



Crossroads Systems **STRONGBox** Appliance Solutions

Leveraging Network Intelligence for Security, Compliance and Performance Solutions

Crossroads Systems, Inc.

February 9, 2005

Safe Harbor Statement

Please note that this document was created and reflects management views as of 8/26/2004. The Company assumes no obligation to update the information in the document. This document may contain certain forward-looking statements that are subject to known and unknown risks and **uncertainties** that could cause actual results to differ materially from those expressed or implied by such statements. Such risks and uncertainties include, but are not limited to the Risk Factors noted in the Company's Financial Releases and the Company's filings with the Securities and Exchange Commission

Crossroads Systems STRONGBox Appliance Solutions

Today's system requirements are expanding rapidly in a number of crucial areas. First, there are security concerns due to changing access modes, inside and beyond the firewall. Second, issues of compliance with government regulations have never been more acute. These issues are driving a rapid expansion in the need for application performance monitoring and enhancement tools. Crossroad Systems StrongBox family of products leverages the power of the network to meet the expanding requirements of security, compliance and performance:

- **Security:** The core computer systems of enterprises today are more vulnerable to breaches than ever before with exposure to the extranet. For many organizations, their systems are their business. This is particularly important with respect to databases. Solution: Monitor all database traffic on the network; provide reports, alerts and a permanent, immutable repository.
- **Compliance:** Transparency in operations, integrity of the systems that generate the reports and governance of the whole process are now strictly mandated by a host of new regulations including Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley Act (GLBA) and Basel II. Solution: Keeping records in an unassailable repository, conforming to the separation of responsibilities mandated, such as DBA and Security/Audit functions.
- **Performance:** Reporting on service level agreements is required, but monitoring performance without affecting it is crucial. Solution: Generating warnings and alerts before thresholds are breached and maintain a permanent record of the database activity without disrupting or degrading database performance, for further audit and analysis.

While databases provide a level of support for security and performance and can indirectly support compliance efforts, diversity in the way database applications are employed can diminish these controls and tools. Whatever network topology is employed, native database tools are often not adequate:

- **Thick client/direct connection:** Simple login is not sufficient as ID's and passwords can be shared. Database vendors often leave default administrator passwords unchanged. The databases can also be accessed by other connection methods. Attaching a user identity to a transaction is not always possible.
- **Client/server:** Many application vendors, SAP for example, completely encapsulate the database as part of a wider application, but the database is still vulnerable to direct, extra-application access.
- **Service-Oriented Architecture:** Though not widely deployed yet, Service-Oriented Architecture (SOA) will be a common topology in a few years. An SOA will be a collection of services that communicate with each other across a network, ranging from simple passing of messages to complex collaboration on a task. The heart of SOA is web services, which is an approach that allows interoperation of services to occur, but at the same time vastly complicating the security, compliance and performance landscape.

Because all three generations of network topology may exist at a given point in time, often within the same organization, the risks that exist at every point will only grow over time.

Compliance issues are largely statutory, but the trend in the past few years has definitely been more, not less. The need for new approaches to these services is clear and a network-based solution provides a convenient mechanism for meeting these requirements. Creative and nimble technology providers are rising to this challenge, providing tools to snap into a network in an unobtrusive way and participate as service providers (and consumers).

Security

Enterprise systems today are exposed to substantial risk from data loss, theft or manipulation and efforts to manage this risk are

expensive and complicated because these threats adapt quickly. In the past, only employees from internal, standard terminals and network connections accessed applications. Today, access is granted to people anywhere, anytime; some organizations effectively use the Internet as a backbone for wide-area networking of their critical business applications. In many cases, these systems are not designed for the broader audience and processes they now support and they lack sufficient protection. In today's enterprise environment, it is critical to know not only who is accessing systems, but what critical data is being accessed and by what means.

In addition, the threat to enterprise systems is not only from external sources. Malicious employees pose a substantial risk to deliberately wreak havoc with critical operational systems or manipulate data, quietly leading to inaccurate processing and a cascade of consequences. These perpetrators often guard their own records of mischief. A superior approach would archive the records in a system outside of the control of the perpetrator, however, this approach is not possible without expensive additional hardware and/or software that could potentially impact system performance and require incremental staff training/time.

Compliance

Even the organization itself can be the culprit, deploying systems that fail to meet regulatory and statutory requirements for disclosure, audit trail, transparency and retention, often with good intentions but with unwelcome results. In addition, the pace of change in the regulatory environment has quickened and issues like privacy, governance, disclosure and law enforcement are driving ever more extensive and demanding requirements.

Schemes to detect hackers in real-time and spectacular "Star Wars" types of defenders are popular in the press, but tightening defenses is not enough. An audit trail and powerful software analysis tools are critical in understanding/diagnosing after-the-fact events and for providing the kind of transparency called for by regulations such as:

- Sarbanes-Oxley Section 404 requires publicly-traded companies to demonstrate the integrity of the systems, applications and data used to generate financial reports. The company must also show evidence of supervision, governance and segregation of duties, and certify this evidence via an annual internal control report.
- Gramm-Leach-Bliley Act (GLBA) requires that financial companies ensure the security and confidentiality of personal information against internal or external threats.
- Healthcare and insurance organizations are required to ensure prevention, detection, containment and correction of security violations against personnel health records

Existing tools for monitoring database activity require stitching together scripts and stored procedures to read the logs. This approach is often coupled with the limited built-in monitoring capabilities of standard databases in a tedious process that has a severe negative impact on database performance.

Performance

The need to monitor and analyze network database traffic goes beyond security and compliance. Typical optimization techniques in use require careful study and testing, and implementation takes time. The rapidly changing pace of business systems shortens or eliminates the time spent on careful optimization. In addition, application usage patterns may shift when the audience for them is broadened, so that existing "rules of thumb" for optimization and tuning are not as effective.

The ideal solution would be an unobtrusive, secure set of tools, independent of the database or application, that provide monitoring, alerting, auditing and analyzing of network database traffic for security and compliance and, in the process, leverage the architecture to address application and development performance.

Problem: Pieces of the Puzzle

Meeting regulatory requirements for disclosure and transparency in operations would seem to have a simple solution – keep data safe and maintain audit trails. Unfortunately, problems arise in a number of areas:

- **People and Procedures:** New procedures for capturing and safeguarding information and transactions have to be developed, people have to be trained and management and oversight roles are needed. Implication: time and money.
- **Technology and Implementation:** New software has to be developed or purchased, and personnel have to be trained and supported on an ongoing basis. Implication: time, money and adoption issues.
- **Impact on Infrastructure:** Many organizations run an infrastructure that cannot bear the introduction of a new set of loads without build-out. Current methods such as replication put an unacceptable burden on stretched resources, carrying a hidden cost. Implication: time and money.
- **Roles and Responsibilities:** Human beings cannot be divided into pieces. If a production DBA is responsible for tuning and maintaining the logs, and a new approach requires those roles to split, there is no way around the requirement for another headcount. Implication: delay, cost, staffing.
- **Continuing Challenges:** Security threats are constantly evolving, looking for weak points. The problem is growing and requires vigilance on a 24/7 basis. Implication: machine-based sentries and software are needed; a few smart DBA's can no longer handle the problem.

Database monitoring tools typically included with relational databases are insufficient for the range of security, compliance and performance demands required in today's distributed computing environments. The difficulty in applying upgrades and keeping applications in synch only adds more complexity and latency to implementation schedules. In fact, standard monitoring tools use the database server itself to investigate transactions, often significantly degrading database performance. DBA's tend to use database monitoring tools as merely a starting point, often adding scripts and programs to already complex processes. This creates a further potential for performance degradation and adds to the growing stack of narrowly focused, proprietary code that has to be maintained.

The propriety, ever-evolving capabilities of enterprise database monitoring makes accommodating new regulations an even greater challenge. Many computer systems have evolved over time, making the change of internal processes tedious. Where packaged applications have been used, the "configurable" quality may be more a principle than a feature – making changes to production systems cumbersome. Networked applications are especially hard to manage because modeling the usage patterns of a dispersed audience is difficult and requires simulation of a production environment in the testing phase. Creating test sets is an expensive and time-consuming process and because they are usually contrived, they often test the things the developers considered in the design, not what they may have overlooked. Being able to capture the totality of transactions in a real production environment and replaying them in a test environment, without disrupting the availability of performance of the production system would be an ideal way to solve that problem.

In addition, the logs that are saved are generally managed by the same groups, if not the same person, whose stewardship is ultimately being evaluated, creating a potential conflict of interest or in extreme cases, concealment. The lack of a secure, permanent repository of all transactions, untouchable by any person, poses a severe risk that the audit trail can be lost, altered or compromised.

Security, compliance and performance are pieces of the same puzzle. Existing solutions are too costly, too complicated and too expensive.

Implications

Failure to address compliance and security demands can lead to substantial setbacks including fines, loss of licenses, and loss of customers and even failure of the enterprise. For example, if compliance requirements are not met, regulators have the power to shut a business down or to revoke a license. These are extreme measures, not usually taken until all other remedies are examined, but once the non-compliance is surfaced, loss of esteem and goodwill can occur as well as closer scrutiny from regulators going forward. Lapses in security can lead to anything from the unauthorized release of customer records to total system shutdown. As an example of the consequences of a security breach, consider California regulation SB1386. Companies doing business with customers in California that suffer a security breach may be required to notify those customers that their personal information may have been compromised. This notification can be avoided if it is determined that the breach did not expose any data deemed restricted by the regulation. Without an audit trail to determine what was accessed during the breach, which may not be noticed until well after the attack has occurred, a company may unnecessarily need to broadly disclose damaging information about the security breach. Existing “DBA” approaches have drawbacks. Patchwork integration of “best-of-breed” point solutions is too expensive, too time consuming to implement and maintain and often introduces a new set of problems, particularly performance problems. Patchwork solutions impede change and often add so much latency in their operation that they are unable to deliver.

The Solution

An ideal solution would address all of these concerns in a unified and coherent architecture that is simple to implement, easy to maintain and leverages existing infrastructure:

- Capturing all SQL transactions while creating a secure audit trail of database access in a “black box” that cannot be altered
- Monitoring database activity for security and service level performance
- Capturing all SQL transactions while creating a secure audit trail of database access in a “black box” that cannot be altered
- Providing broad and critical functionality that is inexpensive and easy to install
- No additional software to maintain or support
- Zero impact on network and database
- Real-time alerts of security events, performance issues
- Built-in reports such as “Slowest Queries” at the aggregate, user and table level

Crossroads StrongBox Family of Products

Crossroads StrongBox family of network appliance products is designed to meet enterprise auditing, access control, security, analysis and performance needs, providing vital services for today and for future expandability. Current services include the StrongBox Monitor, which is an appliance that senses database traffic in the network, understands and decodes the database protocols and parses SQL statements in order to provide a series of canned and configurable reports and alerts about database performance. Available later in 2005, the StrongBox Tracker appliance will capture the same data as the Monitor, but is designed to archive everything it captures for a configurable period in a “black-box” that cannot be tampered with. Both the Monitor and the Tracker will eventually have expanded functionality beyond SQL traffic to include, for example, Web Services traffic. In addition, the Tracker platform is designed to host the upcoming Analyzer package, which will leverage the information managed by Tracker. The Analyzer service will provide advanced analytics and reporting against the transaction stream. These pattern matching tools and rules-engines will provide real-time analysis for intrusion detection and suspicious use patterns.

The StrongBox family line is an unobtrusive set of appliances that leverage Crossroads abilities and knowledge of the network so installation and maintenance is simple. For example:

- Requires no change to server code.
- Installs easily and quickly, in a matter of hours.
- Needs no agents or server software.

STRONGBox Monitor

The StrongBox Monitor is a network-attached appliance and software for capturing network SQL traffic of active databases. Monitor appliances will serve as the “sensors” for follow on StrongBox services and currently includes packaged reports and real-time alerts, as well as authoring tools to allow for the customization of these reports and alerts. Monitor also provides monitoring of service levels (ability to provide information on whether or not queries are executing within the agreed upon performance windows), trended and historical measures (system performance over a period of time), transaction response times, and detailed performance and usage metrics. By operating “out of band”, Monitor provides this functionality without affecting the performance of applications or databases.

StrongBox Monitor also includes an Acceleration Improvement Estimator that analyzes the events processed and advises users to what extent a result set caching application accelerator could improve performance.

STRONGBox Tracker (Available 2H05)

StrongBox Tracker is another network-attached appliance that will work in concert with one or more Monitor devices to provide long-term, secure, “black-box” logging and forensics for database network traffic (SQL). Tracker will permanently store information at a selectable granularity, down to every SQL statement that each StrongBox Monitor captures and will maintain this data in a protected environment that cannot be altered – providing an ideal solution for compliance to regulatory requirements and an unimpeachable resource for examining data history. Initially, Tracker will use its own storage resources but will be extended to leverage storage systems that may be present in the enterprise.

Tracker will operate as a “black box” repository to separately manage assets currently controlled by the database administrator or any other systems administrator. The benefits of StrongBox Tracker are:

- Refers to a secure repository of database events captured from the network.
- Performs a wide variety of analysis on captured data.
- Works with virtually no impact on the network or database systems.
- Scales easily.

Tracker will provide network forensics - capturing, recording and analyzing network audit trails to discover the source of security breaches, policy violations and other information assurance problems. In addition, Tracker will provide the computing resources for a family of analytical software and applications, referred to as StrongBox Analyzer.

STRONGBox Analyzer (Available 2006)

StrongBox Analyzer software is an entire family of applications and tools that are part of the Tracker appliance covering a broad range of diagnostic and active applications such as:

- Intrusion detection via pattern recognition and rules-based analytics.
- Outbound data protection violation detection and/or scrubbing (e.g. query is returning credit card numbers, shut it down).
- Ad hoc search across the entire dataset, with resources completely isolated from the production systems (e.g., did the pattern of database traffic from a department change after a personnel action).

Analyzer applications and tools will solve the problem of patchwork and point solutions by providing the software and hardware infrastructure for a broad range of security, compliance and performance problems.

Conclusion

Demands on organizations to provide increased security and compliance, without degrading performance, are greater than ever, and so are the stakes. Most organizations are hard-pressed to meet their current requirements. Deploying network-attached, intelligent appliances to handle some of these crucial requirements, without modifying any of the existing patchwork of applications is a perfect solution. Most security schemes in place were designed before the current set of regulations went into effect and simply cannot handle many aspects of compliance related rules gracefully - rules requiring actions that include the need to separate responsibilities for database administration and database forensics. The Crossroads StrongBox family of products is designed to slip into those roles and provide complete, reliable and scalable services with an absolute minimum of installation effort, maintenance or application degradation.

Credits

Neil Raden is the founder of Hired Brains, Inc., <http://www.hiredbrains.com>. Hired Brains provides consulting, systems integration and implementation services in Business Intelligence, Data Warehousing and Performance Management for clients worldwide. Hired Brains Research provides consulting, market research and advisory services to the Business Intelligence, Data Warehousing and Information Integration industry. Based in Santa Barbara, CA, Raden is an active consultant and widely published author and speaker. He welcomes your comments at nraden@hiredbrains.com.