Wire Data Analytics | Get Real-time and Historical Insight

> *"No agents and getting a visibility by grabbing traffic straight off the wire is a major advantage for us. Much more detail, superior to Netflow."* Information Security Officer, City National Bank, USA

What is wire data analytics?

Wire data is data contained within the headers and payloads of packets and their associated flow data as traffic moves from one node to another.

Wire data is a rich source of user and application information. Wire data can be derived from SPAN ports, TAPs, packet brokers or locally on systems using promiscuous mode packet captures.

Wire data analytics is the process by which raw packet data is transformed into real-time and historical business and IT insight. Wire data analytics is the only way to get to granular detail and fully understand what is happening on a network.

Why do you need wire data analytics?

Gathering data off the wire can be accomplished without invasive probes or software agents that add overhead and complexity.

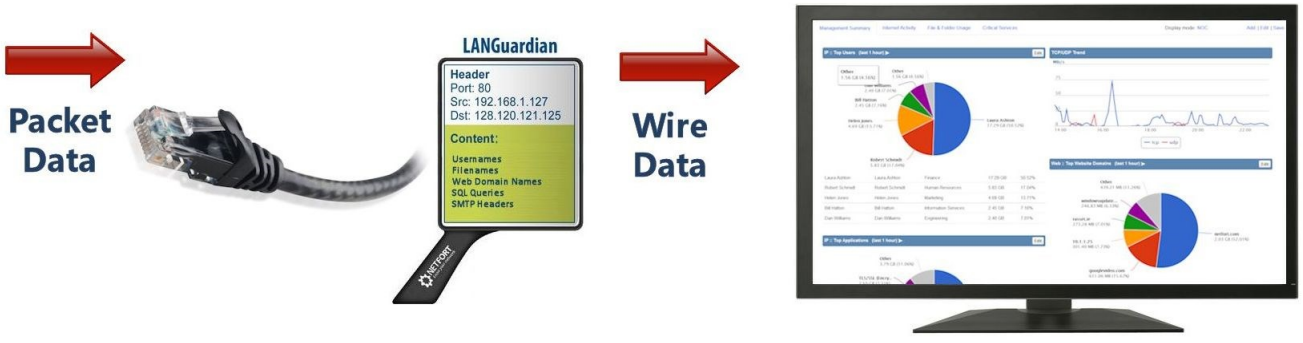
Wire data capture does not require auditing on servers so you wont slow down business critical applications. Use wire data analytics for:

* Network security monitoring.
* User activity monitoring.
* Root cause analysis.
* Real time and historical troubleshooting.
* Bandwidth usage analysis.
* Detailed web usage monitoring, both proxy and non-proxy.
* Network and user forensics.

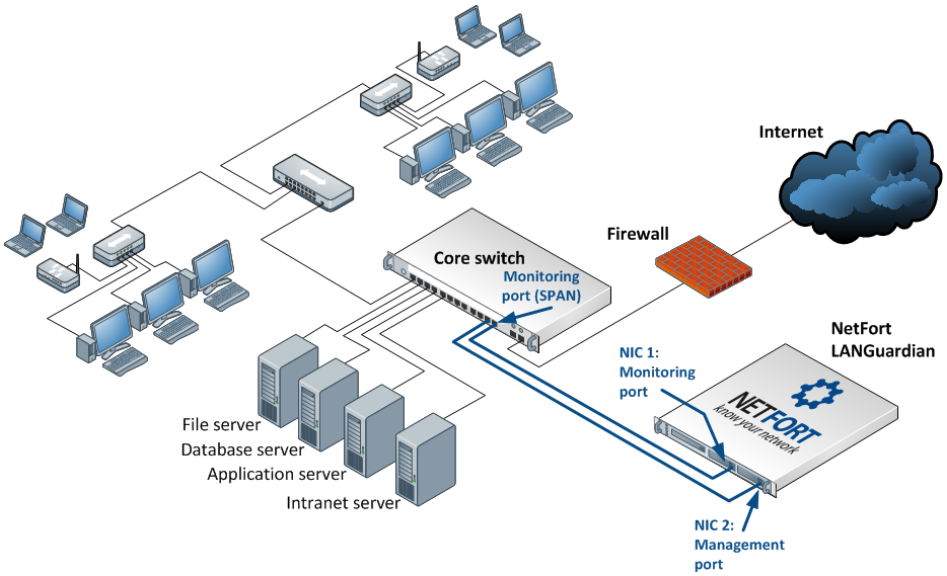
Why LANGuardian should be your only choice for Wire Data Analytics

LANGuardian is deep packet inspection software for investigating, monitoring, and reporting on user and network activity.

- Logs and reports on activity by IP address and actual user name.
- Unique levels of detail using NetFort metadata for critical protocols including SMB, HTTP and SQL.
- All wire data retained in a built in database.
- Go back on data days, weeks or months without the need for expensive hardware and storage.
- Built in application recognition engine tracks usage by application and user name.
- Connect to a SPAN or mirror port and instantly monitor anywhere across your network.
- Download and deploy on standard server hardware, VMware or HyperV.



Wire data analytics transforms raw packet data into human readable formats.



This diagram shows a LANGuardian installation at a single site, with a single core switch. LANGuardian can also be deployed on networks with multiple core switches.

Bandwidth troubleshooting

Identify users and applications that devour bandwidth. Troubleshoot saturated links and network bottlenecks.

- See at a glance how bandwidth is being used across your WAN, LAN, and Internet links.
- See details of usage by specific network links, users, clients, servers, applications, and websites.
- Drill down to greater levels of detail, ultimately to details of the start-time, end-time, and size of each individual data transfer.

File activity monitoring

Find out who accessed or deleted files. Prevent data leakage and unauthorized access to confidential data.

- See exactly what is happening on your file sharing infrastructure.
- Search for file activity by IP address, subnet, username, or file name.
- Identify the users who have accessed a file or file share over a specific time period.
- Receive alerts to unusual file activity, such as large downloads by a single user over a short time period.

Network Security Monitoring

Add an extra dimension to your IT security posture. Identify internal threats and get early warnings about zero-day threat activity.

- Use trends and alerts to identify suspicious activity like Ransomware.
- Detect port-scanning and port-sweeping activity.
- Identify instances of spam generation.
- Optional security module combines Snort intrusion detection with LANGuardian database to create a unique historical IDS.

Network forensics

Full packet capture, storage of historical network events, and comprehensive analytical capabilities make LANGuardian the ideal solution for your network forensics requirements.

- Analyze an incident by simply entering an IP address, subnet, or username.
- Respond to queries about network activity with all the pertinent facts.
- Troubleshoot network problems and identify anomalous or illegal behaviour.
- Identify misconfigured systems and deliberate or unwitting misuse of the network by authorized users.

Web activity monitoring

Drill down into user activity by website, download type, and traffic volume. Track down viruses, malware, and other security issues.

- Get an unrivalled level of visibility into the Internet traffic generated by the users on your network.
- Search for web activity by IP address, subnet, username, or website name.
- See everything from the total amount of traffic generated in a year, to the date and time a user visited a specific web page.
- With alerts, trends, reports, and drilldown capabilities, LANGuardian can tell you everything you need to know about user Internet activity on your network.

Application Monitoring (CBAR)

CBAR enables LANGuardian to generate consolidated reports that show bandwidth and usage patterns from an application perspective.

- Uses DPI to analyze packet content as well as packet headers. More detailed and accurate reporting than NetFlow based monitoring tools can provide.
- Eliminates reliance on source address, destination address, and port number to identify the application associated with network traffic.
- Enables network engineers and system administrators to identify applications that use random port numbers or that use standard port numbers for non-standard purposes.

"Seeing what the users are doing in multiple different areas is really what made us purchase" Senior IT Specialist, Country Casual, USA

"As a benefit it also provides unique out-of-band network forensics for troubleshooting or identifying odd network traffic" Network Analyst, Illinois Community College

Contact Information:

Web: www.netfort.com

E-mail: sales@netfort.com

Phone: +1 (646) 452 9485