feedzai

Proactive. Continuous. Silent.

Session Summary

Device Anomalies 19		90
Fraudster Behavior		70
Suspicious Behavior	10	

Initial Analysis

- Mobile RAT Installed
- (+) AnyDesk

Device

Battery Level	57%
Status	Charging
Device ID	d508c34279ff7
Disk Space	75.45GB
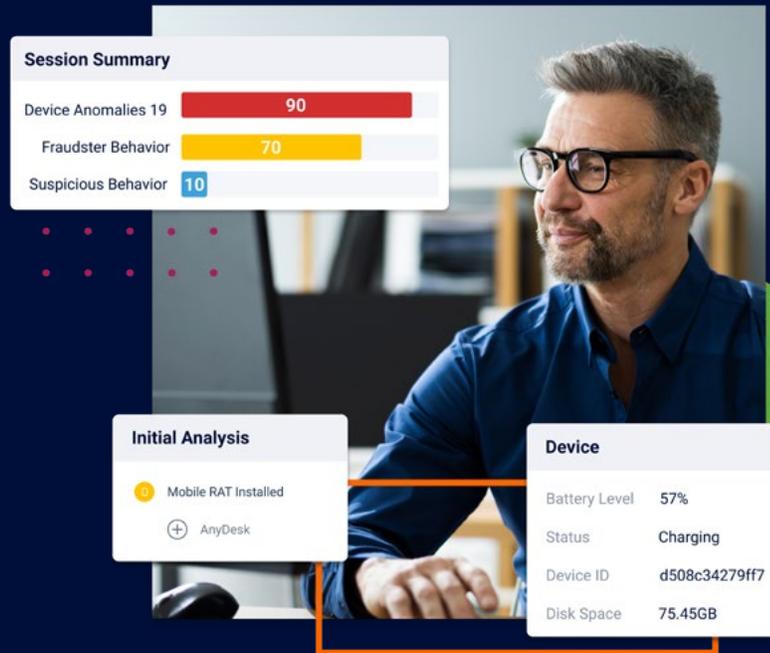
Trusted by 80% of the world's Fortune 500 companies

fiserv.   citi   ◆ Santander   LLOYDS BANKING GROUP

A decade of data breaches and malware have exposed billions of PII elements and stolen identities. Fraudsters have capitalized on this through various attacks, like account takeover, manipulation attacks, scams, and more. Traditional point solutions don't provide a 360-degree view of risk and notify the bank reactively at the point of transaction. As the world increasingly adopts real-time payments, banks need a single fraud platform to stop attacks before the transaction stage. It's time to change the game; prevention needs to happen proactively, not reactively, without impacting customer friction.

Proactively Prevent Fraud and Build Trust.

✓ **Stop online attacks in real-time**
Stop attacks at every online interaction by collecting and analyzing customer biometrics and behavior, network, device, and threat data – their BionicID™ in real-time. Feedzai's Active Defense proactively stops malware, phishing, and Remote Access Trojans before they steal identities and cause harm.

✓ **Continuously verify customers**
Feedzai's Know Your User approach continually and silently asks, "are you really you?" utilizing a user's BionicID™ to identify legitimate customers, stop fraud before it happens, and improve the customer experience by eliminating step-up authentications and reducing false positives.

✓ **Improve transaction decisioning**
User BionicID data and analysis are pre-integrated with Feedzai's Transaction Fraud for Banks. They can also be used by other transaction monitoring or SIEM solutions to provide user interaction data and analysis to improve transaction decisioning accuracy and reduce operational risk.

Key Features

Comprehensive customer verification

Customers are verified at every interaction by collecting and continually analyzing their BIonicIDs comprised of online biometric actions, behavioral patterns, device data, account behavior, geolocation, and more, looking for anomalies.

Active defense

Stop ID-stealing malware or phishing attacks. By preventing users from being manipulated into compromising their credentials. Protect customers from Remote Access Trojan session hijacking malware automatically via step-up authentication or automatic session logoff actions.

Hybrid AI

Customer BionicIDs are analyzed, updated, and verified at every interaction with hybrid AI technology that enables you to really know your user and protect them during every session.

Real-time

All customer BionicID interaction data is pre-integrated into Feedzai's Transaction Monitoring for banks and can be integrated into other transaction monitoring systems or SIEM systems to improve transaction monitoring decisioning.

Silent customer experience

Prevent customer friction by silently authenticating users at every interaction without the need for friction-inducing verification methods.

Flexible deployment model

Pre-integrated with Feedzai for Transaction Fraud for Banking, standalone, or in conjunction with other Transaction Monitoring solutions, SIEMs, or other fraud management systems via API.

Awards and Recognition

Quadrant Knowledge Solutions — Feedzai named a Behavioral Biometrics Leader.

FORRESTER® — Feedzai named a Strong Performer in Enterprise Fraud Management.

Aite Novarica Fraud & AML WINNER — Feedzai named Best in Class Fraud and AML Machine Learning Platform.

Are you ready to start proactively protecting your customers?

Request a Demo