NarusInsight™ Solution for Intercept

Meeting the need for precision data capture

Real-Time IP Traffic and Application Monitoring and Capture

The NarusInsight Solution for Intercept delivers unmatched flexibility to intercept IP communications content and identify information, enabling law enforcement and government organizations around the world to effectively gather evidence of illegal activity in the multifaceted world of IP communications.

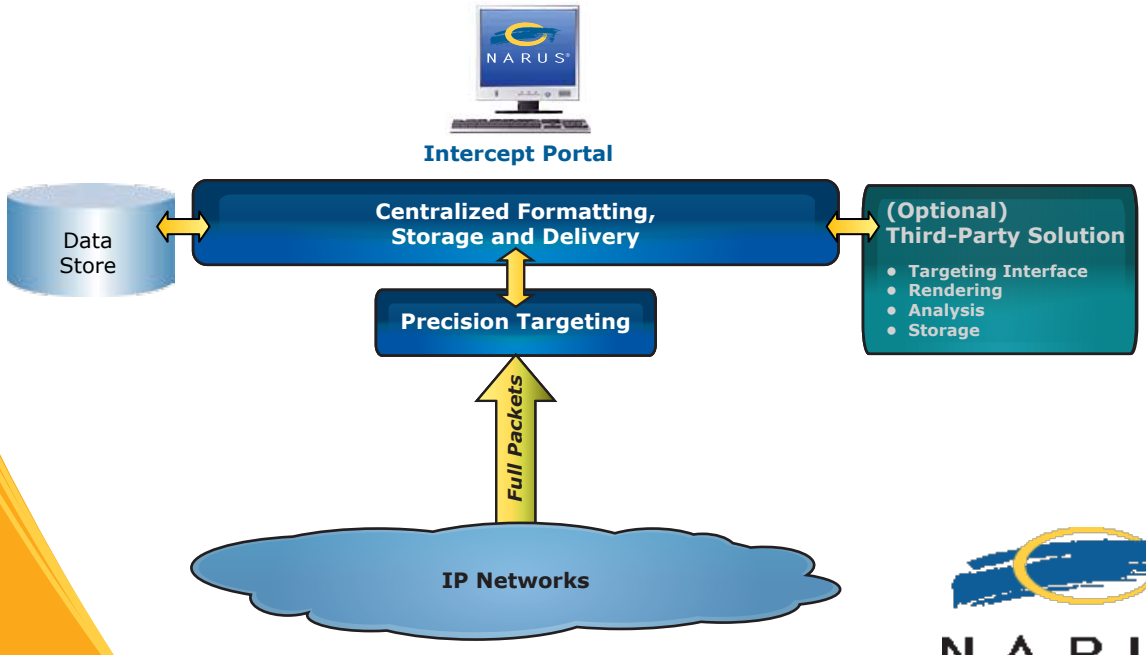
Built on the NarusInsight Traffic Intelligence system, the NarusInsight Solution for Intercept passively monitors multiple links on the network. It monitors each packet on the network link and analyzes it against a target list input by the providers or directly by a law enforcement agent. If the packet matches the target criteria, it is captured for formatting and delivery to storage, law enforcement or directly to optional content rendering and analysis tools.

Key Features

Precision Targeting at Broadband Speeds
- Vendor, service and network-agnostic
- Target by application including, Webmail, chat, VoIP, e-mail, URL and more
- Target by phone number, URI, e-mail address, login account, keyword and more

Capture and Delivery
- Passive model collects off the line at wire speeds
- Architecture supporting data capture from asymmetric networks
- Flexible structure to support standards-based and other optimized forms of intercept

Rendering and Analysis
- Playback of multiple application types as they happen or from past events
- Support for built-in or third-party options
- Secure and scalable administration functions



NARUS®

Cyber criminals are real. Countries worldwide are under attack. Government organizations and administrations mandate Intercept.

As service providers and government organizations migrate to next-generation networks and continue to offer new communications services, the complexity associated with monitoring those networks for intercept purposes increases dramatically. Whether the intercept requirement is for compliance with lawful intercept mandates (via published standards or through other means) or purely for managing private government or national networks, the solution must be scalable and flexible enough to deal with multiple environments and traffic patterns.

While intercepting communications on circuit-switched voice networks follows a well-known and established process, intercepting IP traffic can be far more complex, requiring the ability to see and extract only targeted data from large, heterogeneous networks over which millions of communications sessions are constantly and simultaneously moving. Operators must be selective in their warrant-based targeting while still having the ability to ensure complete data capture for defined users and services. This requires a solution with multiple forms of targeting criteria, while not losing focus on the real need to ensure the privacy of non-targeted users sharing the same communications paths as the targeted users.

Key Differentiators

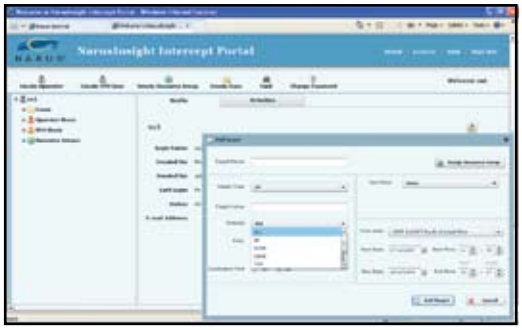
Advanced targeting, capture and rendering system
- Precision targeting using behavioral and signature analysis
- Real-time targeting and capture of multiple IP-based protocols and applications (layer-2 to layer-7)
- Non-intrusive monitoring transparent to network
- Support for multiple rendering and analysis tools

Vendor-service and network-agnostic
- Support for wireline and wireless networks at broadband speeds
- Internet, Webmail, VoIP and e-mail all in one platform
- Support for fully asymmetric traffic across large heterogeneous networks
- Targeting and capture in MPLS VPN environments

Market-leading scalability to enable monitoring networks of any size
- Carrier-grade speed and performance with support for links up to 10GigE/OC-192/STM-64
- Distributed collection across very large, geographically and technologically distributed networks
- Centralized analysis and presentation of networkwide information in real time

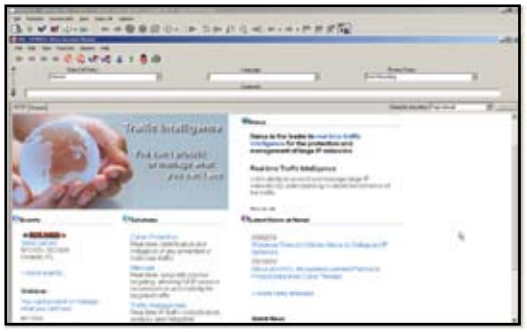
Easily extensible and highly modular
- Modular structure enables users to add new application components as needed via plug-in framework
- Flexible output format ensures support for national standards or non-standard output to law enforcement or forensic analysis applications

NarusInsight™ Solution for Intercept Operational Flow



1. Specify and manage targeting criteria

- Associate targets to case IDs
- Define locations to capture data/traffic
- Define destination for captured packets
- Report on active targets/cases



4. Reconstruct, render and/or analyze captured content

- Repackage raw packets into consumable content
- View Web pages, read text and e-mail/Webmail messages, listen to VoIP calls
- Examine raw packet output for network forensic analysis

2. Monitor the network and capture target traffic

- Communicate target IDs to collection components
- Passively analyze all traffic in designated locations
- Capture only traffic associated with targeting criteria

3. Format and deliver full packets

- Convert traffic into required format
  - o PCAP, XML, IPDR, ASCII, standards by region
- Deliver intercepted communications directly to LEA or to file for rendering and forensic analysis

NARUS®

Functional Capabilities

Target Types
- IP address/address range/subnet
- Single port or port range (client or server)
- IP protocol (TCP, UDP, ICMP and more)
- Radius attribute
- DHCP attribute
- MAC address
- Layer-2 or layer-3 MPLS labels including Dynamic MPLS labels
- Application Protocol
    - o Chat (AIM, IRC, SIP, MSN, XMPP/Gmail, Yahoo! IM)
    - o Email address/login (SMTP, IMAP, POP3)
    - o Webmail address/login (Gmail, Yahoo!, Gawab, Hotmail, Live Hotmail)
    - o VoIP phone number/URI (SIP, H.323, MGCP, IAX2)
    - o Web URL
- Keyword or string

Capture Interface Types
- E3/T3
- 10/100/GigE/10GigE
- STM-1/OC-3
- STM-4/OC-12
- STM-16/OC-48

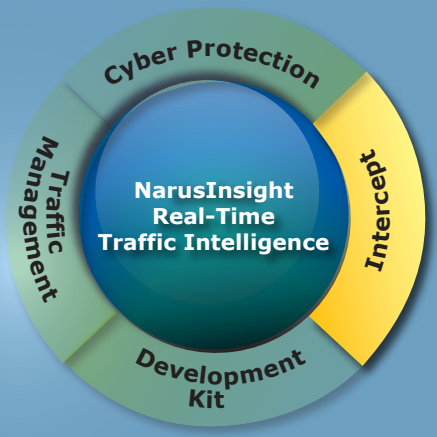
Output/Delivery
- PCAP
- XML
- TEC/GR Interface
- ETSI Handover Interface
- IPDR, ASCII for metadata

Built-in Security
- Target console password protected for secure access to target information
- Encrypted communication of target data
- Target information accessible only by target creator
- Full audit logs of target activity

NarusInsight is the most scalable, real-time traffic intelligence system for capturing, analyzing and correlating IP traffic. It delivers one common system that can be configured to deliver cyber protection, intercept and traffic management solutions or can be used to develop custom application using its Development Kit.

Narus Offerings

1. **NarusInsight™ Solution for Cyber Protection**
   Real-time network and application protection
2. **NarusInsight™ Solution for Intercept**
   Real-time IP traffic and application monitoring and capture
3. **NarusInsight™ Solution for Traffic Management**
   Real-time application monitoring and policy enforcement
4. **NarusInsight™ Development Kit**
   Configuring all aspects of NarusInsight from collection to processing for building custom applications



Each solution is designed to be modular so information can be collected once and used by multiple northbound applications either in conjunction with one another or for a specific purpose.

NARUS®

Narus, Inc.
570 Maude Court
Sunnyvale, CA 94085
P: 1 408 215 4300
F: 1 408 215 4301

About Narus, Inc.
Narus is the global leader in real-time traffic intelligence for the protection and management of large IP networks. Narus is the only software company that provides cyber security, intercept and traffic management solutions within a single, flexible system. With Narus, service providers, governments and large enterprises around the world can immediately detect, analyze, mitigate and target any unwanted, unwarranted or malicious traffic. Narus solutions provide its customers with complete, real-time insight into all of their IP traffic from the network to the applications, enabling customers to take the most appropriate actions quickly.

www.narus.com
info@narus.com