INETCO BullzAI® — Detect and block individual transactions in milliseconds, without interrupting legitimate payments

Overview & Business Need

INETCO BullzAI® provides issuers, acquirers, merchants, and processors with a unique solution to the challenges posed by real-time payment fraud. Only INETCO BullzAI can identify individual fraudulent payment activities in real-time, decline them before the transaction is completed, return a stand-in code, and alert on the issue — all without blocking or negatively impacting legitimate transactions. INETCO BullzAI also detects, blocks or rate-limits sophisticated payment network fraud attacks including velocity based attacks (e.g. BIN attacks), BOT attacks, DDoS attacks and Man-in-the-Middle attacks. Every payment channel is protected with a single solution.

When it comes to real-time payment fraud, the cost of false declines, disputes, and reputational damage can far outweigh the economic cost of the fraud itself. For this reason, even when payment fraud is detected, a decision may be made not to block it. . The risks of blocking legitimate transactions by blocking transactions at the IP address or port level are deemed too high, as are the risks of adding complexity to the transaction switch configuration.

Why is INETCO BullzAI so special?

INETCO BullzAI is an application layer firewall and state-of-the-art real-time payment fraud detection system integrated in a single solution. With the ability to block fraudulent transactions at the field level, rather than the IP Address or Port level, suspicious transactions can be targeted and blocked immediately. Other fraud solutions cannot detect or take action until after the transaction has completed. With INETCO BullzAI, individual suspicious transactions can be blocked without blocking at a port or firewall level which stops many legitimate transactions. Additionally, INETCO's patented real-time fraud detection capabilities provide more accurate risk scoring, anomaly detection, and behavioural modeling than other fraud systems.

USE CASE 1: Identifies & Blocks Individual Fraudulent Transactions Before They Complete

FEATURES	BENEFITS
Evaluates every payment transaction from every channel in real-time without adding latency or increasing customer friction	**Reduce Customer Friction, Respond to New Attacks More Quickly** • Assesses the risk of every payment transaction in milliseconds – regardless of the customer endpoint or payment rail • Provides a single source of data for decision analysis enabling faster decisions • More easily identifies weak points where fraudsters infiltrate as well as third party issues • Enables faster response to fraud alerts, meaning lower fraud losses • Reduces call center volumes, reducing operational costs • Improves customer satisfaction through fewer false positives
Detects anomalous payment transactions in real-time and blocks them from completing, without negative impact to legitimate transactions	**Reduce False Positives and Chargeback Fees** • Reduces false positives through the automatic creation of unsupervised ML models for each customer and card. Models are updated in real-time with every transaction. Models leverage algorithms specifically developed to detect payment fraud. • Generates risk and anomaly scores in real-time for every customer and card transaction • Employs behavioural analytics to automatically detect new fraud schemes in real-time
Blocks transactions at the field level rather than the traditional firewall mechanism of blocking at the IP address or Port level	**No Negative Impact to Legitimate Transactions** • Detects and blocks fraudulent and anomalous transactions without blocking or negatively impacting legitimate transactions. • Detects and blocks fraud before the transaction completes, allowing business to keep running smoothly while specific transactions are being investigated

Supports the rapid review of fraud incidents and cross-department collaboration	**Powerful Investigation Tools** • Provides fraud analysts with a single UI where they can see all the data they need to understand why an alert was triggered, eliminating guesswork and improving productivity • Access every detail of every transaction from across the entire payment journey in a few clicks • Integrated fraud case management provides configurable workflows, alerting and reporting • Supports collaboration between fraud and AML/cyber-security teams through easily accessible data
Applies the same level of fraud detection and prevention to every payment channel in a bank, processor or merchant's ecosystem	**Improve Security of Omni-channel transactions** • Assesses the risk of every payment transaction in milliseconds — regardless of the customer endpoint or payment rail • Provides a single source of data for decision analysis enabling faster decisions • More easily identifies weak points where fraudsters infiltrate as well as identifying third party issues • Enables faster response to fraud alerts, meaning lower fraud losses

USE CASE 2: Identify & Block or Throttle Payment Network Attacks

FEATURES	BENEFITS
Identify & block or throttle payment network attacks	**Protects Against Fraud Attacks Other Systems Can't Detect** • Stops DDos and related fraud attacks simultaneously • Detects and blocks sophisticated fraud attacks in real-time (in addition to detecting and blocking individual transactions), thereby reducing fraud losses • Blocks or rate-limits attacks to reduce negatives impact while the attack is investigated • Reduces manual work during investigations **These attacks include:** • Velocity based attacks (e.g. BIN attacks) • Man-in-the-Middle attacks • BOT attacks • DDos attacks • Insider fraud

USE CASE 3: Off-load Fraud Blocking From the Transaction Switch

FEATURES	BENEFITS
Provides an application layer firewall and a transaction fraud system in one solution	**Reduce IT Costs** • Allows for easier consolidation of IT systems • Reduces cost of educating teams how to use multiple solutions • Reduces operational costs
Performs the 'heavy-lifting' of pre-screening transactions before they get to the transaction switch or application server	**Reduce the Risk of Making Changes to the Banking Host or Tx Switch** • Supports the implementation of both static and dynamic rules • Fraud rules can be removed from the Banking Host or Transaction Switch and implemented in INETCO BullzAI • New rules can be quickly implemented without adding risk or complexity to the Banking Host or Transaction Switch • Reduces need for specialized IT knowledge

Deployment Options

INETCO BullzAI is available as an on-premise or Cloud-based solution. To figure out which option is best for you, schedule a demo or contact insight@inetco.com.