# NETWORK INTELLIGENCE OPTIMIZATION:
# Breakthrough ROI for Network Intelligence Tools

Overview Brief

## Defining "Network Intelligence Tools"

***"Network intelligence tools"*** *are network appliances and probes that passively or actively increase the performance and/or the security of network infrastructure, services, and applications within enterprise, government or service provider environments.*

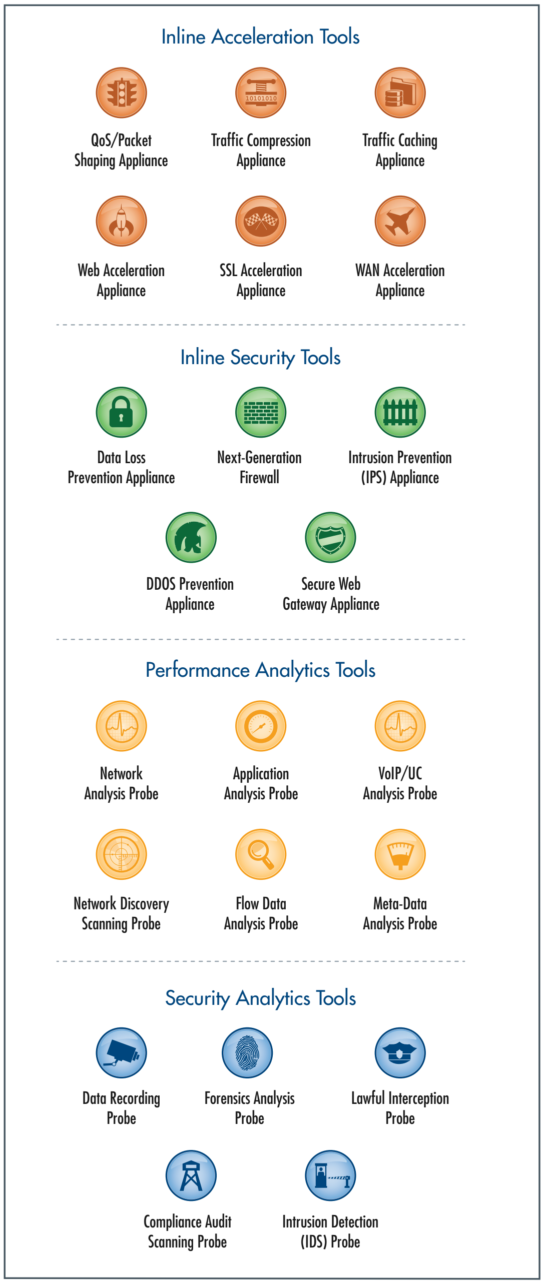
Inline Acceleration Tools
QoS/Packet Shaping Appliance
10101010
Traffic Compression Appliance
Traffic Caching Appliance
Web Acceleration Appliance
SSL Acceleration Appliance
WAN Acceleration Appliance
Inline Security Tools
Data Loss Prevention Appliance
Next-Generation Firewall
Intrusion Prevention (IPS) Appliance
DDOS Prevention Appliance
Secure Web Gateway Appliance
Performance Analytics Tools
Network Analysis Probe
Application Analysis Probe
VoIP/UC Analysis Probe
Network Discovery Scanning Probe
Flow Data Analysis Probe
Meta-Data Analysis Probe
Security Analytics Tools
Data Recording Probe
Forensics Analysis Probe
Lawful Interception Probe
Compliance Audit Scanning Probe
Intrusion Detection (IDS) Probe

*Figure 1. Classification of Network Intelligence Tools*

## *Introduction*

As enterprise IT migrates to new technologies ranging from virtualization to cloud computing, the focus increases on making networks flatter, faster, and more efficient. The network must adapt with faster pipes to handle ever-increasing traffic volumes as well as with more sophisticated network intelligence to meet the expected levels of network performance and security amid growing complexity.

Enterprises continue to make significant investments in network intelligence tools – network appliances for monitoring, security, or acceleration. The deployment growth of these tools has been particularly dramatic over the past five years – it is now a $15 billion market worldwide, accounting for about 20% of total network spend. But with the explosive growth of traffic and the networks themselves, there are growing constraints as to what these tools can do. Whether for improving performance or security, these tools require IT Operations to monitor, capture and examine the actual network traffic in depth. As networks get flatter, there is more traffic at each monitoring point. IT Operations also faces a greater challenge to get that traffic to the increasing number of tools.

Despite these growing requirements, tight budget and resource constraints have become the norm. So what are innovative IT Operations groups doing? In short, they are meeting expected levels for quality of experience (QoE) with a breakthrough return on investment (ROI) for their tool investment by deploying new approaches to real-time performance analysis, security enforcement, WAN acceleration, provisioning, and problem resolution.

## Evolution of Tools Poses Growing Network Challenges

On one hand, the variety of tools have evolved to help IT Operations teams better manage network resources, providing detailed traffic analysis, traffic acceleration, and security enforcement. It would be ideal to deploy tools on every link in the network. In this way, a passive tool can be "hard-wired" and dedicated to a network link using a basic network test access point (TAP) device or by connecting to a mirroring port or SPAN port on a network switch. An active tool can be hard-wired inline on a network link.

On the other hand, significant technical and economic challenges prohibit tool deployment on a "1:1" basis with network links across the entire network environment. Referring to this 1:1 approach of tools and links as depicted in Figure 2 below, let's examine several major challenges that arise from this approach, causing network blind spots, vulnerabilities, and excessive costs.

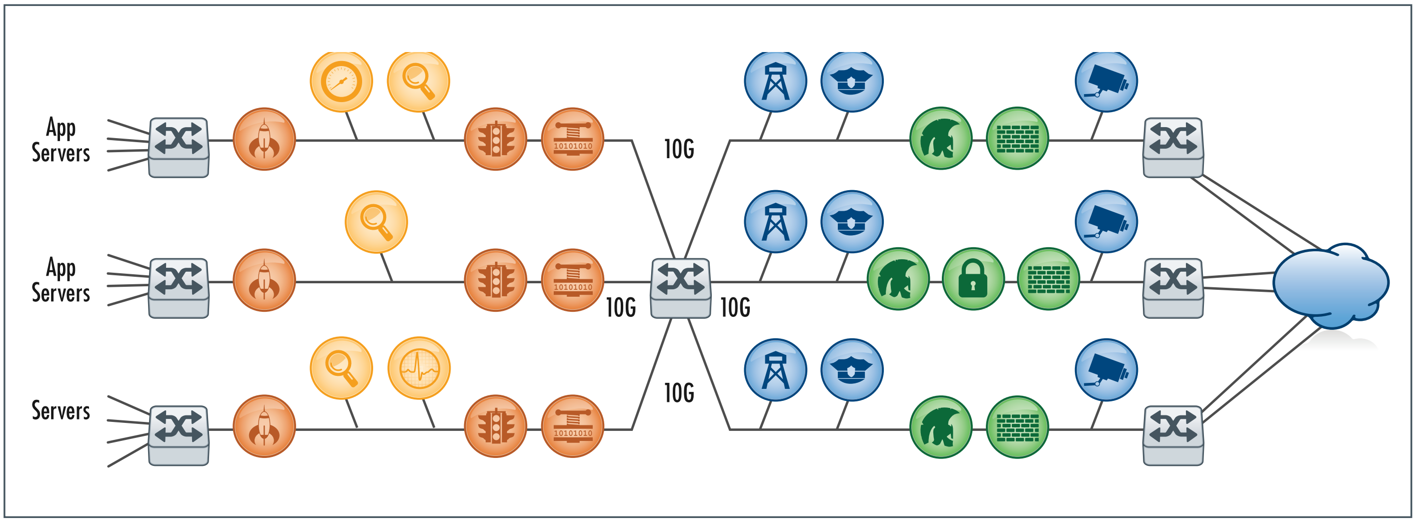

*Figure 2. Fragmented monitoring approaches create further performance and complexity problems*

## SPAN Port Contention and Limited Network Access

The most obvious problem to IT Operations is the inability of multiple tools to access a particular point in the network. A passive tool can collect traffic through a mirroring or SPAN port of a network switch. But if multiple tools are contending for access, there are often not enough SPAN ports to go around, or there is simply no SPAN port available. Moreover, while a SPAN port seems to be the solution to accessing traffic, it has several serious data quality pitfalls:

- Lowest priority in a switch's routing hierarchy; a SPAN port is subject to packet loss
  and possible shut down during peak traffic periods.
- Packet duplication as SPAN ports will commonly duplicate packets that traverse the switch,
  copying from both the ingress and egress points.
- Increasing contention as switches are configured for maximum network throughput,
  reducing the number SPAN ports to networking ports.

The alternative is to use a basic network test access point (TAP) device that effectively copies all traffic in both directions to the tool. However, similar to troubleshooting with a portable test set, gaining physical access to the premise may be prohibitive. For other reasons, such as network speed, footprint, power supply or other mission critical requirements, a basic TAP device may simply be not viable. Both options still result in network "blind spots."

## Tool Oversubscription

To grow network capacity and ever-increasing traffic volumes, IT Operations is adding 10G network links – and beyond. Existing 1G tools are likely to be oversubscribed on 10G links, even if traffic utilization is far below the 10G line rate. The line rate mismatch and the tool's limited processing speed limits the 1G tools use on a 10G link. But 10G tools are prohibitively expensive, and can be overkill on links with relatively low utilization, particularly if existing 1G tools could be re-appropriated, extending their life and helping to minimize tool related expenses.

## High Management Overhead

As shown in Figure 2, the multiple sets of tools are scattered across the network in different physical locations. Each vendor's tools have their own suite of analysis software, which is often not interoperable with other vendors'. If a network configuration change were to take place, the management, reconfiguration and updates of this large number of tool appliances would be overwhelming. Even if basic TAP devices are available to provide access, and minimize the number of "blind spots," the TAP devices are isolated devices with little to no awareness of other network devices and events.

## High Cost

With the configuration and layout of the tools such as those in Figure 2, much of the tool processing resource sits idle, particularly on lower utilized links. Unused tool resource can't be aggregated and reapplied to additional network links or to links with higher traffic utilization. As a result, the tool CAPEX of the inefficiently deployed solution would be substantial, and the OPEX to manage the tool solution could easily become out of control given the management complexity to maintain the sheer quantity of tools.

Tool deployment on a "1:1" basis with network links increases cost and reduces ROI as it requires multiple expensive devices deployed across network boundaries, creating further complexity, performance issues and management overhead.

The enterprise needs to capture the right traffic at the right points in the network, transport this large volume of traffic without compromising network performance and security, and distribute the traffic to the right tools. The best way to do this cost effectively is to add a network intelligence optimization layer as an integral part of the network architecture, managing the connection between the tools and the network.

## Network Intelligence Optimization

As we have seen, responding to the challenge of rapid network evolution by simply deploying more tool application at more network points is simply not scalable. The solution must be future-proof, efficient and adhere to tight operating budgets. With Network Intelligence Optimization, the overarching vision for network monitoring, security, and acceleration is ***visibility, scalability, and efficiency***. This network-wide platform of intelligent optimization devices, acting as a single system for distributed traffic capture, is designed with building block simplicity, able to start small and evolve with network growth. As shown in Figure 3, the Network Intelligence Optimization framework decouples the tools from the network infrastructure, and creates a single traffic capture and distribution layer that is universal to all tools. This is the only way to achieve the goals of network **visibility**, **scalability** and **efficiency**.

## *Self-Discovering Network Intelligence Optimization Layer*

A network intelligence optimization system acts as a universal access layer for all the tools, agnostic to the type of tools as long as they are interested in IP traffic.

The individual system components interconnect with, and auto-discover one another, to interact together as a single system. Within this system, the components in mesh configuration are self healing – traffic routing is optimized from any port to any port within the system depending on the component level utilization. The performance and capacity of the system can be as much as an order of magnitude larger than the components themselves alone.

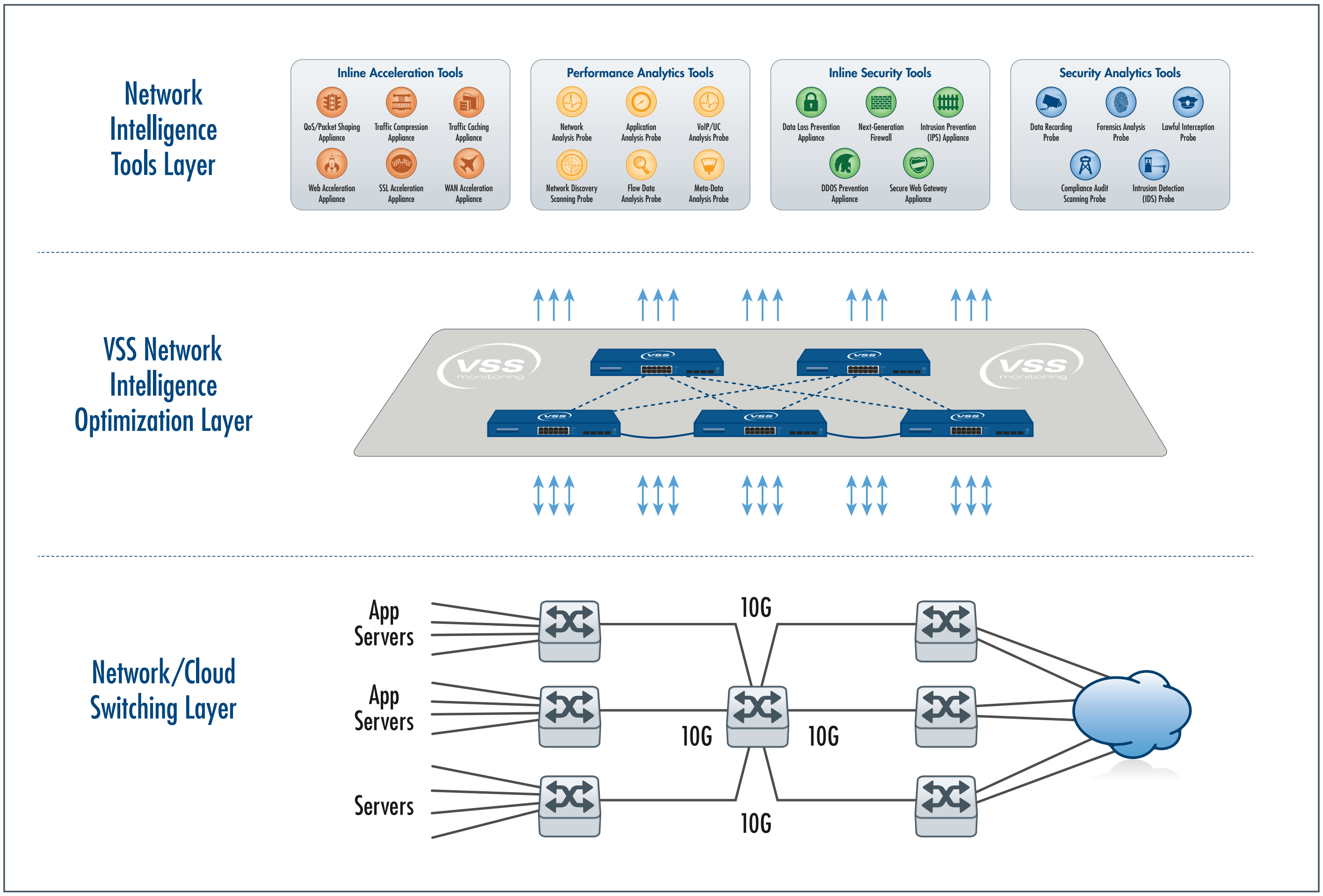
Network Intelligence Tools Layer
Inline Acceleration Tools
QoS/Packet Shaping Appliance
Traffic Compression Appliance
Traffic Caching Appliance
Web Acceleration Appliance
SSL Acceleration Appliance
WAN Acceleration Appliance
Performance Analytics Tools
Network Analysis Probe
Application Analysis Probe
VoIP/UC Analysis Probe
Network Discovery Scanning Probe
Flow Data Analysis Probe
Meta-Data Analysis Probe
Inline Security Tools
Data Loss Prevention Appliance
Next-Generation Firewall
Intrusion Prevention (IPS) Appliance
DDOS Prevention Appliance
Secure Web Gateway Appliance
Security Analytics Tools
Data Recording Probe
Forensics Analysis Probe
Lawful Interception Probe
Compliance Audit Scanning Probe
Intrusion Detection (IDS) Probe
VSS Network Intelligence Optimization Layer
VSS monitoring
VSS monitoring
Network/Cloud Switching Layer
App Servers
App Servers
Servers
10G
10G
10G
10G

*Figure 3. Network Intelligence Optimization system central to simplifying and optimizing network monitoring solutionand complexity problems*

The system can be custom-fitted and scaled to the attributes of each individual network (size, speed, media type, physical environment, number of network interface, types of traffic, number/type of tools supported, etc.).

## *Limitless Network Visibility*

Whether the IT group is centralizing their network intelligence tools or the tools will remain distributed throughout the network - LAN, WAN, or across the Cloud - the network intelligence optimization system in Figure 3 will provide complete visibility to the tools. Network "blind spots" can be eliminated because there is no more SPAN Port contention as the tools access traffic from the network intelligence optimization system. Captured and groomed traffic maintains a centralized view of the network, regardless of physical location of the tools.

The immediate impact of the unprecedented network visibility is simplification of the network architecture, and a significant reduction in number of tools and consequently the management overhead. True end-to-end troubleshooting is now possible, resulting in much reduced response time to outage and repair (e.g. MTTR).

## *Increase Tool ROI*

The intelligence of the system filters and grooms traffic to dramatically improve the efficiency of the tools. Many tools are application-specific, which means they are only interested in certain types of IP traffic coming from certain parts of the network. Selective hardware-based filtering, high data burst buffers and session-aware load balancing as seen in Figure 4 ensure that tools receive only the specific traffic they need to see (e.g. from specific VLANs), and that no packets are lost to due to oversubscription.

## *Reduce Tool Cost*

With a network intelligence optimization system between the tools and the network infrastructure, instead of a 1:1 ratio of tools to network links, network operations can monitor several links or the entire network with a single tool. This dramatically reduces the Capital Expenditure (CAPEX) needed to completely cover the network.

In addition, with the ability for a tool to receive only the traffic of interest, 1G tools can work with 10G network links. They no longer receive all network traffic, they receive only the required traffic at full line rates. The tools therefore can continue to perform effectively and accurately for a higher speed link. This defers or eliminates the need to purchase costly 10G tools.

It is also common that multiple same tools are interesting in subsets of the same traffic type. Here, ***session awareness*** in the system allows traffic to multiple tools to be ***load balanced,*** so that each tool can analyze the entire session or conversation accordingly. The session-aware load balancing of high speed traffic to lower speed tools (e.g. from 10G to 1G) provides better quality data to the tools.

## *Lowest Cost of Ownership*

The network intelligence optimization systems can scale with the evolving network needs simply by adding in more nodes as shown in Figure 4. The overall solution cost of the network intelligence optimization layer is substantially lower than a non-systematic approach to deploying large number of tools. Lower management overhead, shorter time to troubleshoot network anomalies and repair mean further reduction in operating costs, faster ROI, and the ability to meet SLAs.

## *Defense in Depth*

The defense in depth information assurance strategy uses multiple layers of defense, placed throughout the network and data centers. No single system can tackle emergent, evolving cyber threats. The security in layers or defense in depth approach defends the data center against any particular attack using several, varying methods. To implement this defense, it's necessary to gain complete network visibility and be able to optimize the traffic data at origin and filter out the types of data that are of no concern for cyber security tools.

This approach allows next generation firewall or IPS systems, in conjunction with email and web threat prevention systems, to detect the traffic relevant to its unique function - without becoming overloaded having to filter out the irrelevant data. In fact, with a network intelligence optimization layer, traffic can pass through several in-line security tools (i.e. Security In Layers) maximizing their throughput capabilities.

## *Reduce Time to Protection and Lower Costs*

As a vital part of our national and corporate welfare, new network security solutions must be rapidly evaluated and deployed to reduce the time-to-protection against cyber-threats, accelerate technology adoption, and lower cost of operations.

Deploying an in-line security appliance in a mission critical network is a concern for Network Operations, who fear the risk of network outage. The VSS Network Intelligence Optimization System allows testing of new security tools to be conducted in a systematic and error-free way. All network traffic can be sent to new tools, and multiple tools for efficient testing, allowing the InfoSec team to verify proper security protection without network outage or degradation.

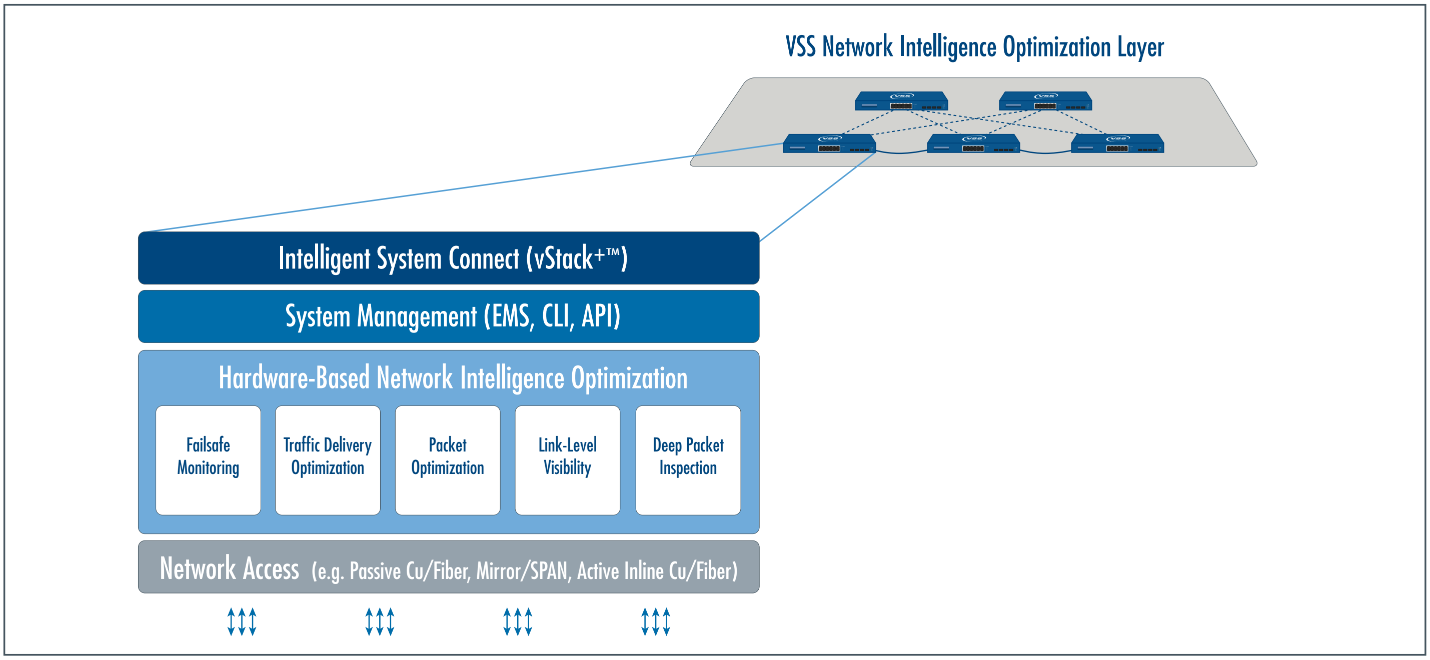
VSS Network Intelligence Optimization Layer
Intelligent System Connect (vStack+™)
System Management (EMS, CLI, API)
Hardware-Based Network Intelligence Optimization
Failsafe Monitoring
Traffic Delivery Optimization
Packet Optimization
Link-Level Visibility
Deep Packet Inspection
Network Access (e.g. Passive Cu/Fiber, Mirror/SPAN, Active Inline Cu/Fiber)

*Figure 4. Intelligence Optimization Capabilities Provided by Network Intelligence Optimization Systems*

## Conclusion – Anticipating the Future

Where does the roadmap of the Network Intelligence Optimization vision lead to? How will the network architecture evolve? This paper offers a perspective on a layered approach to viewing the network infrastructure, by decoupling the network monitoring tools and creating a Network Intelligence Optimization System layer that is much more elegant, cost effective and flexible to scale with the core network.

While there is no one correct answer to the earlier questions, the key for enterprises (large scale enterprises, small scale enterprises, educational institutions or government) is to develop a holistic and forward-looking strategy for network monitoring and network management. More importantly, they must consider carefully the price-performance, diversity, agility and intelligent capabilities of a traffic capture solution. By adopting the Network Intelligence Optimization framework, network monitoring is no longer an ancillary thought.

## About VSS

VSS Monitoring, Inc. Is the world leader in network intelligence optimization, providing a visionary, systems-oriented approach for optimizing and scaling connectivity between network switching and the intelligence ecosystem of network analytical, inline security and WAN acceleration tools. VSS network intelligence optimization systems improve tool usage, simplify operations, increase efficiencies and greatly enhance ROI. The company is headquartered in San Mateo, Calif. For more information, visit www.vssmonitoring.com.

## Acronyms

CAPEX – Capital Expenditure
IDS – Intrusion Detection System
IPD – Intrusion Prevention System
KPI – Key Performance Indicator
MTTR – Mean Time To Repair
OPEX – Operating Expenditure
QoE – Quality of Experience
ROI – Return On Investment
SLA – Service Level Agreement
SPAN – Switched Port Analyzer
TAP – Test Access Point

Network Visibility. Optimized.

USA
(Corporate HQ)
+ 1 650 697 8770 phone
+ 1 650 697 8779 fax
1850 Gateway Drive - Suite 500
San Mateo, CA 94404
USA
www.vssmonitoring.com

Japan
+ 81 422 26-8831 phone
+ 81 422 26-8832 fax
T's Loft 3F, 1-1-9,
Nishikubo, Musashino,
Tokyo, 180-0013
Japan
www.vssmonitoring.co.jp

China
+ 86 10 6563-7771 phone
+ 86 10 6563-7775 fax
C519, 5 Floor,
CBD International Tower
16 Yong'An Dong Li,
Beijing, China 100022
www.vssmonitoring.com.cn

VSS Monitoring, Inc. is the world's leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.