



*We Automate Information Risk Management*

FOR IMMEDIATE RELEASE:

**CONTACT:**

Cara Sloman  
Nadel Phelan, Inc.  
831-440-2411  
cara@nadelphelan.com

Trish Schaefer Reilly  
IPLOCKS, Inc.  
408-383-7513  
treilly@iplocks.com

**IPLOCKS ANNOUNCES DATABASE SECURITY MONITORING SYSTEM  
VERSION 4.1 WITH ENHANCED AUDIT ANALYSIS  
AND COMPLIANCE FUNCTIONALITY**

*IPLOCKS Delivers Database Security Monitoring, Assessment, and Audit Analysis for  
Protection from Information Theft, Loss and Fraudulent Abuse*

**SAN JOSE, Calif. – August 24, 2004** – IPLOCKS™, an innovative provider of database vulnerability assessment, continuous risk monitoring and non-repudiation audit analysis systems, today announced the availability of IPLOCKS version 4.1. IPLOCKS 4.1 expands the functionality of its external, non-intrusive, cross-platform, highly scalable database security management system with the introduction of audit analysis for analyzing transactions. IPLOCKS 4.1 automates the detection and notification of database reads and changes and archives events to ensure data security, integrity and availability for regulatory compliance.

“Protecting corporate data is critical for enterprises today,” said Akio Sakamoto, President, CEO and Co-founder of IPLOCKS. “The majority of IT security products such as firewalls, anti-virus and intrusion detection systems make an important contribution to IT security but do not prevent or expose fraudulent database activity and information theft – which can be achieved through legitimate access. Gartner estimates that more than

70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses. IPLocks has taken another major step forward in database security with version 4.1, enabling customers to easily gain insight into information reads and changes to proactively protect critical information where it resides – in the database.”

IPLocks 4.1 provides database monitoring, assessment, and real-time notification required for secure enterprise-wide database security operations and facilitates regulatory compliance for all major database platforms including Oracle, DB2, SQL Server, Sybase and HiRDB (Hitachi). IPLocks 4.1 captures, displays, and archives the 4Ws of information theft – the who, what, when and where of data changes. With real-time notification, organizations gain immediate access to before and after snapshots to validate changes that occurred.

“Auditing your database security first by establishing key security baselines and then by monitoring the changes over time is a key ingredient to a successful security program,” said Pete Lindstrom, Research Director at Spire Security. “IPLocks provides a comprehensive solution for evaluating database activity and identifying inappropriate or malicious behavior.”

IPLocks 4.1 detects, analyzes and monitors database security policy violations, suspicious or malicious changes, structural integrity changes, as well as user access patterns to ensure secure, authorized business operations. Through the inclusion of more non-deterministic assessment capabilities, the system “learns over time” based on actual usage patterns, and continually tracks against session policy definitions, usage rules and defined parameters. By monitoring changes in user behavior over time, the system is able to detect, and reduce the threat of information theft.

**IPLocks 4.1 New Features:**

- Session Policy and Usage Pattern Monitoring – Alerts to uncommon or excessive access.
- Alternative Audit Analysis Option – Monitors record-level changes and updates by displaying who, what, when and where (4Ws of information theft) about the change, without turning on Oracle's audit trail and provides the ability to delete guarded items without removing them from the audit management tables.
- Server Role Monitoring for MS SQL – Provides insight into users and their corresponding server roles.
- Automatic Discovery of DBMS – Automatically locates active databases on the local subnet and assists in database connection creation.
- Automated Global Amendment of Rule and Policy Descriptions – Provides users with the ability to globally amend rule/policy descriptions and severity levels of pre-defined rules and avoid creating new rules from scratch.
- Penetration Testing Capabilities – Performs brute force attacks on new or existing databases to determine common or easily detected passwords.
- Improved Progress Status and Detailed Reporting in CVA – Provides notice when the CVA is running an assessment and displays passed /failed alarm descriptions.

**About IPLocks**

IPLocks, Inc. is a leading provider of database monitoring, assessment and audit analysis systems used by business operations, global security, risk management and IT personnel to manage business processes, procedures and controls and protects the integrity, security, availability and confidentiality of mission critical databases. IPLocks automates the notification of system level database changes for security and business policy violations, suspicious, malicious or corrupt data, structural integrity and information theft that other security policies fail to prevent. IPLocks enables government agencies, audit services, financial institutions, service providers and other markets to mitigate information risks where database security and monitoring is essential to ensure uninterrupted business operations. Additional information about IPLocks is available at [www.iplocks.com](http://www.iplocks.com)

###