FlowMagic Unified Network Visibility Operating System V5.0 Features

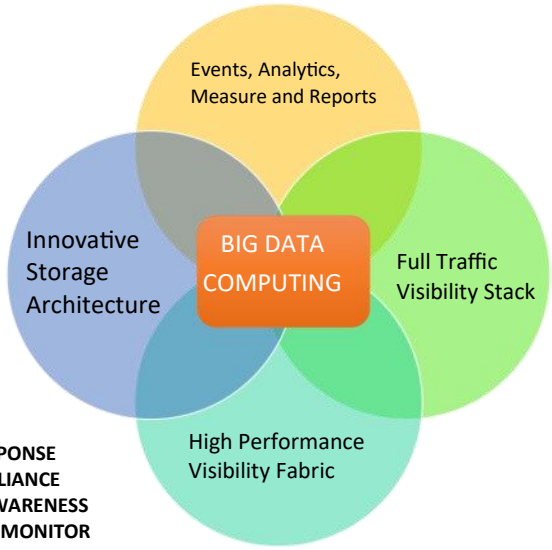
Overview

The InfiniCORE® FlowMagic Product family is the next generation purposefully designed platform to empower network administrators to gain unprecedented visibility into their mission critical networks. With a ground breaking massive parallel processing (MPP) architecture and vertically integrated operating system, FlowMagic becomes an ideal platform for big data driven security analysis, compliance validation, network health monitoring and trouble shooting applications to maximize network availability, security and performance.

It's Time for a Unified Visibility Platform

InfiniCORE FlowMagic product family is a fully integrated high performance solution delivering pervasive visibility, traceability and analytics into today's high speed network. FlowMagic is an essential tool for network administrators. Coupling advanced analytic results with full context at the finest packet level, IT operators can spot issues early, achieve faster incident response with the full situation awareness for their networks.

InfiniCORE FlowMagic Unified Network Visibility Platform

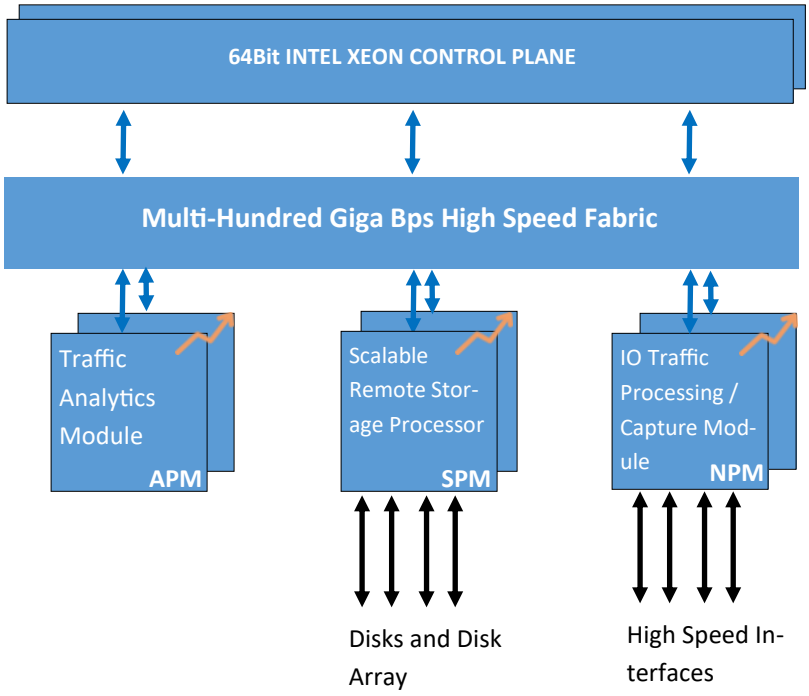


InfiniCORE Elastic Visibility Architecture (EVA)

InfiniCORE's next generation, fully distributed software defined Elastic Network Visibility Architecture is designed to meet today's network visibility challenges. EVA tightly integrates together scalable network packet processing features, scale up and scale out storage features, deep traffic analytics and collaboration features under an innovative service designer.

With the EVA architecture, the tasks involved in the visibility can be decentralized from a single processing element to gain parallel processing and performance. EVA distributes computing across its building blocks that scales proportionally to the traffic volume the appliance handles.

More importantly, the well abstracted functional interface and expansion slots allow EVA to offload tasks to accelerators such as GPU, GPU clusters, P4 switches or dedicated indexer for further performance enhancements.



FlowMagic Innovative Storage Architecture for Capturing Massive Amount of Data

With the ever increasing network traffic volume, operators often find themselves face the challenges of how to safely store more data without increase of the complexity. FlowMagic offers the following expansion methods for the storage subsystem.

- Expansion through local storage
- Expansion through direct attached storage
- Expansion through network attached storage

FlowMagic Software Defined and Hardware Accelerated Operating System Features

Types of User Interface Support

- Web Based User Interface compatible with the following browsers
    - Google Chrome Browser (Recommended)
    - Apple Safari Browser
    - Mozilla Firefox Browser
    - Microsoft Edge Browser
- Command Line User Interface
    - SSH
    - Console
- Application Programmable Interface
    - Python based Client SDK

Management Ports

- Dedicated management ports
- Completely isolated from data plane ports
- Support bonding when more than one management port is available (Model dependent)
- Support split configuration with two independent networks
- Built-in firewall protection rules

Data plane Ports

FlowMagic provides dedicated high speed system side PCI Express interfaces for the following interchangeable modules.

- Module with 2-8 ports 10Mb/100Mb/1Gb RJ45/SFP ports
- Module with 2-8 ports 1Gb/10Gb RJ45/SFP+ ports
- Module with 2-4 ports 40Gb/100Gb ports
- Module with 2-4 ports 1Gb/10Gb SFP+ with bypass
- Module with 2-4 ports 40Gb/100Gb SR/LR with bypass

Integrated Storage Module Support

- Support 4 to 16 ports internal RAID ports for RAID-0,1,5,6,10,50,60 modes
- Support 2 to 4 ports external RAID ports for JBOD expansion
- Support 2 to 4 ports Fibre - Channel, iSCSI, module for network based storage system
- Comprehensive S.M.A.R.T. monitoring and alert

System Time Synchronization Methods

- Network Time Protocol
- Precision Time Protocol over management interface
- Pulse-per-second interface on certain traffic port modules
- CERN White Rabbit Protocol Support through extension (Model dependent)

User Authentication Methods

- Local username password based authentication
    - Access right management through User Group
- Remote authentication methods and protocols
    - RAIDUS
    - TACACS+
    - LDAP
    - LDAPS

Management Related Services

- HTTP
- HTTPS with certification replacement
- SSH
- SNMP and Trap Service
- Configuration backup, download and upload
- Firmware upload, activate and downgrade

FlowMagic Software Defined and Hardware Accelerated Operating System Features (continued)

Event Management System

- Centralized system wide event management system
- Searchable by description, time range and severity
- Centralized log management system

Port and Bypass Module Management System

- Front panel visualization on the UI
    - Link Status
    - Short term and long term traffic statistics
    - Optical module status monitoring
        - Receive and transmit power measurement
        - Temperature and Voltage
- Intuitive bypass control and status monitor

Service Domain Management

- Graphical interface to design, test, monitor service logic with the data path service designer
- Management a large number of service domain effectively
- Critical resource isolation and reservation between service domain
- Bind service domain to individual users
- Activate / deactivate service domain
- Monitor service domain through graphical user interface for runtime statistics, alert and operations
    - Interactive plot over wide range of metrics
    - Engine runtime status
    - Engine error counters
    - Ability to fetch the log down to the component level
- Service domain backup, download, upload, restore and diagnosis

Rich Selection of Components for Service Chaining

- Ingress Traffic Port Component
    - Packet Timestamp
    - Packet Slice
    - Insert or strip packet VLAN tag
    - Strip packet MPLS Tag
    - Strip Cisco Fabric Path Tag
    - Offset length based header stripping
    - Hardware accelerated filters (Module dependent)
- Bypass Controller Component
    - Controls optical and electrical bypass switches
    - Power on-off bypass behavior control and monitor
    - Service on-off bypass behavior control and monitor
- Egress Traffic Port Component
    - Packet Slice
    - Insert or strip packet VLAN tag
- Filter Component
    - Large scale filter support up to 4 Million rules
    - High performance bit masked based match
    - Range match support for the port fields
    - Rich protocol support with comprehensive fields
        - Ethernet
        - VLAN
        - MPLS
        - IPv4 and IPv6
        - TCP/UDP
        - GTP
        - GRE
        - VxLAN

FlowMagic Software Defined and Hardware Accelerated Operating System Features (continued)

- Available actions when filter match
  - Pass through up to 32 selected egress connector
  - Drop
  - Insert or strip VLAN tag
- Filter template support
- Support filter priority
- Enable/Disable individual filters

- Aggregator
  - Aggregate traffic from up to 32 ingress connect-or
- Replicator
  - Replicate packet to up to 32 egress connector
- Mux
  - Select traffic from one or more of ingress con-nector
  - Aggregate traffic to the egress connector
  - Support real-time changing of the settings
- Link Protector
  - Monitor the link state of the ingress ports
  - Master slave ports
  - Promote/demote ports to take master role
- Load Balancer
  - Load balance the incoming traffic to up to 32 egress connectors
  - Load balance the incoming traffic to up to 32 egress ports
  - Load balance hash method
    - S/D MAC+VLAN+ETHERTYPE
    - Source IPv4/6 + Destination IPv4/6
    - S/DIP + TCP/UDP S/D Port
    - Inner SIPv4/6+DIPv4/6
    - Inner S/DIP + Protocol
    - Inner S/DIP + TCP/UDP S/D Port
    - Inner S/DIP + Protocol + TCP/UDP S/D Port
    - User Defined Fields
    - Inner SIPv4/v6 Only
    - Inner DIPv4/v6 Only
    - SIPv4/v6 Only
    - DIPv4/v6 Only
    - Round Robin
  - Tunnel Stack Support
    - No Tunnel
    - IP/UDP/GTP + Inner Packet
    - IP/UDP/VxLAN/Eth/IP/UDP/GTP + Inner Packet
    - IP/UDP/VxLAN/Eth/Inner Packet
  - Two User Defined Fields
    - By offset, length and mask
  - Available Egress Link Monitor Methods
    - By link status
    - By ICMP packet
    - By user defined heart beat packet
      - Flexible egress/ingress port
- Packet Capture Component
  - High performance packet capture engine
  - Packet slicing feature
  - Integrated packet indexer over popular fields such as MAC, IP, Protocols, and Port
  - Scalable file system and file system overlay to provide raw packet data as well as meta-data storage

FlowMagic Software Defined and Hardware Accelerated Operating System Features (continued)

- Support up to 10,000 drives in a single system
- Intelligent drive defect detection and steering
- Intelligent data compression
- Detailed capture performance metrics
- Native indexer over popular fields such as SIP, DIP, Source Port, Destination Port and Protocol fields
- Packet Viewer
    - Realtime and retrospective decoded view over captured packets
    - Time range based packet selection
    - Full wireshark display filter support over the captured traffic
    - Transaction (Ladder) View over high level summarized packet flow
    - Export displayed traces to PCAP

- NetFlow Record Export Component
    - Support NetFlow V5
    - Support NetFlow V9
    - Support NetFlow V10/IPFIX
    - Support configurable collector ports
    - High report interval support
    - Bi-directional or Uni-direction flow record generation
- Field Mask and Privacy Controller Component
    - High performance design to mask fields in single pass
    - Individually configurable source IP, destination IP, ports and protocol map method
    - Store maps to memory or on disk
    - Query interface to recover the original value
    - Export map to CSV for long term offline storage
- Realtime Display Filter Component
    - Support full wireshark display filter syntax
    - Up to 112 parallel instance to achieve high performance filtering
    - Real-time configurable filter
    - Pass through mode
- Deduplication Component
    - Long deduplication time window support from 1 millisecond to 1 second
    - Fast fingerprint searching algorithm
    - Accurate duplication detection with mask capabilities
    - Support rich fingerprint methods for data center, enterprise and mobile network
        - L2, L3, L4 headers or combination
        - Ability to include 16 or 64 bytes payload as fingerprint input
        - Ability to use full packet as fingerprint input
        - Operable under tunnel packets
        - The following field can be configured to be masked out from fingerprint process
            - IP TTL field
            - IPv4 ToS field
            - IPv6 TC field
    - Three operating modes
        - Statistic only, bypass packets
        - Output unique packets only
        - Output duplicated packets only
- Tunnel Stripper Component
    - Rich tunnel protocol support
        - Packet with GRE tunnel

FlowMagic Software Defined and Hardware Accelerated Operating System Features (continued)

- L2 Ethernet Switch Component
  - Up to 32 ports
  - Support up to 10 Million MAC addresses
  - Static MAC support and programmable MAC time out
  - Advanced mode to learn IPv4 address binding in addition to the MAC port binding
- Microburst Controller Component
  - Smooth up to 100Gb incoming burst
  - Provide up to 2TB high speed burst buffer
  - Controlled egress bandwidth starting from 1Mb/s to 100Gbps at the step of 1Mbps
  - Accurately control egress packet rate from 1K PPS to 28Mpps at the step of 1K PPS
- Match-Action Component
  - Up to 4M addresses and FQDN based rules
  - Automatically track the DNS response to map FQDN to IP address and apply the action
  - Large scale batch add/delete/update the rules
  - Programmable API to add/delete/update the rules
  - Capability to download the rules as a file
  - Permit and drop action with log to one or more Syslog servers
  - Support up to 32 Syslog servers
- Pattern Matcher
  - Cache session for prespecified size up to 128MB
  - Use binary pattern match to match against provided regular expression rules
  - Output the entire buffered session when match is found

Packet Export Features

- Export packets from the capture repository into PCAP files
- Support export from multiple repositories
- Accelerate traffic export with the index database
- Time range and filter based export
  - Time range selection by starting date and duration
  - Partial second selection for sub-second export
  - Filter based export by specifying fields of the following protocols
    - Ethernet
    - VLAN
    - MPLS
    - IPv4 and IPv6
    - TCP/UDP
    - GTP
    - GRE
    - VxLAN
  - Support display filter syntax
  - Support regular expression based filter to select matched packets
  - Acceleration when indexer option is enabled and indexer database is available
- Support of Packet slicing
  - Support protocol based slice to include only the protocol portion
  - Support fixed size based slicing
- Support export privacy control
  - Support zeroize or random fill payload or certain layer of protocols
- Split exported file to certain size from 16MB to 4GB at the step of 16MB

FlowMagic Software Defined and Hardware Accelerated Operating System Features (continued)

Traffic Analyzer and Meta Data Extraction

- Time range based analysis or always on continuous analysis and extraction
- Rich metrics extraction and searchable analysis database construction
    - Uni-directional packet count
    - Uni-directional byte count
    - Events and logs generated during inspection
    - Meta data fields based on per protocol meta data extraction
- Rich presentation and query interface
- Rich data mining and programmable API
- Endpoint related analysis methods
    - End Point and Protocol Analysis
    - MAC address, Ether Type and VLAN statistics
    - End Point with timeline information
- Session and conversation related analysis methods
    - Connection Analysis
    - Connection Analysis with timeline information
    - Conversation Analysis
- Network Quality and QoS Analysis
    - RTP Media Quality Analysis
        - Jitter
        - Order
        - Packet loss
    - TCP Key Performance Indicator Analysis
        - Packet Order Issue
        - Zero Window
        - Retransmission
        - Latency issue
    - RFC2697 Single Rate Tri-Color QoS Analysis
    - RFC2698 Dual Rate Tri-Color QoS Analysis
- DPI based Connection and Transaction Meta Data Extraction
    - Session identification by 8 Tuples
        - Service domain
        - Capture repository
        - Interface
        - VLAN
        - Source IP
        - Destination IP
        - Protocol
        - Source Port
        - Destination Port
    - Geolocation of public routable IP
    - Autonomous System information of public routable IP
    - Application metadata extraction
        - IPv4 and IPv6
        - ICMP
        - IGMP
        - Tunneling protocols GRE, VxLAN, L2TP, IPIP
        - IPSec
        - DNS
        - DHCP
        - HTTP and HTTPS
        - SSL and TLS

FlowMagic Software Defined and Hardware Accelerated Operating System Features (continued)

- RADIUS
- SMTP
- POP3
- IMAP
- LDAP
- SSH
- DIAMETER
- CIFS and SMB
- NFS
- Heuristic based database protocol recognition
    - MySQL
    - Oracle
    - PostgresSQL
    - MSSQL
- Heuristic based Remote access application recognition
    - Teamviewer
    - Remote Desktop
- DNS tracking based Application Recognition

Traffic Replay and Regeneration

- Support Traffic replay from packet capture repository
- Select traffic by time range or through filter
- Pre-extract traffic or extract traffic on the fly
- Replay through dedicated traffic ports
- Support three replay modes
    - Continuous/Burst/Multi-burst
- Rate specification in Packet Per Second, line rate percentage or L1/L2 bandwidth

Traffic Scan and Rescan with IDS Tool

- Support traffic scan using the IDS Tool over the packet capture repository
- Support multiple OSS IDS tools
    - Snort
    - Suricata
    - Bro/Zeek
- Support multiple versions of IDS tools or multiple versions of rules
- Collect the IDS tool output into CSV or parsed into the JSON
- Work flow from the IDS alert to full session PCAP extraction
- Work flow from the IDS alert to investigation panel with the following information:
    - Decoded packets and interaction among them
    - Information about the source and destination
    - Alert information