IRI Chakra Max
DB Firewall & Dynamic Data Masking

- Approve Access and Activity
- Monitor, Protect, and Alert
- Mask Data Dynamically
- Create and Query Audit Logs

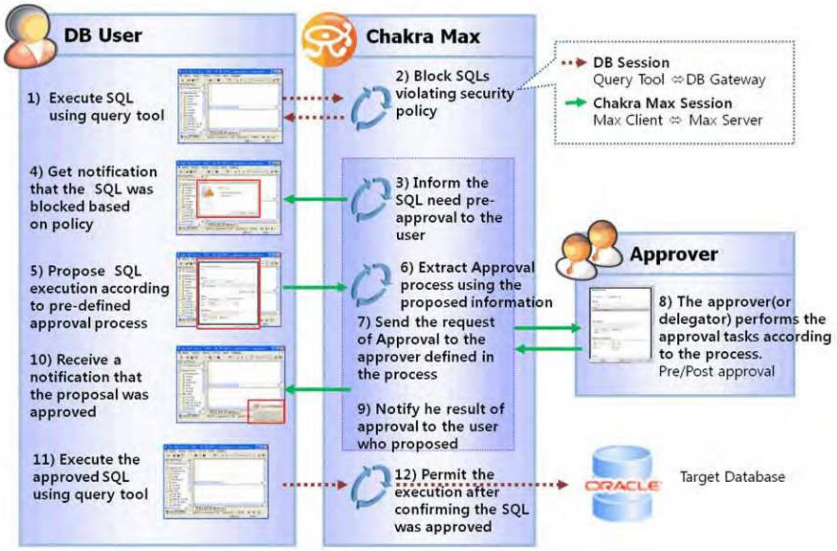
Proven Database Firewall Software

Product Summary

What is Chakra Max?

IRI Chakra Max is proven, robust data-centric audit and protection (DCAP) and data loss prevention (DLP) software for databases that contain sensitive information. Chakra Max allows you to:

- Scan and identify sensitive data in your databases
- Control, monitor, and log all accesses and executions
- Find and handle over-authorized or dormant users, and regularize your rights review cycle
- Speed incident responses with dashboard analytics and advanced audit log search capability
- Leverage high-availability gateway clustering to scale protection operations rapidly and reliably
- Spot, stop, isolate -- and send detailed alerts about -- attacks and unauthorized activities in real time
- Improve operational efficiency and time-to-value by minimizing or precluding DB performance impacts
- Protect and audit relational DW, ELT-appliance, and mainframe databases consistently and simultaneously
- Customize, secure, and share activity logs and reports to revisit protection policies and verify privacy law compliance


DB User
Chakra Max
1) Execute SQL using query tool
2) Block SQLs violating security policy
DB Session
Query Tool ⇔ DB Gateway
Chakra Max Session
Max Client ⇔ Max Server
4) Get notification that the SQL was blocked based on policy
3) Inform the SQL need pre-approval to the user
Approver
5) Propose SQL execution according to pre-defined approval process
6) Extract Approval process using the proposed information
7) Send the request of Approval to the approver defined in the process
8) The approver(or delegator) performs the approval tasks according to the process.
Pre/Post approval
10) Receive a notification that the proposal was approved
9) Notify he result of approval to the user who proposed
11) Execute the approved SQL using query tool
12) Permit the execution after confirming the SQL was approved
ORACLE
Target Database

Why Chakra Max?

Capability

Chakra Max controls access and execution privileges at the user level, monitors all login attempts, transaction commands, and result sets, and saves that history in real time to audit logs. It performs dynamic data masking without modifying the original database content so that sensitive data is revealed only to authorized users. Chakra Max supports automated reports from the logs with custom selected criteria.

Performance

Chakra Max is the most stable and best-performing DB monitoring and protection solution for high-traffic-volume environments, firewalling thousands of DBs at once. At 100K SQL/second monitor speed, and 10K-25K SQL/second audit speed, Chakra Max runs faster, and with less impact, than competing products.

Compliance

Chakra Max complies with internal business policies for securing access to databases, plus the data privacy laws applicable to PII. Strong and flexible auditing facilities provide both real-time alerts and logging, and subsequent forensic investigations of the logs. Database user and usage history -- as well as the actions of the Chakra Max administrator -- are also reliably available means for re-evaluating user authority and administrator responsibilities.

Interoperability

Chakra Max supports 20 different databases running on Unix, Linux, or Windows platforms, including: Oracle, MS SQL, DB2, Sybase ASE and IQ, Teradata, Informix, Tibero, Altibase, MySQL, Cubrid, Symfoware, and PostgreSQL. Chakra Max can be bundled with IRI Voracity -- the all-in-one data discovery, integration, migration, governance, and analytic platform.

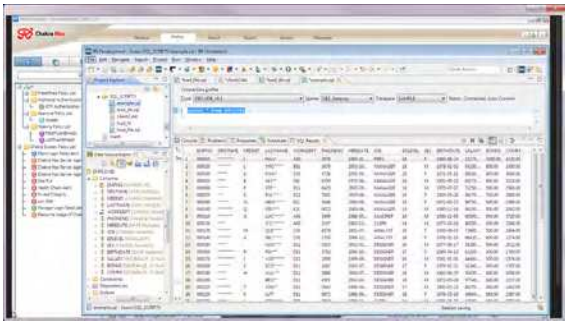
Features and Benefits

Streamline Protection and Privacy Law Compliance - Rather than tax DBA time, or rely on costly compliance assessment experts, Chakra Max allows you to centrally manage thousands of databases, big data nodes, and files after you find and protect the sensitive information they contain. Centralized policy setting and enforcement, plus detailed after-action reports, reduce the need for custom programs, SQL procedures, and compliance consultants.

Monitor and Block Activity - One way to prevent hackers from accessing critical data is by blocking an attack as it happens. Chakra Max monitors all traffic for security policy violations and stops attacks at the protocol and OS level, and blocks unauthorized SQL activity. Chakra Max can quarantine activity pending user rights verification, or block the activity without disabling the entire account. It can also send real-time alerts to the right people based on specified event conditions.

Manage User Access - Chakra Max allows you to configure the login, execution, and the rights to see certain values, by user, or defined duty (role), location, etc. -- and to enforce those rights across disparate data stores.

Nullify Data Breeches - Protect enterprise data from misuse by masking it dynamically in Chakra Max. Automatically redact (string-mask) full or partial column values in motion for all but authorized users, while retaining plain text in the source.



Discover and Classify Data - Results of a sensitive information scan are registered and used in a report on who accessed specific columns. This can be combined with the data discovery and classification features of IRI Workbench for both dynamic and static data masking operations.

Secure the Audit Trail - Audit data on connection and SQL execution history are saved in daily log files, which get encrypted, compressed, and backed up automatically. Backup activity and resources on the (optionally separate) audit server are monitored to assure scheduled backups run normally. Restoration to their query-ready state is possible after deletion.

Granular Deployment - IRI supports the provisioning of protection services through Chakra Max (and IRI FieldShield) API libraries, which you can seamlessly embed into, and distribute with, your software. You can also share and change-track your job configuration and policy definitions in Chakra Max, and your post-discovery data class libraries (in Voracity). The automatic, consistent deployment of these settings and policies across multiple database instances means much faster time-to-implementation and more consistent data governance.

Cloud and Managed Service Options - Chakra Max supports customers whose databases are in the cloud, on-premise, or deployed in a hybrid model. Chakra Max runs in both Amazon Web Services (AWS) and Microsoft Azure, and can even be hosted to provide managed DCAP services where qualified staff are responsible for, and dedicated to, your data’s security.

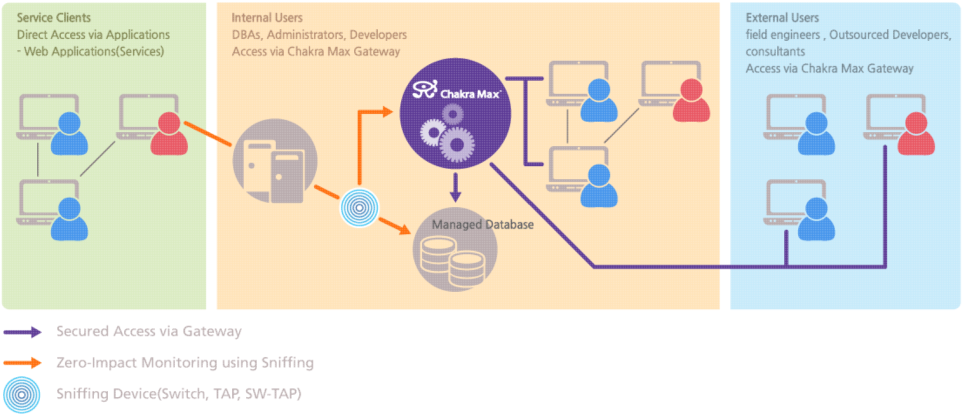
Connection Options

Chakra Max has multiple ways to protect data in databases and the applications that rely on them. Unlike competing tools, a separate hardware appliance is an *option* in Chakra Max, *not a requirement* for each one of these cases:

Sniffing Mode - Chakra Max can audit and control DB access with no impact on the DB by logging 100% of the audit data in ‘sniffing’ mode. With agent at the user or DB level, there is no impact on existing business or network environments.

Gateway Mode (Inline + Forwarding) - Chakra Max can control the movement of data into and out of the DB in ‘gateway’ mode, which works with or without an installed agent on a user laptop. This mode allows you to increase security by deploying it across internal development or outsourced work environments.

HA (High Availability) - Maintain the availability of your DB and access controls by configuring the Chakra Max server in either Active-Active or Active-Standby mode.


Service Clients
Direct Access via Applications
- Web Applications(Services)
Internal Users
DBAs, Administrators, Developers
Access via Chakra Max Gateway
Chakra Max
Managed Database
External Users
field engineers , Outsourced Developers, consultants
Access via Chakra Max Gateway
Secured Access via Gateway
Zero-Impact Monitoring using Sniffing
Sniffing Device(Switch, TAP, SW-TAP)

Supported Databases

IRI Chakra Max monitors and protects the activities in these database environments, on premise or in the cloud:

Oracle 7.3, 8.0, 8i, 9i, 10g, 10gR2, 11g, 11gR2, 12c	Sybase ASE 12, 15 & Sybase IQ 12, 15	Teradata 2R6, 12, 13	MariaDB	Fujitsu Symfoware 7-10	Greenplum
Microsoft SQL Server 6.5, 7, 2000, 2005, 2008 (32, 64bit), 2012	IBM Informix 7-11	Altibase 3-6	Amazon Aurora	Postgres 7.4+	SAP HANA DB
IBM DB2 UDB/LUW 7-9, AS/400 i5/OS 5-6, and z/OS	Tibero 3-6	MySQL	Cubrid 6-9	IBM Netezza 4-7	Kairos
WareValley PetaSQL	SunDB	Dameng DM7	Amazon Redshift	Oracle Exadata	Oracle ASO & SSL

The Chakra Max host agent runs on AIX, HP-UX, Linux (x86), Solaris (SPARC only), and Windows.

IRI
Total Data Management

CELEBRATING
40 YEARS
2018
The CoSort Company

2194 Highway A1A, 3rd Floor
Melbourne, FL 32937 USA
1.321.777.8889 ❋ 1.800.333.SORT

WWW.IRI.COM