Solution Guide

Digital Trust

Legal Terms And Intellectual Property

The information contained in this document is the property of REVELOCK, a Feedzai company, and is CONFIDENTIAL and may not be subject to total or partial reproduction, computer processing, or transmission in any form or by any means, whether electronic, mechanical, by photocopy, registration or any other. Similarly, it may not be disclosed or distributed to third parties, nor may it be subject to a loan, rental, or any form of assignment of use without the prior written permission of REVELOCK, a Feedzai company, (hereinafter referred to as Feedzai), the Copyright holder. Likewise, no modification of this document or its contents is allowed; any modification to this document must be requested of and expressly approved by Revelock or Feedzai personnel to be valid. Failure to comply with the limitations indicated by any person who has access to the information contained herein will be prosecuted in accordance with the law.

This document aims to describe and provide more detailed information on Digital Trust for the detection and prevention of online banking fraud. It is addressed to FINAL CUSTOMERS, Revelock or Feedzai PARTNERS, as well as to potential end customers from the last batch.

PARTNER is any Revelock, a Feedzai company, a partner company that is certified in the Digital Trust solution and/or that has received this document in an authorized way from Revelock, or to any FINAL CUSTOMER to whom the PARTNER makes an authorized delivery of this document complete or any part thereof.

Confidentiality and its mandatory compliance extend to any person within REVELOCK, the PARTNER or the additional FINAL CUSTOMER, and in accordance with the terms of the NDA that may exist signed between any of the parties FINAL CLIENT, PARTNER, and REVELOCK. The three parties, FINAL CLIENT, PARTNER, and REVELOCK are obliged to guarantee the security, integrity, and confidentiality of the information not only of this document but of any other sensitive information that could be generated and exchanged between the three companies during the process of analysis, evaluation, acquisition, possible deployment, and subsequent use of Digital Trust by the FINAL CUSTOMER concerned.

Purpose of this Document

This document provides more detailed information on Digital Trust (formerly known as the Revelock Fraud Detection and Response Platform) and its capabilities. Feedzai's Digital Trust solution is for the detection and prevention of online banking fraud for banking or financial organizations (hereafter referred to as the BANK).

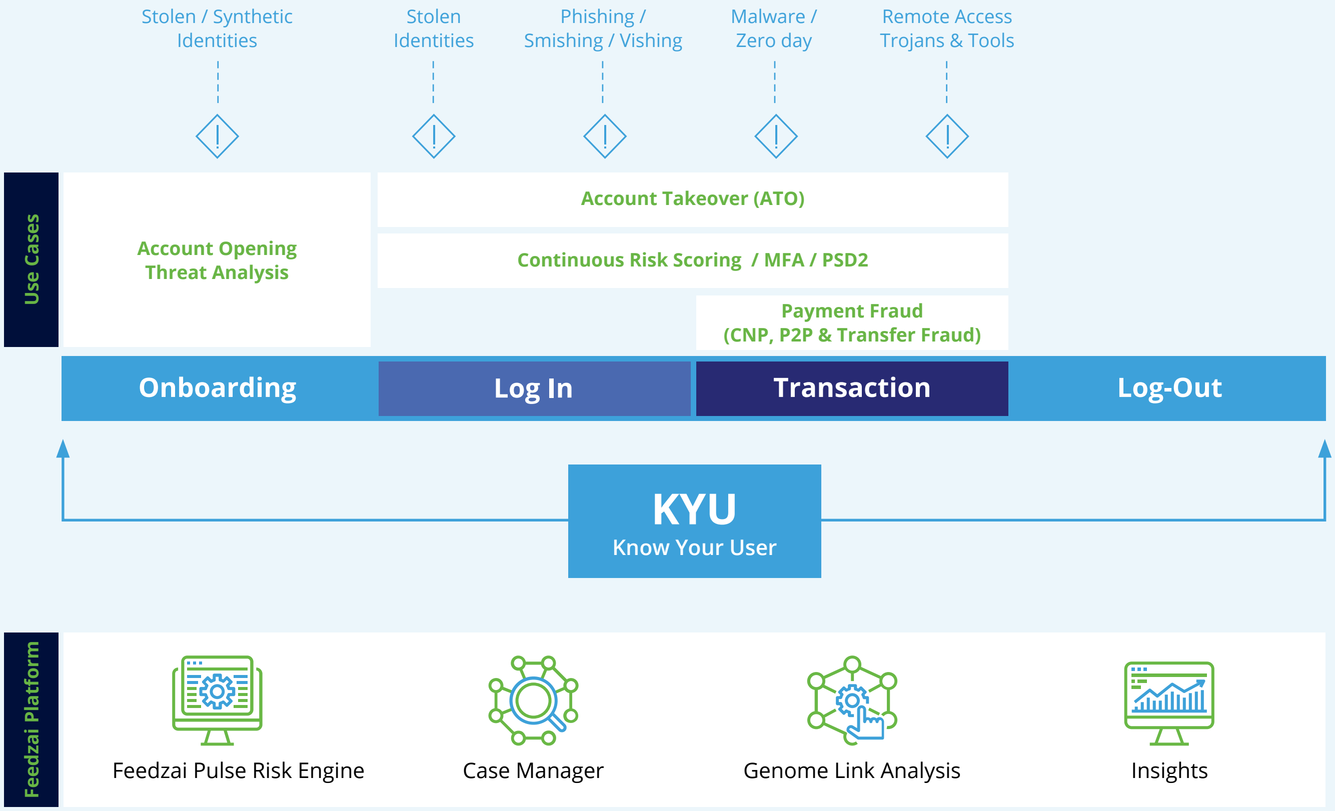
The BANK referred to in this document is a banking or financial organization interested in knowing more about Digital Trust and its operation, and to which Feedzai authorizes access to this complete document or any part of therein.

Contents

1. Introduction

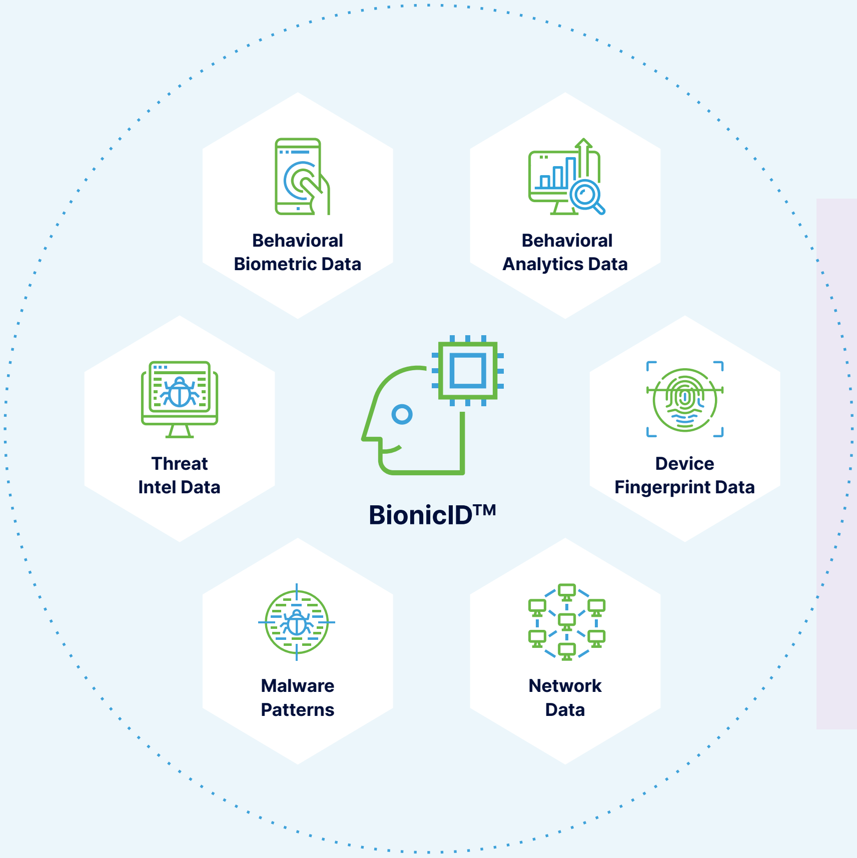
Digital Trust from Revelock, a Feedzai company, is a SaaS/cloud-based solution that enables financial services and FintTech companies to reveal and respond to online identity impersonation and manipulation attacks from login to logout, across every user interaction, all without hindering the customer experience.

Financial Institutions (FIs) use Digital Trust for continuous risk scoring that enables completely silent and fully transparent Strong Customer Authentication (SCA) and PSD2. It is also used to prevent Account Takeover (ATO).


Stolen / Synthetic Identities
Stolen Identities
Phishing / Smishing / Vishing
Malware / Zero day
Remote Access Trojans & Tools
Use Cases
Account Opening Threat Analysis
Account Takeover (ATO)
Continuous Risk Scoring / MFA / PSD2
Payment Fraud (CNP, P2P & Transfer Fraud)
Onboarding
Log In
Transaction
Log-Out
KYU
Know Your User
Feedzai Platform
Feedzai Pulse Risk Engine
Case Manager
Genome Link Analysis
Insights

The first line of defense Digital Trust delivers protects end users and banking customers from malware and phishing attacks aimed at stealing user credentials or taking over sessions to commit fraud.

A second, deeper line of defense combines user behavioral biometrics (how you type, swipe, hold, and use your device to access a protected web or mobile app), behavioral analytics (when and what you do), device and network data, and analyzing this data using hybrid AI models including Deep Learning to create a **BionicID™** for every user, at sign-up. Starting from that point, the **BionicID™** is continually updated and analyzed at every interaction to **Know Your User (KYU)** thoroughly. The system examines the user's identity performing each action, allowing verified users to proceed while blocking bad actors.



Digital Trust includes Active Defense and Pre-Emptive Defense capabilities.

The most efficient way to actively protect users is to stop fraud losses before they can occur. The second most efficient way is to allow fraud teams to configure automated processes that prevent impersonation attacks and block known bad actors – stopping fraud and minimizing the fraud analysts' workloads. Digital Trust includes Active Defense and Pre-Emptive Defense capabilities that automatically and proactively prevent fraud losses, improve fraud operational efficiencies, and prevent negative customer experiences.

1.1. Preventing Impersonation & Manipulation Attacks

Digital Trust combines behavioral biometrics, behavioral analytics, advanced malware detection, and network and device assessment with hybrid AI models including Deep Learning, to create and continuously analyze **BionicID™**, to Know Your User (KYU), spot bad actors, and mitigate risk regardless of the type of attack.

From login to logout, across every interaction, the all-in-one solution non-intrusively detects behavioral and environmental anomalies while protecting customers from impersonation and manipulation attacks. These include remote access trojans, zero-day malware, bots, and social engineering-based attacks.

How Digital Trust Stops Impersonation Attacks

Impersonation Attacks start with stolen credentials. Feedzai's Digital Trust blocks impersonation attacks by preventing malware or phishing attacks from stealing user credentials in the first place. Feedzai Active Defense also allows FIs to determine the appropriate actions when malware or phishing attacks are detected on user devices. Users are immediately, automatically, and often silently protected from threats while the FI's fraud teams are automatically alerted.

In today's post-breach world, stolen credentials are readily available for bad actors to use to impersonate legitimate users. Stolen credential attacks require a different approach to stop since they are both executed both by credential-stuffing bots and manually by humans. These kinds of attacks are detected, and account takeover is prevented, by **BionicID™** analysis.

How Digital Trust Stops Manipulation Attacks

Manipulation Attacks utilize remote access software, through malware web injections or app/screen overlays, and deceive victims into executing a RAT attack. Both types of attacks are designed to gain control of a victim's device.

More frequently, cybercriminals seek to gain control of a user's banking session. This form of attack is easier to execute because it bypasses traditional account security allowing a bad actor to take control of a victim's account temporarily. Feedzai's Active Defense **BionicID™** analysis can detect and defeat both remote access attack types stopping attempted session takeovers –- protecting users and notifying the FI.

Feedzai analyzes thousands of users, network, and system parameters collected during every online interaction or operation to protect users from impersonation and manipulation attacks. This data is processed in the cloud using hybrid AI models, including Deep Learning to create a **BionicID™** for all users –- whether legitimate or bad actors –- at sign-up. The **BionicID™** is continually updated and analyzed at every interaction to calculate a holistic risk score for each customer.

> *The BionicID™ is continually updated and analyzed at every interaction to calculate a holistic risk score for each customer.*

The system either silently grants legitimate users access or stops bad actors, depending on the risk. The FI has access to risk scores at all times and can configure when it should be alerted and automate appropriate action to be taken.

If an impersonation or manipulation attack is detected, FIs are offered two flexible response paths. The first is to immediately protect users at the point of attack. The second is to simultaneously alert the FI's fraud teams of the attack and execute a follow-up response – ranging from sending user notifications, stepping up authentication, terminating a session, or locking the account – to stop fraud before it happens.

1.2. Comprehensive & Continuous User Verification

The primary goal of fraud prevention solutions has traditionally been to ask the question, “are you a bad actor?” But approaching fraud prevention strictly from the “are you a bad actor?” approach is not a comprehensive strategy for solving a very complex problem.

User Types

✓ **Legitimate**

Customers who account for the largest percentage of users;

☒ **Illegitimate**

Bad actors who account for the smallest percentage of users;

⊖ **Indeterminate**

Users who cannot be easily classified due to being new account owners or due to an environmental change (suspicious or otherwise).

That’s why Feedzai’s Digital Trust solution has unique biometric processing capabilities that distinguish it from other solutions by answering the fundamental question “are you really you?” Both questions must be asked and answered repeatedly, from login through logout.

The first and foremost priority for Feedzai is to let legitimate customers access their accounts and lock out illegitimate or bad actors. Feedzai does this with a fine-grain analysis of the BionicID™ of each user at every interaction. This enables FIs to really perform KYU and sort legitimate from illegitimate actors. A seemingly straightforward concept, but one that is challenging to do because of the complexity of a third type of user: the indeterminate user.

A small percentage of users who are classified as indeterminate AND who turn out to be bad actors are actually responsible for the majority of a FI's fraud-related costs. These include:

→ **Costs related to dealing with false negatives or false positives;**

→ **Actual fraud losses from not stopping these bad actors;**

→ **Customer churn resulting from fraud, or excessive friction resulting from implementing onerous fraud prevention technologies.**

Properly identifying indeterminate users quickly, without adding unnecessary friction, is critical to reducing fraud losses, avoiding fraud investigations, and preventing lost business due to upset customers. Answering the simple question – are you really you? – dramatically increases the speed and accuracy with which Feedzai is able to reduce the number of users classified as indeterminate and assess whether a user is legitimate or a bad actor.

Answering the simple question – are you really you? – dramatically increases the speed and accuracy to reduce the number of users classified as indeterminate.

User Verification is performed using several steps:

Step 1

First, it quickly identifies and filters out known **bad actors** using data, identifiers, and analysis techniques commonly used in the industry. From there, indeterminate users can be more closely scrutinized to further separate legitimate customers from bad actors.

Step 2

Next, **login verification** ensures continuity of BionicID™ data from the last logout to the current login, making sure nothing changed from the previous interaction to the current interaction to confirm only known good users are granted access. This verification phase can quickly detect impersonation attacks by identifying device and network anomalies –- clearly suspicious activity indicators. Following network and device verification, biometric and behavioral data is analyzed against previous BionicID™ data. This more detailed analysis can verify an attempted account takeover, especially in conjunction with an initial device and network verification.

Step 3

The final step is **in-session verification**. Once a user is identified and login is granted, the next validation phase begins. From here, each successive interaction (check balance, move funds, etc.) conducted by the customer “in the moment” requires a BionicID™ check. Continually verifying customers throughout their session is critical to prevent in-session manipulation or a session hijack. These forms of attack are particularly insidious since they avoid the difficulty of committing an ATO attack. Instead, a bad actor hijacks a banking session, executes a fraudulent transaction, and disappears without a trace. These point impersonation attacks are usually executed using RAT malware. In some cases, attacks are carried out by bad actors using legitimate but compromised applications to access a user’s computer called Remote Access Tools.

A user’s BionicID™ is examined at every point in the session to ensure that the user who was initially verified and logged in is the same person executing every transaction. This is one of the primary use cases where continually verifying “are you really you?” not only avoids session hijacking but also greatly minimizes customer friction. The need for stepped-up or multi-factor authentication during the customer’s journey is eliminated.

2. Digital Trust Components

Digital Trust is comprised of **three functional blocks**:

Collect

Data Collection from every web and mobile interaction;

Reveal

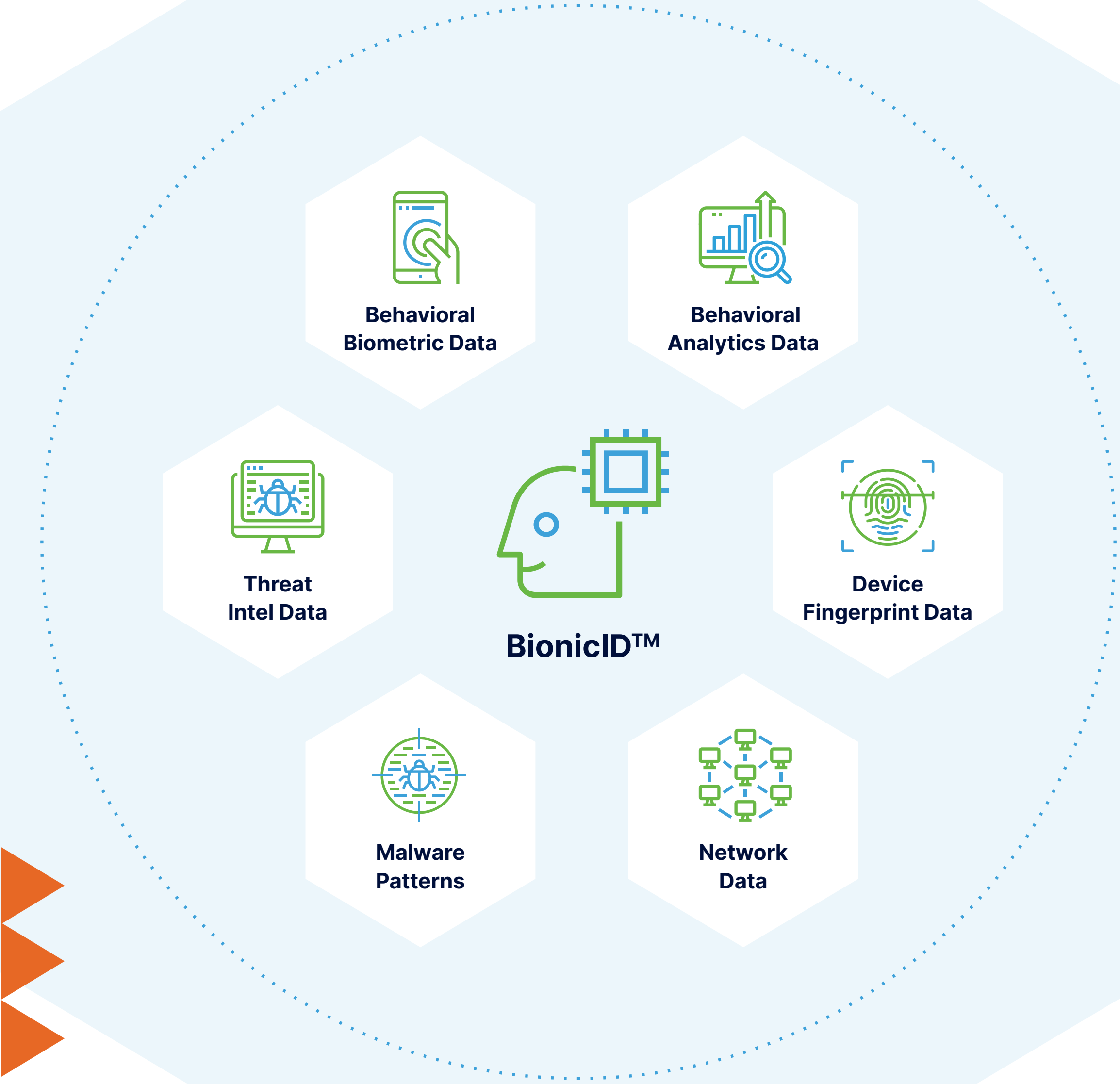
Continuous BionicID™ analysis and risk assessment;

Respond

Active and Pre-Emptive defensive capabilities.

2.1. Collect

Data collection is enabled via JavaScript for web banking and an SDK for mobile banking apps. The system continuously collects thousands of data parameters to create user context that is used to establish and verify a user's digital fingerprint or BionicID™. These data sources and parameters include:



Behavioral Biometric Data

- Touch/keystroke
- Mouse
- Mobile spacial sensors

Behavioral Analytics Data

- User journey
- Velocity check
- Date/time of connection

Device Fingerprint Data

- Mobile device characteristics
- Computer characteristics
- Operating system info
- Applications
- Languages installed/used

Network Data

- IP address/domain/ISP/ASN
- Connection type/speed
- Geolocation
- Wi-Fi SSID/BSSID

Malware Patterns & Threat Intel Data

While data on every user interaction is collected, third-party data feeds and threat intelligence are used to enrich what is known about the user and determine if there are obvious signs of fraudulent activity that are immediately actionable. This parallel data stream includes:

- Malware signatures
- Phishing Site locations
- Fraudulent identifiers that can be connected back to devices
- Network
  - Device
  - Email
  - Mobile number
- Lists of tools and applications related to fraudulent behavior and known to be commonly used by bad actors

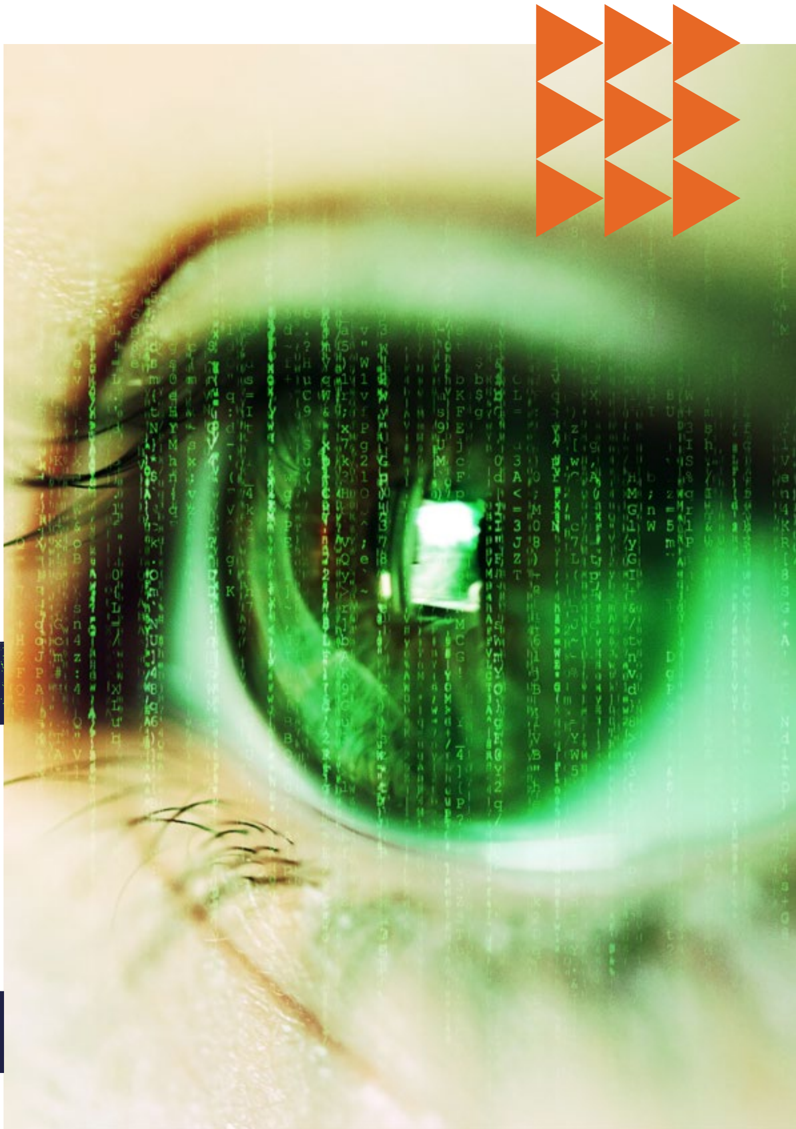
2.2. Reveal

At every point in the customer journey, the Digital Trust Anomaly Detection & Classification Engine continually makes decisions and determines the current risk associated with a customer's BionicID™ during each customer session and at every point in the customer journey.

The analysis selected is determined by the type of data being examined. This ranges from simplistic - (e.g., comparing against known compromised IP addresses) to very complex (e.g., determining changes in a user's biometric data) anomalies between the current BionicID™ and the previous verified state.

Digital Trust uses per-user models, population-based models, and bad actor models along with hybrid AI techniques including:

- Decision Trees
- Supervised Machine Learning
- Unsupervised Machine Learning
- Deep Learning



Preventing Fraud Impersonation & Manipulation Attacks

Feedzai's Digital Trust solution was designed to detect all online identity-based account takeover attempts:

2.2.1. Credential-stealing Attacks

Malware attacks

Trojan bankers that modify the information the user sees, or code designed to steal credentials in order to perform an account takeover at a later time.

- Feedzai's Digital Trust identifies previously discovered and classified malware using continually updated industry black and whitelisting threat data.
- Feedzai's Digital Trust is also capable of identifying malware patterns not previously identified through a process called "grey-listing." This process routes newly discovered code anomalies to the Digital Trust malware classification system where they are analyzed using Deep Learning algorithms under expert supervision.

Phishing attacks

Generally delivered by convincing-looking emails designed to direct users to a fraudulent, cloned website that was created to steal their credentials.

- Phishing Prevention detects when a customer clicks on a phishing link to a fraudulent website and redirects them away from the harmful site.

2.2.2. Stolen Credentials-Fueled Attacks

Customer impersonation

A targeted attack against a customer account utilizing stolen credentials. Customer impersonation attacks are detected by:

- Analysis of bad actor indicators, including network data, device data, or other indicators that are continually analyzed and compared to threat data collected by Feedzai and 3rd party threat data feeds.
- BionicID™ analysis to determine suspicious behavioral or biometric data anomalies.

Credential stuffing

Generally a bot-driven, broad-based attack utilizing stolen credentials and used across a wide range of accounts attempting to take advantage of user email/ password reuse. Bot-driven attacks are detected by:

- Analysis of threat indicators including network data, device data, or other threat indicators that are continually analyzed and compared to threat data collected by Feedzai and 3rd party threat data feeds;
- Behavioral threat indicators that identify a bot's ability to rapidly navigate and load credential data faster than humanly possible;
- Biometric threat indicators to detect bots employing sophisticated "low and slow" modes of operation to better copy human behavior.

2.2.3. Manipulation Attacks

Digital Trust can detect the difference between Remote Access Trojans and Remote Access Tools. In conjunction with Digital Trust's Active Defense can proactively mitigate these attacks by disabling the attacking RAT.

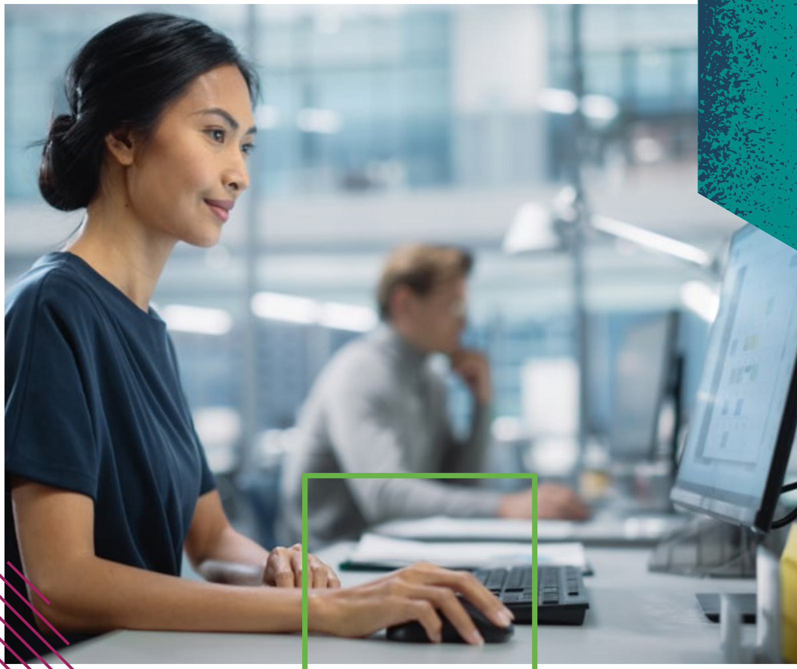
Remote Access Trojans

A specific malware type that permits attackers to take control of a victim's computer during a banking session.

Remote Access Tools

Legitimate applications that can be misused by bad actors to take full control of a user's computer, or just a session.

2.3. Respond



Digital Trust Active Defense delivers a highly flexible set of response capabilities to prevent a user from being manipulated into taking an action that would compromise a session or expose their credentials.

Active customer protection is executed in **three simultaneous steps:**

Step 1

Immediate Protection

When an attack is detected, the Customer is immediately and transparently redirected to safety;

Step 2

Response Automation

Ranges from notifying the customer, stepping up authentication, terminating the session (auto-logoff), or locking out the account;

Step 3

FI Notification

Alerts the FI’s fraud teams to take any necessary action.

Digital Trust Active Defense detects and responds to a variety of threats including:

Malware Blocker

Delivers a highly flexible response capability to keep up with the latest malware threats (browser-based).

- Validates browser Document Object Model (DOM) and blocks suspicious web malware/inject code.
- Intelligently identifies bad code to minimize false positives.
- Detects and stops browser page overlay attacks designed to redirect users to fraudulent/malicious destinations.
- Auto-responds with customizable defensive overlays and notifies the FI to mitigate the attack by configuring automated stepped-up authentication, session termination (auto-logoff), or locking out the account.

mRAT Blocker

SDK-based, RAT protection that detects and responds to a remote access attack.

- Auto-responds with customizable defensive overlays to block the attacker's view of the victim's app.
- Delivers transparent protection without interfering with the customer's mobile bank interaction.

Phishing Blocker

Detects when a customer clicks on a phishing link that redirects them to a cloned website created to steal their credentials.

- When a phishing redirect is detected, customer navigation to the fraudulent site is automatically redirected back to a customizable, legitimate page keeping them safe from the phishing attack.

Auto Logoff

One of the response options designed to protect customers from having their accounts compromised.

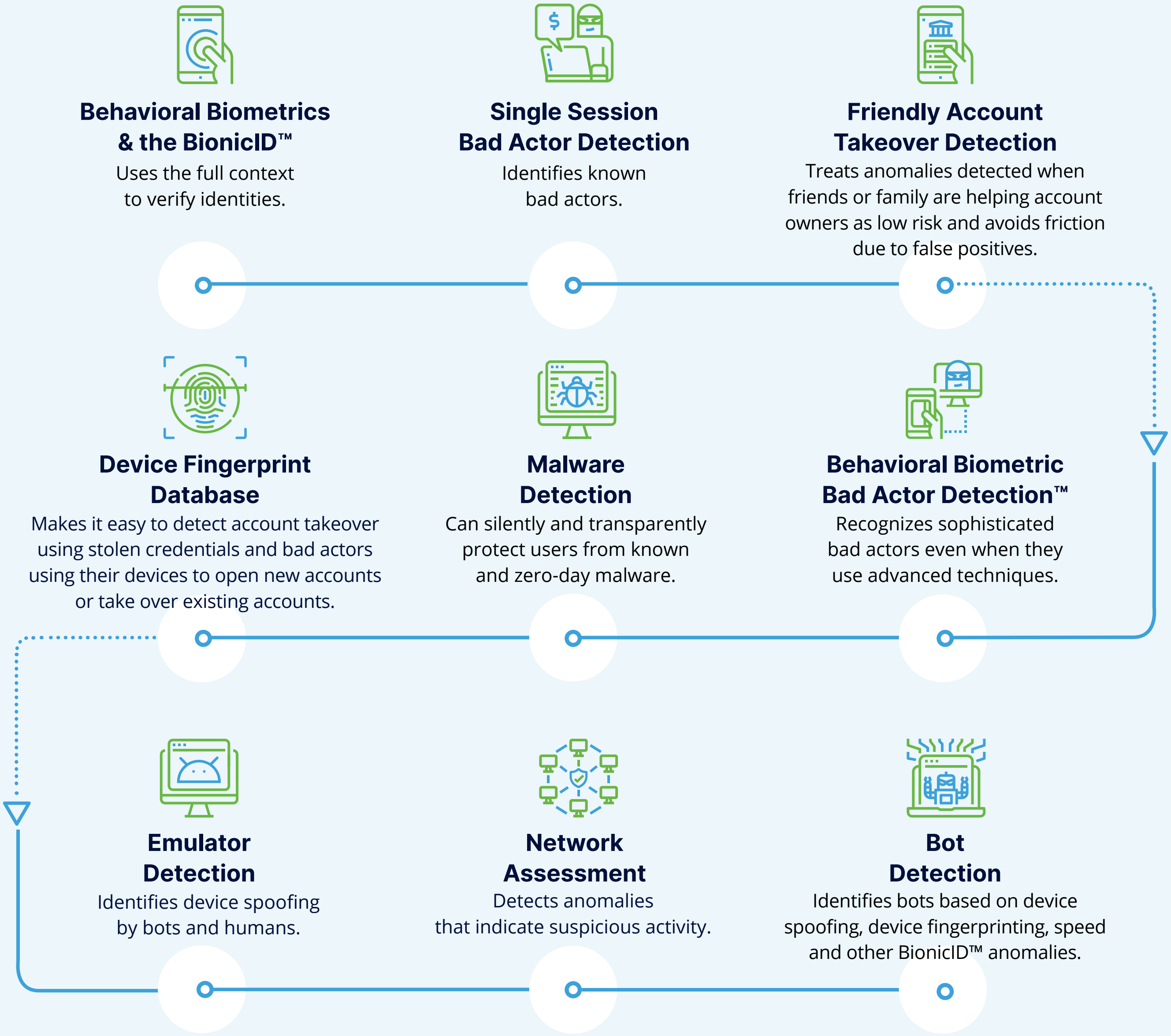
- Browser auto-logoff cleans banking cookies and ends the current session, requiring customers to log back in to establish a new, clean session.
- Mobile app – app shutdown/auto logoff terminates the mobile app session.

Digital Trust Pre-Emptive Defense

Provides a comprehensive fraud prevention capability to discover bad actors, mule accounts, and networks and stop them from committing fraudulent attacks from the point of discovery.

3. Digital Trust Operations

Digital Trust goes through several steps to detect fraud:



Behavioral Biometrics & the BionicID™

Uses the full context to verify identities.

Single Session Bad Actor Detection

Identifies known bad actors.

Friendly Account Takeover Detection

Treats anomalies detected when friends or family are helping account owners as low risk and avoids friction due to false positives.

Behavioral Biometric Bad Actor Detection™

Recognizes sophisticated bad actors even when they use advanced techniques.

Malware Detection

Can silently and transparently protect users from known and zero-day malware.

Device Fingerprint Database

Makes it easy to detect account takeover using stolen credentials and bad actors using their devices to open new accounts or take over existing accounts.

Emulator Detection

Identifies device spoofing by bots and humans.

Network Assessment

Detects anomalies that indicate suspicious activity.

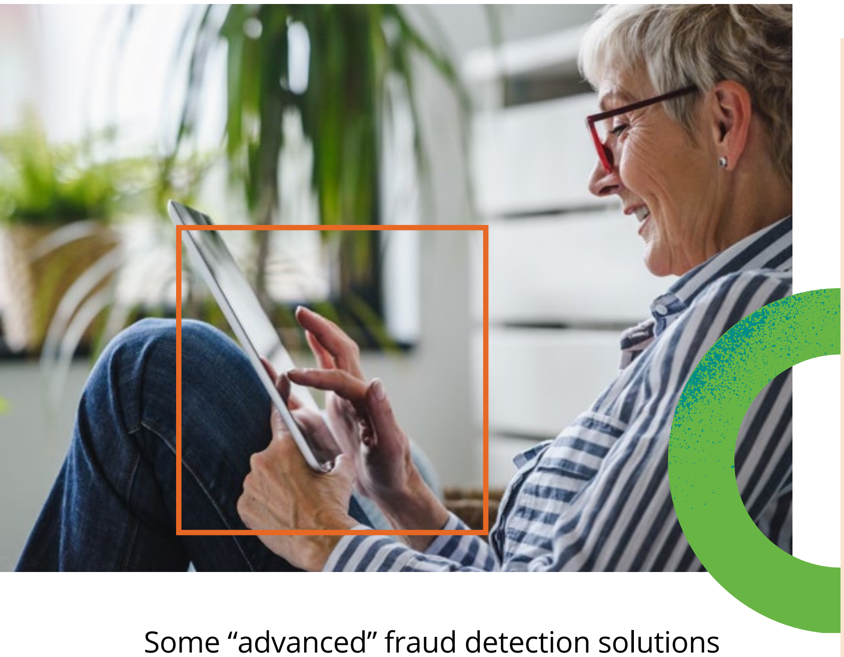
Bot Detection

Identifies bots based on device spoofing, device fingerprinting, speed and other BionicID™ anomalies.

3.1. Behavioral Biometrics & the BionicID™

Digital Trust's unique KYU approach answers the question "are you really you?" using a BionicID™. BionicID™ is a digital fingerprint or digital DNA that is unique to every single user and is created through the collection and analysis of thousands of non-PII parameters relating to the user's context - what they use to access a protected website or mobile application and how they access that app.

Many "advanced" fraud prevention solutions use behavioral biometrics to identify users based on how they type, move their mouse, hold a mobile device, etc. However, the actual determination requires the current user behavior to be judged against a baseline of behaviors. These solutions typically compare the user against a baseline database of bad actors, essentially asking the question, "do you look like a bad guy?" While this is an effective approach in many cases, it does not provide complete coverage.



> *BionicID™ is a digital fingerprint or digital DNA that is created through the collection and analysis of thousands of non-PII parameters relating to the user's context.*

Some "advanced" fraud detection solutions combine behavioral biometrics with device fingerprinting. These solutions often generate extraneous false positives resulting from analyzing device data from shared devices that are used to access accounts belonging to the same FI. In this case, one user or the other may not exactly look like a bad actor, but common device fingerprint indicators can be misread or cross-assigned to one or more users, generating false positives.

The “do you look like a bad guy?” method of determining legitimate users vs. bad actors is also extremely limiting in scenarios where insiders – people who have verified identities and are not part of the larger universe of cybercriminals – attempt unauthorized access to bank accounts.

BionicIDs™ are based on full user context and built to recognize every single user. They are established quickly and can start answering the question “are you really you?” accurately, in as little as two to four interactions.

BionicIDs™

answer the question
“are you really you?”
in 2 to 4 interactions

BionicIDs™ are based on full user context and built to recognize every single user.

3.2. Single Session Bad Actor Detection

The system begins to capture biometric, behavioral, device, and network data to establish “are you really you?” and build the starting baseline BionicID™ as soon as it encounters a new user. The initial analysis compares the new user’s BionicID™ to the BionicIDs™ of known bad actors, and checks against a database of devices and networks linked to known fraudulent activity. Bad actor BionicID™ data helps identify bad actors working inside an online banking system who may be trying to create a new mule account.

Digital Trust also checks other suspicious identifiers, such as the apps discovered in use by the new user that are only used by bad actors, or email addresses or mobile phone numbers linked to fraudulent activity in order to uncover other bad actors.

3.3. Friendly Account Takeover Detection

There are many situations where we see a friend or family member helping a customer out with their online banking account. In most cases, this is not fraud. We clearly saw this use case spike in the first few months of the pandemic when online banking use spiked. At a time when in-person banking wasn't possible, new or infrequent online banking customers were often helped by trusted friends or family.

The BionicID™ recognizes when someone other than the real user is accessing an account and uses the full context to determine that the risk of fraud is low. Instead of generating false positives or blocking access and upsetting the customer, the system allows low-risk activity to proceed undisturbed. Solutions that solely rely on comparing user behaviors to those of bad actors do not perform as well in similar circumstances. These solutions either do not raise an alert about possible fraud or are too aggressive and raise a false positive.

3.4. Behavioral Biometric Bad Actor Detection™

Bad actors who do little to conceal their identities, use brute force credential stuffing bots, or have hundreds of compromised accounts and devices connected to their computers are not difficult to detect. On the other hand, bad actors who are better at their craft, just like criminals in the physical world, are harder to detect and stop.

Sophisticated bad actors who are more careful, use clean hardware and networks along with previously unseen humans as proxies. These bad actors will not be detected by solutions that focus on the “do you look like a bad actor?” approach that simply compares biometric, device, and network indicators with those in their bad actor database.

On the other hand, with the ability to create the BionicID™ and achieve 99% accuracy quickly, the ability to continuously verify “are you really you?”, recognize anomalies, and perform fine-grained analysis of suspicious activity, Feedzai is in a far better position to detect sophisticated criminals and their more advanced manipulation and impersonation attempts.

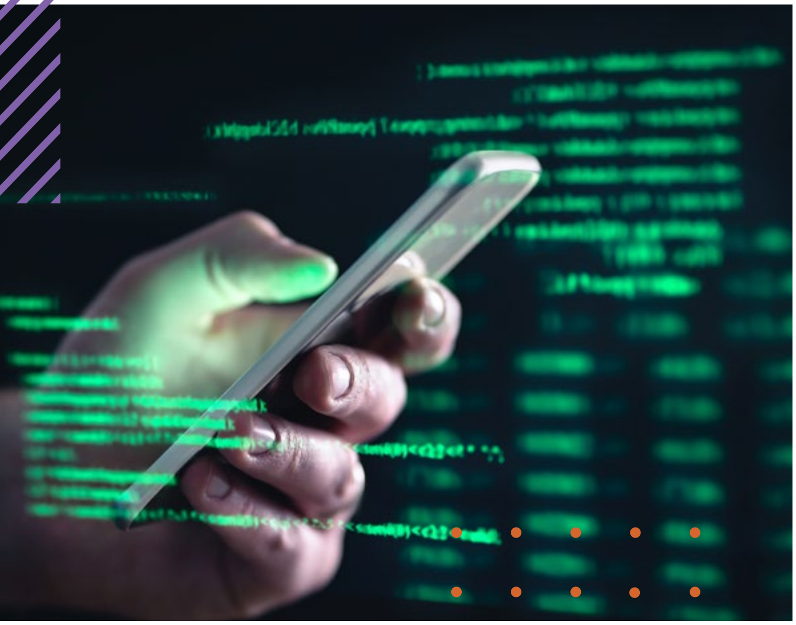
99%

Accuracy

> *The ability to continuously verify “are you really you?”, recognize anomalies, and perform fine-grained analysis of suspicious activity*

3.5. Malware Detection

Banking malware designed to steal credentials or take over banking sessions is a crime of opportunity with substantial payouts and very little risk. Malware code is constantly being modified, encrypted, redirected, and combined with other techniques to execute complex fraud campaigns. Even two-factor authentication (2FA) schemes are being circumvented with current-generation malware. With well-financed and organized criminal rings constantly innovating, significant financial losses occur between the time a new malware variant is released and the time it can be identified and stopped by anti-virus solution providers.



The Digital Trust Malware Anomaly Detection & Classification Engine can identify previously discovered and classified malware through the use of continually updated industry lists of black and whitelisting threat data. Whitelisting is designed to identify suspect code as “safe”, posing no threat to customers, and blacklist code signatures are used to identify previously identified malware as “unsafe.” In both cases, identification is highly accurate resulting in no false positives or false negatives.

The Digital Trust Malware Anomaly Detection & Classification Engine is also uniquely capable of identifying more dangerous zero-day malware – malicious code and malware patterns that have not yet been identified – through a concept called grey-listing. This process routes newly discovered code anomalies into the Digital Trust Malware Classification Engine where they are analyzed using deep learning algorithms under expert supervision. This process results in the classification of samples as either presenting no risk or confirmed to be risky.

Once classified as risky, the next time this zero-day malware is detected, Digital Trust’s active defense capabilities will transparently and proactively protect the user by disabling the attack. In addition, the system will respond according to pre-configured rules with actions ranging from stepped-up authentication, terminating the session, and locking the account to notifying the user and generating an alert.

3.6. Device Fingerprint Database

Device fingerprinting is a way to combine certain attributes of a device -— such as its operating system, the type and version of the web browser being used, the browser's language setting, and the device's IP address, etc. – to identify it as unique.

The BionicID™ includes the user's unique device fingerprint and Feedzai uses this data to determine if a user's device fingerprint is consistent or has changed for some unknown reason, requiring more granular examination.

For example, it is easy to detect these types of account takeover attempts if stolen credentials are used to access an account from a browser or mobile app with a device fingerprint that is different from that of the legitimate user.

Similarly, bad actors' BionicID™s also include their unique device fingerprints. When these bad actors use their devices to try to open a new account or take over an existing account, it is easy for Feedzai to discover and stop these attempts.

3.7. Emulator Detection

An emulator is a virtual mobile device simulator. Essentially, it's software capable of running one, or multiple mobile environments on a PC or Linux computer. Emulators are flexible, easy to set up, and can run in virtual environments –- all reasons that make them appealing to cybercriminals. They help bad actors avoid detection systems by emulating or spoofing device sensors and bypassing previous device fingerprinting verification.

The Digital Trust Anomaly Detection & Classification Engine detects device and network anomalies which are clear indicators of emulator-based device spoofing, such as brute force credential stuffing bot attacks or attacks launched manually.

Feedzai also detects suspicious device activity by analyzing BionicID™ profiles. Any attempt to duplicate BionicIDs™ by automated or human proxies (which are virtually impossible) is quickly detected, analyzed, and assessed as high risk so that the fraud team can investigate and take appropriate action.

3.8. Network Assessment

Network data collected includes all the infrastructure elements used to access online banking. The BionicID™ includes the user's network data and Feedzai uses this data to determine if a user's network infrastructure is consistent or has changed for some unknown reason and requires deeper examination. BionicID™ network data includes:

- → Network infrastructure data
- → IP address and ISP
- → User mobility patterns
- → Geolocations

Network data is enriched with Feedzai's and third-party threat intel to discover anomalies:

- → Dangerous geolocation
- → Known network infrastructures used for fraud
- → Connection masking
- → Malicious mobile applications

The Digital Trust Anomaly Detection & Classification Engine analyzes infrastructure data at each interaction. It can identify how, when, and where each user is accessing a service to discover anomalies related to sessions originating from an unusual location, whether the user is a frequent traveler, or how quickly a user travels from one location to another –- and whether such movement is even possible.

3.9. Bot Detection

Digital Trust detects bots in several ways:

- The simplest detection techniques include emulator detection and device fingerprinting.

- The next level of detection is based on analyzing the speed at which credentials are entered into the login form/page. Unsophisticated bot attacks enter information significantly faster than humans and are easily spotted.

- More advanced bot attacks are based on low and slow attempts to mimic human behavior such as non-linear mouse movements and typing, but these too have no chance of succeeding because of anomalies detected during BionicID™ analysis.

Once a bot attack is detected, the fraud team is immediately notified and can take appropriate action.

4. Use Cases

Digital Trust is used by FIs in a number of use cases:

Continuous Risk Scoring

Completely silent and fully transparent SCA, PSD2, CNP, 3D- Secure, AML compliance.

Account Takeover (ATO) Prevention

4.1. Continuous & Real-time Risk Scoring

Digital Trust's KYU approach analyses the risk of every user interaction by continually examining user BionicIDs™ for anomalies, scoring risk based on per-user models, population-based models, and bad actor models, as well as making sure user devices are not infected by malware and that user sessions have not been hijacked.

This continuous user verification and real-time risk analysis enable BANKs to comply with a range of regulations including Strong Customer Authentication (SCA), PSD2, CNP fraud prevention, 3D-Secure verification, and AML compliance while improving the efficiency of New Account Opening and Transaction Monitoring systems.

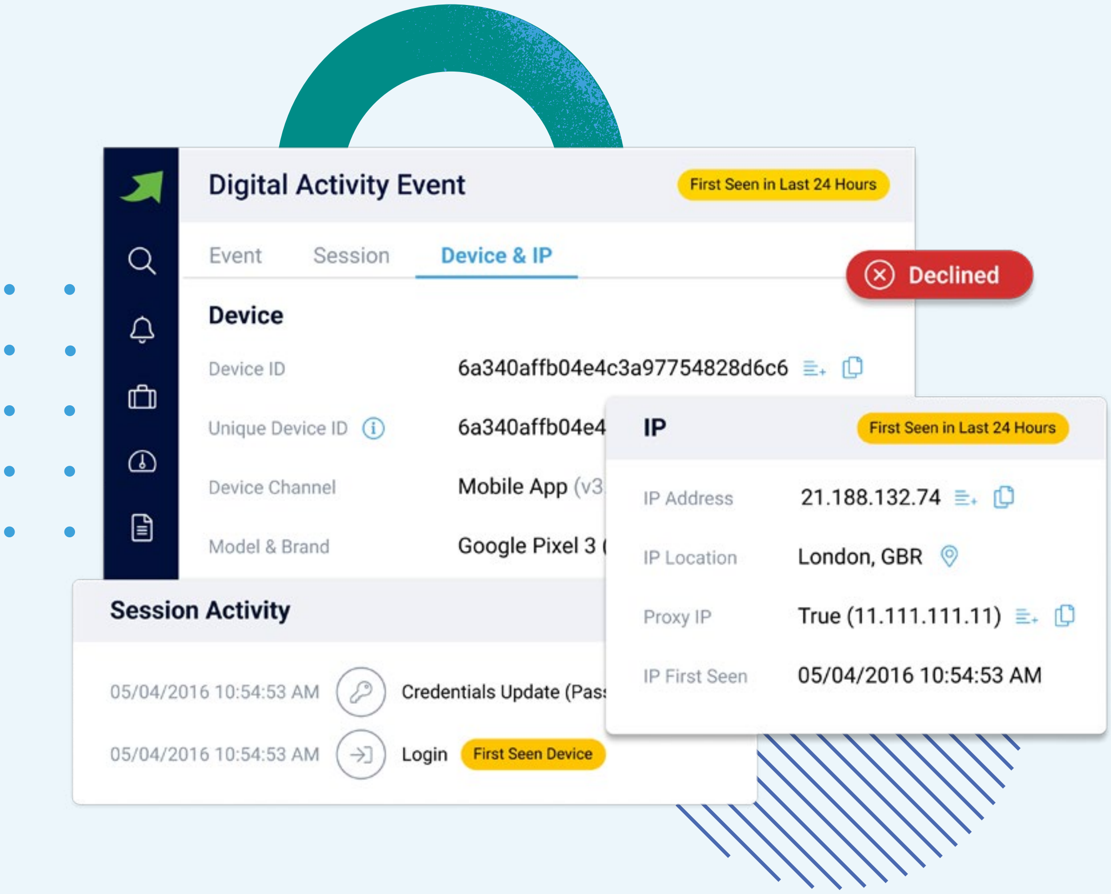
Should this analysis uncover BionicID™ anomalies, Digital Trust immediately takes pre-determine follow-up actions. For example, if malware has compromised a user's device, the mobile app or web page can provide the first line of defense and stop the attack.

Verifying users at every interaction reduces false positives and user friction by instantly safeguarding against issues such as hijacked sessions while minimizing the need for step- up-authentication. Feedzai's continual verification of users and devices is completely silent and fully transparent.

4.2. Account Takeover (ATO) Prevention

Digital Trust instantly determines whether an account has been taken over by answering one simple question – “are you really you?” We know who a user is because we start digitally fingerprinting them the moment they log in to a site, instantly capturing baseline biometric, behavior, device, and network data. Feedzai then silently and continuously compares the actor controlling the session to the user’s baseline profile to ensure a legitimate user is still in charge.

In contrast, other solutions ask, “are you a bad actor?” Answering this question requires combing through databases containing millions of bad actors looking for a match. This identification process can take numerous sessions, leaving new users in a grey area where they are not classified as good or bad. It is the unidentified bad actors in this grey area who are responsible for the majority of fraud and related costs.



Digital Activity Event — First Seen in Last 24 Hours

Device

Device ID: 6a340affb04e4c3a97754828d6c6

Unique Device ID: 6a340affb04e4

Device Channel: Mobile App (v3

Model & Brand: Google Pixel 3 (

IP — First Seen in Last 24 Hours

IP Address: 21.188.132.74

IP Location: London, GBR

Proxy IP: True (11.111.111.11)

IP First Seen: 05/04/2016 10:54:53 AM

Session Activity

05/04/2016 10:54:53 AM Credentials Update (Pas

05/04/2016 10:54:53 AM Login First Seen Device

5. Fast & Easy Integration

5.1. Deployment Overview

Digital Trust has been designed for fast and scalable SaaS deployment. Here are some key points to keep in mind:

Client Integration

- Digital Trust is agentless and frictionless. It does not require the installation of local agents or software on the bank's clients' devices. Customers simply access the bank with their usual browser or the bank's mobile app. Digital Trust is highly compatible with commercially available web browsers, operating systems, and hardware platforms. Mobile support is available for iOS and Android OS-based devices.
- Data collection on the client is easy and integration only requires the inclusion of JavaScript code in the FI's web portal, and the integration of a light mobile SDK in the FI mobile app.

Cloud Deployment

- Digital Trust operates in the cloud and no installation or update to any hardware or software in the FI's data center is required.
- Digital Trust is complementary to and only enriches other third-party or proprietary security platforms or fraud hubs the FI may already have in place.
- If the FI or bank decides to upgrade or add new capabilities, no changes to their infrastructure are required and no modifications to the web code or the mobile App are necessary.
- Integration requires a secure connection (VPN, HTTPS) between the FI's data center and the Feedzai cloud.

Back-end API Integration

- Digital Trust uses a REST API or Web Sockets to send and receive events, alarms, and risk scores. Integration requires a secure connection (VPN, HTTPS) between the FI's data center and the Feedzai cloud.

feedzai

RiskOps

Transform your risk management.

Feedzai's AI stays ahead of emerging fraud and financial crime and mitigates even the most deceptive schemes so that banks, issuers, acquirers, and merchants can focus on growth. We deliver explainable and actionable outcomes with the proven value of protecting millions of customers worldwide.

But we're not just the best technology. Partnering with Feedzai means financial institutions receive best practices that help create exceptional customer experiences while preventing and detecting financial crime.

Account Opening | Anti-Money Laundering | Transaction Fraud

Request a demo

feedzai.com **info@feedzai.com** **sales@feedzai.com**