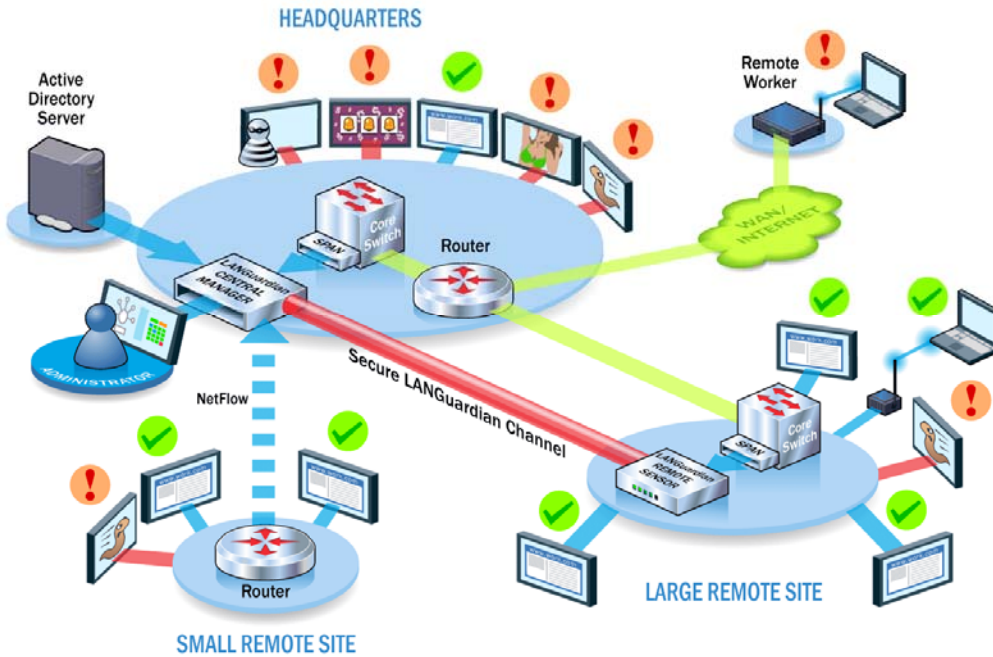


# NetFort LANGuardian

Network Activity Monitoring

## Introduction



NetFort Technologies is the leading provider of **network activity monitoring** solutions, serving customers throughout Europe and the US in a range of sectors including Finance, Education, Healthcare, Local Government, Pharmaceuticals, Technology, Telecoms, Manufacturing and Utilities. Clients include Wyeth, Xilinx, Kerry Group, Fingal Council and the London School of Economics.

LANGuardian enables IT directors, operations managers, network administrators, compliance and security staff to analyze their network activity using one consolidated interface. LANGuardian monitors internal network usage, helps troubleshoot performance issues, identifies security breaches, reduces network operational costs and helps enforce compliance. Often deployed to identify and mitigate potential security exposures, LANGuardian additionally provides immediate cost and operational management benefits.

Network activity monitoring (also known as **network behavior analysis**) refers to the analysis of an organization's use of network resources from both a **security** and **operational performance** perspective. This analysis can be complex and time-consuming, requiring access to multiple log files and systems to monitor, detect, troubleshoot and report. LANGuardian makes it easy to monitor network activity in real-time with graphical dashboards, identifying problems before serious damage occurs, and capturing usage information that can be subsequently reported on. LANGuardian provides a comprehensive suite of features in one package, and has the fastest time-to-deploy in the market, ensuring you gain real benefits from day one.

## Benefits

**Accelerated Troubleshooting** – easy-to-use interfaces with fast drill down lets administrators pinpoint and resolve problems as they occur

**Network Performance** – minimizes downtime and service interruptions, monitors network utilization, highlights traffic patterns, visually portrays network usage, indicates how performance can be optimized

**Security** – identifies inappropriate network usage, helps prevent damage from worms and viruses, alerts management when breaches threaten or occur, detects suspicious activity or infected machines

**Compliance** – monitors compliance at a number of levels, including security policy compliance, network usage policy compliance and compliance to privacy and Internet usage policy

**Capacity Planning** – provides the information on resource utilization and usage patterns that managers need for capacity planning and resource management

**Risk Reduction** – mitigates the risk of security breaches, combats spy-ware and avoids non-compliance with legal security, privacy and Internet usage requirements

**Cost Reduction** – identifies redundant or unused network resources, highlights areas of highest demand, discourages non-work related network usage

# Delivering Unified Network Visibility.

## Product Components

LANGuardian is an all-in-one **network activity monitoring** solution that provides a single view of all critical network performance data. LANGuardian installs as a rack mounted device in less than an hour. The network administrator can then access the device from any workstation on the network, using its features to view, analyze and report on network usage. LANGuardian is non-intrusive – there are no agents or clients to be installed anywhere on the network. LANGuardian's components are described in more detail below.

### Traffic and Network Data Repository

At the core of LANGuardian is a central database that stores critical and useful network data including

- All network traffic flows
- Security, network and Internet related events
- IP address, machine names and **user names**

Collecting this data at one point enables the product to provide a consolidated overview of all network activity. This enables easier detection and troubleshooting of anomalies or suspicious network events occurring in real-time. It also enables network and security managers to drill down and report on network activities for any previous time period, supporting forensic analysis of incidents that have occurred.

Importantly, LANGuardian does not simply record information to enable you to subsequently view it. The product can also generate alerts, letting network managers know when a problem occurs and ensuring that incidents are highlighted and dealt with as soon as they are detected.

### Traffic Collection Engine

The Traffic Collection Engine collects both raw traffic and Cisco NetFlow traffic, via copper or fiber sniffer ports. The support for Cisco NetFlow allows for visibility onto both local and wide area networks (WANs). The key benefit of the Traffic Collection Engine is both real time and historical visibility of network usage, with built-in drill down to enable rapid troubleshooting.

### Network Intrusion Detection

LANGuardian uses Snort, a network intrusion prevention and detection system utilizing a rule-driven language. Snort combines the benefits of signature, protocol and anomaly-based inspection methods. Our implementation uses several pre-processors to perform complex stateful protocol analysis and normalization, detecting protocol anomalies.

The key benefits of the integrated NIDS is that it enables real-time detection and alerting, as well as historical analysis, supporting forensics.

*"This was the first product I've seen that was as easy to implement as we'd been told – that was a pleasant surprise. LANGuardian is very easy to install and use. One of the LANGuardian engineers spent a couple of hours with us after hardware installation and from that point we were able to operate the product without assistance. LANGuardian also has very low ongoing administration requirements from the customer's point of view. We're really pleased with the solution."*

Brian O'Hora, Network Manager,  
Trinity College Dublin

## Highlights

- Immediately detects suspicious activity
- Monitors network utilization, maximizes performance and dramatically reduces downtime
- Detects infected machines, worms that have bypassed anti-virus systems and compromised workstations
- Monitors all Internet activity (proxy and non-proxy) highlighting access to inappropriate sites and content
- Self-governance features encourages 'self-policing' by employees, reducing administration and enforcement costs
- Detects spy-ware or P2P activity
- Identifies the sources of worms and viruses that can harm your network
- Monitors breaches of network policies and minimizes risk from inappropriate network usage
- Ensures compliance with security and privacy regulations
- Provides fine-grained visibility of real-time and historical network activity
- Generates ad-hoc and scheduled reports
- Supports remote monitoring

# Delivering Unified Network Visibility.

## Product Components



### Highlight: Self Governance

The **self governance** option sends each user a report on a weekly or daily basis showing them their personal web usage, any security or usage events they may have generated and network traffic usage for the previous day or week. Tests have shown that where this feature is enabled there has been a significant reduction in the amount of inappropriate Internet activity on the network being monitored.

### Internet Monitoring Engine

LANGuardian can report on all attempts to connect to inappropriate websites (either directly or via a proxy). This can include spy-ware, pornography, or sites which are known to be associated with virus activity. It can also log all web access attempts. When the Active Directory module is in use Internet activity reports can identify the originating workstation or username. Access attempts to dubious web-sites are identified by checking the site name against a 'blacklist' database. Customers can specify sites to be added to this 'blacklist' database according to company policy.

### Network Traffic Analysis

Through passive monitoring, a system administrator gains a thorough understanding of how the network is used; detects anomalies; observes trends; understands the network's topology; and becomes familiar with what services are available, what operating systems are in use and what vulnerabilities may be exposed on the network.

The benefit of the traffic analysis engine is that managers can monitor activity without impacting on network performance. Users can drill down to session level on all traffic reports for fine-grained detail. Administrators can create custom reports based on IP sub-nets and physical locations.

### Portscan & Netscan Detection

The Portscan and Netscan detection engine monitors for **portscans** which are systems making large amounts of connections to other hosts on multiple ports. This could be associated with network scanning activity, especially if the source address is external to the internal LAN subnets. The Portscan Engine also detects systems which are establishing connections to lots of other hosts on specific port numbers (**netscans**). The netscan detection feature is also known as a **zero-day detection signature** as it does not need to know the exact Worm or Virus involved.

### Reports Wizard

The Reports Wizard ensures network administrators can immediately customize standard reports or generate new ones to access the concise critical information they require. It also enables NetFort support engineers to refresh customer systems with up-to-the minute reports covering attempted exploits of the latest security vulnerabilities, usage of the latest applications (e.g. Skype) and other relevant updates. Reports can be used to trend network usage, detect anomalies and support capacity planning and management reporting. The Reports Wizard allows the LANGuardian administrator to define multiple distribution lists for the standard daily and weekly reports, and each distribution list can contain a different selection of reports.

### Active Directory Module

The recently developed Active Directory module enables tracking of events and network traffic flows on the company network by IP address, machine name and user name. Events that can be monitored include large network downloads, all network sessions, security events, Internet access, system logon times, number of systems logged onto over a period of time, etc. When troubleshooting issues LANGuardian can identify the user and the associated workstation.

### Alerting Engine

Customized email reports can be defined with LANGuardian so that individuals and groups responsible for network management receive the information they need when they need it. LANGuardian can generate and send alerts and instant reports to network, security and operations staff in the case of a serious incident on the network. Examples of serious incidents could include a Worm outbreak, a network infrastructure modification, or an attempt by an external party to locate vulnerable hosts.

# Delivering Unified Network Visibility.

## Core Monitoring and Reporting Features

### Filters

The reporting engine provides fine-grained control through the use of filters. It is possible to create reports based on specific parameters and then save these for future re-use. For example it is possible to show all traffic between two sites or subnets, or the top servers on a site. Network administrators can refine this search by IP address, hostname, username, subnet or application.

### Historical and Real Time Reports

Reports can be run for specific times on specific days, months or years. This capability is very useful for a range of data forensic applications, for example 'who was on the system over the weekend', 'which users used most bandwidth last month.'

The screenshot shows the 'View Reports' interface. A list of reports is displayed, including 'All Windows 95 Systems on Network', 'Bandwidth Usage From HQ to Regional Office', 'Inbound Traffic From Internet', 'Internet Usage in Public Library', 'NetFlow Traffic Report From Core Router', 'Outbound Traffic From Internal Subnets Through The Firewall', 'Top Users - Access To SAP Servers', and 'Users Downloading .exe Files'. A filter configuration window is open, showing 'Time: last 24 hours', 'Sensor ID: any', and 'Source: any'. The window also includes a calendar for selecting start and end times.

### Email and SMS Alerts

LANGuardian provides immediate notification on a wide variety of network and security events. Reports can be sent by email to specific individuals, based on the type of event and the corresponding staff responsibility. Specific events can be marked and individuals alerted as they occur by email or on their mobile via a SMS gateway.

### Network and Security Incidents

All critical events that occur on the network can be grouped and displayed on-screen in real-time. A range of reports can be produced highlighting infected machines, Skype users, large data transfers, spy-ware infected machines plus user specific reports identifying who is doing what on the network

The screenshot shows a security incident report table with columns for 'FULLNAME', 'LOGON', 'SIGNATURE', 'PRIORITY', and 'EVENTS'. The data is as follows:

FULLNAME	LOGON	SIGNATURE	PRIORITY	EVENTS
SARAH JONES	JONES	Netscan	2	221
MICHELLE JOHNSON	JOHNSON	Netscan	2	86
MORGAN ROSENBERG	ROSENBERG	P2P eDonkey connor response	1	50
VAL CARMONA	VCARMONA	Netscan	1	36
MICHELLE JOHNSON	JOHNSON	MISC Jabber/Google Talk Incoming Message	1	27
SARAH JONES	JONES	WEB-CLIENT Microsoft wmf metafile access	1	2
MORGAN ROSENBERG	ROSENBERG	MISC Google Talk Logon	1	2
MORGAN ROSENBERG	ROSENBERG	P2P Cynet Server Announce	1	2
MORGAN ROSENBERG	ROSENBERG	MISC Jabber/Google Talk Outgoing Auth	1	1
MICHELLE JOHNSON	JOHNSON	MISC Jabber/Google Talk Logon Success	1	1
SARAH JONES	JONES	Banned site access	2	77712
MICHELLE JOHNSON	JOHNSON	Banned site access	2	46462
MICHELLE JOHNSON	JOHNSON	Portscan	2	7263

### Firewall Validation

Using the report filters network managers can view all traffic and detect whether traffic that should be blocked is actually entering the network.

The screenshot shows a firewall validation report. It includes filter configuration fields: 'Time: last 24 hours', 'Sensor ID: all', 'Src Filter: IHOME\_NET (subnet "192.168.0.1", or "10/8")', 'Dst Filter: any (subnet "192.168.0.1", or "10/8")', and 'Port: any (port "143", or "imap")'. A 3D bar chart shows traffic distribution by protocol and time. Below the chart is a table of traffic data:

PROTO	SERVICE	TOTAL	PERCENT
TCP	80 (http)	35.07 GB	96.50
TCP	443 (https)	413.25 MB	1.11
TCP	1433 (ms-sql-server)	372.48 MB	1.00
TCP	1026	219.43 MB	0.58
TCP	25 (smtp)	205.98 MB	0.55
TCP	22 (ssh)	40.52 MB	0.10
TCP	2706	19.95 MB	0.05
TCP	445 (microsoft-ds)	9.69 MB	0.02
TCP	2434	3.40 MB	0.00
TCP	3715	2.17 MB	0.00

### Bandwidth Usage

LANGuardian enables Network Managers to understand exactly where traffic is being distributed in the network. A simple traffic distribution report identifies all of the traffic that traverses in and out of the network, and on which port it is traveling. Reports can be generated on a user, department, IP address and application basis. Network staff can view the top users on the network over a 24 hour period, with drill down to view all sessions initiated by those users during that period.

### Policy Violations

LANGuardian tracks web accesses, large traffic volumes, machines sending more traffic than receiving and other anomalous activity on the network. Policy violation reports can be generated for the usage policies defined for the network.

The screenshot shows a policy violation report table with columns for 'Report Name', 'Time', and 'Run'. The data is as follows:

Report Name	Time	Run
Bad Accesses	last 24 hours	[Run]
P2P Users	last 24 hours	[Run]
TrafficSentGreaterThanTrafficRecy	last 24 hours	[Run]
Volume Overflows	last 24 hours	[Run]

### Network Inventory

The system provides audit reports and validation of servers and operating systems on the network. The local servers report indicates any machines inside the network that are running a service/server on their machine, and what port they are running it on. A fingerprinted OS report can confirm operating system compliance on the network.

# Delivering Unified Network Visibility.

## Case Studies

### Higher Education

This major European university had its network distributed across multiple sites. Operations staff wanted visibility of internal links as well as traffic routed across their perimeter links in order to monitor and troubleshoot network performance issues. They also required visibility into student Internet activity in order to detect overuse and/or misuse. LANGuardian was deployed with a slave unit at each of the main sites. All network activity reports are now accessible from a central console giving staff visibility across all sites, and custom reports highlight activity on specific network links

### Mobile Phone Operator

The network team for this Mobile Phone Operator had multiple systems gathering information about network usage and security events. There was no central dashboard to provide a 'complete picture'. LANGuardian was deployed with slave units monitoring firewall connections and internal activity. Customized user profiles were created to allow managers, operational and security staff to gain access to the LANGuardian reports

### Airline Industry

This airline wanted a solution that would assist with the validation of their network, in order for them to meet stringent compliance and governance requirements. LANGuardian was deployed with the Active Directory module, enabling network staff to monitor network usage, policy breaches and security incidents, and to provide an audit report to external assessors for compliance purposes.

### US Healthcare

This US based global healthcare corporation wanted to monitor network activity at username and departmental level. Company policy specified that departments were to cross-charge for services, and the IT department needed to monitor which network applications and resources were being used by which department. LANGuardian's Active Directory module was installed, enabling the IT department to track Internet usage by username and department for billing purposes, and to verify that the Internet usage policy is being complied with.

### Hospital

This major teaching hospital has a complex network linking many specialized health systems. Very high volumes of patient data are routed across the network. Network management needed a system that would alert them when suspicious activity was discovered on the network as well as giving them visibility of network traffic. LANGuardian with Active Directory was deployed to monitor their core network. Custom reports were defined to monitor bandwidth usage across links to regional offices.

### Financial Services

The network staff for this international financial services corporation had to manage large numbers of partners connecting to their network. They had no clear view of overall traffic and found it difficult to predict and analyze problems caused by the large volumes of connections. LANGuardian was deployed and customized reports were quickly developed showing the network administrators all associated traffic and events with these external networks.

*"LANGuardian immediately detected security and inappropriate usage issues which we had not previously identified. NetFort Technologies have been exceptionally responsive to our needs, and their product has continually improved. Overall the deployment of LANGuardian and our relationship with NetFort Technologies has been a huge success."*

John Cannon, Network Manager  
Liverpool John Moore University

### Government Agency

This government agency had a large distributed network which was being migrated to MPLS. IT Operations staff needed to monitor and compare network performance before and after the migration. LANGuardian was deployed at the core with sensors monitoring VLAN's on the core switches. NetFlow sensors were also deployed to give Wide Area Network visibility.

### Regional Government

This European regional authority had an Internet filtering solution in place but no way to provide visibility to end users and management. LANGuardian was installed with the Active Directory module capturing traffic from main VLAN. The 'self governance' option was configured so that each user on the network received a weekly report showing them their personal Internet and network usage, which resulted in dramatic reductions in inappropriate network activity and policy breaches.

## Our Services

- Remote Monitoring service – NetFort can remotely monitor network traffic on your behalf through our daily, weekly and monthly monitoring services
- Consultancy on security and threat analysis
- Network performance analysis and network capacity planning
- Implementation and Training



## Why you should choose LANGuardian

**Integrated Suite** – LANGuardian includes a Network Intrusion Detection System, an historical traffic analysis engine, Internet access monitoring, PortScan and NetScan detection engines, an Alerting engine and a report engine – competing solutions cannot provide the same breadth of functionality

**Speed of Deployment** – the product can be installed in less than an hour, providing immediate value, because LANGuardian is an all-in-one solution that does not require any agents installed, requires no lengthy configuration and causes no network disruption

**Consolidated view of network activity** – instead of multiple systems, logs and files, LANGuardian provides you with a unified, easy-to-use view of network traffic, resource usage and suspicious activity, so you don't have to chase after 'needles in haystacks' when troubleshooting

**Active Directory integration** – LANGuardian can map network activity and resource usage to individual user names through our integration to Active Directory, providing very fine grained network activity analysis

**Platform independent** – LANGuardian can be used to monitor any equipment running on any operating system on any kind of network

**Remote Monitoring Service** – NetFort Technologies can provide customers with the product, or we can offer a remote monitoring service, where we help protect and manage your network on your behalf

**Networking and Security Insight** – NetFort Technologies don't just provide a great product, we can provide a team of network analysts and security advisors to assist you in assessing network vulnerabilities and capacity bottlenecks and quickly identify the most effective solutions

Netfort Technologies is a global leader in Network Activity Monitoring and Network Behavior Analysis. We provide solutions to the world's leading universities, to government agencies in Europe and the United States, and to some of the world's leading manufacturers. Customers include the London School of Economics, Wyeth Pharmaceutical, Trinity College Dublin, Xilinx Laboratories, and Cork and Kerry local authorities.

### Headquarters

NetFort Technologies  
IDA Innovation Centre  
Upper Newcastle  
Galway  
Ireland  
Tel +353 (0)91 520501  
Fax + 353 (0)91 526 571  
Email [sales@netforttechnologies.com](mailto:sales@netforttechnologies.com)

### UK Sales Office

NetFort Technologies  
27 Old Gloucester Road  
London WC1N 3XX  
England  
Tel + 44 (0)207 060 2850  
Fax + 44 (0) 207 060 2890  
Email [sales@netforttechnologies.com](mailto:sales@netforttechnologies.com)

**Web** [www.netforttechnologies.com](http://www.netforttechnologies.com)

*"Initially we deployed LANGuardian to obtain real time visibility into suspicious network activity and to validate our IT security/network usage policies and network configuration. We found LANGuardian very easy to deploy and configure and required minimal training. The integrated IDS and traffic analysis system ensures we always know what is going on in our network and gives us instant access to troubleshooting information when required. Now, twelve months on, LANGuardian is a critical component of Xilinx's network infrastructure."*

Jonathan Smith, European Systems  
Manager, Xilinx.

