Nine Ways to Rapidly Deploy, Scale and Optimize DPI Solutions with Confidence using VSS Monitoring

Deploy

1) Deploy network intelligence tools in controlled phases
2) Cover network blind spots with best of breed network intelligence tools
3) Help meet regulatory compliance and IT governance requirements

Shorten POC Cycles

Drive more efficient and effective POCs for DPI and Security tools

Challenges: Today, POC cycles can be lengthy, risky and consume many IT and network operations resources – all of which delay the time to deployment and protection against emergent cyber threats

Solution:

- Cable once and evaluate one or more systems at a time, installed inline via software configuration
- Shorten POC cycles with minimum operational overhead, dramatically reduced outage window
- Run POCs for multiple security and DPI tools in parallel
- Reduce the potential risk to your environment during POCs
- Validate new tools with live traffic
- Remove uncertainty when moving from POC to production

Scale

4) Gain borderless visibility across LAN, WAN and the Cloud
5) Extend investment in 1G tools
6) Easily scale network intelligence and DPI solutions beyond 80 Gbps for Inline tools and virtually limitless for Passive tools

Cover and Protect Network Blind Spots

Support Mixed 10G and 1G Environments

Challenges: Networks are growing beyond 1G at alarming rates - leading to oversubscription of 1G tools, a mismatch between 1G and 10G speeds and media, and an increased level of traffic saturation (VoIP, Video, Data). IT security teams must aggregate multiple compartmentalized network segments while retaining integrity of individual security zones and adhering to various regulatory compliance requirements (PCI, ITAR, HIPAA).

Solution:

- Gain Universal, always-on access
- Deduplicate and defragment packets, and deliver only actionable data to each tool with hardware-based L2-L7 filtering
- Enable intelligent session aware load-balancing among multiple inline and passive tools
- Increase scalability for network security and DPI architecture with HA and fault tolerance for your tools
- Share access between Inline active and Passive security and intelligence tools

Optimize

7) Maximize efficiency of DPI Tools with distributed DPI-preprocessing
8) Gain Security Information and Intelligence Acceleration
9) Only send Actionable Information to your Security and DPI tools

Implement Best of Breed Network Intelligence

Optimize your DPI Infrastructure

Challenges: Emerging cyber-threats require new layers of cyber defense. Security teams need to be able to confidently add new scalable layers of security and visibility with minimal change and risk to the production environment as well as only send traffic of interest to each security

Solution:

- Perform stateful data acquisition with application layer intelligence to rapidly find the critical information that you need to analyze with your Security and DPI tools.
- Implement active-active load-balancing to achieve High availability with customizable fault-tolerance options
- Enable intelligent hardware-based filtering and inline fail open/fail close bypass options
- Optimize your network intelligence and cyber-defense through a highly scalable and efficient layered security model

www.vssmonitoring.com | + 1 650 697 8770 phone | 1850 Gateway Drive - Suite 500, San Mateo, CA 94404 USA

ObjectFinder™

Real-Time Specialized DPI

ObjectFinder 1023 | ObjectFinder 2022

Benefits

- Precise, needle-in-a-haystack filtering for Lawful Intercept, Fraud Prevention, and Ultra-Sensitive Perimeters
- Stay close to the source at Line-rate keeping data fresh and pro actionable
- Stay compliant by ensuring "clean" searches for authorized target data capture
- Allow use of Gigabit inline tools with 10 GigE Networks
- Spread traffic across multiple instances of same tool
- Reduce load on monitoring tools
- Easy to install and manage
- Local and Remote management

Features

- Intelligent Speed Conversion (10 GigE/Gigabit)
- Full line-rate traffic searching and redirection
- Low latency
- Session-Aware tool load balancing
- Inspect Gigabit and 10 GigE inputs at Full Line-rate
- Simultaneously Track and Forward for Monitoring up to 65,535 Unique Streams or IP/Port Bindings
- Content Matches Can be Used to Tag Specific Streams or IP/Port Bindings for Further Monitoring
- Update and Modify a Running Engine Without Loss of Monitored Data
- No Storage of Transiting Data in Non-Volatile Memory
- Selective Aggregation
- Intelligent stacking with vStack+™
- Access via Command line, Web browser, and SNMP
  - SSH/Telnet and HTTP/HTTPS for management
  - SNMPv3 with RMON for reporting
  - RADIUS and TACACS+ for AAA security
- Supports full Distributed Traffic Capture System capabilities on non-ObjectFinder ports
- In-field upgradable

Deep Packet Inspection

VSS Monitoring is at the forefront of deep packet inspection coupled with traffic capturing technology to help end-users get the most from their security monitoring and analysis tools. ObjectFinder is a hardware-based deep packet inspection and filtering platform that performs specialized line-rate traffic search and capture.

The ObjectFinder product series allows users to find specified objects (E-mail/IM addresses, currently) within a packet, which can then be coupled with source and destination data (and/or other criteria) to create a precise framework for matching and retrieving live network traffic for security and monitoring applications.

The ObjectFinder can also simultaneously support passive monitoring and analysis tools, if required, as well as selective aggregation, hardware-based filtering, and session-aware load balancing.

Product Description

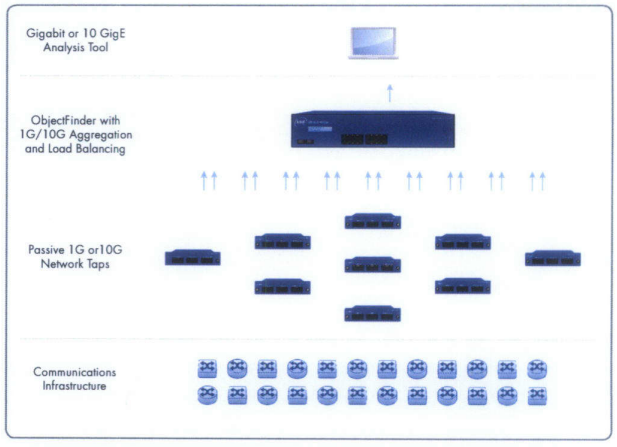
The ObjectFinder allows real-time deep packet inspection, load balancing, aggregation, and grooming of traffic from 10 Gigabit networks using one (ObjectFinder 1023) or two (ObjectFinder 2022) of its twenty-four ports. The ObjectFinder is designed to scale to any size deployment for virtually any budget. The product ships with four fixed LC ports and twenty SFP+ sockets. Four ports are enabled by default, and the remaining twenty ports may be enabled using a license key from VSS Monitoring for Gigabit or 10 Gigabit networks or monitoring tools. Except for the one or two ObjectFinder ports, all ports are independently controllable and flexible, allowing the operator to designate any port as input, output, or a stack port.

Intelligent Speed Conversion

Real-time conversion of speed enables one or multiple Gigabit tools to be deployed on a 10 GigE network. The ObjectFinder converts all packets for matched flows from a 10 GigE network to Gigabit and forwards these out to the monitoring tool.

Session-Aware Load Balancing

The distribution of traffic across groups of tools can be defined by the user so that session consistency is maintained for each tool. Once session criteria have been defined, based on the available options, the traffic is automatically (dynamically) load balanced across the monitor ports. Load balancing can be conducted over a group of monitoring tools that are connected to multiple different ObjectFinder units, using VSS Monitoring's vStack+ technology.



Capabilities

ObjectFinder detects user-specified email or IM addresses from anywhere within an TCP/IP packet carried over Ethernet. Upon detection of an object (i.e. an email address), ObjectFinder will lock onto the user's related session, by way of IP address and TCP port number, and transfer the entire session to the target monitor port(s) where the session is then externally forwarded to an analyzer or storage device.