# Network intelligence

**Network intelligence** (**NI**) is a technology that builds on the concepts and capabilities of Deep Packet Inspection (DPI), Packet Capture and Business Intelligence (BI). It examines, in real time, IP data packets that cross communications networks by identifying the protocols used and extracting packet content and metadata for rapid analysis of data relationships and communications patterns. Also, sometimes referred to as Network Acceleration or piracy.

NI is used as a middleware to capture and feed information to network operator applications for bandwidth management, traffic shaping, policy management, charging and billing (including usage-based and content billing), service assurance, revenue assurance, market research mega panel analytics, lawful interception and cyber security. It is currently being incorporated into a wide range of applications by vendors who provide technology solutions to Communications Service Providers (CSPs), governments and large enterprises. NI extends network controls, business capabilities, security functions and data mining for new products and services needed since the emergence of Web 2.0 and wireless 3G and 4G technologies.[1][2][3][4]

## Contents

## Background

The evolution and growth of Internet and wireless technologies offer possibilities for new types of products and services,[4][5] as well as opportunities for hackers and criminal organizations to exploit weaknesses and perpetrate cyber crime.[6][7][8] Network optimization and security solutions therefore need to address the exponential increases in IP traffic, methods of access, types of activity and volume of content generated.[9][10] Traditional DPI tools from established vendors have historically addressed specific network infrastructure applications such as bandwidth management, performance optimization and quality of service (QoS).

DPI focuses on recognizing different types of IP traffic as part of a CSP's infrastructure. NI provides more granular analysis. It enables vendors to create an information layer with metadata from IP traffic to feed multiple applications for more detailed and expansive visibility into network-based activity.

NI technology goes beyond traditional DPI, since it not only recognizes protocols but also extracts a wide range of valuable metadata. NI's value-add to solutions traditionally based on DPI has attracted the attention of industry analysts who specialize in DPI market research. For example, Heavy Reading (http://www.heav yreading.com) now includes NI companies on its Deep Packet Inspection Semi-Annual Market Tracker.[4]

## Business Intelligence for data networks

In much the same way that BI technology synthesizes business application data from a variety of sources for business visibility and better decision-making, NI technology correlates network traffic data from a variety of data communication vehicles for network visibility, enabling better cyber security and IP services. With ongoing changes in communications networks and how information can be exchanged, people are no longer linked exclusively to physical subscriber lines. The same person can communicate in multiple ways – FTP, Webmail, VoIP, instant messaging, online chat, blogs, social networks – and from different access points via desktops, laptops and mobile devices.

NI provides the means to quickly identify, examine and correlate interactions involving Internet users, applications, and protocols whether or not the protocols are tunneled or follow the OSI model. The technology enables a global understanding of network traffic for applications that need to correlate information such as who contacts whom, when, where and how, or who accesses what database, when, and the information viewed. When combined with traditional BI tools that examine service quality and customer care, NI creates a powerful nexus of subscriber and network data.

## Use in telecommunications

Telcos, Internet Service Providers (ISPs) and Mobile Network Operators (MNOs) are under increasing competitive pressures to move to smart pipe business models. The cost savings and revenue opportunities driving smart pipe strategies also apply to Network Equipment Providers, Software Vendors and Systems Integrators that serve the industry.

Because NI captures detailed information from the hundreds of IP applications that cross mobile networks, it provides the required visibility and analysis of user demand to create and deliver differentiating services, as well as manage usage once deployed.

| Requirement | Purpose | Example Applications |
|---|---|---|
| Customer Metrics | Understand customer demand | ▪ Audience measurement<br>▪ User behavior analysis<br>▪ Customer segmentation<br>▪ Personalized services |
| Network Metrics<br>▪ service ( Delivery )<br>▪ events | Identify / deliver / manage services | ▪ Bandwidth / resources optimization<br>▪ Content / application-aware billing<br>▪ Quality of Experience (QoE) analysis<br>▪ VoIP fraud monitoring<br>▪ Regulatory compliance |

NI as enabling technology for smart pipe applications

Customer metrics are especially important for telecom companies to understand consumer behaviors and create personalized IP services. NI enables faster and more sophisticated Audience Measurement, User Behavior Analysis, Customer Segmentation, and Personalized Services.

Real-time network metrics are equally important for companies to deliver and manage services. NI classifies protocols and applications from layers 2 through 7, generates metadata for communication sessions, and correlates activity between all layers, applicable for bandwidth & resource optimization, QoS, Content-Based Billing, quality of experience, VoIP Fraud Monitoring and regulatory compliance.

## Use in cloud computing

The economics and deployment speed of cloud computing is fueling rapid adoption by companies and government agencies.[11][12][13] Among concerns, however, are risks of information security, e-discovery, regulatory compliance and auditing.[14][15][16] NI mitigates the risks by providing Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) vendors with real-time situational awareness of network activity, and critical transparency to allay fears of potential customers. A vendor can demonstrate hardened network security to prevent Data Leakage or Data Theft and an irrefutable audit trail of all network transaction – communication and content – related to a customer's account, assuming compliance to regulation and standards.

## Use in government

NI extracts and correlates information such as who contacts whom, when where and how, providing situational awareness for Lawful Interception and Cyber Security. Real-time data capture, extraction and analysis allow security specialists to take preventive measures and protect network assets in real time as a complement post-mortem analysis after an attack.

## Use in business

Because NI combines real-time network monitoring with IP metadata extraction, it enhances the effectiveness of applications for Database Security, Database Auditing and Network Protection. The network visibility afforded by NI can also be used to build enhancements and next-generation solutions for Network Performance Management, WAN Optimization, Customer Experience Management, Content Filtering, and internal billing of networked applications.

## References

1. Jessica Schieve (2011-02-23). "Light Reading report: Network Acceleration - Managing Data Growth" (https://web.archive.org/web/20110511192950/http://www.fiercetelecom.com/offer/windriver_intel?source=ebook_tab). Light Reading. Archived from the original (http://www.fiercetelecom.com/offer/windriver_intel?source=ebook_tab) on 2011-05-11. Retrieved 2011-03-15.
2. Brian Partridge (2010-05-17). "Network Intelligence is Key to Profiting from Anywhere Demand" (http://www.yankeegroup.com/ResearchDocument.do?id=53513). Yankee Group Anchor Report. Retrieved 2010-06-15.
3. Thibaut Bechetoille (2009-03-25). "The Everyday Relationship Between You and 'Your' Information: What's Out There on the Internet" (http://ipcommunications.tmcnet.com/topics/ip-communications/articles/52992-everyday-relationship-between-and-information-whats-out-there.htm). TMCnet. Retrieved 2010-06-15.
4. Simon Sherrington. "Deep Packet Inspection Semi-Annual Market Tracker" (http://www.heavyreading.com). Heavy Reading. Retrieved 2010-06-15.
5. Aditya Kishore (2008-07-21). "Market Research: New Opportunity for Service Providers?" (http://www.lightreading.com/document.asp?doc_id=159415). Light Reading. Retrieved 2009-07-27.

6. Shireen Dee (2009-02-03). "Qosmos Network Intelligence Helps Development of Smart Pipe Solutions" (http://caas.tmcnet.com/topics/caas-saas/articles/49997-qosmos-network-intelligence-helps-development-smart-pipe-solutions.htm). TMCnet. Retrieved 2009-07-27.
7. "MessageLabs Intelligence: 2008 Annual Security Report" (http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf) (PDF). MessageLabs. 2009. Retrieved 2009-07-27.
8. "Big Data and Bigger Breaches With Alex Pentland of Monument Capital Group" (http://www.huffingtonpost.com/shane-paul-neil/big-data-bigger-breaches-_b_6109928.html). 2015. Retrieved 2015-01-14.
9. "2008 Internet Security Trends" (http://www.ironport.com/securitytrends/). IronPort. 2008. Retrieved 2009-07-27.
10. Jordan Golson (2009-07-21). "A Brave New World: 700M New Net Users Seen By 2013" (http://gigaom.com/2009/07/21/a-brave-new-world-700m-new-net-users-seen-by-2013/#more-59899). GigaOM. Retrieved 2009-07-27.
11. Stacey Higginbotham (2009-07-21). "Will P2P Soon Be the Scourge of Mobile Networks?" (http://gigaom.com/2009/07/21/will-p2p-soon-be-the-scourge-of-mobile-networks/#more-59491). GigaOM. Retrieved 2009-07-27.
12. "IDC Finds Cloud Computing Entering Period of Accelerating Adoption and Poised to Capture IT Spending Growth Over the Next Five Years" (https://web.archive.org/web/20091123195427/http://www.idc.com/getdoc.jsp?containerId=prUS21480708). IDC. 2008-10-20. Archived from the original (http://idc.com/getdoc.jsp?containerId=prUS21480708) on 2009-11-23. Retrieved 2009-07-28.
13. Tom Sullivan (2008-03-29). "More Cash for Cloud Computing in 2009" (https://www.pcworld.com/article/162157/more_cash_for_cloud_computing_in_2009.html). PC World. Retrieved 2009-07-28.
14. Henry Sienkiewicz (2008-04-30). "DISA's Cloud Computing Initiatives" (http://www.govinfosecurity.com/podcasts.php?podcastID=229). Government Information Security Podcasts. Retrieved 2009-07-28.
15. Ephraim Schwartz (2008-07-07). "The dangers of cloud computing" (http://www.infoworld.com/d/cloud-computing/dangers-cloud-computing-839). Info World. Retrieved 2009-07-28.
16. Jon Brodkin (2008-07-02). "Gartner: Seven cloud-computing security risks" (https://web.archive.org/web/20090318162846/http://www.networkworld.com/news/2008/070208-cloud.html). Info World. Archived from the original (http://www.networkworld.com/news/2008/070208-cloud.html) on 2009-03-18. Retrieved 2009-07-28.