Bottomline Technologies

DATA SHEET

Bottomline Cyber Fraud & Risk Management

Insider Fraud

The Challenge

Corporations face increased threats from their own employees and other insiders who are authorised to access sensitive applications and data. Surveys show that about 78% of insider fraud and data theft is carried out by authorised users employing simple, legitimate commands to manipulate systems and data.

Distinguishing between malicious and ordinary activity is, however, challenging since both innocent and malicious employees use legitimate system commands. Detecting breaches effectively requires full visibility into user behaviour, but most organisations rely on partial data based on logs of confirmed transactions, excluding user queries and incomplete transactions.

Detecting insider fraud is a challenge, also because of the many ways in which well informed employees can manipulate business processes and bypass controls. Identifying these manipulations requires a system with a wide range of fraud scenarios, advanced analytic capabilities and high flexibility to detect anomalies within seemingly regular behaviour patterns.

The Recognised No. 1 Internal Anti-Fraud Solution*

Bottomline introduces the first of its kind, end-to-end insider fraud solution: most vendors provide mainly analytics and investigative functions, and require organisations to prepare the data for analysis (ETL). Bottomline's Cyber Fraud and Risk management, on the other hand, conducts sniffing of corporate networks, and prepares data for analysis, reducing the need for lengthy and laborious ETL (traditional data sources such as logs and data warehouses may be used additionally if needed).

The result is full coverage of all user activity provided in real time, alerting to suspicious activity and stopping fraudsters while they are still planning the crime - with minimal effort and set up time on the part of the customer. The analytic engine, containing predefined rules based on knowledge from over 200 deployments, is able to detect anomalies with minimal false positives. The rules can be easily adapted to the specific risks of the organisation and additional rules may be added if needed.

*Based on research conducted by a leading analyst firm.

The Bottomline solution provides:

- Unique patented real-time sniffing of the network, in additions to log files
- Real-time alerts for immediate action before data or money are lost
- Pre-packaged rules, alerts and reports based on more than 200 deployments worldwide
- Statistical/analytic tools for detecting suspicious activity (profiling, peer group, link analysis)
- Advanced investigative functions, including screen-by-screen replay of user activity

The Difference

Proven insider fraud detection experience is embedded in our pre-packaged solution

Bottomline has deployed insider threat solutions in more than 200 organisations worldwide. Based on our accumulated experience we have created a comprehensive library of rules covering a wide range of fraud and data theft scenarios.

Genuine behaviour analysis with no need to rely on log files

End-user behaviour profiles are reflected in their screen activity. There is no need to rely on log file data, which typically does not provide the required details.

Visual audit trail that provides proof when it matters

Every screen and keystroke can be reconstructed and used as proof of misuse.

 # 1 in Deployment Simplicity*

Immediately, upon installation (typically lasting a few hours) Bottomline's Cyber Fraud and Risk Management begins capturing network data, so internal auditors can perform investigations within a short period of time, reaping immediate business value. In addition, only parts of the captured screens are required in order to start implementing business rules – so auditors and risk officers start receiving alerts within a short period of time.

*Based on research conducted by a leading analyst firm.

Monitoring of privileged IT users

Privileged IT user activity is monitored along with other types of users. Monitoring includes audit trail, behaviour profiling and real-time alert generation.

Fully configurable, packaged solution solution

The solution is flexible and adaptable to the specific applications and processes of each organisation. Corporate investigators can adjust scoring parameters, calculation methods and thresholds with no need for assistance from IT.

Low false positive rates

Bottomline keeps false positives low with unparalleled visibility to user activity and advanced analytics that enable a genuine understanding of user behaviour.

The Business Value

- **Reduce fraud** losses and data theft
- **Become proactive** in protecting your brand and assets
- **Comply** with government 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 analysed

Pre-Packaged Analytics

The rule libraries and implementation process have been developed and refined throughout scores of deployments at customer sites worldwide. Our knowledge-base of rules covers both common and infrequent internal fraud attacks:

- **Identity Theft:** employees manipulating account data to steal customer identity
- **Misuse of Position:** opening accounts for money mules/deposit fraud schemes
- **Incentive Fraud:** opening accounts or falsifying applications to meet quotas/incentives
- **Embezzlement from Customers:** via checks, cards, ACH, wire, transfer, cash
- **Embezzlement from Bank:** via ACH, wire, transfer, cash
- **Corporate Card Abuse:** personal charges on corporate card accounts
- **Employee Self-Service:** servicing one's own account or the accounts of family and friends
- **Data Theft:** stealing customer information for passing it on to criminals or the media
- **Unauthorised refunds:** unauthorised claims, rebates, refunds, reversals, etc.
- **Elderly Abuse:** employees deliberately targeting elderly customers
- **Branch Collusion:** multiple employees in a branch colluding to commit fraud
- **Policy Violations or Operational Errors:** common mistakes or issues that might violate policy
- **Avoiding Detection:** schemes by knowledgeable employees to circumvent controls

Connect with us

bottomline.com/uk

London Office
10 Aldersgate St
London EC1A 4HJ,
England, United Kingdom
Phone (Local): 020 71050 000
Phone (Int) : +44 (0)20 71050 000
Fax: +44 118 982 2253
emea-info@bottomline.com