CGI Hotscan360
Fraud Detection
System (FDS)

CGI

Introduction

In today's digitally interconnected world, the threat of fraud looms large over financial institutions, fintechs and their customers. As technology advances, so do the tactics of fraudsters, necessitating sophisticated solutions to mitigate risks effectively.

In response to this challenge, we propose the collaborative integration of CGI Hotscan360 Fraud Detection System (FDS) and Wultra In-App Protection. This cooperation outlines the synergistic benefits of this integration and elucidates the enhanced capabilities it offers in combating fraudulent activities across various digital channels.

Cooperation overview

In an era marked by escalating cyber threats, the cooperative integration of CGI FDS and Wultra Device Analytics System represents a proactive approach to combating fraud in the digital realm. By harnessing the collective capabilities of these two systems, financial institutions can fortify their defenses against fraudulent activities, safeguard customer assets, and uphold trust in the financial ecosystem.

Cooperation model

The CGI Fraud Detection System is a robust platform designed to identify and prevent fraudulent transactions, leveraging advanced algorithms and machine learning techniques.

Wultra Device Analytics System provides real-time insights into device behavior, enabling the detection of anomalous activities indicative of potential security threats.

By integrating these two systems, financial institutions can establish a comprehensive fraud detection framework that addresses the evolving nature of cyber threats.

Benefits:

Enhanced Fraud Detection Accuracy:
By combining transactional data with real-time device insights, the integrated solution offers enhanced accuracy in identifying fraudulent activities, thereby reducing false positives, and minimizing financial losses.

Improved Customer Experience:
Proactive fraud detection measures instill confidence in customers regarding the security of their transactions, thereby enhancing overall customer experience and fostering long-term loyalty.
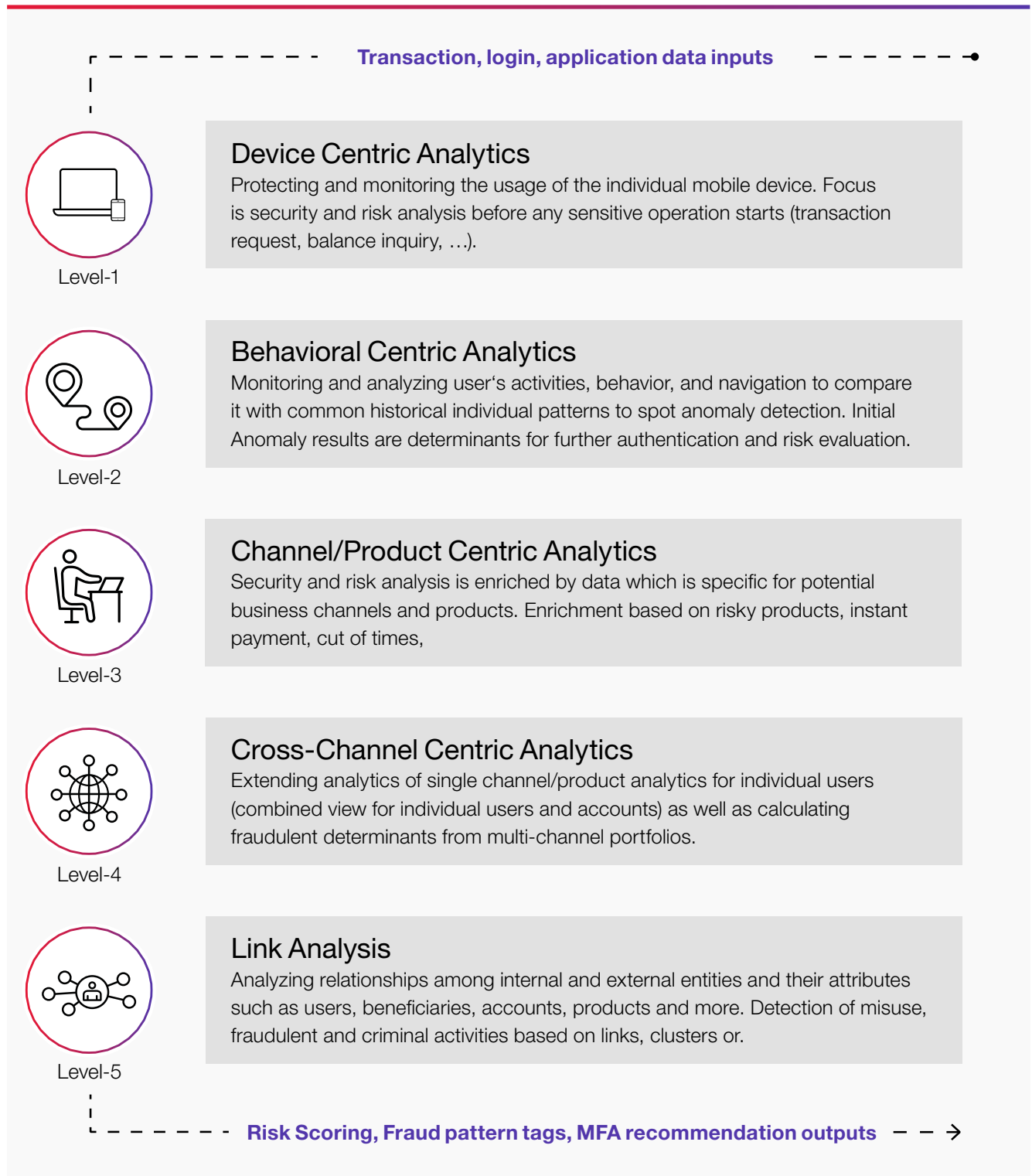
Cost Savings:
By mitigating fraud-related losses and reducing manual intervention for fraud investigation, financial institutions can realize significant cost savings over time.

Regulatory Compliance:
The integrated solution helps financial institutions comply with regulatory requirements pertaining to fraud detection and prevention, thereby mitigating compliance risks, and avoiding regulatory penalties in ever rising regulatory pressure.

Main analysis flow for mobile banking fraud detection

Transaction, login, application data inputs

Device Centric Analytics

Protecting and monitoring the usage of the individual mobile device. Focus is security and risk analysis before any sensitive operation starts (transaction request, balance inquiry, …).

Level-1

Behavioral Centric Analytics

Monitoring and analyzing user's activities, behavior, and navigation to compare it with common historical individual patterns to spot anomaly detection. Initial Anomaly results are determinants for further authentication and risk evaluation.

Level-2

Channel/Product Centric Analytics

Security and risk analysis is enriched by data which is specific for potential business channels and products. Enrichment based on risky products, instant payment, cut of times,

Level-3

Cross-Channel Centric Analytics

Extending analytics of single channel/product analytics for individual users (combined view for individual users and accounts) as well as calculating fraudulent determinants from multi-channel portfolios.

Level-4

Link Analysis

Analyzing relationships among internal and external entities and their attributes such as users, beneficiaries, accounts, products and more. Detection of misuse, fraudulent and criminal activities based on links, clusters or.

Level-5

Risk Scoring, Fraud pattern tags, MFA recommendation outputs

Functional integration Wultra In-App Protection and HS360 FDS

Wultra Device analytics inputs	HotScan360 FDS key features:
Extended warnings:	**Monitoring**
• Mobile malware	• SLA and Business real-time monitoring
• Debugger connection	• Application monitoring
• Emulator or virtual environment	• Infrastructure monitoring
• Rooting or jailbreak	• Managerial reporting and distribution
• Runtime library injection	**Client profiles**
• Hooking frameworks	
• Tapjacking	• Online profiles
• Remote access	• Long term client profiles
• Code injection	• Behavioral profiles
• System and user screenshots	• Internal data-warehouse based profiles
• Untrusted keyboards	• Client specific profiles (optional)
• Untrusted screen-readers	**Real-Time Risk engine**
• Sensitive process identification	
• Native code hooks	• Velocity of funds validation
• External screen sharing	• Anomaly detection
• Man-in-the-app scenarios	• Client specific validations
• Man-in-the-middle scenarios	• 3rd party systems data integration
• Insecure HTTP Proxy	• Machine learning integration
• App repackaging	**Screening engine (optional)**
• Compromising asset integrity	
• Overlay attacks	• Fuzzy match search
• Passcode not set	• Sanctions list match
• Key extraction (white-box crypto)	• Internal blacklists match
• Extraction of other sensitive data	• Custom watchlists integration
• Device cloning	**Case management**
• Untrusted App Marketplaces	
• Outdated OS version	• Natively integrated case management, or
	• REST API for customization for client specific case management and investigation workflow

Key Features and Capabilities:

Advanced Fraud Detection Algorithms: CGI Fraud Detection System employs sophisticated algorithms to analyze transactional data and identify patterns indicative of fraudulent behavior. By integrating Wultra Device Analytics, additional contextual information regarding the device used for the transaction is obtained, enhancing the accuracy of fraud detection

Real-time Device Profiling: Wultra Device Analytics System captures and analyzes device attributes, including device type, operating system, geolocation, and behavioral patterns. This real-time device profiling enables the identification of suspicious activities associated with compromised or unauthorized devices.

Multi-channel Fraud Detection: The integrated solution extends fraud detection capabilities beyond traditional channels to include mobile banking, online transactions, and other digital touchpoints.
By correlating transactional data with device information, suspicious activities can be flagged across multiple channels, thereby reducing false positives, and enhancing fraud detection accuracy.

Adaptive Machine Learning: Both CGI Fraud Detection System and Wultra Device Analytics System employ adaptive machine learning algorithms that continuously learn from new data and evolving fraud patterns. This adaptive approach ensures that the fraud detection framework remains effective in detecting emerging threats and evolving attack vectors.

Unified Dashboard and Reporting: The integrated solution provides a unified dashboard for monitoring and reporting fraudulent activities across all channels. Financial institutions gain actionable insights into fraud trends, enabling proactive measures to mitigate risks and protect customer assets.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit: cgi.com

Email: enquiry@cgi.com

CGI