Solution Overview

Highlights

- Validated and certified high-scale network Flow Sensor for Cisco Secure Network Analytics (Stealthwatch)
- Simple, software-defined FPGA-powered architecture provides high-density, wire-speed 10, 40, 100 and 400G monitoring
- Seamless integration into Cisco Secure Network Analytics monitoring architecture and into Cisco SecureX unified workflows
- 1:1 unsampled metadata feeds into Cisco Flow Collectors consistent with network devices and Cisco Flow Sensors
- Passively monitors traffic in real-time at wire-speed via TAP or SPAN connections
- Generates accurate Flow data for segments where network equipment is unable to provide NetFlow
- Off-loads NetFlow generation burden from critical network devices
- Optional Advanced Packet Processing services eliminate redundant tools and accelerates ROI

cisco Partner

NetQuest

NetQuest 100G Flow Sensor for Cisco Secure Network Analytics

Cisco Secure Network Analytics (Stealthwatch) is a comprehensive Network Detection and Response (NDR) solution that collects, aggregates, and analyzes network-wide telemetry to detect and respond to security threats. The solution observes and continuously analyzes network, application, and user activity to create a baseline of normal network behavior to proactively identify anomalies and respond to threats in real-time.

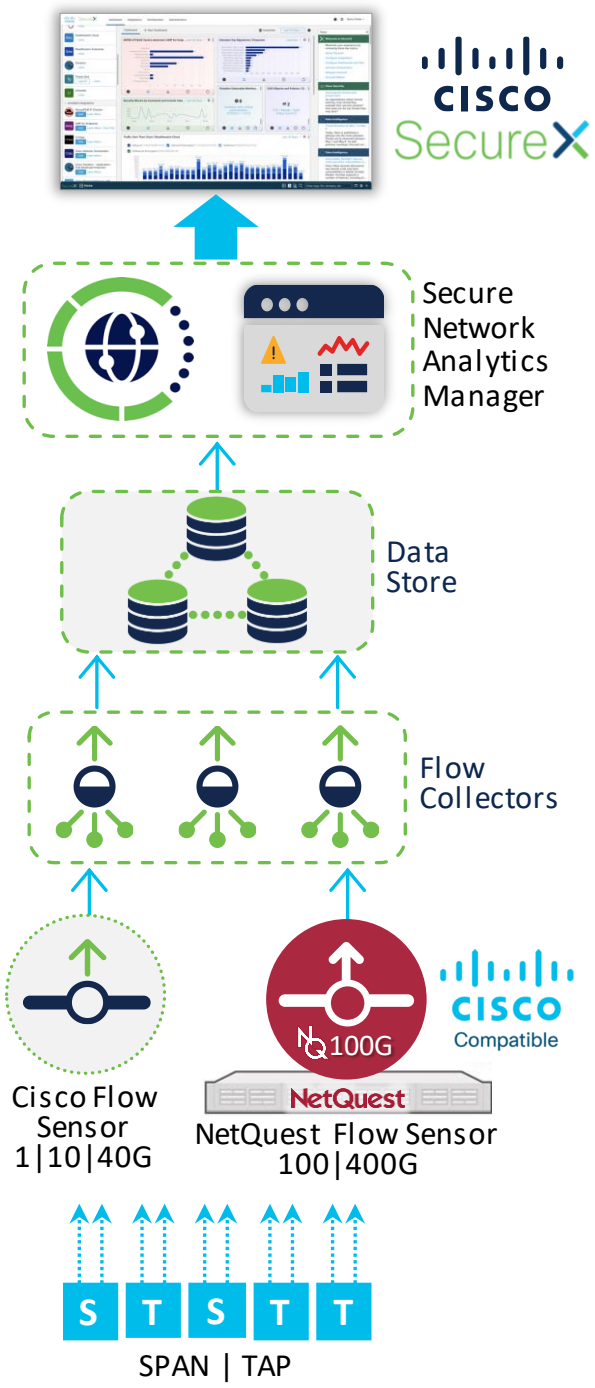
Everything touches the network. Consequently, achieving end-to-end visibility across the entire network to see all traffic in motion is crucial to an effective security strategy. Acquiring and analyzing network packets provides deep context into network traffic and behavior, but collecting and analyzing every network packet comes with a significant processing burden, massive storage requirements and high costs. Based upon network wire data, Flow-based metadata extracted from network packets is a rich, high-value, lower footprint data source that provides valuable insights about who is connecting to the network and what is being accessed without the burden of collecting and storing high volumes of packets. Context-rich metadata data can detect emerging threats and identify high-risk behavior from hostile insiders that may have bypassed existing controls with relevant context. This knowledge empowers the security team to proactively respond to high probability threats before they can have a major impact.

High-Performance 100G Flow Sensor for Cisco Secure Network Analytics

OMX3200™ is an FPGA-based appliance purpose-built to deliver wire-speed unsampled Flow metadata and advanced packet processing services for high-performance 100G and 400G monitoring environments. Its software-defined architecture enables multiple operational modes on the same hardware for unmatched operational flexibility and investment leverage. The platform's unique distributed architecture, with multi-stage pipeline processing, delivers sustained performance at scale for the most demanding network environments.

The NetQuest 100G Flow Sensor scales-out to support from four to 16 100G links per chassis in a single rack unit (RU), allowing in-place expansion for additional 100G or 400G ports as needed. To facilitate comprehensive network-wide visibility, the OMX provides flexible packet access with interface support for 10, 40, 100 and 400G Ethernet and for WAN traffic, including OTN and SONET/SDH with automated discovery and integrated transcoding.

When deployed as a 100G Flow Sensor, OMX3200 seamlessly integrates into the Cisco Secure Network Analytics architecture to bring high-scale, cost-effective network segment visibility. Cisco validated and certified, the NetQuest 100G Flow Sensor produces accurate and granular network telemetry and can be deployed alongside Cisco 10G and 40G Flow Sensors to achieve uncompromised visibility with relevant context and consistent metrics to enhance security analytics.



Flow Data Where It's Needed

The Flow Sensor passively acquires network traffic via a network TAP or a mirroring (SPAN) port and generates metadata based on observed traffic in real-time. OMX3200 is an ideal complement for network segments where the switching and routing infrastructure can't generate NetFlow or when it is desirable to off-load intensive NetFlow processing impacts from performance-sensitive switches and routers. Optional advanced services, such as wire-speed packet-flow delivery for packet-based tools, and application-level metadata from the same sensor leverages investments, eliminates redundant tools, increases platform value, and accelerates ROI.

IPFIX Metadata Creation and Delivery at Scale

OMX3200 delivers up to 1.6 Tbps of IPFIX traffic processing per system. Its high-scale, distributed processing enables metadata creation for up to 800 million active flows per sensor (50 million per interface) with performance predictability across modules. Wire-Speed Deep Packet Inspection enables IPv4 and IPv6 traffic analysis inside tunnels and packet headers to reveal the inner IP payload for comprehensive metadata creation. OMX3200 provides 1:1 unsampled Flow metadata with 100% of all traffic processed for uncompromised security intelligence. For environments requiring lower volume of metadata analysis, intelligent sampling can be leveraged to reduce the metadata output volume.

Metadata is delivered to Cisco Secure Network Analytics Flow Collectors upon flow completion in a consistent manner as Cisco Flow Sensors, so no customization is required. OMX3200 offers user-definable ingress filtering, reducing the need for Packet Brokers or SPAN traffic filtering, off-loading the processing burden from network devices.

OMX3200 provides configurable load balancing to manage and scale metadata delivery and can deliver metadata to 16 collectors. Metadata outputs can be delivered to multiple monitoring platforms and/or segregated into pre-defined groups to optimize upstream collection and analysis. In addition, metadata output can be filtered to target delivery of the specific metadata of interest to reduce noise and minimize the upstream data collection burden.

Extensible Optional Advanced Services

To meet a broad range of monitoring requirements, OMX3200 can also be leveraged to deliver packet flows and enriched metadata to diverse security tools from a single-point-of-instrumentation (TAP or SPAN) without performance impacts. With flexible deployment modes, the software-defined platform enables mixing services per module to meet diverse monitoring requirements. Advanced services are software-enabled and extend the value of the platform while reducing TCO and operational complexities associated with managing multiple probes, sensors, and Network Packet Brokers.

Advanced Packet Processing

When packet-flow traffic is needed for capture and analysis activities, the OMX3200 can deliver live packet traffic to separate tools using the same ingress network traffic for Flow metadata creation. This traffic can be delivered as collected or can be groomed and conditioned to deliver targeted and relevant packet-flows similar to a Network Packet Broker.

Advanced Packet Processing is enabled via software licenses on the same hardware. Metadata creation and advanced services are applied to monitored traffic simultaneously, in one pass, so advanced packet services are enabled with no performance trade-offs or cross-functional performance impacts.

Advanced Packet Processing capabilities include:

- Header stripping & tunnel decapsulation
- Traffic source tagging
- Packet slicing and traffic filtering
- Packet timestamping
- MAC replacement
- Load balancing for optimized traffic forwarding
- GRE encapsulation for secure remote delivery

Application-Layer Enriched Metadata

When application-layer metadata is required, the OMX3200 can deliver metadata with Enriched Flow Intelligence to reveal application classifications and protocol-specific attributes for clear and encrypted traffic. Application layer analysis of encrypted traffic identifies fingerprints, signatures, and heuristics for accelerated threat detection and identify potential indicators of compromise without the need for expensive decryption.

Enriched metadata is derived from the same traffic flows used for standard metadata and advanced packet processing and is enabled via a software license and additional enrichment hardware.

Enriched Metadata capabilities include:

- Identifies 3800+ Layer 7 applications
- Protocol-specific metadata, such as DNS, HTTP, SIP, BGP, MPLS
- Encrypted traffic analysis of TLS, IETF QUIC, Google QUIC, SSH
- Encrypted traffic fingerprints, such as JA3C, JA3S, HASSH

Summary

NetQuest OMX3200 enables organizations to extend the visibility of Cisco Secure Network Analytics into 100G and 400G network segments where the existing switching and routing infrastructure can't generate NetFlow or when it is desirable to off-load intensive NetFlow processing impacts from performance-sensitive infrastructure. The OMX3200 can be deployed alongside Cisco 10G and 40G Flow Sensors to acquire accurate and consistent unsampled metadata to provide definitive evidence for identifying, investigating, and responding to network security issues. Optional software-enabled advanced services extend the value of the OMX™ platform while reducing TCO and operational complexities associated with managing multiple probes, sensors, and Network Packet Brokers.

NetQuest provides market-leading Ethernet and WAN Flow and Packet-Based traffic monitoring solutions that deliver the highest levels of accuracy, capacity, and performance at scale. Monitoring solutions from NetQuest are deployment-proven across thousands of network segments in enterprise, carrier, government, and defense agency networks across the globe, empowering security operations teams with high-scale visibility and actionable traffic intelligence.

NetQuest Corporation
523 Fellowship Road, Suite 205
Mount Laurel, NJ 08054 USA
+1-856-866-0505 | sales@netquestcorp.com
www.netquestcorp.com