Flow-Based Network Intelligence you can depend on.
Top 10 reasons why it is critical to have Visibility of the traffic on your network?

1. Root Cause Analysis
2. Detecting the source of malicious traffic
3. Capacity Plan Trends and Substantiate IT Spend
4. Manage Change
5. Profiling & Chargeback
6. Proactive Baselining
7. Compliance
8. Verify Policy
9. Optimize & Consolidate
10. Keep service provider honest.

“... The network never stops growing and it never gets a rest ...”

Purdue University Network Mapping Project
Scalability: Don’t underestimate scaling needs when capturing flow data. Scalability is an important aspect to appreciate when comparing tools. NetFlow Auditor can handle copious amounts of flows per second and therefore key data won’t be missed when pipes burst or when flows increase.

Granularity: it is critical to have the ability to see Network data in all perspectives. Network traffic is very dynamic and new traffic behavior can be tricky to track. NetFlow Auditor provides complete drilldown tools to fully explore the data and to perform Comparative Baselining.

Flexibility: An inflexible tool limits ability to create relevant outputs for engineers, management and customers and can increase workload rather than decrease it. NetFlow Auditor allows easy customization of every aspect of the system from tuning of data capture to producing templates and automated Reporting and Alerting.
Network Auditing: Companies are challenged with maintaining too many tools that all show a slightly different view of the same data. Often with limited Visibility. Hence the need for a convergent toolkit.

Capacity Planning
Accounting
Rising IT Costs
Exponential Bandwidth Growth

Security Surveillance
Lockdown
Intensifying Security Concerns

QoS
Business Intelligence

Knowledge

Copyright 2009 IdeaData Pty Ltd
How can Netflow Forensics and Anomaly Detection help me in Security?

- **Botnets**
  - Have the visibility to identify all computers who are communicating on IRC channels to IRC Servers.

- **DDoS**
  - Identify rising thresholds outside of learnt baselines. Find all IP’s and port patterns to divert and derisk.

- **SlowDoS**
  - Identify long-talkers holding up your server threads.

- **P2P**
  - Identify P2P conversations and shadows.

- **Data Leaks**
  - Counter Surveillance. Find systems that are slowly copying their data outbound.
Flow-Based Network Intelligence ROI

### Business ROI

- Flow Based technology provides huge reduction in time and costs spent understanding, alerting and reporting on network issues.
- The information is required by many groups from Security and Performance teams to Capacity planners and Accountants.
- Real-time visibility **AND** Archive/Reporting
  - Act on issues as they occur or track and trace with historical forensic insight.
  - Hindsight gives you visibility to forecast

### Technical (IT) ROI

- Already inbuilt in Cisco IOS or other Vendor OS
- No Probes
- No Appliances
- Non Intrusive
- Scalable
- Ease of Deployment
- Handles Moves, Adds, Changes Easily
- Historical and Real-Time Information Wanted/Used by Many

Copyright 2009 IdeaData Pty Ltd
How Does Netflow work?

1. Conversations “flow” through the network.
2. Flow records are sent to NetFlow Auditor.
4. Data is analyzed for real-time troubleshooting.
5. Data is analyzed over long-term for capacity planning and network baselining.
6. Automated alerts are configured and sent.
7. Custom reports are created, scheduled and delivered.
The Architecture is modular and scalable

NetFlow Auditor was built from the ground up for scalability and utilizes scalable intelligent agent technologies (Bots) to manage large amounts of network traffic information in real-time.

NetFlow Auditor Agents

- Collect, tag and process data as the data passes through a nominated gateway.
- Pass collected data between one another and the NetFlow Auditor database.
- Can continue to function if separated from the data warehouse.
NetFlow Auditor licensing
Performance, Professional or Enterprise

We know that customers needs are different at different times and NetFlow Auditor therefore comes in three scalable license tiers. A simple license change means that our customers investments are safe. So if budget only allows a small start, we provide the very best small start in the industry and the ability to add granularity and features.

**Our Performance license** scales well beyond other products in the NetFlow arena and is designed to provide only real-time functionality with Top Analysis data in line with the other NetFlow products.

Our Performance license offers an low-cost-entry option that still goes deeper in granularity than competitors and can still handle hundreds of devices.

Enterprise license can also be coupled with Performance for fast ISP troubleshooting.

**Our standard “Professional” license** provides a complete view of all the traffic and 100% raw flow capture. It enables you to have intelligence, anomaly detection capability and perform NetFlow Forensics far beyond any other NetFlow tool and includes intelligent baselining and long-term trending and also includes the ability to measure 95th percentile to 5 minute intervals for a month.

**Our Enterprise license** is Telco grade for very large flow captures. Options are available for service providers such as ISP’s Telco’s or Campuses who need a highly fault tolerant solution and for environments that have millions of flows per second.
Flow-Based Network Intelligence you can depend on
NetFlow Auditor Smart Investment
Grows as your needs grow

Anomaly Detection Add-on
- Learns Baseline and Alerts when traffic deviates on link, servers, services P2P profiling, DDoS, ICMP, DNS, QoS, Nefarious Traffic.

Scalable Flow Capture
- For very high-flow capture
  - Coupled with Professional 100% Full Flows for full compliance and billing
  - Coupled with Performance Supports very high-flow environment for real-time root cause analysis

Security / Compliance
- Forensics
- Comparative Baselining
- QoS
- 95th Percentile Billing
  - 100% Full Flow forensics, Supports Detailed Anomaly Detection and 95th Percentile or usage based Billing.
  - Comprehensive Network Behavior Anomaly Detection from intelligently learnt baselines.

Root Cause Analysis
- QoS Billing
  - Top Traffic.
  - Supports Anomaly Detection on top traffic.
  - Couple with Enterprise for high-flow eg ISPs

Troubleshooting
- QoS
  - Hot Top Traffic.

Bandwidth Utilization
- Interface
NetFlow Auditor Unique Capabilities

- Comparative Baselining
- Real-Time Forensic Analysis
- Network Behavior Anomaly Detection \textit{option}
- Long-Term trending
- Event alerting by Time of day and thresholds
- Highly flexible exceed and degrade threshold capability
- Learn traffic baselines
- Collection Tuning

- Unattended Alerting and Reporting
- Flexible Filters
  - Root Cause Analysis
  - Security Forensics
  - Performance Analysis
  - Data Center Analysis
- Multi-device Correlation and De-duplication
- 95th Percentile
- Scalability in collection
- Self Healing

Scalability, Granularity, Flexibility