DATA SHEET

IPLocks Armour

Key Features

IPLocks Armour hardens databases by eliminating weaknesses in passwords, access privileges, configuration settings, and more. Expert knowledge of database and application security and compliance requirements is built in, providing businesses with an efficient foundation for compliance and security programs.

- Automatically Discover All Databases
- Accelerate Security & Compliance Best Practices (PCI, SOX, HIPAA)
- Centralize Policy Management
- Easily Create Custom Policies
- Brand Reports for Easy Identification
- Implement Expert-level Remediation Advice
- Analyze Database Security Trends

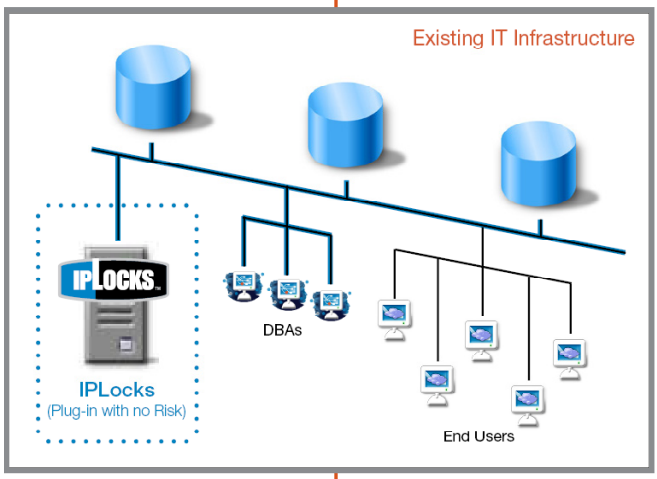
Product Overview

IPLocks Armour is a cost-effective, automated solution for improving data security within enterprises. Installation is quick and intuitive -- initial security reports can be viewed within minutes. IPLocks Armour's centralized, web-based application ensures consistent database security policies across the organization. And, IPLocks agent-less architecture does not interfere with database operations or put applications at risk.

Improve database security with a TCO at least 40% less when compared to other options.

Auto-Discovery

IPLocks Armour searches and finds all databases on the network. The high-performance scans can find databases in seconds even if the databases are using irregular ports. Scans can also cross subnet boundaries for comprehensive WAN searches.



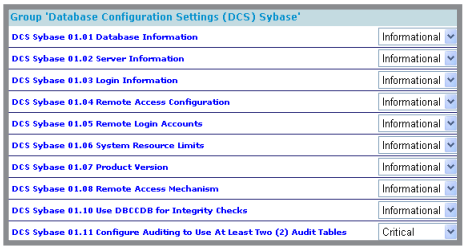
Accelerate Security & Compliance

IPLocks Armour is pre-populated with hundreds of policies that cover:

- Known database exploits
- Best practices in security and compliance
- Operating System issues that relate to database security
- Database access privileges

IPLocks Armour identifies, explains, and recommends remediation procedures for policy exceptions. Derived from research centers such as CERT, industry best practices, and IPLocks own research, policies identify security loopholes, known exploits, configuration weaknesses, and operational risks.

Policy researchers analyze latest information from CERT, Mitre, Oracle, Microsoft, IBM, Sybase, SAP, and more.

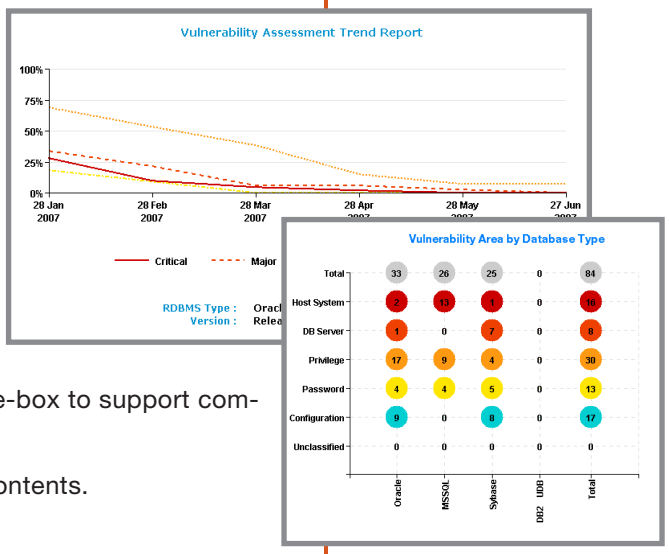


IPLocks policies are periodically updated to meet new security threats and compliance needs. Users are automatically notified when new policies are available.

IPLocks policies are easily customizable, so administrators can rapidly tune IPLocks for their environment. Additionally, users may also create their own policies. For example, many companies create custom policies to:

- Verify that databases conform to corporate standard configurations
- Extend IPLocks Penetration Testing to test for passwords that are commonly used within an organization
- Implement tests for custom applications

Branded reports are very handy during audits as each business unit can be easily identified.



Analysis and Reporting

IPLocks Armour stores the results of all vulnerability scans for reporting and analysis. IPLocks reports are designed out-of-the-box to support compliance programs. Reports are also highly customizable:

- At run-time, users can supply parameters to adjust report contents.
- Templates reserve space for business names and logos.

Additionally, reports and report data can be exported to PDF, Excel, Comma Separated Values (CSV) and Tab-Delimited for use with third party tools.

Enterprise Management

IPLocks Armour is a web-based application that users can access via web-browsers. The central repository stores all vulnerability data -- for thousands of databases and even more scans -- and enables trend analysis, easy report distribution, and consistent policy enforcement across the IT landscape.

Assess 1,000's of databases, even across WANs, from a single IPLocks installation.

IPLocks SNMP interface provides integration with Ticket, Change, and Configuration Management systems for closed-loop processes. In addition, administrators can automate vulnerability assessment and administration tasks using IPLocks Command Line Interface (CLI).

Command Line Interface (CLI) and SNMP enable IT to automate tasks.

Databases Supported

- Oracle 7.3, 8.0.x, 8i, 9i, 10g
- IBM DB2 UDB v7.x, 8.x
- Microsoft SQL Server 7, 2000, 2005
- Sybase ASE 12.0, 12.5

IPLocks can be installed on Windows, Linux, Solaris, and AIX!

IPLocks

IPLocks, Inc.'s award-winning software is *Keeping Data Safe* for companies around the world. From hardening databases against attacks to real-time activity monitoring, IPLocks is the solution to your compliance and security needs.
www.iplocks.com

2665 North First Street
San Jose, CA 95134
Telephone: 408.383.7500
www.iplocks.com