

Get Traffic Visibility and Control with nLive

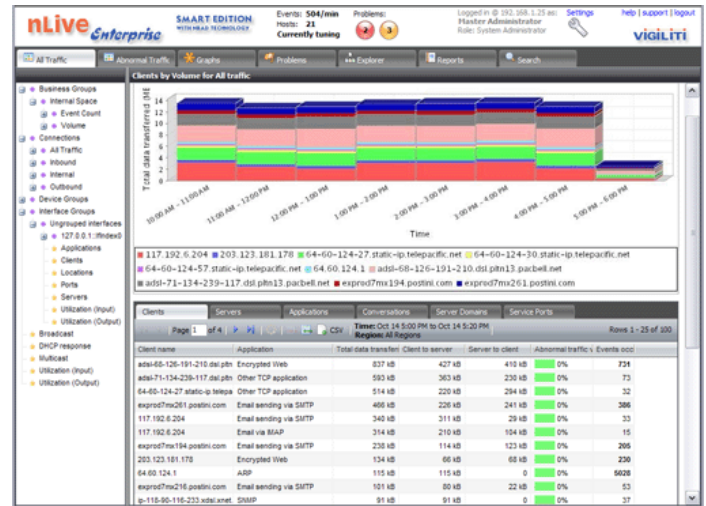
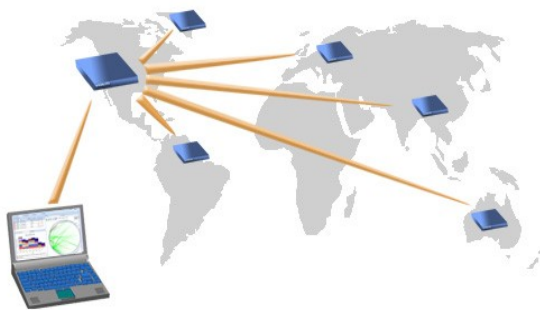
nLive is the flagship product suite from Vigiliti that continuously watches network traffic in enterprises. nLive stands for Network Learning Intelligent Visibility Engine. It performs the following*:

- ◆ Traffic analytics and visualization so you get visibility and control of 'who, what, where, when' of network traffic enterprise-wide.
 - ◆ Provide enterprise-wide real-time and historical visibility into network traffic
 - ◆ Analytics with drill-downs, filtering, searching, sorting, visualization, and reporting.
 - ◆ Ability to see abnormal activities and ill-behaving hosts/applications in the network, be it malware, abusive users or network faults
 - ◆ Observe bandwidth utilizations by subnets, locations, departments, applications, hosts etc.
- ◆ Automatic problem detection in real time using Network Behavior Anomaly Detection (NBAD), so you can pinpoint trouble spots and root causes in your network quickly
 - ◆ See a list of problems as they occur in the network so one can narrow down into the root cause quickly, be it malware, abusive users or network faults
 - ◆ Allow an administrator to investigate root causes of issues in traffic by drilling down and following the cues provided by machine-based intelligence built into nLive
 - ◆ Ability to get notified or visually identify problem areas, hosts and applications

How nLive is deployed

nLive can be deployed in a small to mid size enterprise at a single location. In a mid to large enterprise, it can be deployed with multiple traffic sensors and a centralized console. The unique architecture of sensors and their distributed database ensure that little traffic overhead is placed on the network by nLive. Traffic is sensed via router netflow exports or via mirrored packets from a switch.

nLive is available as a hardware appliance or as software installation that runs on Windows or Linux based PC.



Problems addressed by nLive

A few examples of the types of issues detected by nLive are shown in the figure below. Due to the nature of the technology employed in nLive, it is not possible to list all types of problems caught by it.



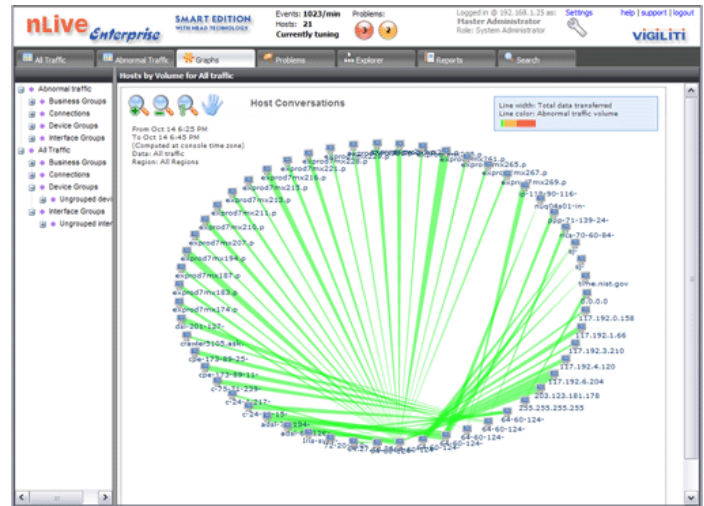
Benefits of nLive

- ◆ Gives you comprehensive traffic visibility, and hands you back your control over what is happening in your network.
- ◆ Save hours of frustration and stress troubleshooting traffic, bandwidth and security problems.
- ◆ Proactive problem detection works automatically, saving you from after-the-fact troubleshooting under pressure.
- ◆ Acts as an intelligent assistant to watch over your traffic 24 hours a day, 7 days a week, so you don't have to.
- ◆ Non-intrusive. No network change necessary.
- ◆ Scalable, fault-tolerant distributed database system that does not hog your precious bandwidth.
- ◆ Turn-key deployment. No policies to set.

* Not all features are available in all nLive editions

Feature Sets*

- ◆ **Traffic storage:** Stores traffic sources, destinations, conversations, applications, ports etc. Storage takes place in distributed sensors so that large quantities of netflow or packet traffic data need not be sent across WAN links.
- ◆ **Problem detection:** Using a proprietary implementation of NBAD, nLive detects the sources of problems. This is accomplished by creating a multi-dimensional baseline traffic model which is sensitive to time and day, and then determining violators of this model.
- ◆ **Search and report:** nLive allows comprehensive search into traffic, problems, abnormal host behavior, network devices, interfaces, hosts etc. Self-updating dashboards and standard reports are also provided.
- ◆ **Network topology determination:** nLive Enterprise edition can match the switch port to the connected host, and provide search capability on this data.
- ◆ **Visualization:** nLive provides graph visualization of traffic. Interactive tables as well as charts are also provided for easy visualization.



Feature Matrix

Product edition	nLive Flow			nLive Core			nLive Enterprise
	Free	Standard	Smart	Free	Standard	Smart	
Netflow analysis	✓	✓	✓				✓
Packet analysis				✓	✓	✓	✓
Reports, dashboards, graphs	✓	✓	✓	✓	✓	✓	✓
Search		✓	✓		✓	✓	✓
Drill-down		✓	✓		✓	✓	✓
Problem detection, NBAD			✓			✓	✓
Switch port topology							✓
Distributed sensors							✓

Recommended hardware: For software installations, the recommended system is an Intel Xeon or equivalent quad core processor with 8MB L2 cache, 4GB RAM, 200 GB free disk space, Windows XP/Vista/2003/2008 or Red hat compatible Linux. For packet analysis, two or more free Ethernet ports are recommended, but at the minimum, one is required. Equivalent virtual machines can be substituted. Lesser systems are acceptable for lighter loads or for trial purposes.



Vigilanti Systems, Inc.
P.O. Box 1358
Cupertino, CA 95015-1358
USA

Toll free: (877) 248-8688
Internet: www.vigilanti.com

Vigilanti Systems, Inc. is a privately-held Delaware corporation based in Santa Clara, California with operations in India. Vigilanti develops and markets a product line called nLive. It is a network traffic and netflow analytics product for enterprises of all sizes who like to proactively monitor network traffic and gain control over it.

* Not all features are available in all nLive editions