



Blue Core Research, Inc.
949-502-0627
info@bluecoreresearch.com

THE CORE AUDIT SUITE

- Database and sensitive data discovery
- Baseline snapshots of configuration & users.
- Continuous monitoring, reporting & alerting
- Activity analysis and anomaly detection
- Forensics
- SQL blocking & separation of duties
- Provisioning & static data masking

SYSTEM REQUIREMENTS

Audit Server:

- Physical or Virtual machine
- Windows or Linux x86
- Oracle client

Supported databases:

- Oracle 10g, 11g, 12c
- SQL Server 64 bit
2008 R2, 2012, 2014

Oracle Operating Systems:

- Solaris (SPARC or x86)
- Linux 64bit & 32bit
- AIX (PowerPC)
- Windows 64bit & 32bit

THE CORE AUDIT SUITE



The Core Audit suite contains an integrated set of solutions to help you achieve your database security and compliance goals. From simple demands to some of the most complex challenges in IT, Core Audit handles it all with a unique combination of proprietary technologies wrapped in a easy to use solution.

WHY?

Any information worth storing in a database has value, and would be harmful if changed or stolen. Threats to this data come from a variety of internal and external sources using a wide array of tools and attacks.

PRODUCTION STRATEGY

Like any implementation, security should follow a maturity process from the most fundamental elements to the most advanced.

LEVEL 1 | DISCOVERY & BASELINE

The first step to secure your data, is to identify where your data resides, who has access to it, and what is the environment in which you operate.

This is accomplished through the generation, validation, and tracking of changes in the baseline.

LEVEL 3 | ANALYSIS & FORENSICS

Going beyond declarative auditing, level 3 offers powerful forensics on all database activity and deep analysis that highlights the needle in the hay stack you want to look at.

Instead of discarding most of the Full Capture data, we leverage it to give you unparalleled visibility into everything that happens.

NON-PRODUCTION STRATEGY

As an alternative to the 4 level security strategy, non-production databases like QA & Dev, can be secured by eliminating the sensitive data in them.

The provisioning and masking module allows you to control the copies of production data in your organization, and ensure they do not contain information that needs to be properly secured.

In addition to controlling sensitive information, this module also improves productivity by allowing to refresh Test and Dev systems on a schedule or on demand.

BLUE CORE RESEARCH

Based in Irvine, California, Blue Core Research provides innovative enterprise class software solutions for security & compliance based on technologies we developed and own.

LEVEL 2 | CONTINUOUS MONITORING

The next security level constantly monitors what happens in the database.

Our Full Capture technology allows you to see everything that happens in your database, from privileged user activity, sensitive data access, to baseline changes and more.

LEVEL 4 | PREVENTATIVE CONTROLS

Finally, implementing preventative measures allows you to graduate from reporting and alerting to actual enforcement.

Our SQL blocking module can help restrict privileged users, control the application user, perform dynamic masking, enforce proper separation of duties, and more.