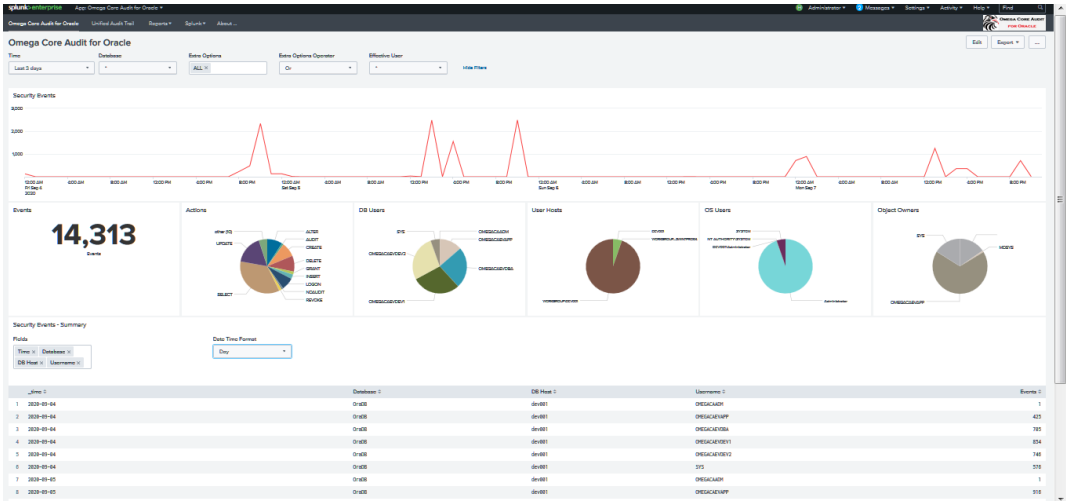
- "Push" directly through TCP in XML format - built-in supported by the LMS module
- "Pull" by Oracle query - supported by its open structure and as specifically by each SIEM

Splunk

Automatically send your audited event records straight to Splunk SIEM from Omega Core Audit; thus enabling storage of your scans results in a central location, visualization and quick access of scan data history.

Delivery of audited events to Splunk is built-in supported; can also be with Splunk DB Connect App. Monitor the security events of your Oracle database via the graphical interface of our next solution:

Omega Core Audit App for Splunk - running on top of the Splunk system.



About DATAPLUS

DATAPLUS is an information security consulting and solution provider company, founded in October 2007 in Tirana, Albania. We provide Oracle database security software only solutions and services.

Contact us

For more information about Omega Core Audit please visit 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
Cel: +355 68 2061664
Tel: +355 42419275