

防制內部詐欺



內部詐欺是個代價高昂的問題，雖然任何企業都有可能成為內部詐欺受害者，但銀行和金融服務占了內部詐欺案件的最大份額，除了財物損失，還包括聲譽損害，尤其是當詐欺公之於眾時。



偵測內部詐欺具有挑戰性，因為這類威脅來自於那些可以輕鬆規避傳統防制內部詐欺的方法，或是能夠刪除他們自身活動軌跡的行員。而傳統防制內部詐欺系統，通常是靜態和基於規則的，用於判斷已知的內部詐欺手法，但不能在詐欺發生之前阻止其發生，也無法偵測到新的內部詐欺行為模式。

NetGuardians開發了最先進的人工智慧NG 3D AI 風險管理平台 NG | Screener，可以檢測並分析行員（客戶經理、前台 / 後台、具有管理權限使用者）和客戶銀行帳戶行為，用於識別內部詐欺交易的異常情況。

在支付詐欺發生之前阻止

不同於傳統以規則為基礎的防制內部詐欺系統，採用 NG | Screener可以做到：

- 根據過去的交易行為建立行員和客戶檔案
- 在任何錢離開帳戶之前，計算每筆交易的風險評分以檢測異常活動
- 檢測新的內部詐欺模式



✓ **時時保護您客戶的銀行帳戶：**
透過NetGuardians創新人工智慧科技(3D AI)技術，分析行員與客戶銀行帳戶行為，及時發現並阻止可疑交易。

✓ **完全控制管理員帳戶：**
確保透過管理權限操作變更及修改可被NetGuardians監控，並保證使用者帳戶對應真實的客戶姓名。

✓ **運用可解釋性3D AI提高營運效率：**
大幅減少需要查看的事件警訊和檢視每一個事件所需的時間。
輕鬆理解事件警示發生原因，提供即時事件前後關係的完整背景資訊；透過強大的圖表解析工具，讓調查方便直觀。

✓ **自動化稽核文件和報告：**
建立有效的案例與證據，並自動產生報告、文件與稽核軌跡。

導入效益

- 減少誤報，提高營運效率
- 發現新的內部詐欺行為
- 降低聲譽損害
- 系統快速部署
- 監控可疑交易，而非監控您的行員

使用案例

行員共謀串聯

客戶經理規避內部控制

內部和外部共謀串聯

違反四眼原則

特權 / 後端資訊管理人員私自變更

屢獲肯定：

GARTNER 2020年網路詐欺防制市場指引

CHARTIS 2021年企業詐欺報告

AITE 2021年詐欺&反洗錢機器學習平台報告

更多產品資訊洽詢

BAOYI / 寶誼資訊股份有限公司

02-2308-7700 | sales@baoyi-info.com.tw | <https://www.baoyi-info.com.tw>