WHITEPAPER

INGRES

THE INGRES DATABASE AND COMPLIANCE

Ensuring your business' most valuable assets are secure

TABLE OF CONTENTS:

INTRODUCTION

Data security is a top priority for any CIO and the requirements, both internal and external, for ensuring data security continue to grow in number and complexity. The Public Company Reform and Investor Protection Act of 2002, also known as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act of 2002 (FISMA), the European Directive, California SB 1386, and the Payment Card Data Security Standard (PCI DSS) are just a few of the regulations with which IT departments must comply. In addition, many organizations have their own requirements for protecting valuable data assets. Much of the data subject to these rules and regulations today reside in costly proprietary relational database management systems (RDBMS) such as Oracle, DB2 and SQL Server which provide protection mechanisms to aid with compliance. As IT budgets shrink, many organizations are looking to cost-effective Open Source Software(OSS)

Regardless of the specific regulations an organization is subject to, the process and requirements for compliance are the same: establish an adequate internal control structure and substantiate adequate levels of security to industry and government regulators and auditors. Unfortunately, most OSS RDBMS systems lack the features and functions necessary to provide adequate levels of data security. Data security keeps data safe from corruption, ensures access to it is suitably controlled, helps to ensure privacy and helps protect personal data. The exception is the Ingres Database. Ingres has helped customers ensure data security for over thirty years.

Maintaining regulatory compliance requires organizations be able to demonstrate their systems are secure, and adequate processes and procedures are in place to quickly address any gaps in security posture and compliance that may arise. Detailed below are some key requirements for an RDBMS to ensure data security, how Ingres helps manage these requirements and how other OSS solutions may leave you vulnerable.

REQUIREMENTS TO ENSURE DATA SECURITY

Though details of security regulations vary, the basic steps to ensure data security are the same. To ensure data security, IT shops are required to:

1. Build and Maintain a Secure Network
2. Protect Sensitive Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

This paper will go through each requirement with respect to database management systems.

BUILD AND MAINTAIN A SECURE NETWORK

Failing to ensure security at the network level can be very costly. Last year, Native Americans were awarded $455 million in damages because the U.S.Department of Interior failed to adequately secure the systems which manage the lands held in trust by the department. While most measures for maintaining a secure network fall outside the responsibility of the RDBMS systems and Data Administration teams, one requirement applies to every software component used by an IT organization: default passwords and security parameters.

Because RDBMS systems can be used for non-sensitive data or sensitive data, inside or outside a firewall, it is important to understand both the security capabilities of the product and the default settings. Some RDBMS systems ship with a number of predefined user accounts and/or user passwords. It is essential each of these be identified and changed or deleted as appropriate for the use case.

The Ingres database allows an installation password to be set during the product installation and has no default passwords that need to be changed. Ingres does, however, provide a number of security mechanisms to allow for maximum flexibility to adapt to numerous use cases. The default configuration setting for security mechanisms rarely needs to be changed. Multiple mechanisms are supported concurrently. Valid mechanisms are:

Null

Allows users to authenticate without providing passwords or other types of authentication. Use of the Null security mechanism is strongly discouraged.

System

Allows authentication through Ingres user names and either OS-level passwords or installation passwords. When using system authentication, user names can be given expiration dates to ensure user names can be easily validated and renewed periodically.

Ingres

(Default) Allows user authentication against the operating system. The Ingres security mechanism is the preferred standard (static) mechanism. It provides better protection against malicious servers, and employs a more secure encryption mechanism than the System security mechanism.

In addition, Ingres allows for use of third-party pluggable authentication modules.

Other OSS RDBMS systems are much more restrictive regarding user authentication. MySQL provides authentication only through DBMS usernames and passwords. PostgreSQL allows for DBMS usernames and passwords as well as OS authentication.

PROTECT SENSITIVE DATA

Whether your organization is required to comply with HIPAA, SOX, FISMA , the European Directive, California SB 1386, or PCI DSS, the RDBMS systems you select to manage your data is critical to your success. Many components of compliance do not require a technology-based solution such as the SOX requirement for top management to establish an adequate internal control structure. However, other requirements such as the requirement to secure transmission of sensitive data across the network require your RDBMS solution to provide encryption capabilities. There is no more critical requirement than the need to protect sensitive customer data such as credit card information in its stored state. The RDBMS plays a critical role in this task, particularly through the proper implementation of appropriate access control. Compliance with this requirement cannot be assured unless the RDBMS processing and storing the data have been comprehensively reviewed. Ingres supports Kerberos encryption to ensure which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM AND IMPLEMENT STRONG ACCESS CONTROL MECHANISMS

These objectives are closely tied together. These requirements include maintaining secure systems and applications; restricting access to sensitive data by business need-to-know; assigning unique IDs to each person with computer access and restrict physical access to sensitive data. Meeting these objectives requires an RDBMS designed specifically to manage critical business sensitive data. The Ingres database supports the discretionary access security to meet these requirements. Ingres allows for each user to have a unique logon ID and a password, which they must enter before they can access the system. The user's logon ID and password is be protected from capture or eavesdropping. Because Ingres ships with a complete audit suite, users are completely accountable for all their actions and the actions of the processes they initiate including any user's or process's attempt to access, read, write, or delete any object.

Other OSS RDBMS systems such as MySQL and PostgreSQL do not meet these requirements for a number of reasons. In both products, audit is based on triggers which cannot detect unauthorized attempts to read data: the primary way in which hackers attempt to infiltrate

target systems. Ingres allows Security alarms to be set up to monitor events against a database or individual tables. Such triggers on important databases and tables are useful in detecting unauthorized access. Security alarms can monitor success or failure of connecting or disconnecting from a database, and selecting, deleting, inserting, or updating data in a table.

Another area covered by these objectives is enforcing Segregation of Duties (SoD), also known as Role Seperation. One key aspect of a Sarbanes-Oxley audit is checking that rights and duties are separately assigned to different individuals so no individual has the power to divert business or transactions in a fraudulent manner. It is the regulatory auditor's job to check that individual permissions and roles are organized in such a way as to not make the company vulnerable to fraud. For example, no single individual should be able to both set data security permissions and control system auditing because that makes it easier for that person to commit fraud. The principle of separation of duties and rights is often implemented using the concept of "roles" within an IT system. Ingres provides an extensive framework for maintaining role-based security and segregation of duties. A key principle in the setting up of role-based security, however, is the principle of least privilege and it should be applied when assigning permissions within the system. Any individual should be given only the permissions he/she needs in order to carry out his/her job. This violation of the least privilege principle is one of the most prevalent open SOX audit issues across many corporations. The management of privileges is greatly simplified in an RDBMS through the implementation of Roles. Not all OSS RDBMS systems support Roles. Ingres supports Roles and other features such as subject privileges to simplify security management within the RDBMS. Subject privileges define the operations a user can perform, and are assigned to a user or a role. Subject privileges include: Auditor, Create Database, Maintain Audit, Maintain Locations, Maintain Users, Operator, Security, and Trace.

Another often overlooked aspect of secure applications is the requirement that objects that have been deleted cannot be reused. With PostgreSQL, deleted objects remain available until a separate "Vacuum" process has been run. This leaves deleted data vulnerable to attack.

REGULARLY MONITOR AND TEST SYSTEMS

This requirement is the core regulation addressing the need to validate the security of sensitive information. It directly addresses the foundation of secure applications: the introduction of security processes and review throughout the software development lifecycle. Planning, design, development, and deployment: all the stages of the lifecycle must make security considerations a top priority to make compliance possible and demonstrable. Monitoring assesses the quality of the compliance system over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities and other actions personnel take in performing their duties and should include an assessment of the effectiveness of this control structure in the company's annual report. Features such as built in auditing and security alarms, functionality missing from some OSS RDBMS systems, greatly simplify and reduce the cost of ongoing monitoring. Ingres Security alarms can raise a database event (dbevent), which can be monitored by background programs to respond accordingly.

Security alarms can be assigned to specific authorization identifiers to limit the monitoring to selected users, groups, or roles. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

Additionally, an external auditor needs to verify the management's assertions. The tools should be very easy to use and to learn and should not require the user to know any programming. This ease-of-use is the key requirement to enable business users to use this software. Ideally, these tools should work across a range of possible applications so the same tool can be used for many different types of applications across many different applications. Ingres audit allows logs to be analyzed, monitored and reported against using standard SQL and standard off-the-shelf reporting tools. This minimizes deployment costs and training requirements across the enterprise.

MAINTAIN AN INFORMATION SECURITY POLICY

Although this is often considered the most important element of regulatory compliance, it is often the most often overlooked. While RDBMS help enforce a compliance policy, the policy itself must be documented, maintained and managed as a vital corporate asset. A comprehensive security policy along with tools such as the Ingres Database, help provide a secure environment for your sensitive data and applications. The ability of organizations to secure and protect sensitive personal information has come under increasing scrutiny in recent years. Ingres has provided robust, secure information management solutions to government, financial and healthcare organizations for over two decades. To meet increasing security requirements, Ingres provides these features:

- Sarbanes Oxley / HIPPA Compliancy- Government regulations today require access to personal and financial information must be controlled and monitored. Ingres provides support for roles, role separation and Kerberos support to meet these demands.

- Support for role separation- Ingres supports role separation as part of the Ingres subscription. Role separation ensures administrators of the system and developers have all the access needed to fully administer the DBMS or develop solutions without granting them access to the business information.

➢ Support for Roles- Not all information within an enterprise should be available to everyone within the enterprise. To provide cost-effective securing of information, Ingres supports roles. Using roles, Ingres can allow or restrict access to information based on a class of user or by individual user.

➢ Support for Kerberos- Ingres provides support for SSL and Kerberos because enterprise customers need mutual authentication to protect against eavesdropping and replay attacks.

➢ Provides audit support- Enterprise customers need the capability to monitor sensitive data to prevent unauthorized access. Ingres provides this capability with an Enterprise subscription. Audit solutions for other open source DBMS products may only be available through 3rd parties

at addition costs and may not provide the full level of auditing required by current regulations. Many current regulations require the ability to audit both updates to information as well as read access to the sensitive data.

When planning an enterprise open source project, be sure your database provides the features and functions to help you comply with the ever-increasing regulatory requirements you business faces today.

Ingres understands the demands of an enterprise and has focused their development and support efforts for the last 25 years in supporting enterprise customers. Ingres offers a compelling solution to the marketplace that ensures an enterprise's needs are fully met with no compromises to performance, scalability, security, or availability. Ingres offers enterprises an informed and responsible choice. Customers can take their projects from development to full production, without risks to their network, while enjoying the added value of an open source solution. Shouldn't your next open source solution contain Ingres?

About Ingres Corporation

Ingres is the leading open source database management company. We are the world's second largest open source company and the pioneer of The New Economics of IT, providing business-critical open source solutions at dramatically reduced cost than proprietary software vendors. As a leader in The New Economics of IT, Ingres delivers low cost and accelerated innovation to its more than 10,000 customers worldwide.

Ingres Corporation
500 Arguello Street, Suite 200
Redwood City, California 94063
USA
Phone: +1.650.587.5500

Ingres Europe Limited
215 Bath Road
Slough, Berks SL1 4AA
United Kingdom
Phone: +44 (0) 1753 559550

Ingres Germany GmbH
Ohmstrasse 12
63225 Langen
Germany
Phone: +49 (0) 6103.9881.0

Ingres France
7C Place Du Dôme
Immeuble Elysées La Défense
92056 Paris La Défense Cedex
France
Phone: +33 (0) 1.72.75.74.54

Ingres Australia
Level 8, Suite 1
616 St. Kilda Road
Melbourne, Victoria, 3004
Australia
Phone: +61 3 8530.1700

For more information, contact ingres@ingres.com

INGRES

WP-313A