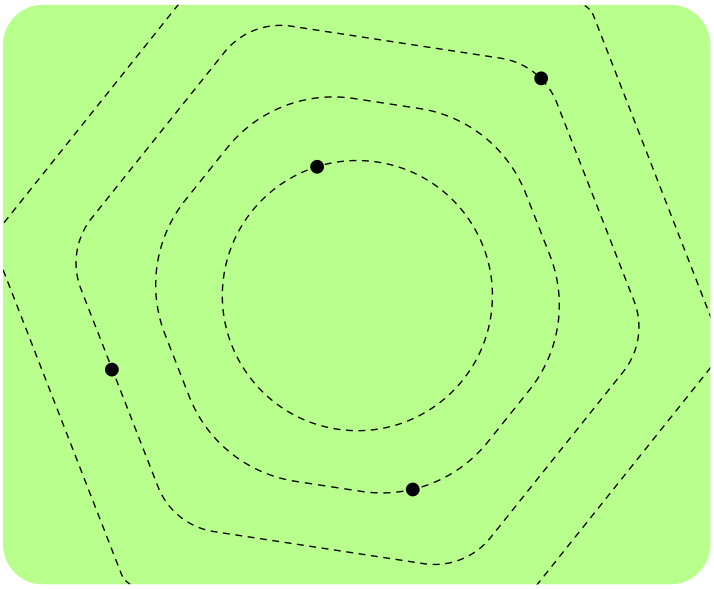
feedzai



Digital Trust

Stronger Fraud Protection Starts with Trusted Signals

Trusted by 1B+ customers worldwide to stop $1B+ in losses every year

Raiffeisen Bank · Ibercaja · Backbase · CaixaBank · SEB

Fraudsters are security-savvy now. AI agents are already accessing customer bank accounts. Axios reported that major US banks are confronting unvetted third-party agents, including activity that appears to go beyond customer instructions.[1] Banks need to understand who or what is acting, what the customer authorized, and whether the activity remains within those limits.

These decisions depend on evidence banks can trust. Malware and attackers can target the SDK, app, or device to alter what a fraud system sees or suppress risk signals. Zimperium's 2026 Mobile Banking Heist Report found full-device-control capabilities in 25 of the 34 malware families it analyzed.[2] As agentic banking adds new ways to access accounts, protecting the controls that collect this evidence becomes foundational to safer banking.

Continuous adaptive trust starts with trusted signals.

Feedzai Digital Trust brings endpoint security into the bank's broader risk assessment. It checks for threats across the SDK, host app, and device environment, protects risk signal collection, and reports findings to the bank.

Traditional fraud and scam prevention controls only focus on behavioral signals or device assurance. Getting ahead of fraudsters requires trusting the signals device, behavior, and network risk rests on, and sharing those risk signals across the fraud, cyber, and identity teams.

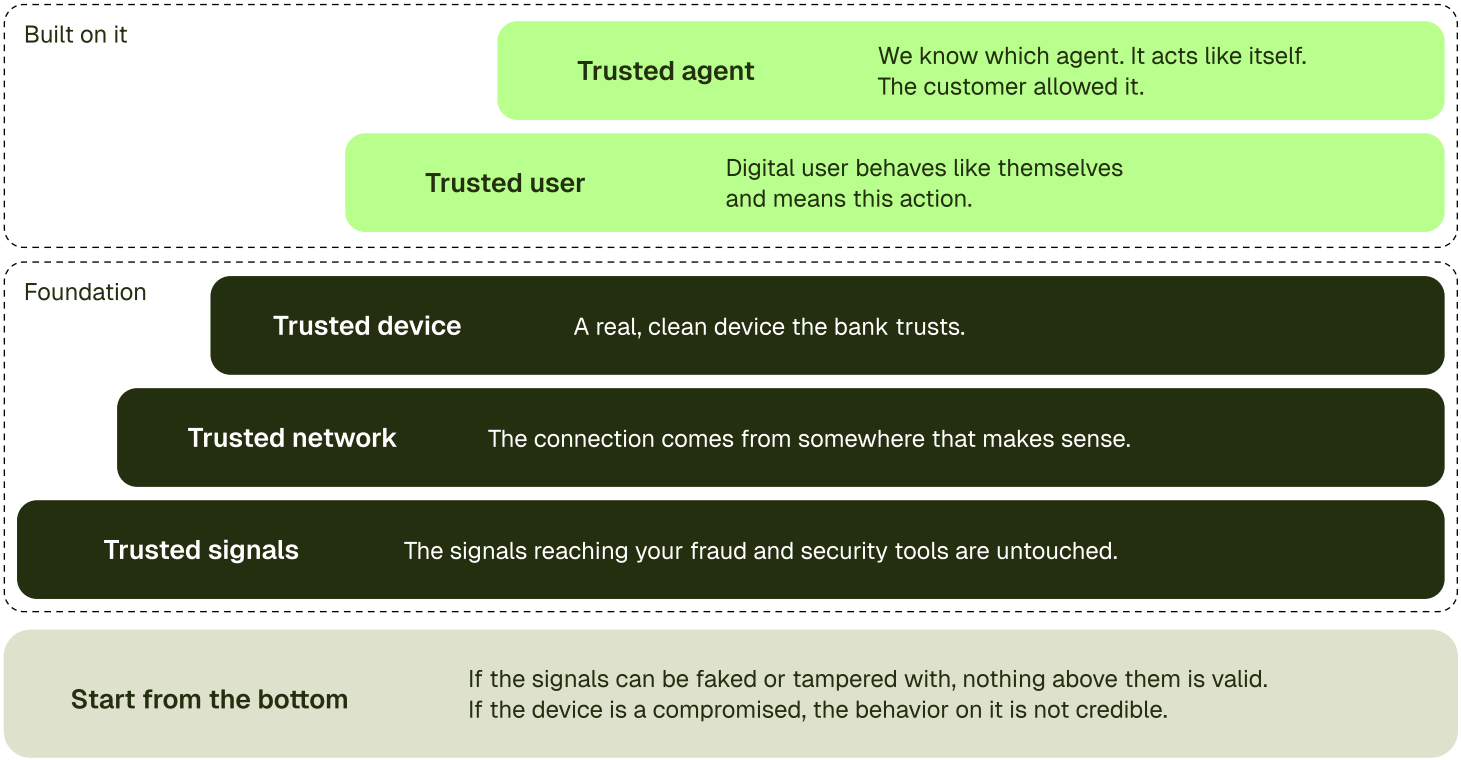
[1] https://www.axios.com/2026/10/22/ai-agents-banks-unauthorized-accounts-access
[2] https://lp.zimperium.com/2026-mobile-banking-heist-report

Digital Trust's built-in endpoint security identifies risky devices, detects app manipulation, and assures signals you receive are untampered. The SOC has the same risk indicators so that the cyber team can visualize the security posture.

Trust is built in layers, and each layer depends on the layer below it. Behavioral and device signals are only worth collecting if you can trust the device collecting them. That makes endpoint security the foundation of continuous adaptive trust. Digital Trust secures signals in real time and lets the bank decide what the session can do.

Trust is built in layers. Each one needs the layer below it

Behavior only means something when you can believe the device and the data it came from.



What trusted signals make possible.

Detect threats earlier
Digital Trust identifies signs of rooted devices, cloned apps, hooking, SDK tampering, malware, and remote access, helping the bank assess compromise before allowing sensitive actions. Missing or altered signals also become evidence to assess, rather than an automatic sign that everything is safe.

Share defenses across cyber, fraud, and identity.
Digital Trust risk indicators can feed SOC and SIEM tools, helping cybersecurity teams investigate threats in their existing dashboards. Identity teams can use risk assessments to inform authentication and recovery decisions.

Apply smart friction. Personalize every banking journey.
Use endpoint risk indicators in your own rules to apply smart friction without just terminating the session. Your bank decides what happens next:
- **Restrict access:** Allow balance viewing while preventing payments.
- **Step-up verification:** Ask for additional proof where it addresses the risk.
- **Block activity:** Stop access or transactions when the environment is too risky.

Achieve compliance and malware-driven mandates.
Secure the path signals take to the bank, from behavioral biometrics to device and network intelligence, and provide white-box explainability for every decision to help financial institutions meet regulatory guidance and mandates.

Protect the risk signals in transit.
Protect signals from unauthorized tampering, including attempts by malicious agents to alter data in transit, by using authenticated message-level encryption and temporary session keys.

Endpoint security within Digital Trust

Trust the signals before you trust the session

Identify risky devices

Is this a real device, and is it clean?

- Bots
- Virtual machine
- Emulators (iOS, Android)
- Jailbroken devices (iOS)
- Rooted devices
- USB debugging enabled
- Bootloader tampering
- Managed work-profile context
- Malware: banker
- Malware: stealer
- Malware: PUP
- Suspicious app

Detect app manipulation

Is your app running the way you shipped it?

- App integrity
- Cloned apps
- Virtual environments
- Debuggers (iOS, Android)
- Runtime manipulation
- Hooking (Web, iOS, Android)

Strengthen signal integrity

Can you trust the signals you receive?

- SDK code integrity (Web, iOS, Android)
- SDK security controls (iOS, Android)

Digital Trust: Proven where it counts

Earlier detection
84% of phishing fraud detected within the first 30 days live.

Less alert volume
90% fewer alerts in 60 days. Every avoided investigation saves $15–$50 and gives your team more time for the threats that matter.

Fewer unnecessary OTPs
6,000 more returning customers recognized per million logins.
40.3% fewer OTPs with no added risk.

Fast deployment at scale
Live in 10 days, enriching your current stack. Proven on 25B+ sessions a year at millisecond speed.



Recognized by Celent. Chartis datos INSIGHTS IDC

See the Threat. Control What Happens Next.

Request a Demo

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

