INETCO SOLUTIONS SHEET

INETCO Solutions for Payments System Security

Notifying you when terminals, cards or transaction switches are under attack

Organized crime syndicates are exploiting vulnerabilities in payments systems through a combination of specially crafted malware, social engineering, and coordinated attacks (collectively Advanced Persistent Threats) to steal millions from banks, processors, and retailers.

These Advanced Persistent Threats (APTs) are designed to fly under the radar of traditional payment fraud defenses, or to bypass these mechanisms entirely.

Extend switching and card processing security with INETCO

Immediately spot APTs that often go undetected by traditional risk monitoring systems:

- Know when a transaction enters a payments switch, but never leaves for authorization
- Be immediately alerted to repeat card usage at the same terminal, or across an unlikely geo-graphical area
- Watch for anomalous patterns such as multiple cards used in sequence at the same terminal

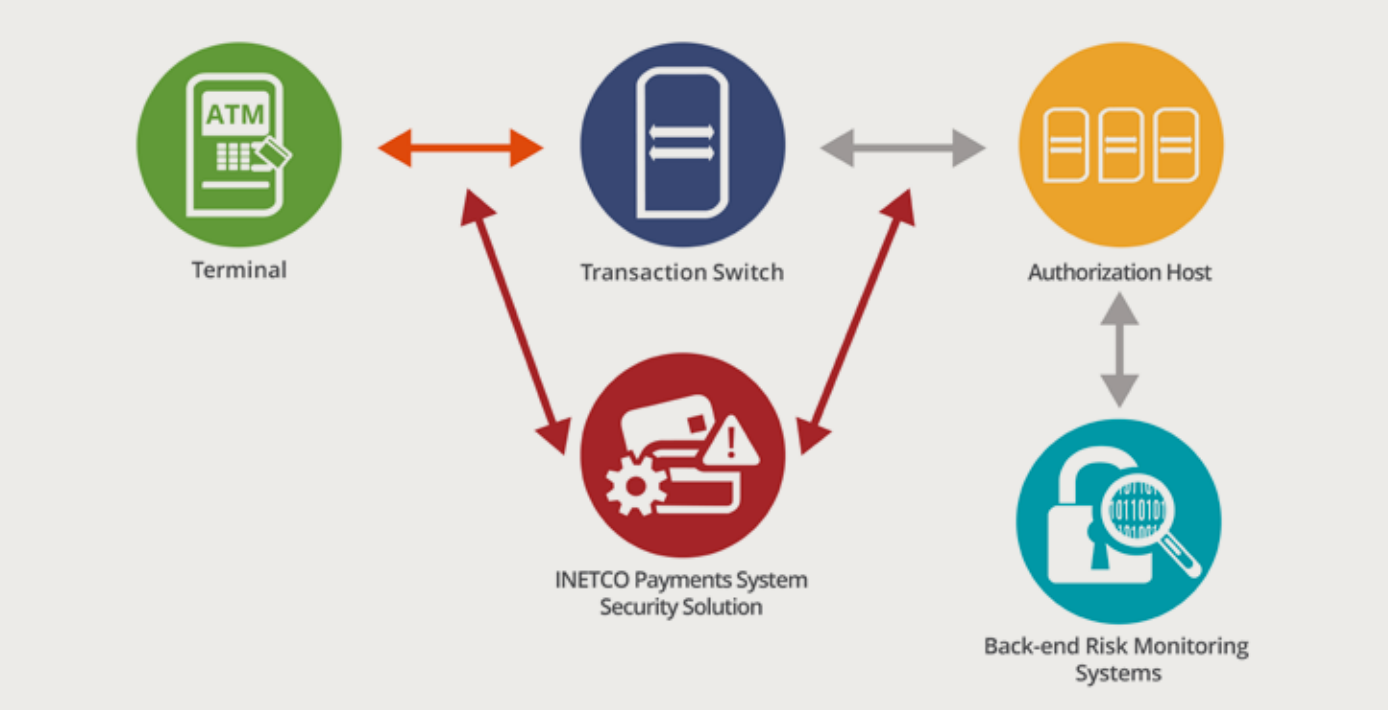


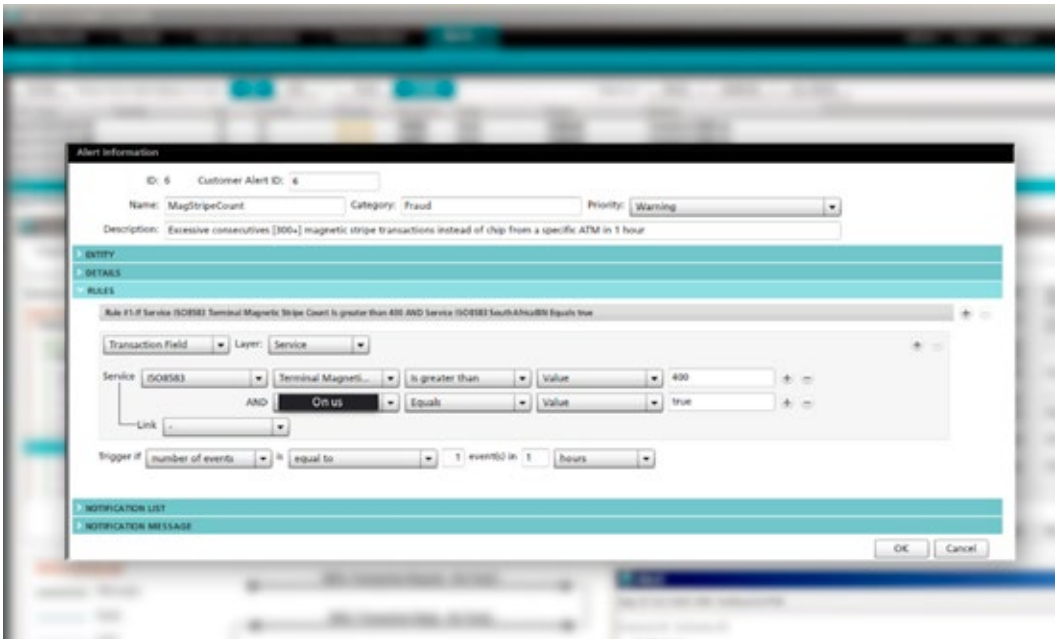
DIAGRAM 1 - Risk monitoring systems that reside on the back-end of your payments system cannot easily identify when attacks occur on the front-end. With the ability to correlate front-end and back-end transactions, the INETCO Payments System Security solution will help you quickly identify transaction behavioral anomalies and compromises to the payments switch.

INETCO's Payments System Security (PSS) solution complements your existing fraud detection systems by adding a new layer of defense against APTs. It can catch threats that bypass your traditional fraud detection systems, spot compromised cards before they make it onto a hot list, and isolate which terminals or devices are being used to conduct coordinated attacks on your payments infrastructure.

The solution consists of INETCO Insight® for real-time transaction monitoring, a set of alerting and notification rules tailored by our professional services team for your environment, and INETCO Analytics® dashboards to support forensic analysis.

Real-time notifications can be forwarded into your existing security information and event management or terminal / device management system.

Where the INETCO Payments System Security solution helps



SCREENSHOT 1 - Customize your notifications using INETCO's real-time alerting engine. This is an example of an alert that has been created to warn when there are excessive consecutive magnetic stripe transactions happening instead of EMV chip, from a specific ATM in a one hour timeframe.

Discover compromised cards that are not on your hot card list yet

Skimmed cards are typically used for a bunch of transactions in a row, coordinated across multiple devices, as criminals try to do as much damage as possible before the card can be flagged and various hot card lists get updated.

The INETCO PSS solution looks for this kind of rapid, repeat card usage and notifies you immediately so you can take action. Thresholds can be set based on key variables such as card type, transaction values, and location to minimize false positives.

SUPPORTING FEATURES:

- **Real-time alert on repeat card usage over short time windows**
- **Set different thresholds based on BIN ranges and geographies (e.g. high risk vs. low risk countries)**
- **Receive notification when there is an excessive number of issued cards carrying out withdrawals on foreign terminals within a specified time interval**
- **Identify when there is an abnormal number of foreign cards completing withdrawals on one or more of your terminals**

Pinpoint vulnerable terminals and devices

Criminals will often target specific devices or locations for coordinated attacks and exploit flaws in the equipment, cards, or geographical characteristics that make their attacks more successful

The INETCO PSS solution can detect anomalous transaction activity at the terminal level immediately, so you can investigate suspect terminals. Thresholds can be set differently based on terminal type, manufacturer, and location to detect rapid, repeat transactions, fallbacks to magstripe at EMV-capable terminals, excessive reversals, and transactions occurring outside normal business hours.

SUPPORTING FEATURES:

- **Real-time alert on repeat terminal usage over short time windows**
- **Set different thresholds based on terminal type, manufacturer and location**
- **Real-time alert on specific response codes and transaction fields (e.g. EMV capable card falling back to magstripe at EMV capable terminal)**
- **Set business hours for each device**

Know when your payment switch has been compromised

Specially crafted malware can cause your payment switch to authorize transactions locally instead of dispatching them to back-end fraud and authorization systems for evaluation. This malware is often designed to support card skimming or coordinated withdrawal attacks.

The INETCO PSS solution detects these front-end attacks by tracking transactions at the network level, and looking for transaction requests that enter the switch, but never exit into back-end systems.

SUPPORTING FEATURES:

- **Network-based deployment so you see what is actually happening, even if criminals have disguised their activity from traditional change and transaction logging systems**
- **End-to-end transaction correlation, across multiple hops and protocols**
- **Real-time alerts on transactions that do not follow your conventional authorization path**
- **Immediate notification of unexpected stand-in behavior**

Managing your risk and financial exposure with INETCO

Organized crime syndicates are targeting payments systems, exploiting software and process vulnerabilities to bypass or remain undetected by traditional fraud defense systems. The INETCO Payments System Security solution will enable you to limit your risk and financial exposure and enhance your Defense in Depth approach by adding a new layer to spot threats earlier and react faster.

For more information on INETCO's Payments System Security solution, contact sales@inetco.com