INETCO Insight®

PAYMENT FRAUD DETECTION AND PREVENTION

INETCO Insight® — Detecting transaction-level payment fraud attacks in real-time

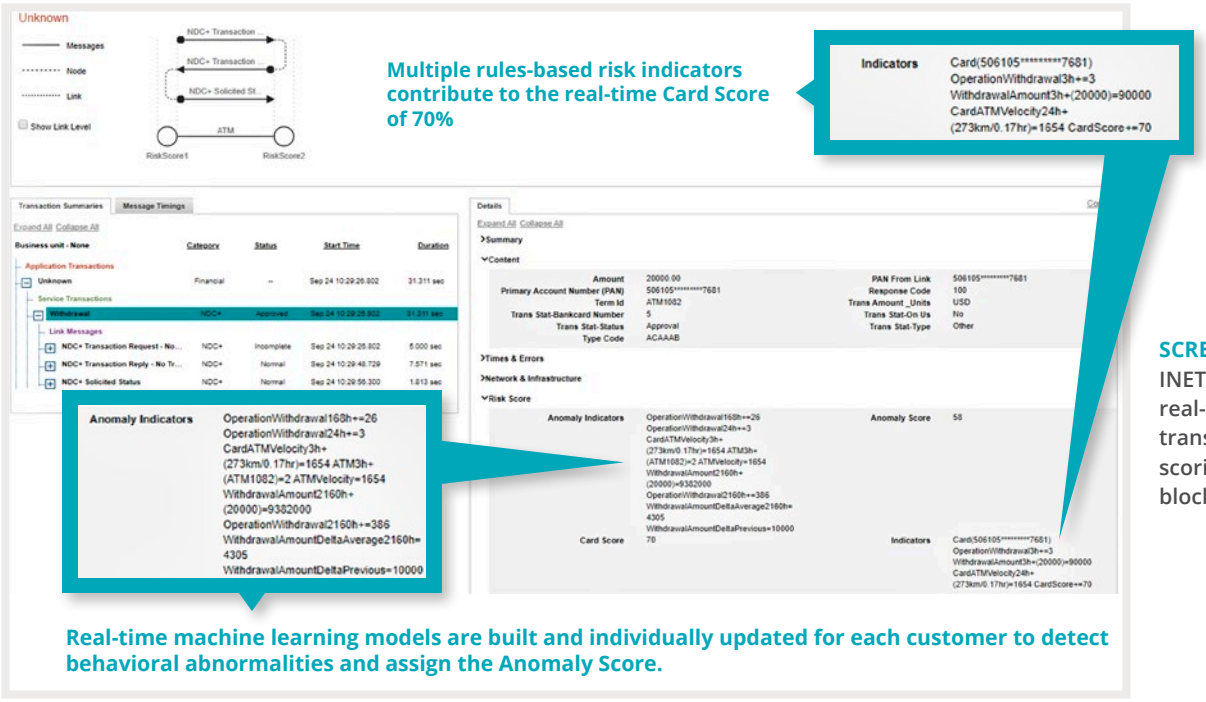
By the time payment fraud is detected, it's often too late

Detecting and preventing payment fraud attacks — before customer, reputation and financial damage is done — is a complex and costly problem to solve. Sophisticated fraudsters are exploiting fraud defense gaps quickly and quietly. Multi-vector attacks are often launched unnoticed, using a combination of social engineering, malware and advanced persistent threats.

Fraud investigation is also getting more difficult, as it is taking more time and effort to collect data across disparate data stores, multiple payment rails and channels. These factors are making it challenging for CISOs, cybersecurity and payment fraud teams, already facing tight budgets and spending hours sifting through thousands of false positives, to accurately detect suspicious behavior and block payment fraud before it impacts customer experience, reputation and the financial bottom line. This is why financial institutions, retailers and payment service providers are now turning to INETCO Insight®.

With INETCO Insight, CISOs, cybersecurity and payment fraud teams can:

- **Protect reputation and financial bottom line** — Use deeper, faster payment intelligence and pattern recognition to detect, research and block payment fraud attacks in milliseconds - including suspicious transaction activity, man-in-the-middle malware attacks, internal fraud, EMV fallbacks and cash-outs.
- **Reduce customer friction and false positives** — Configure real-time risk scoring models, rules-based alerts and machine learning algorithms to increase precision and reduce the number of customers accidentally blocked from accounts.
- **Mitigate the risk of card-present and card-not-present payment fraud in an efficient, cost effective way** — Optimize the independent, real-time collection and decoding of transaction data across every link in the payment journey. Detect missing links, message field tampering and suspicious transaction patterns that would fly under the radar of individual security components. Have the option to stream in-depth transaction data to other fraud applications of choice.



SCREENSHOT: INETCO Insight's real-time transaction risk scoring and blocking

Applying real-time data acquisition and machine learning across payment ecosystems

INETCO Insight solves the payment velocity and data acquisition challenges that are impacting the speed of fraud detection and the accuracy of transaction risk scoring and blocking — across all payment channels. With independent, network-based transaction data acquisition, in-depth transaction profiling and multi-point correlation capabilities, you gain unprecedented visibility into every link and every transition point along an end-to-end payment journey. CISOs, cybersecurity and payment fraud teams can add an enhanced layer of real-time transaction-level defense, scoring and pattern recognition to their payment fraud strategy — in an easy, cost affordable way.

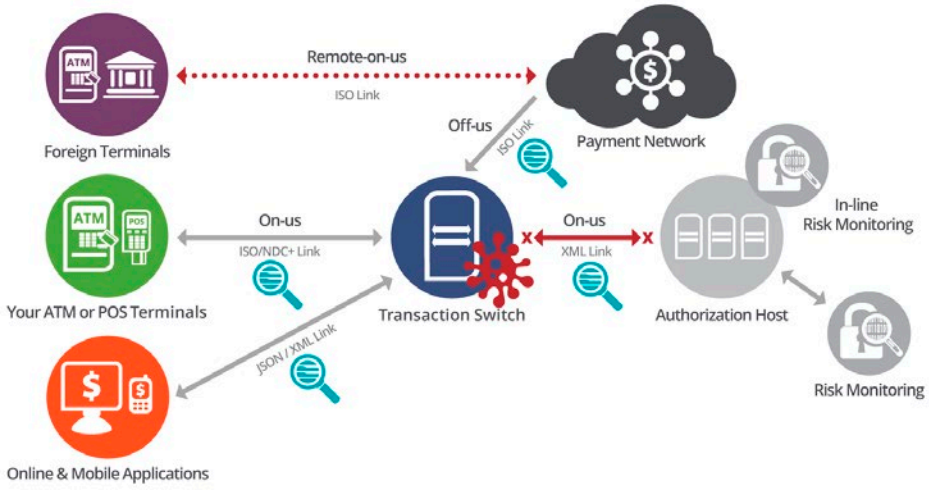


DIAGRAM: Identify man-in-the middle and cash-out attacks in milliseconds.

INETCO Insight provides real-time monitoring for potential fraud patterns across "on-us", "remote-on-us" and "off-us" transactions. This data can be compared against imported card blacklists or negative country lists for immediate action. By decoding all application payload message fields, metadata, response and request times, and network-level communications data for each link of a transaction path, you can remove blind spots along any payment journey and proactively detect suspicious transaction-level activity, missing links and message field tampering in milliseconds — before major damage is done.

Speeding up the research and investigation of flagged activity

INETCO Insight makes it easy to establish a real-time data pipeline for payment transactions – across ATM, POS, Card, Mobile, Online and Real-time Payments channels. This data is continuously fed into a configurable rules-based alerts engine, supervised- and unsupervised- machine learning models, and case management workflows built to manage both the service and fraud aspects of every end-to-end transaction from one affordable solution. Example real-time fraud alerts for card-present and card-not-present transactions include:

- Device fingerprint and IP geolocation change
- Cash withdrawal observed on an ISO link with no matching database transaction (man-in-the-middle malware attack on the switch)
- Repeat card usage or customer ID by device, distance or store
- Repeat terminal usage (isolate ATMs used in coordinated cash-out attacks)
- Distance-based card usage or device log-ins
- High ticket purchases or rapid succession of transactions
- High number of changes to a device fingerprint over a certain time period
- High withdrawal velocity in a short amount of time
- Unexpected EMV fallbacks, reversals and stand-in modes
- Status and response code errors

Strengthen your payment fraud defense strategy with:

- **Real-time suspicious activity monitoring** for card-present fraud, card-not-present fraud, account takeovers, DDoS attacks and payment outlier detection
- **Real-time detection of "man-in-the-middle" switch malware attacks,** message field tampering, cash-outs, and internal fraud attacks
- **Real-time transaction risk scoring and the blocking** at the IP, firewall or application level

Reducing customer friction and false positives through more precise risk scoring

INETCO Insight features adaptive machine learning algorithms and rules-based alerts that utilize real-time transaction intelligence to rebuild individual device or card models on the fly and increase risk scoring precision. Card activity is continuously assessed and compared against past behavioral patterns and predisposed customer behavior. Based on a configurable set of rules and risk scores, automated action scripts can be triggered to block suspicious transactions at the IP address, application layer or firewall level.

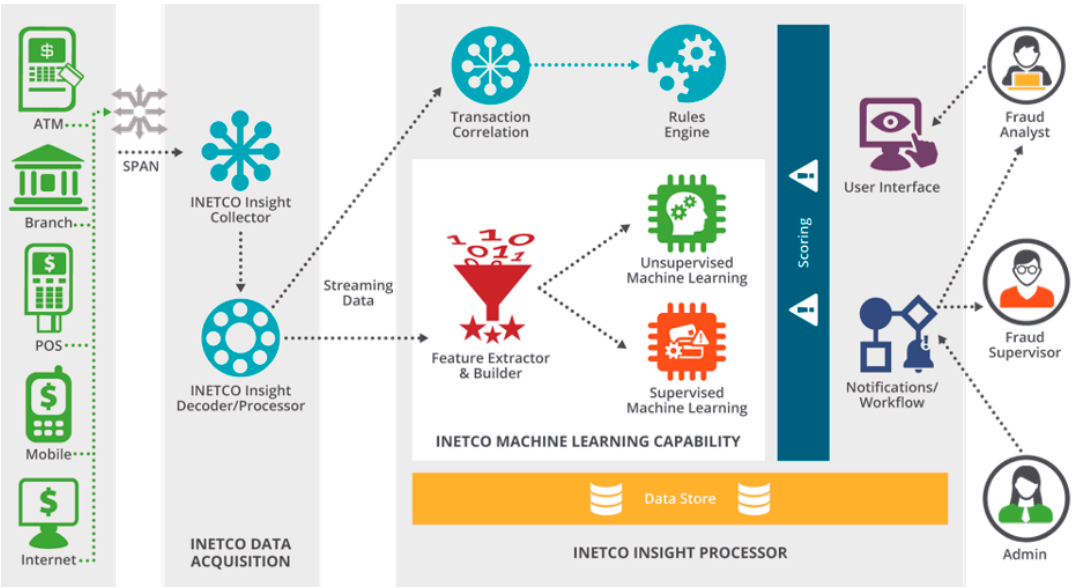


DIAGRAM: INETCO Insight for Payment Fraud — Featuring a combination of real-time transaction data acquisition and payment protocol decoding, custom rules-based alerts, machine learning capabilities, risk scoring and case management workflows.

"When we approached our IT operations team and learned about the robust transaction data gathering capabilities of INETCO Insight, our fraud prevention team was very excited, especially about the fact this data came with a complete set of message fields. Our team now has the flexibility and visibility it needs to significantly speed up our ability to identify and respond to fraud attacks."

ANDER MURILLO ZOHN — DEPUTY DIRECTOR OF BIG DATA TECHNOLOGIES AT E-GLOBAL

Features

Out of band, network-based transaction data acquisition Centrally collect real-time transaction data across all payment channels, without deploying heavy instrumentation, touching the switch or creating new points of potential failure. Avoid valuable contextual information (e.g. terminal ID, EMV data elements, IP addresses) from being stripped at the terminal handler or switch level.

Real-time transaction profiling analysis Extract and assemble application payload messages, metadata, response/request timing and network communications information — across correlated transaction links — to detect message tampering and speed up investigations.

Payment protocol libraries for message decoding Decode all transaction protocols and message types found in banking and payment ecosystems, including: TCP/IP, UDP, ISO 8583, ISO20022, VISA 2, FIX, NCR/NDC+, Diebold, Triton, XML, SOAP, HTTP, SQL, IBM WebSphere MQ, and AMQP

Configurable web-based dashboard displays Access dashboards, alerts, transaction profiles, logs, trends and statistics via the INETCO Insight HTML 5 web user interface.

Transaction logs with search, query and filter capabilities Perform on-demand research queries on up to 13 months' worth of transaction data.

Configurable real-time transaction risk scoring Combine in-depth transaction intelligence with rules-based alerting and adaptive machine learning capabilities. Examine transactions in real-time, rebuild individual customer models on the fly and extract behavioral patterns from past card transactions that signal potential fraud.

Configurable rules-based alerts engine Set up real-time alerts around suspicious transaction-level activity. Add an independent layer of defense against fraud and switch system alerts that are overridden by malware.

Device state monitoring Showcase the location and status of each terminal or device, flagging potential security issues such as card reader tamper or safe opening without supervision.

Case management workflows Track, evaluate and prioritize flagged payment transactions. Streamline fraud investigations — with alert specifics, risk scores and transaction details linked directly to each task.

Supervised and unsupervised machine learning models Configure supervised machine learning models to look for existing fraud patterns in real-time, and rebuild individual customer models every time a customer event occurs. Use unsupervised machine learning to identify and flag new event anomalies.

IP address/application layer/firewall blocking Set up automated action scripts to block offending card transactions. Immediately research flagged individual profiles and take action to reduce false negatives and positives.

Data forwarding options and APIs Forward transaction data to any team or application of choice. Also utilize this rich transaction intelligence to feed adaptive machine learning algorithms and predictive analytics.

Switch application monitoring Combine internal OS statistics, application processes statistics and log file data with the state of your transactions.

Deployment Options

INETCO Insight 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.

INETCO Every transaction tells a story®

+1.604.451.1567 | insight@inetco.com | www.inetco.com