TruValidate™

數碼洞察

智能裝置風險防範方案

概覽

企業營商環境瞬息萬變，數碼詐騙手段越來越高明。從帳戶接管、合成身份、到偽冒裝置與多重裝置攻擊，詐騙形式變得多元化並不斷演變。在這樣的挑戰下，企業仍需要持續提升業績。如何在推動業務增長與有效防範詐騙之間取得理想平衡，變得比以往更為重要。

TruValidate™ 智能裝置風險防範方案有助實時防禦數碼詐騙

TruValidate 智能裝置風險防範方案為主動應對上述挑戰而設，提供先進偵測與防範功能，全面保障你的企業安全。TruValidate 智能裝置風險防範方案結合具前瞻性的的分析能力及機器學習技術，配合高效的規避與異常偵測功能，讓企業能夠在不影響客戶體驗的前提下預先部署防綫，以攔截騙徒。

TruValidate 智能裝置風險防範方案讓企業能夠：

在不影響潛在優質客戶的情況下打擊詐騙活動

透過先進的裝置識別技術、情境分析及行為洞察，有效區分騙徒與真實用戶，確保真實的用戶享有流暢的體驗，同時將騙徒拒諸門外。

與可信的用戶建立關係

運用龐大的裝置歷史紀錄，結合由全球裝置風險網絡中已確認的詐騙報告而得出的裝置與裝置（device-to-device）及裝置與帳戶（device-to-account）的關聯分析。企業可以掌握來自超過 1,110 億次裝置信譽檢查及逾 1.85 億份詳盡詐騙報告所提供的風險洞察，進一步強化保安措施。

專注識別風險

運用裝置數據，結合個人化、可配置的業務規則，有效應對詐騙帶來的挑戰。為你度身訂造的解決方案有助提升保障能力、強化偵測詐騙效率與準確度。

*環聯內部分析

TransUnion 環聯

提升營運效率

以自動化的風險評估及實時提示，簡化詐騙偵測流程，減少人手干預，讓資源更集中於策略部署。

促進客戶轉化

以不影響消費者體驗的前提下，在後端系統中評估數碼交易風險，在客戶體驗流程初期偵測高風險個體，從而提升真實用戶通過率。

獲取可化為行動的洞見

利用來自全球最大並已建立多年的裝置風險網絡中的詳盡分析及報告，深入掌握不斷演變的詐騙趨勢與模式。透過數據作出明智的決策，以持續改善防騙策略。

如何運作

TruValidate 智能裝置風險防範方案利用裝置歷史紀錄以及經我們龐大的全球詐騙分析團隊確認的實時詐騙報告，追蹤裝置與帳戶之間的關係。此工具可輕鬆整合至任何原生應用程式或網絡應用程式。

你現在可以在整個客戶流程中全面保護你的企業 —— TruValidate 智能裝置風險防範方案適用於任何有可能出現詐騙風險的客戶接觸點，包括帳戶建立、申請、登入、資料變更、付款及結帳。

創新技術，多元功能

在無需使用個人識別資訊（Personal Identifiable Information）的情況下識別已連接網絡的裝置，智能裝置風險防範方案提供了一層獨立於個人資料之外的數碼身份分隔，與可能已遭洩露的個人資料隔離。

符合企業獨特需求

以靈活規則引擎，根據你的企業獨特的防詐騙策略，設定個人化規則。由機器學習驅動的追蹤、搜尋及報告功能，偵測可疑交易及裝置行為模式。

追蹤並揭露隱藏詐騙模式

先進分析技術、機器學習模型與細緻的報告功能，能夠識別可疑交易及裝置模式。我們靈活的業務規則編輯器更可迅速對可疑交易及裝置模式進行追蹤。

提高詐騙識別的準確度

結合豐富的歷史數據模式，趨勢分析與細緻度更高的數據，從而提升識別精密詐騙手法的準確度。並以先進偵測能力預防潛在的新興威脅。

運用先進規避偵測功能

更有效防範詐騙分子利用 Proxy 伺服器、TOR 網絡、VPN 及其他匿名技術隱藏身份，同時偵測時區的不一致性、異常的語言設定、螢幕解析度偏差及 IP 地址數據異常等高風險活動。

偵測虛擬環境與殭屍裝置

大部分自動化攻擊源自虛擬裝置，使騙徒能進行大規模惡意活動並抹去痕跡。透過瀏覽器數據分析、IP 信譽訊號及先進的異常與規避偵測技術，有效識別虛擬環境。

揭示高風險裝置與帳戶連結

即使橫跨不同客戶及行業，亦能找出裝置與帳戶之間的隱藏連結，有助揭露詐騙集團及與其有關聯的裝置。

精準確認所有裝置類型

智能裝置風險防範方案分析數以千計的裝置屬性組合，從而準確識別裝置，同時降低誤報率。

TransUnion
環聯

以具主動性的機器學習預測模型分析複雜模式

透過具預測能力及動態調整能力的機器學習模型，配合專屬規則及強大的裝置訊號，精準分析複雜行為模式，主動偵測詐騙活動。讓數據科學家的專業知識能用於專注識破詐騙行為，而非管理靜態規則。

提升防詐騙策略功效

善用環聯的數據科學知識及由數據科學主導的風險策略完善服務 - 此自選產品透過具預測能力的機器學習模型，偵測一般情況下難以察覺的詐騙行為，從而減少對昂貴且有限的數據科學資源的依賴。

智能裝置風險防範方案的常用案例

預防帳戶接管

→ **挑戰：**網上銀行平台面對帳戶接管帶來的風險，詐騙分子利用盜取所得機密資料對帳戶進行未經授權存取。

→ **解決方案：**智能裝置風險防範方案能偵測異常裝置行為，識別潛在的帳戶盜用，有效防範未經授權存取，保障客戶帳戶安全。

減少付款詐騙

→ **挑戰：**電商企業面對大量詐騙交易，造成財務損失及信用卡退款。

→ **解決方案：**智能裝置風險防範方案能識別可疑裝置行為，偵測高風險交易，有效減少詐騙及信用卡退款情況。

合成身份詐騙偵測

→ **挑戰：**金融機構面臨合成身分詐騙的挑戰，詐騙分子透過結合真實與虛構資料，建立假身份。

→ **解決方案：**智能裝置風險防範方案能分析裝置行為與使用模式，識別潛在合成身份的不一致特徵，協助機構在詐騙發生前主動採取行動。

預防濫用促銷

→ **挑戰：**網上零售商及服務供應商經常面對詐騙分子不當利用折扣及優惠活動的濫用促銷情況。

→ **解決方案：**智能裝置風險防範方案能監察裝置行為，偵測濫用促銷的可疑模式，確保推廣優惠由真實客戶使用。

行業特定使用案例

預防電商詐騙

→ **挑戰：**網上零售商面對大量詐騙交易，造成財務損失及信用卡退款。

→ **解決方案：**智能裝置風險防範方案能識別可疑裝置行為，偵測高風險交易，有效減少詐騙及信用卡退款情況。

銀行與金融服務

→ **挑戰：**金融機構正面臨合成身份詐騙的挑戰，詐騙分子透過結合真實與虛構資料，建立假身份。

→ **解決方案：**智能裝置風險防範方案能分析裝置行為與使用模式，更有效偵測及防止未經授權的存取，有助確保客戶帳戶安全。

TransUnion 環聯

保險詐騙偵測

→ **挑戰：**保險公司需有效識別欺詐索償及潛在虛假的保險經紀，以防止保單被濫用。

→ **解決方案：**智能裝置風險防範方案能揭露裝置與帳戶之間的隱藏連結，有助偵測及防止欺詐索償行為。

電訊

→ **挑戰：**電訊供應商面對欺詐帳戶開設及裝置盜竊風險。

→ **解決方案：**智能裝置風險防範方案能核實裝置真實性，偵測可疑活動，有效防止詐騙行為並減少損失。

醫療保健

→ **挑戰：**醫療保健機構需要保障病人資料，防止未經授權存取醫療紀錄。

→ **解決方案：**智能裝置風險防範方案能監察裝置行為並偵測異常情況，確保只有經授權裝置方可存取敏感資料。

電競與線上服務

→ **挑戰：**線上電競平台及服務面對帳戶接管及各類欺詐活動風險，其中包括濫用促銷。

→ **解決方案：**智能裝置風險防範方案能透過裝置數據識別並阻截可疑行為，有效保障平台安全性與公平性。

旅遊與款待

→ **挑戰：**旅遊及款待業需防範預約詐騙及對客戶資料未經授權的存取。

→ **解決方案：**智能裝置風險防範方案能於預約流程中分析裝置行為，偵測可疑活動並預防詐騙。

如欲了解更多關於如何運用裝置數據與洞察以強化防詐騙策略及與客戶建立信任，請瀏覽：transunion.hk/device-risk