NETFORT
know your network

LANGuardian gives complete visibility across your network

No shipping of appliances | No complex setup
No NetFlow | Just detail

NetFort LANGuardian

NetFort LANGuardian is the industry's leading deep packet inspection software for investigating, monitoring, and reporting on network and user activity. It is a passive network traffic analyser, not inline, so it doesn't impact on network performance. It can be downloaded and deployed on standard physical or virtual hardware and ready to go in minutes. Because it gathers information from network traffic, there is no need to install agents or clients on devices connected to the network, making it easy to install. Its primary data source is a SPAN or mirror port on a switch. LANGuardian's generation and storage of network metadata, results in a massive data reduction while still retaining rich detail over long periods critical for multiple network security and operational use cases. LANGuardian helps IT and Security Professionals to:

- ✓ Find out what users are doing internally
- ✓ Troubleshoot bandwidth issues
- ✓ Find out who's deleted a file or folder from a network share
- ✓ Track access to confidential data
- ✓ Create a dashboard to track Ransomware attacks
- ✓ Receive an immediate security alert on suspicious activity on the network
- ✓ Perform forensics to diagnose recent network issues

Who uses LANGuardian?

LANGuardian is used to monitor, troubleshoot and report on everyday network and user activities for customers like these:

HONDA

TRINITY COLLEGE DUBLIN

Washington Gas

Kanes Foods

accenture
High performance. Delivered.

Dubai Airports

Key Features

Simple Deployment

Use your ports to get traffic from any switch; no NetFlow modules required.
No bespoke hardware required

Total Visibility

Use powerful deep packet inspection (DPI) techniques to analyze the traffic anywhere on the network.

Comprehensive Search

Search for network information by username IP address, subnet, file name or web address

Alerting Engine

Get an instant alert for any unusual network activity

Report Mechanism

Generate powerful reports, built-in and custom, with drilldown capability to show the minutest level of detail and context to drive decision-making

Track Users

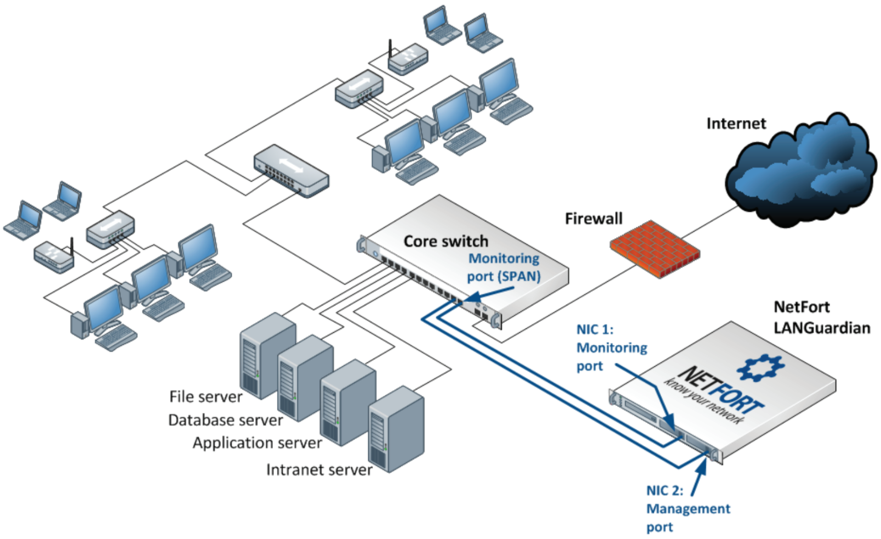
Integrate with Microsoft Active Directory to give reports that list real user names rather than just IP addresses

Real-Time and Historical

Display dashboards that show both real-time and historical reports of network activity data

Integration

Easy integration with tools like SolarWinds and Splunk



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 user and applications that hogg 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 web-sites
- Drill down to greater levels of detail, to view 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 Windows 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

> *Seeing what the users are doing in multiple different areas is really what made us purchase*

Information Security Officer
City National Bank, USA

Security

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
- Detect port-scanning and port-sweeping activity
- Identify instances of spam generation
- This security module combines Snort intrusion detection with the 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 usernames
- 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

Network Traffic Analysis

LANGuardian uses advanced content based application recognition 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 – the foundation for more detailed and accurate reporting than NetFlow based monitoring tools can provide
- Eliminates reliance on source address, destination address, and port numbers to identify the application associated with network traffic
- Enables IT and Security Professionals to identify applications that use random port numbers or standard port numbers for non-standard purposes

Much more detail superior to NetFlow

Information Security Officer
City National Bank, USA