



Nine Ways to Rapidly Deploy, Scale and Optimize Security Solutions with Confidence Using VSS Monitoring

Deploy

- 1) Deploy inline tools in controlled phases
- 2) Extend current investment in 1G tools
- 3) Comply with regulations

Shorten POC Cycles

Drive POCs for Inline Security Solutions without Fear

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

Solution:

- Cable once and evaluate one or more systems at a time
- Install inline via software configuration rather than physical
- Minimize operational overhead
- Reduce the need for outage window
- Shorten POC cycles
- Run POCs for multiple tools in parallel
- Reduce the potential risk to your environment during POCs
- Validate tools transparently with live traffic
- Remove uncertainty from POC to production

Scale

- 4) Gain complete, multi-segment network visibility
- 5) Achieve high availability for security tools
- 6) Easily scale security solutions beyond 80 Gbps for Inline tools and virtually limitless for Passive Tools.

Protect Multiple Security Zones

Support Mixed 10G and 1G Environments

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

Solution:

- Speed media conversion between 10G and 1G tools and networks
- Enable hardware-based filtering (L2-L7), selective aggregation, and intelligent session-aware load-balancing among multiple inline and passive sensors
- Increase scalability for network security architecture
- Increase tool performance, efficiency, and availability
- Fully redundant and self-healing mesh architecture (up to 63 connected devices)

Optimize

- 7) Maximize efficiency of security tools
- 8) Maintain inline tools without service impact
- 9) Add best of breed security in layers with confidence and achieve defense-in-layers.

Implement Best of Breed Network Security in Layers

Rapidly Architect, Validate and Deploy Defense-In-Layers

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

Solution:

- Implement active-active load-balancing, HA and customizable fault-tolerance configurations
- Enable intelligent hardware-based filtering and inline fail open/fail close bypass options
- Deliver a true defense-in-layer solution deployment
- Maximize operational efficiency
- Optimize network security and cyber-defenses through a highly scalable and efficient layered security model