TRANSACTION MONITORING

WITH INETCO Insight

Solution Guide

NCR

INETCO Insight

OVERVIEW

INETCO Insight's® ability to collect and process rich transaction-relevant Layer 2-7 data at high volumes, high speeds, and in real-time is a culmination of years of research and experience. This software platform presents a fundamental breakthrough in application protocol analysis, especially since it does not need proprietary hardware or silicon to achieve this.

INETCO Insight's transaction decoding, semantic correlation and statistical analysis engines can be rapidly configured to monitor any application type (custom, packaged, or industry-specific) and can simultaneously monitor hundreds of distinct applications and transaction flows. Regardless of protocol, platform, or application, the result is a single rich transaction record containing business, application, infrastructure, and network performance information.

TABLE OF CONTENTS

For more information, visit ncr.com, or email ncr.financial@ncr.com.

1. INTRODUCTION

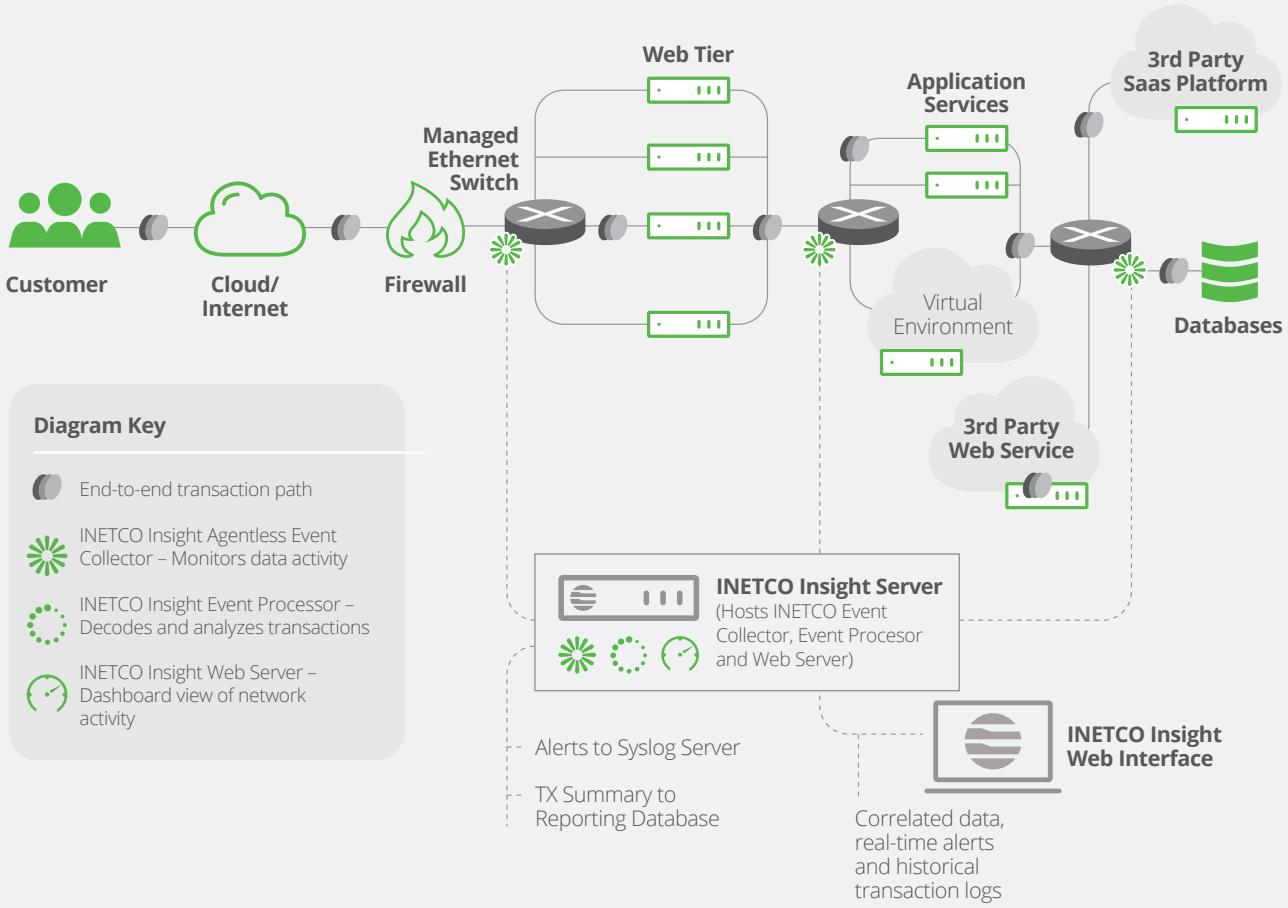


Figure 1: INETCO Insight deployment. This diagram illustrates how INETCO Insight can be deployed in an n-tier application environment.

INETCO Insight® is a software based passive network monitor for application transactions.

It decodes transaction messages in real-time from raw network traffic forwarded by a managed Ethernet switch, packet capture equipment, or application servers.

2. INETCO INSIGHT ARCHITECTURE

The INETCO Insight Architecture is made up of four major components:

- **INETCO Insight Event Collectors** for monitoring data activity
- **INETCO Insight Decoders** for message decoding and single link correlation
- **INETCO Insight Processor** for transaction analysis
- **INETCO Insight Web Server and Client** dashboard view of network activity

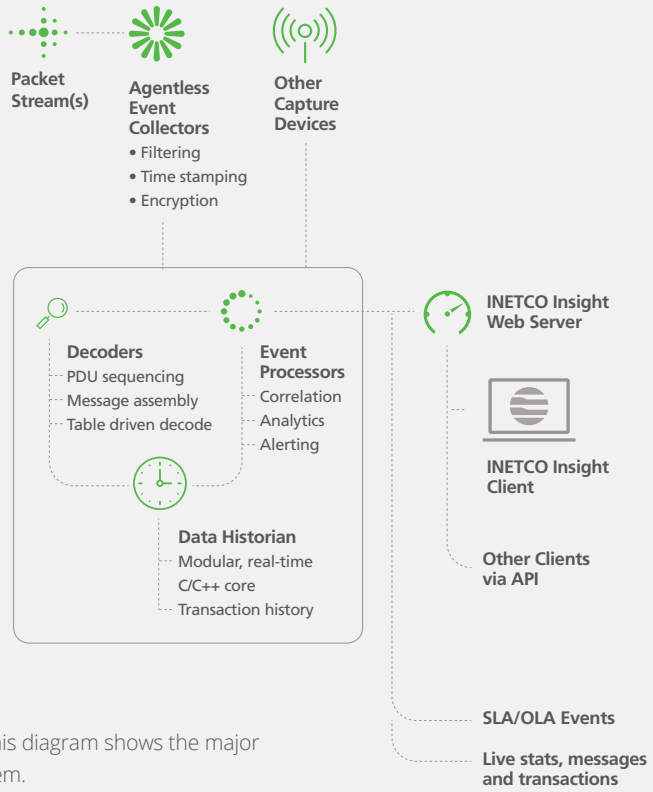


Figure 2: INETCO Insight operation. This diagram shows the major components of the INETCO Insight system.

The process of transforming raw network traffic into complete transactions is a complex process that presents three key challenges:

Data Acquisition Handling the volume and security requirements of network data relating to a wide range of transaction types, including sensitive financial transactions.

Message decoding Recognizing a wide variety of application message formats across packet boundaries in real-time and preserving the relationship between lower level network/transport aspects of a transaction and the higher level protocol and application message aspects.

Transaction correlation Grouping application messages into complete transactions and calculating transaction based metrics such as rates, ratios, durations, and concurrency.

This paper outlines these key challenges and explains how INETCO Insight addresses each in high-volume application environments.

3. DATA ACQUISITION

The first operation in INETCO Insight involves getting the raw transaction data.

This is the job of the INETCO Insight Data Collector software. For the purpose of this discussion the Data Collector can be thought of as an advanced network sniffer or datascope.

INETCO Insight provides three ways of getting raw data. One method is to obtain data directly from the network using a router's SPAN port, also called "port mirroring." In virtualized environments, equivalent features are available for mirroring network traffic.

The use of SPAN ports is not always possible or desirable. In this case the Data Collector can be loaded directly onto packet capture equipment, endpoints (e.g. ATMs), or application servers to gather the required data. In these deployments the Data Collector acts as a passive "shim" between the application services and the communications channel of interest. This method can also be used to collect network data in virtualized environments.

Finally, transaction data can be acquired from log files where access to the network or application components is impossible (e.g. cloud environments). INETCO Insight has multiple mechanisms for ingesting log data.

DATA	INTERFACE	POTENTIAL APPLICATION
Individual application messages	INETCO Insight Decoder	Forward every authorization request so a fraud monitoring system could check it
Decoded transactions and response time information via TCP	INETCO Insight Processor	Incorporate into load balancer policies to prioritize high-value transactions
Decoded transactions and response time information via database	INETCO Insight Reporting	Build a long-term profile of application performance
Count of transactions by type for a group of nodes or endpoints over an interval	INETCO Insight Processor ~~(Analytics)~~	Displaying a summary of transaction activity for a particular user or device
Recent transactions for a specific customer	INETCO Insight Data Historian	Display transaction details in a customer portal
Application/transaction dependency information	INETCO Insight Data Historian	Update application dependency models
Events/Alerts	INETCO Insight Processor	Forward SLA violations to alarm consoles and reporting systems

In all cases, capture can be performed "out-of-band," without introducing agents or code changes to application components.

Upon collection the raw network data is time stamped. INETCO Insight can integrate with GPS-based packet capture equipment, where precise time-stamping is critical. A filter is then applied to remove any data with IP addresses and ports not involved with transaction processing (e.g. video, voice, SNMP, etc.). This dramatically reduces the volumeof data forwarded for analysis by eliminating extraneous data. At this stage a sequence number is also added to the data to allow downstream detection of any missing or duplicated data.

The filtered data is then encrypted before being sent to the INETCO Insight Server. This ensures that sensitive transaction information is never available "in the clear." Integration with hardware security modules is supported.

NOTE: INETCO Insight can also collect raw data via the diagnostics port on many proprietary network gateways and from third party network "sniffers." Contact INETCO regarding such support.

4. MESSAGE DECODING

The second major operation of INETCO Insight involves decoding the incoming raw network data to extract application message information.

This is the job of the INETCO Insight Decoder. It involves sequencing the incoming raw network data, assembling application messages from the data, decoding the individual data fields within the application messages, and masking or deletion of any sensitive fields (e.g. credit card numbers for financial transactions, patient numbers for healthcare records flows, etc.).

To process the incoming data, the INETCO Insight Decoder must first sequence the incoming raw network data units (i.e. "protocol data units" or PDUs) from the INETCO Insight Data Collector(s) to ensure they are analyzed in the correct order. This involves the use of the tim e stamps and internal event sequence numbers added to the data when it is first collected. With multiple Data Collectors this information may not be sufficient as the real time clocks of the distributed Data Collectors will vary even when the Network Time Protocol is used for time synchronization. In such cases the INETCO Insight Decoder may also use contextual information within the raw network data to properly sequence PDUs.

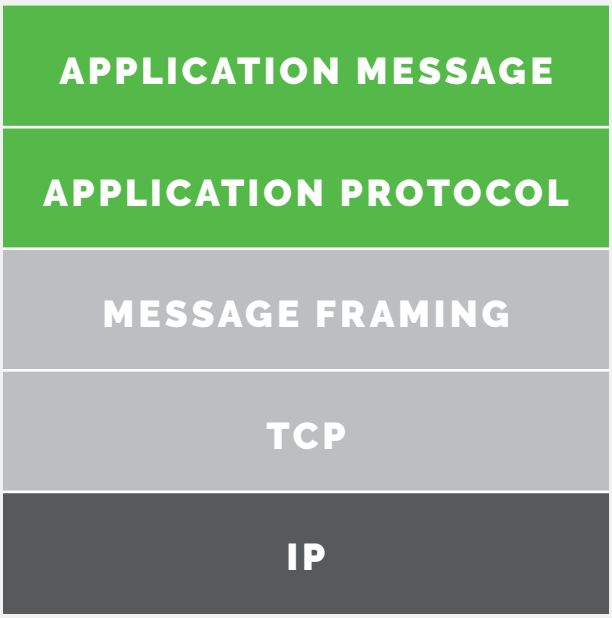


Figure 3: Protocol levels for application messages. This diagram illustrates the different protocol levels involved in a simple application-level message delivery using TCP/IP.

Next, application messages are assembled.

Application messages typically do not fit within a single low level PDU. Instead they are often spread out over multiple PDUs as shown in Figure 4. For this reason decoding of the application message stream includes not only reading data embedded in a PDU at each layer, but also includes assembling PDUs to create higher level messages. The INETCO Insight Decoder run time architecture allows message assembly to occur in real-time. The event collection component of the INETCO Insight Decoder receives the relevant PDUs (i.e. network data fragments) and stores them in the high performance INETCO Insight data store. All PDUs that could potentially become part of an application level message are grouped together in sequence so that application level messages can be assembled from more than one PDU.

Once a complete application message is assembled, a new application level message entry is inserted into the data store and information is associated with this entry for upstream correlation.

This entry is also linked to the PDUs in the data store to support a key feature of INETCO Insight, the ability to drill down through the various protocol layers. This mechanism is further extended (by the INETCO Insight Processor) to support more complex correlation of multi-hop transaction flows and drill-down from high-level business transaction to a low-level link transaction.

Once a complete application message has been assembled, it must be decoded.
This is not a trivial task, and a variety of methods must be used. Three general types of transaction message formats prevail. One is a field separated one of which there are many variants (e.g. Visa II financial messages). The second is a bit field oriented one of which there are also many variants (e.g. ISO 8583, FIX FAST, etc.) that are often used in high-speed, low latency environments where communication efficiency is paramount. The third is a tagged field one commonly implemented using XML or HTTP, of which, again, there are many variants, but they are often self-describing.

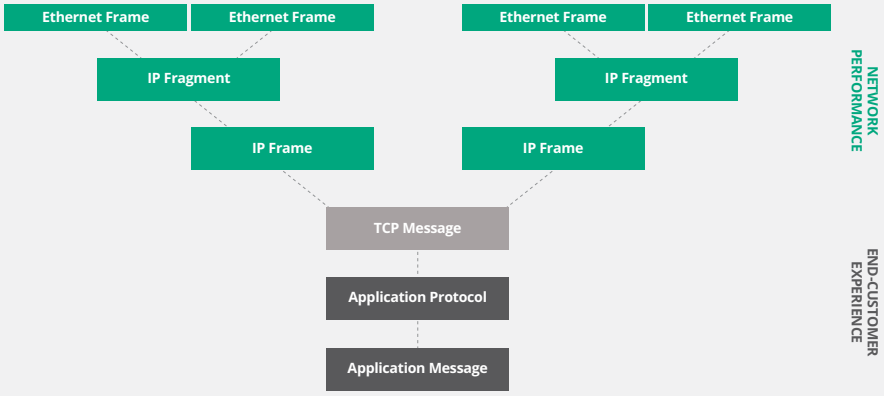


Figure 4: Protocol levels for application messages. This diagram illustrates the different protocol levels involved in a simple application-level message delivery using TCP/IP.

Decoding each of these transaction message formats presents its own set of challenges.
Field-separated messages require prior knowledge of where to find specific data e lements, the ability to recognize missing elements, and the ability to apply a semantic model to add mean ing to the raw data fields extracted. Bit field oriented messages are often tuned and adjusted by various parties to meet stringent performance criteria and often include unassigned fields that application developers can use to pass proprietary details. Tagged field messages can be extremely large and contain a lot of "non- transactional" data. In all cases, there are endless variants, even in tightly standardized application protocols.

Hard coding all of the many variants is not a practical solution.
As such, the INETCO Insight Decoder uses a "table driven" approach to quickly define the decode tables for each message type within a transaction. Once this is done the table is compiled and installed on the INETCO Insight Decoder for fast access.

When a message is received the appropriate decode type is detected automatically for each incoming message and the message is forwarded to the appropriate decoder component for decoding in real time. Note that INETCO Insight contains a wide variety of transaction decode tables for common message formats. New tables are continuously added to the product and custom formats can be produced by INETCO's service organization.

Table changes or additions are handled out of the core product engineering team, ensuring customer requests can be fulfilled on an as-needed basis by INETCO's serv ice organization.
As part of the decoding operation special entries in the decode tables allow masking and dropping of sensitive application information. In the case of financial messages this includes masking the credit card number and dropping other sensitive information such as the PIN block.

Some specific protocol support consists of:

- IP, TCP (v4 and v6), UDP and other network layer protocols
- HTTP, HTML, SOAP, XML, and other "Internet" protocols
- AMQP, CLNP, TPDU, NIST, SQL, WebSphere MQ and other transport layer protocols
- ISO 8583, FIX, IFX, OFX, VISA, NDC+, Diebold, Triton, and other application layer protocols both within and external to the financial segment
- X.25, SNA, Bisync, dial, and other "legacy" communications protocols

Finally, once a message has been decoded, it is passed on to the INETCO Insight Decoder's correlation component to be correlated with other relevant messages into a service transaction.

5. INITIAL TRANSACTION CORRELATION

The third operation of INETCO Insight is the correlation of messages into single link transactions. This is also the responsibility of the INETCO Insight Decoder.

The transaction correlation process is shown in the following diagram:

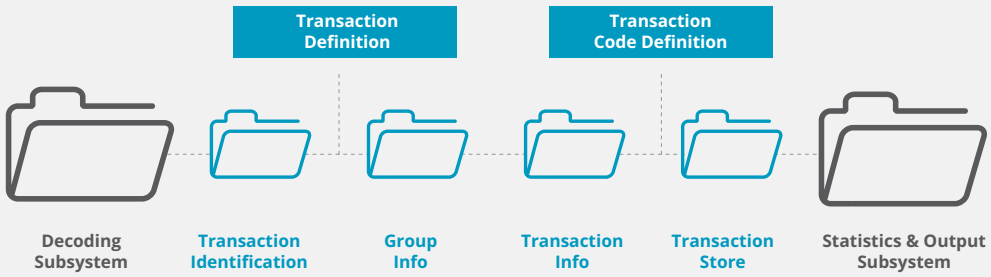


Figure 5: Transaction correlation process. This diagram illustrates the steps used by INETCO Insight to correlate transactions.

The first step in transaction correlation is to identify the PDUs that make up a transaction. This is done by the "transaction identification" component of INETCO Insight (ie TransIdent) as shown in Figure 5. This component uses a "Transaction Definition" specification for two operations:

First it determines the logical boundaries of a transaction (i.e. the messages or events that start and end a transaction). For a given network type a set of rules is defin ed in the Transaction Definition to determine the bounds of the transaction. These rules allowthe recognition of single or multiple transactions within a network connection, successful transactions, and failed transactions. Using this mechanism all messages are flagged with a uniquetransaction identifier to identify the one they belong to.

Knowing something is a transaction is not of much use unless tr ansaction specific information is also readily available. The "Transaction Info" component of INETCO Insight is responsible for mining relevant transaction information from the decoded fields and configuration information. This includes the type of transaction (ie withdrawal, add to cart, update customer information, etc.), whether the transaction is successful, error information, and any other information of importance. The result is a Service Transaction (e.g. a SQL insert, a card authorization, an HTTP request/response).

6. MULTI-HOP TRANSACTION CORRELATION

The fourth operation of INETCO Insight is to correlate service transactions into multi-hop application and business transactions.

Two things make INETCO Insight unique in this respect. First, it includes semantic models for various application protocols that capture how messages are exchanged in order to execute certain transactions. This goes beyond the simple atomic transaction modeling most network-based APM systems use, where a response is simply paired to the originating request, and allows the assembly of messages into much more complex multi-step transactions.

Secondly, INETCO Insight uses an analytic framework called the Unified Transaction Model to organize application and network messages into a higher level business transaction – which is analogous to a user task or business process.

This model is driven by a set of Application Category definitions that describe the structure, relationships and message events of interest for different styles of applications (e.g. an n-tier J2EE application, a redundant ATM or POS application, etc.). Correlation, even at a single link level, is not easy since all possible error conditions that may be encountered in real life protocols, including timing errors, must be considered. A business transaction in a modern, distributed application consists of a large number of discrete steps that span many different application components and 3rd party services.

Users can also define transaction groups to segment a large appl ication into meaningful buckets. This is done in the “Group Info” component which matches configured decoded fields and their values against user configured groups. The relevant group names are then attached to the associated transaction information.

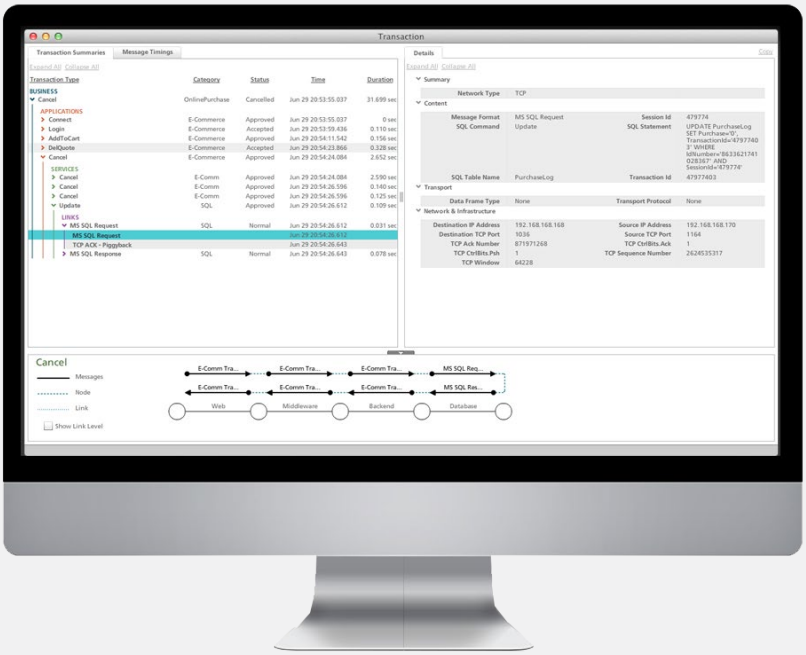


Figure 6: Online purchase transaction. This screenshot illustrates how INETCO Insight ties together dozens of application messages into a single business transaction, while preserving all the important details of how the transaction is executed at a technical level.by INETCO Insight to correlate transactions.

The final function of the correlation component of the INETCO In sight Server is to put the correlated and labeled transaction in a “Transaction Store” where it may be later accessed for queries and drill down.

This information is then handed off to the statistics and output component of the INETCO Insight Server to enable interactive querying, web-based display, transaction log ging, transaction forwarding, event notification, and syslog output.

7. SUMMARY

INETCO Insight's data collection, message decoding and transaction correlation technology enables real-time monitoring of complicated and diverse transaction flows from a handful of non-disruptive network access points.

INETCO Insight's proprietary processing engine inspects every packet related to an application, assembling these

packets into messages, decoding the contents of every message, correlating messages into atomic transactions, and then re-constructing multi-tier and multi-hop transactions. At each step, relevant header information, message payload details, addressing information, and timing attributes are captured.

As a result INETCO Insight is able to dramatically improve visibility into complex application environments, enabling proactive problem detection, faster troubleshooting, and more accurate capacity planning.

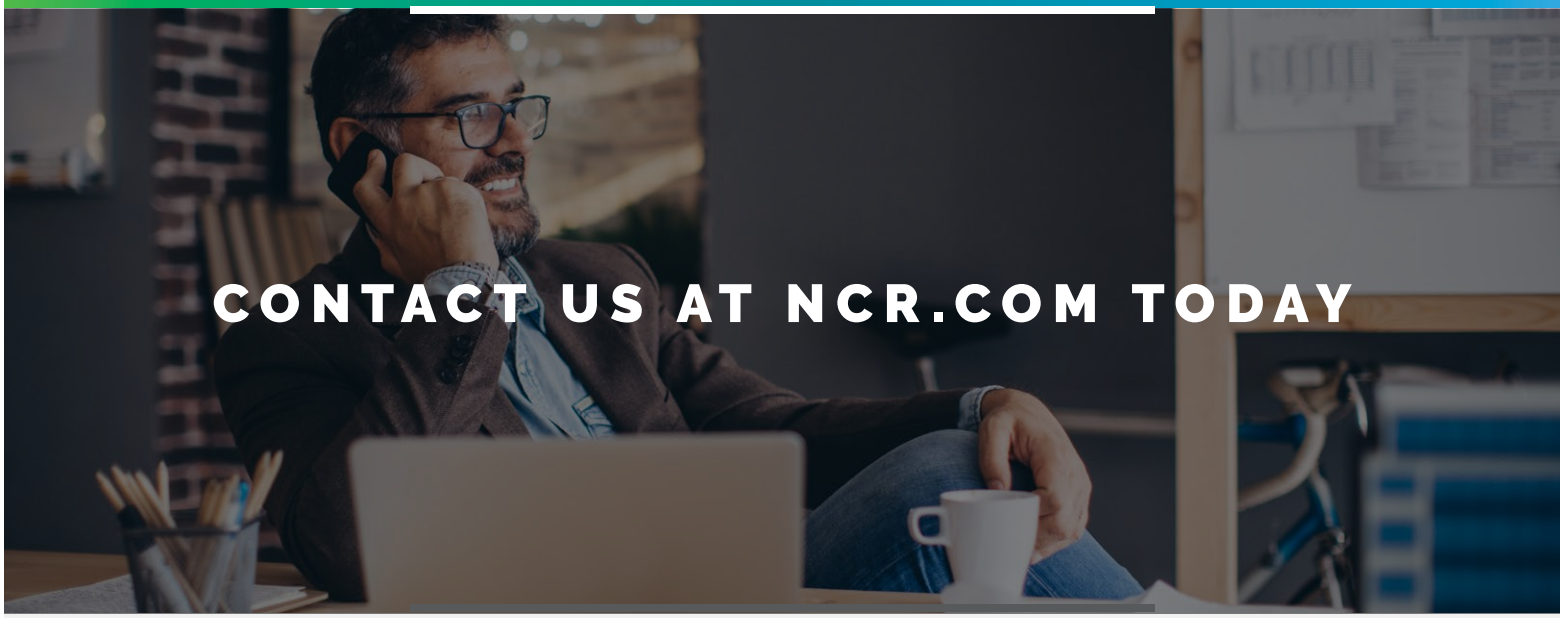
DEFINITIONS

The following terms are used in this document:

PAN **Transaction "Primary Account Number"**

PDU **Protocol Data Unit** A low level data packet received by the INETCO Insight Event Collector and forwarded to the INETCO Insight Server.

SPAN **Switch Probe Analyzer Port** A port on a network switch router or other network device which can be used to monitor traffic on other ports This functionality is also called port mirroring.



CONTACT US AT NCR.COM TODAY

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Atlanta, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

ABOUT INETCO®— EVERY TRANSACTION TELLS A STORY®

INETCO® Systems Limited provides market leading transaction monitoring ~~and analytics~~ software that helps line of business and IT operations teams improve profitability, reduce operational costs and deliver an amazing customer experience. INETCO's proven solutions are currently deployed in over 50 different countries. Happy INETCO Insight® ~~and INETCO Analytics~~™ partners and customers include some of the world's largest companies spanning the banking, ATM, retail, telecommunications and payment processing markets. www.inetco.com

NCR

INETCO Insight