A Remote Access Trojan (RAT) is a type of malware that fraudsters or other bad actors use to take control of a device or banking session via a remote connection. Once installed, cybercriminals will use RATs to:

- Gain access to a user’s device or online account.
- Commit fraud by hijacking a legitimate user’s banking session. RATs can go undetected by anti-virus software and two-factor (2FA) solutions.
Keep your customers safe with dynamic RAT protection

The Fraud Detection and Response Platform (FDR) from Revelock, a Feedzai company, protects web and mobile banking apps by detecting RATs and stops them from hijacking user sessions or taking over online accounts or connected devices.

- **Stop RATs in Real Time**
  The FDR platform stops both types of RAT attacks at the point of detection by requiring actions such as additional authentication, automatically terminating the session, or locking the account.

- **Prevent Session and Account Takeovers**
  The FDR platform identifies web page and mobile app anomalies and stops RATs from directing users to accept fraudulent one-time passcodes or compromising their credentials.

- **Frictionless and Transparent Protection**
  The FDR platform offers completely transparent protection to customers from all forms of RAT attacks regardless of the type of device they use (e.g., desktops, laptops, tablets, or smartphones).

**Key Features**

- **BionicID™**
  An analysis of each user’s unique digital identity to detect an attack and stop fraudsters from hijacking user sessions or taking over accounts or devices.

- **Behavioral Biometrics**
  Analysis of unique biometric anomalies in mouse movements and typing variances to quickly identify a potential RAT compromise.

- **Hybrid AI**
  Hybrid artificial intelligence analyzes the BionicID™ data at each interaction to identify whether a RAT attack is being executed and to determine if the real customer is making changes to an account.

Ready to see our technology in action?

Schedule a Demo