feedzai

Fraud Detection & Response Platform

How Feedzai Enhances Malware Detection

Malware attacks are used to steal user credentials, take over accounts, compromise mobile devices, or compromise browsers to hijack banking sessions. These attacks are on the rise and backed by organized crime syndicates, nation states, and terrorist organizations. What's more, the programs are becoming increasingly sophisticated and more difficult to address. Some malware programs are even capable of bypassing two-factor authentication (2FA) solutions. Malware attacks can lead to ransomware, which cost companies $133,000 on average[1]. Today's known and unknown malware variants make it challenging to detect and prevent attacks.

Forbes 2019 AI 50 MOST PROMISING AI FIRM

Feedzai ranked #15 on the Forbes list of most promising AI companies.

Aité

Feedzai named best-in-class fraud and AML machine learning platform vendor

MEDICI | EY

Feedzai bestowed Top 21 RegTech Innovation Award

Protect your customers by stopping malware attacks in real-time

The Fraud Detection & Response Platform (FDR) from Revelock, a Feedzai company, protects web and mobile banking apps by detecting and stopping malware impersonation attacks. Enhanced detection technology can identify cyberattacks from both previously compiled, known malware blacklists, as well as previously unknown, zero-day malware patterns.

[1] *Safe At Last*, 22 Shocking Ransomware Statistics for Cybersecurity in 2021

Key Benefits

Identify New Malware Patterns
The FDR platform identifies, classifies, and stops zero-day malware attacks using deep learning algorithms, expert supervision and an understanding of how suspicious code interacts with banking websites and mobile apps.

Prepare for Future Attacks
Most fraud detection solutions simply detect malware and alert banks to take follow-up actions. The FDR Platform uses a malware detection engine that learns how malware executes an attack and constantly identifies new strains to improve detection and protect against future attacks.

Contain Fraud, Minimize Detection Costs
By constantly identifying new malware strains and improving detection capabilities, the FDR platform protects against future attacks, keeping customers safe and minimizing the fraud analyst teams' workload.

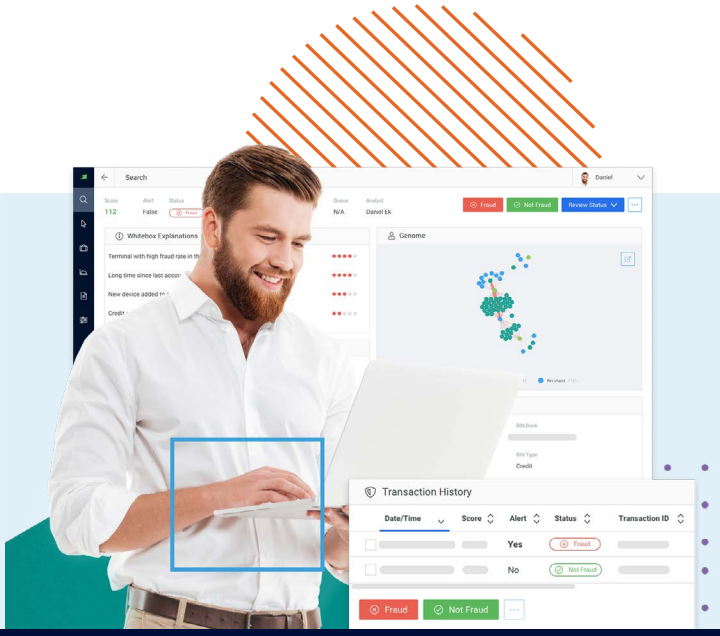
Enhance Your Brand Image
FDR Platform protection is completely transparent and protects customers regardless of their choice of device - desktops, laptops, tablets, or smartphones. Banks can enhance their brand image by securing their customers' accounts and delivering a seamless banking experience.

Key Features

Malware Classification
The FDR platform uses a comprehensive classification system that records both known and unknown malware strains that reduce false positives and avoid false negatives, ensuring teams can focus on real fraud threats instead of chasing false alerts.

Continuous Learning
The FDR platform uses a malware detection engine that learns exactly how malware executes an attack - whether by downloading additional malicious code or manipulating browser or mobile app content - to improve detection and protect against future malware attacks.

No Standalone Apps Required
The FDR platform protects customers from malware-related compromises without requiring them to install standalone anti-malware apps on their devices.



Ready to see our technology in action?

Schedule a Demo