THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006104 December 4, 2006

IPLocks Secures the Heart and Soul of the Data Center

Analyst: Dianne McAdam

Management Summary

There have been numerous reports about the tremendous growth of unstructured data. Articles every day discuss how to manage, control, and audit unstructured data – such as emails and Microsoft *Office* documents. Most of these have ignored the critical importance of managing databases. Let's face it –news about databases is not as exciting as discussing out-of-control email systems. Databases have been around for a long time, they are mature and stable products, and we know how to administer databases effectively.

While this may seem like "old news", they forget one very basic premise. **Most financial data resides in databases. For this reason, databases can be defined as the heart and soul of the datacenter.** Without this critical financial information, enterprises could not continue to exist. Since this information is so critical, it must be protected securely.

There are numerous ways to protect people on the outside from retrieving this information through network protection, such as firewalls. **While it is important to secure the computing environment from outsider threats, it is also important to protect information from *insider threats.*** Many surveys estimate that the majority of information threats are by insiders; in fact, many of these are by authorized users. The integrity of databases can also be comprised by adding incorrect information accidentally to these databases. These databases require a high level of monitoring and auditing to ensure that the data stored within the database structure is valid. Databases must be constantly monitored to ensure that disgruntled employees are not using sensitive data for their own personal gain. Databases must be protected, yet must still be available to those that need to retrieve the information.

IPLocks has developed the *Database Security and Compliance Solution*, designed to secure enterprise databases. It not only monitors the activity on the database, but also provides the tools to perform an assessment of the database vulnerabilities. Read on to find out more about this solution from IPLocks.

Database Security and Compliance Solution

The Database Security and Compliance Solution is not IPLocks first foray into securing databases but is an expansion of its original products. The IPLocks Solution resides on a *Linux* or *Windows* server and uses its own internal database to maintain records about the activity within the enterprise databases. There are three components to the Database Security and Compliance Solution. The first component is the *vulnerability assessment* which determines if data bases are configured using current best practices. The second part continuously *monitors database activity* to ensure that personnel only access the data that they are permitted to view and the third component is the *audit and analysis process.* The results of the audit and analysis process provide reports that allow current policies and activities to be reviewed and refined. These three phases are continuously repeated allowing enterprises to fine-tune the processes and security measures that are in place.

Solutions that secure databases must protect all databases within the enterprise to be effective. The

IN THIS ISSUE

IPLocks solution can discover all active databases, whether they are running in the main datacenter or are running in remote offices. IPLocks currently supports various versions of database management systems from IBM, Microsoft, Oracle, and Sybase, and will support Teradata in a future release.

Vulnerability Assessment

During this assessment process, IPLocks gathers information about each active database, such as configuration settings, user privileges and patch levels, and compares that information to current best practices. Any detected configuration that does not conform to industry norms is flagged and assigned a *severity level*. Recommended actions are provided to guide administrators to the best approach to resolve these vulnerabilities.

It is important that all enterprise databases be configured in the same secure and consistent manner. Since IPLocks has visibility across all databases within an enterprise, it is easy to determine if all databases, both remote and local, follow best practices. Following these best practices ensures that enterprises remain compliant and databases remain secure.

Monitoring

Databases must be accessed by many people in the course of the day. It is necessary that databases remain available to those that are authorized to review and change their content. At the same time, it is important that authorized users do not access sensitive data for their personal gain. Achieving the balance between providing easy access to users but preventing insider theft or willful corruption is difficult to achieve.

IPLocks provides continuous monitoring of databases. However, continuous monitoring alone is not sufficient. Software without an understanding of human behavior cannot detect if an authorized user is involved in fraudulent activity or is just completing their required work activity. IPLocks takes monitoring to the next step by monitoring user behavior. For example, let's assume that a customer service representative accesses about fifty customer records during a typical day to resolve customer complaints. However, one day, this representative decides to access thousands of customer records at one time. This unusual behavior would be flagged and alerts would be generated allowing supervisors to determine if the action was outside of the normal job requirements.

Other types of suspicious behavior can be detected. These may include accessing other tables within a database that contains sensitive information, such as Social Security numbers or payroll information, that are not required for an employee to complete their daily activities. Database administrators can also be monitored and alerts can be generated if administrators go beyond their normal scope of responsibilities and access sensitive application data. Now, enterprises can reduce or eliminate insider threats before the theft of customer records makes the front-page news.

Audit and Analysis

Monitoring activities to databases can detect a single unauthorized access but cannot recreate the events over the course of days or weeks. Corruptions can occur within databases but it may not be detected immediately. This corruption could be accidental or intentional. The audit reports detail all activities to that particular database, which can be reviewed to determine when the corruption occurred and whether the intent was malicious or not. Analysis is also important when an employee with access to sensitive information is terminated. All access to that information over the last few weeks can be reviewed and additional steps can be taken in case potential information leaks are a concern.

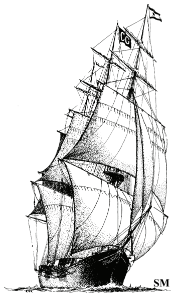
Conclusion

Government regulations require that corporations carefully control access to their enterprise information. Intentional or unintentional access to sensitive information must be disclosed publicly in many cases. This can lead to fines, negative publicity, and loss of business.

Restricting access to many files can be accomplished easily. Restricting information within databases can be very difficult. Many employees need access to databases, but must also be restricted to accessing only the information that is required to do their job.

The IPLocks Database Security and Compliance Solution makes the problem of securing databases manageable. It can discover and review local and remote databases to determine if best practices are following. It continuously monitors activities and generates alerts when suspicious activity is detected. And, it can analyze historical transactions to detect when corruptions occurred, or verify that all updates were properly completed.

For most enterprises, databases contain financial information that its heart and soul. As such, it must be protected and secured properly. **IPLocks can ensure that the heart and soul receives the security it deserves**. Check it out.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

***Dianne McAdam* is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group *Captain's Log***, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.