ADLINK
Leading EDGE COMPUTING

Network Packet Visibility Solution

Real-time analysis of network traffic exposes malicious attacks & enhances information security

Joint release by
ADLINK Technology
PacketX Technology
N-Partner Technology



PacketX N-Partner

www.adlinktech.com

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Index

Cybersecurity today P1

You can't defend against what you can't see: security depends on visibility P2

Network packet visibility keeps malicious attacks from slipping through the cracks P4

Real Life Use Case: IT department at a tech company P7

ADLINK Hardware Solution P9

Conclusion P10

Cybersecurity today

Increased connectivity and network bandwidth means that cyber threats are growing in number at a rapid pace. Business organizations are now faced with complex cybersecurity challenges. The increasing intelligence and autonomy of cyber threats have made them harder to detect as well. New threats are constantly emerging in addition to old threats being upgraded and unleashed again. According to the Cisco 2017 Annual Cybersecurity Report, more than one-third of all companies that had their data compromised in 2016 reported losing more than 20% of their customers, business opportunities and revenues. In 90% of these cases, companies affected by cyberattacks undertook three types of improvements: (1) separation of IT and cybersecurity functions (38%); (2) employee training on cybersecurity awareness (38%); and (3) adopting technologies to reduce risk (37%). Cyberattacks became increasingly “business-oriented” in 2016. Digital developments not only spurred drastic changes in the technology environment but also created opportunities for cyber criminals. The effective prevention of cyberattacks and the implementation of effective protective measures after an attack has occured have become a key challenge for cybersecurity vendors. Effective assessment of cybersecurity implementations is the key to defending against cyberattacks.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

You can't defend against what you can't see: security depends on visibility

To prevent cyberattacks, one must first know what abnormal changes in network traffic look like. Take an airport for example. An airport is equipped with many X-ray machines that inspect luggage and expose any hidden contraband. But if any luggage manages to bypass the X-ray inspection stations, having the best X-ray equipment in the world won't do much good. If we replace luggage with network packets and X-ray inspection devices with intrusion detection and prevention systems (IPS/IDS), then network visibility is the mechanism for ensuring that “all luggage passes through the X-ray inspection stations.” Visibility is without a doubt the cornerstone of security.

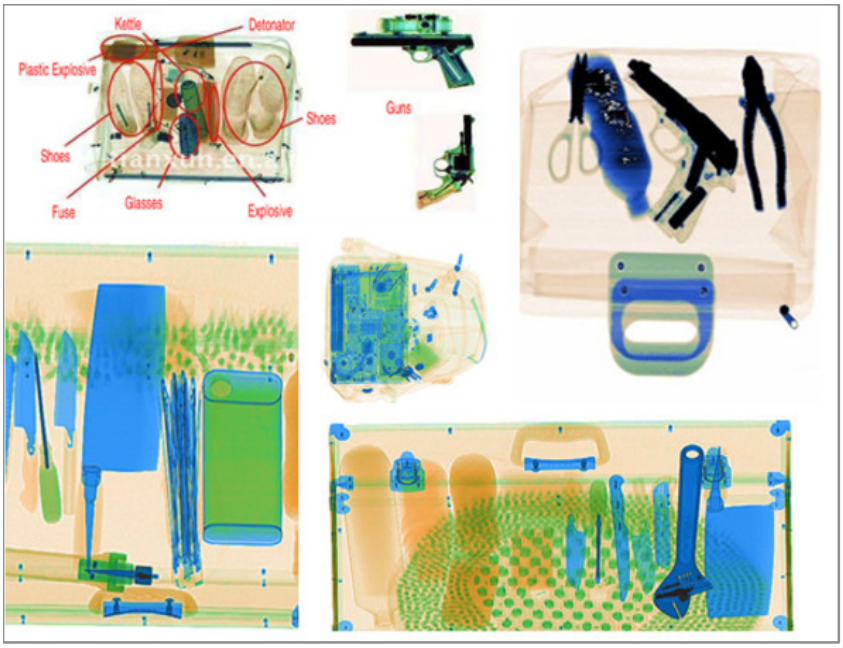


Figure 1: Like X-ray inspection stations at the airport, network visibility solutions reveal all network traffic.

Common visibility solutions in the past used a network tap or a switch’s built-in port mirror function to send a copy of the network traffic to the network management or cybersecurity equipment for analysis. In other words, if there are multiple analytical devices, the traffic must be copied multiple times. In practice, the tap function does not support multiple copies, nor does a switch have many free ports for mirroring. Large amounts of mirroring also have an impact on performance. The next step for visibility solutions is the network packet broker (NPB). Traffic from multiple mirror sources are consolidated and then duplicated or filtered as necessary before being distributed to different analytical devices. Such solutions are now in general use today.

Many analytical devices process network metadata instead. Traditionally, the router or core switch performs traffic sampling (picking one packet out of every N packets for processing) to generate the metadata for analysis by dedicated equipment. Applications include the monitoring of the network performance by network administrators as well as the detection and identification of abnormal network activity. This type of metadata-based visibility solution is sufficient for network administration but provides incomplete data from a cybersecurity perspective,

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

making it more difficult to use for detecting malicious activities such as DDoS attacks or abnormal network access, both important areas in cybersecurity analysis today. A non-sampling network metadata generation mechanism is therefore essential for meeting the current cybersecurity requirements. However, performance limitations prevent most routers and core switches from implementing this, nor is it supported by most access switches.

An effective NPB must therefore provide both “traffic-based” and “metadata-based” visibility solutions. Such an NPB must not only process and forward the copied traffic it receives, it must also be capable of analyzing all the traffic (and not only a sample) to generate a complete set of network metadata. The solution is to use Netflow enabled routers and switches which are able to ...

NPB visibility solution

NetFlow is a network packet exchange protocol introduced by Cisco. The protocol was first used to accelerate the exchange of data between network devices. It can also simultaneously implement the measurement and tracking of IP data flow during high-speed switching. Over the years, the data acceleration function of NetFlow was gradually taken over by dedicated application-specific integrated circuit (ASIC) chips, thus increasing efficiency. Netflow’s ability to measure and track IP flow information through network devices has matured and it is now the industry standard for IP traffic analysis, statistics and billing.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Network packet visibility keeps malicious attacks from slipping through the cracks

As networks become larger and network management/cybersecurity equipment more prevalent, the performance improvements that can be extracted from NPB increase as well. IT administrators can set filter conditions and forwarding paths on packet brokering equipment based on the characteristics of the network topology and nodes. Traffic from different sources can then be collated before being distributed to the analytical device at each node to ensure that network management/cybersecurity equipment only receives traffic related to its own analytical functions. The calls for reforms to the underlying network architecture have become increasingly strident in recent years leading to the rise of Software Defined Network (SDN), Network Function Virtualization (NFV) and Server Virtualization technologies. The importance of network visibility is increasingly gaining traction as well. Currently, the virtualized networks of mobile network backbones and data centers make extensive use of tunneling protocols. This also increases the complexity of network traffic and makes analysis more difficult. As tunneling re-packages network packets before re-transmitting them again, GPRS Tunneling Protocol (GTP), Multiprotocol Label Switching (MPLS) and IEEE 802.1Q Tunneling (QinQ) packet-sniffing then become essential for network management and cybersecurity equipment. In practice, these functions are not supported by most network management/ cybersecurity equipment, creating potential security loopholes. To patch these loopholes, we look at network visibility solutions rather than analytical devices. The following section will explain how Netflow data can be used to realize network visibility.

Business organizations faced with cyber threats need software that can receive and analyze NetFlow data. Analysis of NetFlow data enables

(1) More detailed traffic information

(2) Identification of abnormal network behavior such as distributed denial-of-service (DDoS) attacks

NetFlow data analysis is the most efficient solution for detecting DDoS attacks. Once an attack is detected, the malicious traffic can be immediately transferred to traffic cleaning equipment.

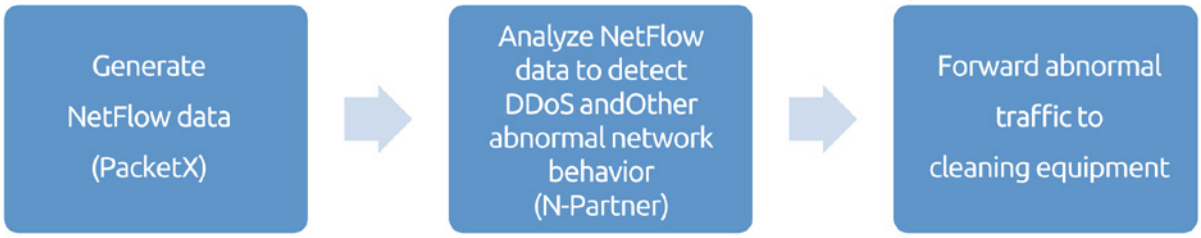


Figure 3: How network traffic is handled by a network visibility solution

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

PacketX GRISM Network Visibility Solution

- The industry-leading GRISM Network Visibility Solution from PacketX is a next-generation NPB based on a deep packet inspection (DPI) engine. It can consolidate mirror or in-line traffic, pre-processing for packet analysis (remove tunnel context from GRE/VxLAN/MPLS/QinQ/VLAN), and accurately sort traffic through the analyzer function, or generate NetFlow data for NetFlow analyzers.

- The most common application of NPB is to screen packets by destination IP or source IP, and then forward them to the designated address. In the telecom industry, for example, every subscriber has a different set of application services. Any analysis will therefore also involve user-based screening. For such application environments, the NPB can be converted into a network application broker (NAB) to provide matchmaking services for the back-end application system.

Most businesses use in-line cybersecurity equipment as their first line of defense against hacks and exploits. When traffic flow exceeds the limits of the cybersecurity equipment may lead to crashes or delays in packet inspection that can paralyze normal network operations. At the same time, the majority of network traffic is harmless (e.g., YouTube or internal VoIP) while more suspicious traffic such as tunneling packets can't be analyzed by cybersecurity equipment. PacketX's GRISM platform offers a total solution to this problem and helps businesses strengthen their in-line defenses in four key areas.

(1) Zero network risk: Activates bypass mechanism upon in-line equipment failure and prevents BGP/OSPF synchronization time out.
(2) High equipment efficiency: Activates bypass for designated application layer sessions to minimize waste of cybersecurity resources
(3) Lower level protection: Traffic pre-processing mechanism allows existing cybersecurity equipment to analyze tunneling packets
(4) Diversified analysis: Real-time extraction of NetFlow v5/v9 data from in-line traffic

GRISM can analyze NetFlow data extracted from network traffic. In the past, such mechanisms were only implemented by high-end Cisco routers or switches. Generating NetFlow data is very system resource intensive (DPI logs even more so) thus NetFlow is generated through sampling instead. For example, a sampling rate of 256:1 means only 1 out of every 256 packets are processed. Such a sampling ratio works for traffic estimation but is not suitable for detecting abnormal behavior, and attacks using excessive traffic, therefore affecting accuracy and detection speed. GRISM replaces the router's NetFlow data generation function. In addition to allowing the router to focus on its primary mission, the generation of 1:1 non-sampled NetFlow data also enables more effective detection of abnormal behavior.

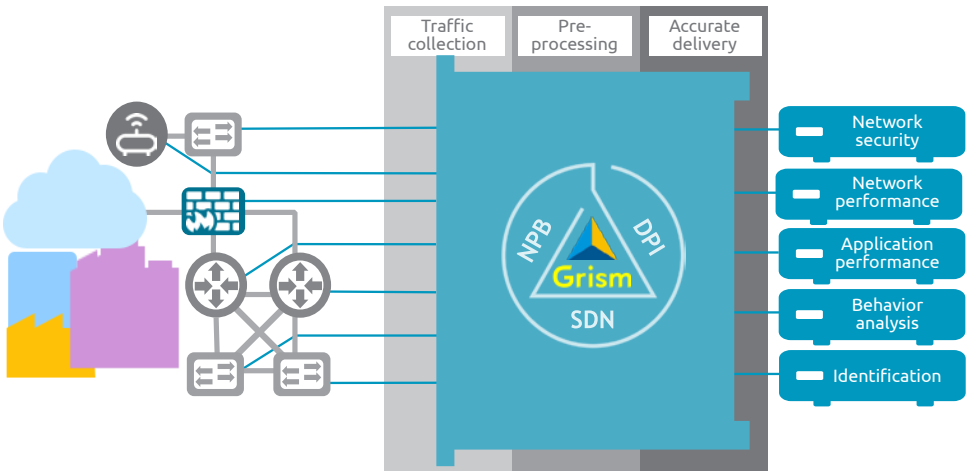


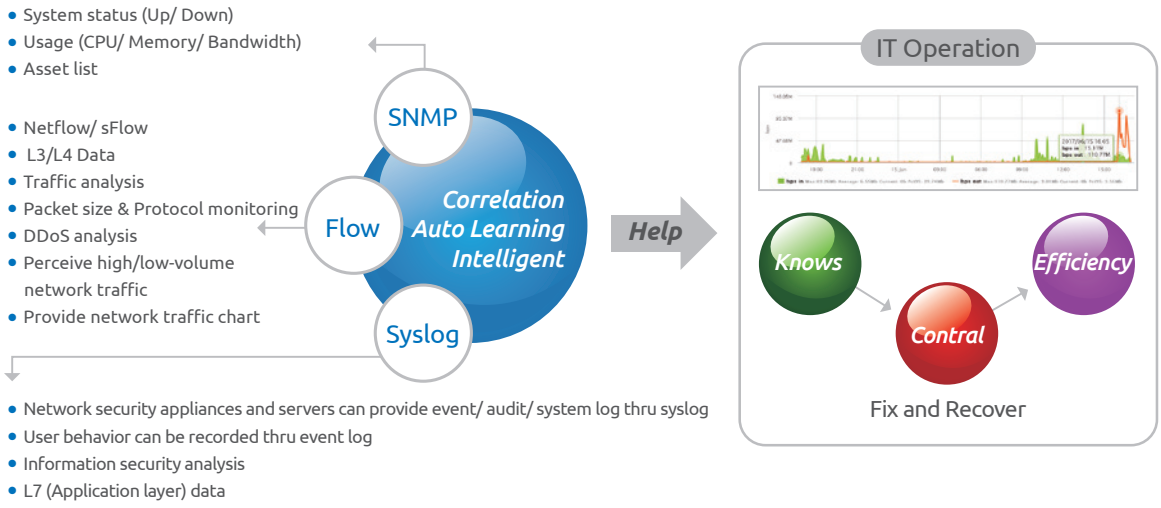
Figure 4：PacketX GRISM Network Visibility Solution

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Real-time network traffic analysis and statistics with N-Reporter track network usage and easily identify the source of anomalies

SNMP is frequently used during IT administration to check on the health of devices. NetFlow/sFlow data produced by routers and switches are used to calculate the number of transmitted packets and bandwidth usage. Syslog can detail all activities including login audits, access logs and cybersecurity events. SNMP/Flow/Syslog are the three main tools of routine IT administration. Traditionally, SNMP (network management software), Flow (traffic analysis), and Syslog (SIEM and log storage) are three separate systems that operate independently of each other. Each type of management mechanism only provides partial information about network usage or cybersecurity status. IT personnel must spend a great deal of time sorting through all the information. They must also use their own experience to look for or find a correlation between the information provided by the three tools before they can try to identify the source of the network problem. This is a very time-consuming process that is often hampered by stability and quality problems with the IT system.

To help system administrators resolve this longstanding problem, N-Partner developed a next-generation IT administration technology that is a perfect fusion of SNMP, Flow and Syslog. The built-in AI automatically conducts correlation analysis of data from SNMP/Flow/Syslog with the goal of helping admins understand every detail of their network. Big data analytics is used to learn all characteristics of the IT systems and users' routine usage patterns. Once a reasonable threshold value is calculated for given time periods, anomalies can be detected right away and the source of problems identified. Problems that used to take IT admins hours, days or even weeks to fix can now be dealt with within minutes. This not only saves large amounts of time but also greatly boosts efficiency. The entire process is recorded in detail and presented graphically to reflect the work performance of the IT department.



The N-Reporter product developed by N-Partner comes with integrated AI trend algorithms that can use the collected Syslog/Flow data to automatically learn the usage patterns of each IP address, and establish a reasonable base line for each type of activity. Incoming Syslog/Flow data is then continuously assessed to identify abnormal increases in the number of events (hit count), packets or bytes, source IP (generally, the attacking side) and the destination IP (generally, the targeted side). The N-Reporter administration platform will display the analyzed results using the trend reporting function. The details of abnormal increases are also emailed to the relevant network administrators so that network anomalies can be dealt with right away. IT admins no longer have to guess at a reasonable threshold value for each unit or IP address they oversee. The Behavior Base detection and analysis function of N-Reporter provides a full picture of all relevant changes in the network environment, making network administration a lot easier.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Real Life Use Case: IT department at a tech company

A normal day for busy IT network admins

A tech company has more than 1,800 employees worldwide. Routine email correspondence as well as the network functions needed for testing by R&D units means a high volume of intensive network traffic is generated every day. Whenever there is a problem in the network, IT personnel can only go to the user terminal and use their experience to determine the probable cause. The user terminal's network connection may have been disabled by a virus, or other users in the same domain may be taking up too many resources. With no monitoring software, a user problem may take hours or longer to investigate. The problem may still be a mystery even then.

Finding an effective solution

To solve the network problem in an effective manner, normal network usage must first be established. The solution that the IT admins at the tech company settled on was to use GRISM from PacketX to monitor the network traffic and back it up with N-Partner's N-Reporter Netflow analytical software. Now, when an employee experiences a network connection error, the Netflow analysis software can be used to quickly pin down the time of the anomaly and IP address. This means the problem can be quickly and efficiently resolved. Using Netflow data for analysis and reporting allows IT admins to effectively monitor and troubleshoot traffic status at any time.

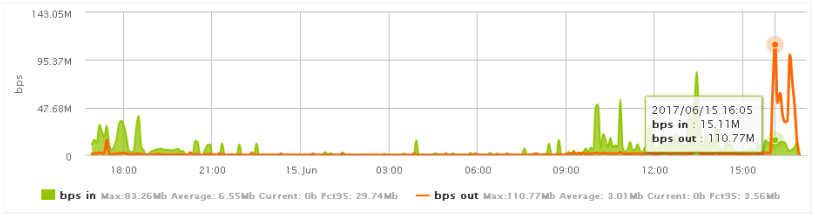


Figure 5: IT can check the network traffic status by viewing Netflow analytics data to prevent attacks or unusual usage.

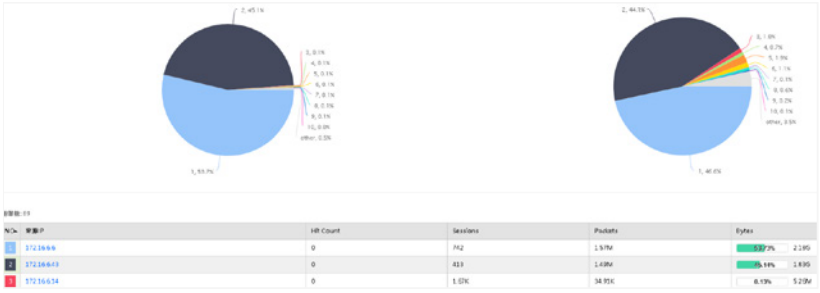


Figure 6: Netflow data report for traffic from a specific IP address.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

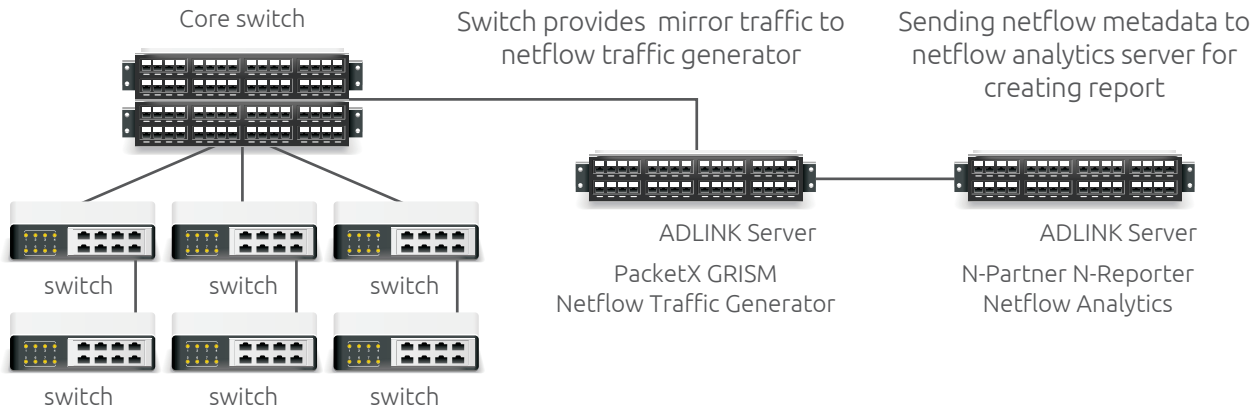


Figure 7：network packet visibility architecture

The above architecture can be deployed on the user-end using entry/mid-level switches. The traffic at each switch can then be copied to the Netflow generator. High-end switches on the market can generate their own Netflow data, but are more expensive and less flexible because they cannot process data from other switches. This was why the IT admins ultimately decided to use this solution.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

ADLINK Hardware Solution

AdvancedTCA Platform



Dual Cavium CN6880 40 Gigabit Ethernet AdvancedTCA® Packet Processing Blade

aTCA-N700

- Two Cavium OCTEON II CN6880 processors, each with 32 cnMIPS64 v2 cores
- Eight memory sockets supporting VLP DDR3-1333 REG/ECC up to 128 GB
- Onboard Ethernet switch BCM 56842 provides connectivity to RTM, OCTEON II processor and backplane (Fabric) with L2 and L3 switch management software
- Dual 1000BASE-T Fabric Interface channels
- Powerful Local Management Processor - Freescale QorIQ P2041, quad-core @ 1.2GHz
- Flexible RTM support on 12 x10G SFP+ ports (RTM-RN710) or 2x 40G QSFP+ and 4x 10G SFP+ (RTM2-RN720)

Network Security Appliance



4U 19" Network Appliance with Intel® Xeon® Processor E5-2600 v3/v4 Family

CSA-7400

- Based on Open Compute Carrier-grade Edge Reference Architecture (OCCERA)
- Intel® Xeon® Processor E5-2600 v3/v4 Family
- 4U high-density platform with four dual Intel® Xeon® Processor E5 v3/v4 systems
- Dual switch modules provide 2x 50G internal Ethernet links to each compute node
- 2x 400Gb/s Ethernet bandwidth, 2x 200Gb/s PCIe bandwidth, total 1.2Tb/s bandwidth
- Flexible IO combinations via choice of switch sleds (MXN-3610, MXN-4100) and Network Interface Modules (NIM-1610, NIM-0440)
- Advanced chassis management
- Redundant AC/DC PSUs (N+1)

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Conclusion

To deal with constantly evolving cybersecurity threats, PacketX Technology's GRISM Netflow data generating software and N-Partner's N-Reporter Netflow data analysis software, combined with ADLINK's hardware platforms were used as the hub of the monitoring network. The client also received assistance with building a highly flexible monitoring network that can be integrated with analysis functions to strengthen cybersecurity protection.

PacketX Technology

PacketX, founded in 2014, consists of a young team dedicated to developing the next-generation of network monitoring infrastructure with innovative software. PacketX has proven they are pioneers in providing DPI-enabled network visibility platforms for monitoring traffic aggregation, pre-analysis processing, accurate delivery and L2-L7 metadata generation.

Network analysis resources in both public or private sectors are having difficulty keeping up with growing throughput demands. Moreover, most analysis systems are incompatible with IT innovations such as server virtualization or software-defined networking (SDN). PacketX technology provides the best strategy for solving these problems in a cost-efficient way and can be tailored the the specific needs of the application.

The PacketX network visibility platform is able to automatically provision threat intelligence such as the blacklists and enable massive IP/Domain/URL blocking when deployed as an in-line node. This especially benefits today's multi-tier security architectures where network visibility has been redefined by PacketX to not only support analysis- but also as first-tier security.

N-Partner

N-Partner products provide functionality for Syslog/Flow/SNMP data collection, storage, real-time analysis, queries and reporting. The most important is the correlation of Syslog/FLow/SNMP. Implementing the correlation of Flow, which reflect the information of L3/L4/ Packet/Byte and Syslog, which is the data indicating L7 applications, is the perfect combination to provide a complete view of the network and security details. N-Reporter is the most advanced, powerful and simple to operate reporting and analysis system for Syslog, Flow and SNMP.

About ADLINK

If you are interested in the above solution, please contact us at networking@adlinktech.com for more details.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

WORLDWIDE OFFICES

ADLINK Technology, Inc.

9F, No.166 Jian Yi Road, Zhonghe District
New Taipei City 235, Taiwan
新北市中和區建一路166號9樓
Tel: +886-2-8226-5877
Fax: +886-2-8226-5717
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.

5215 Hellyer Avenue, #110 San Jose, CA 95138, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-360-0222
Email: info@adlinktech.com

ADLINK Technology Singapore Pte. Ltd.

84 Genting Lane #07-02A, Cityneon Design Centre
Singapore 349584
Tel: +65-6844-2261
Fax: +65-6844-2263
Email: singapore@adlinktech.com

ADLINK Technology Singapore Pte. Ltd. (Indian Liaison Office)

#50-56, First Floor, Spearhead Towers
Margosa Main Road (between 16th/17th Cross)
Malleswaram, Bangalore - 560 055, India
Tel: +91-80-65605817, +91-80-42246107
Fax: +91-80-23464606
Email: india@adlinktech.com

ADLINK Technology Japan Corporation

〒101-0045 東京都千代田区神田鍛冶町3-7-4神田374ビル4F
KANDA374 Bldg. 4F, 3-7-4 Kanda Kajicho,
Chiyoda-ku, Tokyo 101-0045, Japan
Tel: +81-3-4455-3722
Fax: +81-3-5209-6013
Email: japan@adlinktech.com

ADLINK Technology, Inc. (Korean Liaison Office)

경기도 성남시 분당구 수내로46번길4 경동빌딩 2층 (수내동 4-4번지)
(우) 463-8252F, Kyungdong B/D, 4 Sunae-ro 46 beon-gilBundang-gu,
Seongnam-si, Gyeonggi-do, Korea, 13595
Toll Free: +82-80-800-0585
Tel: +82-31-786-0585
Fax: +82-31-786-0583
Email: korea@adlinktech.com

ADLINK Technology, Inc. (Israeli Liaison Office)

27 Maskit St., Corex Building PO Box 12777
Herzliya 4673300, Israel
Tel: +972-54-632-5251
Fax: +972-77-208-0230
Email: israel@adlinktech.com

ADLINK Technology (China) Co., Ltd.

上海市浦东新区张江高科技园区芳春路300号 (201203)
300 Fang Chun Rd., Zhangjiang Hi-Tech Park
Pudong New Area, Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology Beijing

北京市海淀区上地东路1号盈创动力大厦E座801室(100085)
Rm. 801, Power Creative E, No. 1 Shang Di East Rd.
Beijing, 100085 China
Tel: +86-10-5885-8666
Fax: +86-10-5885-8626
Email: market@adlinktech.com

ADLINK Technology Shenzhen

深圳市南山区科技园南区高新南七道 数字技术园A1栋2楼C区 (518057)
2F, C Block, Bldg. A1, Cyber–Tech Zone, Gao Xin Ave. Sec. 7
High–Tech Industrial Park S., Shenzhen, 518054 China
Tel: +86–755–2643–4858
Fax: +86–755–2664–6353
Email: market@adlinktech.com

ADLINK Technology GmbH

Hans-Thoma-Strasse 11
D-68163 Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

PENTA ADLINK Technology GmbH

Ulrichsbergerstrasse 17
94469 Deggendorf, Germany
Tel: +49 (0) 991 290 94 – 10
Fax: +49 (0) 991 290 94 - 29
Email: emea@adlinktech.com

ADLINK Technology, Inc. (French Liaison Office)

6 allée de Londres, Immeuble Ceylan
91940 Les Ulis, France
Tel: +33 (0) 1 60 12 35 66
Fax: +33 (0) 1 60 12 35 66
Email: france@adlinktech.com

ADLINK Technology Inc. (UK Liaison Office)

First Floor West Exeter House,
Chichester Fields Business Park Tangmere,
West Sussex, PO20 2FU, United Kingdom
Tel: +44-1243-859677
Email: uk@adlinktech.com

About the Intel® Internet of Things Solutions Alliance

ADLINK Technology is a Premier member of the IntelR Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 400+ global member companies of the IntelR Internet of Things Solutions Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions. Learn more at: intel.com/iotsolutionsalliance

ADLINK® Leading EDGE COMPUTING

intel® IoT Solutions Alliance Premier

© 2017 ADLINK Technology Inc. All Rights Reserved. All Specifications are subject to change without further notice.
All products and company names listed are trademarks or trade name of their respective companies. Published in Dec. 2017.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000