Bottomline

BOTTOMLINE CYBER FRAUD & RISK MANAGEMENT

Insider and Employee Fraud

The Challenge

Cyber threats are increasingly aggressive, complex, and frequent. Today your investments in security protect against malware and unauthorized access, but that alone can't truly protect you. 78% of cyber fraud is committed by authorized users ("malicious insiders") or by external parties that hijack an authorized user's profile and access – but without visibility into their behavior, organizations are missing a critical layer of defense and are unable to stop fraud and data breaches before they happen.

The Insider and Employee Fraud Solution

The solution records the activity of all users by sniffing the network traffic between the end users and the main servers. The system analyzes the captured traffic in real-time and reconstructs full user sessions, allowing for screen-by-screen replay and behavior analysis.

In addition to network sniffing the system can collect information in a variety of ways from databases, data warehouse, log files and other sources in real-time and batch. The data captured from various sources is stored in one centralized repository and is analyzed by the business rule engine.

The system provides a highly flexible and friendly Web based user interface which presents the results of the analyzed information in dashboards, reports and charts (hourly, daily, weekly, monthly, etc.)

BENEFITS

- Create accountability among authorized users
- Shift from transaction tracking to human behavior monitoring
- Increase organizational security with central visibility into user behavior across all sensitive applications
- Act on suspicious behavior as it occurs, rather than reacting after crimes and fraud have been perpetrated
- Precisely identify, investigate, and document suspicious behavior with session replay
- Use the intelligence the system gathers to preempt crime, data leakage, and theft before it happens

BUSINESS RULE ENGINE FOR REAL-TIME ALERTING

One of the main components of the system is a highly configurable analytic engine which analyzes the data captured from various sources and generates alerts in real-time and batch. The alerts can be provided in a range of areas. Following are a few examples.

- Multiple application or server errors in a sensitive process received by many users in the last minute
- A spike in response time in a sensitive process occurred in the last 15 minutes
- Multiple events of no response from a server experienced by many users in the last 5 minutes
- Suspicious external user activity, e.g. ePayment fraud
- Suspicious internal user activity, e.g. internal fraud or information leakage

ALL ON ONE PLATFORM: CASE, ALERTS, ONLINE, MOBILE

All of the functions are built from the ground up on the same platform. This offers you a number of benefits:

- Any data collected by the system, in any channel, is immediately available for analysis, reporting and alerting
- Network operators and fraud analysts only need to learn a single user interface
- No need to waste time retyping information between your Alert system into your Case system – they are on the same system, so they are fully integrated
- Reports and dashboards can combine information from performance events, suspicious fraud events, alerts and cases

FORENSICS AND DATA COLLECTION

As mobile and online attacks get more sophisticated, it's important to have a set of data that you can analyze to find new patterns, test new rules, and respond to new attacks. Since our solution records and stores all mobile and web traffic (not just log file information), our customers enjoy a much richer repository of stored data to analyze as new attacks appear.

The Business Value

- **Improve system performance** and availability
- **Increase customer satisfaction** by improving user interface and system friendliness
- **Reduce fraud** losses and data theft
- **Become proactive** in protecting your brand and assets
- **Comply** with regulations that require complete audit trail and privacy protection
- **Hold all users accountable** for all activity
- **Deter potential fraudulent users** who will know that their actions are being recorded and analyzed

Sample Monitoring Functions

The system can monitor a variety of performance and fraud indicators. Following are several examples:

- Abnormal drop rate in the middle of a payment process
- Increase in response time in a critical process
- Increase in average response time in all processes
- Application errors in a critical process
- High rate of user errors in a critical process
- High rate of login attempts
- Suspicious user behavior in an ePayment process
- A high rate of failures of a server to respond to users' requests
- A sudden increase or decrease in the number of ePayment transactions per hour
- Suspicious behavior of internal user compared to his/her normal behavior patterns
- Replay of user activity for assisting Help Desk agents

Bottomline

Corporate Headquarters
325 Corporate Drive
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
Fax: +1-603-436-0300
info@bottomline.com