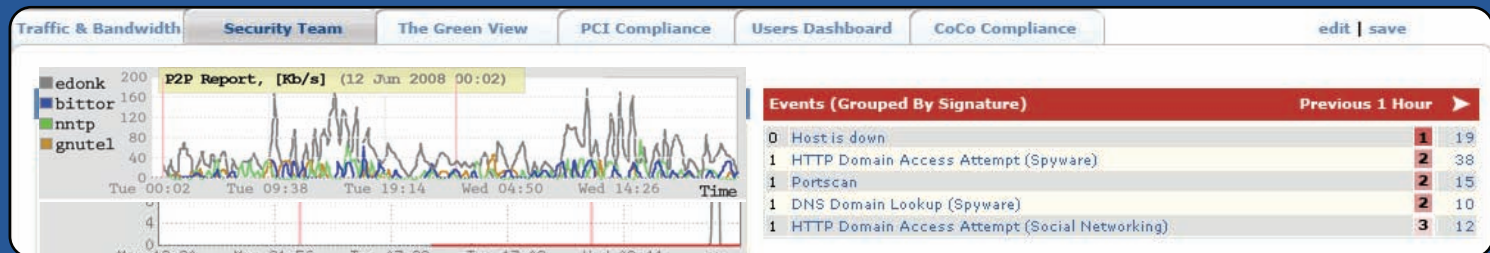


## From Reactive to Proactive... What is NetFort LANGuardian?

The LANGuardian is a searchable data warehouse for user and network activity. It is driven by a Traffic Collection Engine that collects both raw traffic, Cisco NetFlow and sFlow traffic, allowing both real time and historical visibility of network usage. This fusion of applications and historical data retention works seamlessly to form a single point of reference and achieve unique levels of user visibility via built-in drill-down capabilities to enable rapid troubleshooting.

The system includes multiple customizable dashboards used by customers on a daily basis to satisfy a number of requirements including monitoring, troubleshooting and reporting on all aspects of network and user activity. The LANGuardian's ability to provide accurate and relevant data for forensics and auditing also make it the ideal tool used by organizations to satisfy the latest compliance standards (SOX, PCI), policy and regulatory requirements.



## From Susceptible to Safe... NetFort LANGuardian on Security

"We are concerned about the **insider threat to our critical assets**. Is it possible to be alerted immediately to network activity that is in **breach of security policies**?"



The LANGuardian enables IT/Network Professionals to rapidly pinpoint areas where the security of a network is at risk.

- Immediate alerts on the source of any security breaches or network anomalies.
- Instantly detect policy violations for defined network usage policies.
- Instant detection of critical network events e.g. infected machines, social networking accesses, large data transfers and spy-ware/malware entering the network.
- Immediate notification of unauthorised traffic entering the network.

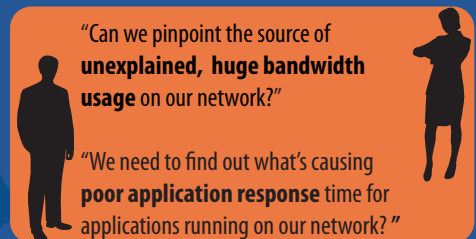
## From Effective to Efficient... NetFort LANGuardian on Operations

The LANGuardian enables IT Departments to leverage existing IT investment through capacity management, minimising the need to continuously reinvest in IT infrastructure.

- Identify resource-heavy areas on the network via traffic distribution reports on users, departments, IP addresses and applications.
- Define specific network trends for observation e.g. continuously monitor traffic generated by a specified user.
- Proactively monitor critical elements on your network such as specified applications, network devices and services for uptime and performance. Visual representations are continuously built of the Round Trip Timing (RTT) for the ping, TCP connect and challenge-response.

"Can we pinpoint the source of **unexplained, huge bandwidth usage** on our network?"

"We need to find out what's causing **poor application response** time for applications running on our network?"



## From Non-Compliant to Compliant... NetFort LANGuardian on Compliance Standards

"I need my network to be **PCI Compliant**. How can we do this and easily illustrate our network compliance to auditors?"



NetFort LANGuardian offers assurance that certain measures required to satisfy compliance audits (PCI, SOX, Code of Connection) are present in the overall corporate IT system, via an established cycle of Risk Prevention, Monitoring Procedures and Actual Event Alerts based historical and real-time reporting capabilities.

- **Risk Prevention:** Using trend reporting, IT security policy enforcement measures, effective audit trail capabilities and applying the IDS (Intrusion Detection System) eases the transition from non-compliant to compliant for key components of the current compliance standards.
- **Monitoring Procedures:** "Always-on" network and user activity monitoring detects systems or network devices that are out of compliance with established standards using signature matching and traffic analysis.
- **Actual event Alerts:** Immediately alerts in the event of access to or removal of restricted data by unauthorized users, buffer overflows, worm infections or Denial Of Service attacks. The LANGuardian does not solely rely on pattern matching or definitions.

**Rogue DHCP Servers Cause Big Operational Problems!**

Customer Site Monday Morning....

Customer Site Monday Morning....

Customer Site Monday Morning....

Customer Site Monday Morning....

NetFort LANGuardian dashboard alert! - Rogue DHCP Server found on network

Wireless router is immediately disconnected!

Thank you NetFort LANGuardian!

**CONFLICKER WORM CAUSES GLOBAL CHAOS**  
Limited Edition Issue 104 2009

NetFort Technologies 26.01.09 03.30

NetFort Security NOC detects new piece of malware... later identified as Conflicker Worm

NetFort Technologies 26.01.09 09.00

NetFort immediately deploys a report for the conflicker worm using its real-time update engine.

Customer Site 26.01.09 09.00

IT Manager logs on to LANGuardian on arriving in to work. Oh dear...the NeFort Dashboard highlights an infected machine on the network.

The machine is immediately removed from the network. Conflicker spread is stopped in it's tracks!  
**Problem Solved!**

Meanwhile...in companies NOT using the LANGuardian...

IT Professionals everywhere are resorting to all possible measures to stop the rapid Conflicker worm spread.

NetFort Customer Sites.... 26.01.09 09.00

Business continues without interruption!

Thank you NetFort LANGuardian!

**NetFort LANGuardian... What Are People Saying About It?**

"NetFort's LANGuardian provides a very comprehensive view of network intelligence. It complements other network security tools very effectively to provide the ability to be able to pin point and respond to network attacks and events"

- Geoff Harris, President, ISSA UK

"We found the NetFort 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"

- Jonathan Smith, European Systems Manager, Xilinx

"[NetFort]...tweaked our system again to give just what we needed as a trend for a particular issue. Brilliant! Thanks for proving again that excellent customer service still exists."

- John Hunt, University of Central Lancashire

"LANGuardian saved the day for us where our AntiVirus scan had failed to detect a suspicious email that filtered into our network"

- Gary Hennessey, Limerick County Council, Ireland



**Corporate Headquarters**  
NetFort Technologies Unit 7  
IDA Innovation Centre  
Upper Newcastle  
Galway  
Ireland

T: +353 (0) 91 520 501  
F: +353 (0) 91 526 571  
E: sales@netforttechnologies.com

**North American Regional Office**  
Netfort Technologies,  
280 Madison Avenue,  
#912 - 9th Floor,  
New York,  
NY 10016.

T: +1 646 924 0732  
F: +1 646 924 0778  
E: nasales@netforttechnologies.com

**EMEA Regional Office**  
NetFort Technologies  
27 Old Gloucester Street  
London WC1N 3XX  
United Kingdom

T: +44 (0) 207 060 2850  
F: +44 (0) 207 060 2890  
E: emeasales@netforttechnologies.com

**STAY CONNECTED!**  
Web: <http://www.netforttechnologies.com>  
YouTube  
<http://www.youtube.com/user/NetfortTechnologies>  
Blogger  
<http://www.netforttechnologies.blogspot.com/>