

FlowIntelligence™ 6425

Adaptive Cyber Defense Platform



- **True Wire-Speed Performance at 25 Gbps**

State-of-the-art high-performance architecture delivers unparalleled performance and processing for open source, proprietary, and commercial off-the-shelf cyber security applications.

- **Secure Linux Operating Environment**

Applications run on a secure and performance-optimized Linux® distribution with industry-leading throughput, agility and capabilities.

- **Robust, Service Provider Hardened Platform**

Dual-redundant and hot-swappable power supplies, solid-state hard drives, redundant system configurations with core elements for carrier-grade reliability and maximum up-time.

- **Scalable Processing Platform**

Quad-socket, multi-core Intel® Xeon processors to provide unprecedented application performance, network throughput and processing efficiency for the FlowIntelligence Cyber Sensor Suite as well as open source applications such as SNORT®, Suricata®, Zeek® and others.



Typical User Deployments

- Deep Packet Inspection
- Network Security and Monitoring
- Network Breach Detection and Prevention
- Web, URL and Application Filtering
- Network Flow Monitoring
- Cyber Security and Network Threat Intelligence
- Network Malware Identification
- Integrated Adaptive Cyber Defense
- Network Sensor Application Consolidation

High-Performance Cyber Security Platform & Network Sensor

The FlowIntelligence 6400 Series Adaptive Cyber Platform is a scalable high-density packet processing system. It delivers unparalleled performance for the FlowIntelligence Cyber Sensor Suite of tools, open source, custom-proprietary, or commercial off-the-shelf (COTS) network security and cyber intelligence applications. The platform is optimized for packet processing through an extensively field-tested and proven architecture which features multi-core Intel® processors and a robust Linux application environment.

The FlowIntelligence 6425 Series platforms are created for the most demanding cyber mission environments via two chassis configurations:

- FlowIntelligence 6425 system for enterprise and data center operations supporting a single cyber sensor at 25 Gbps
- FlowIntelligence 6425-*eXtreme* system for enterprise and data center operations supporting up to two cyber sensor applications or a single processor intensive cyber application at 25 Gbps

The platform is designed specifically to provide wire speed deep packet inspection and applications processing with uncompromising performance and unrivaled flexibility. The FlowIntelligence 6400 Series architecture with quad sockets allows cyber security and network information assurance professionals to rapidly deploy advanced cyber and network application solutions with remarkable speeds of 25 Gbps of packet processing capability. All of this is done in a high-density platform with a lower total cost of ownership than alternative solutions.



FlowIntelligence 6400 Series platforms are fully programmable systems that allow any Linux-based networking applications to perform at wire speed with little or no porting effort. Applications run on a performance-optimized Linux distribution with industry unique packet acceleration technology and standard LibPcap API compatibility so that cyber teams can deploy advanced cyber sensors and solutions within hours of installing the system. The platform also includes the FlowIntelligence tool kit which is a rich set of software infrastructure components that aids developers in implementing advanced application and systems management features as well as supporting sophisticated operational environments.

FlowIntelligence 6400 Series Adaptive Cyber Defense Platforms are ideal for Fortune 500 and Government cyber operations environments, network providers, systems integrators, and commercial software vendors to rapidly deploy scalable, high-performance solutions for Cyber Security, Network Monitoring & Flow Collection, Information Assurance as well as other Deep Packet Inspection services.

Proven Architecture for High Performance Sensors

The extraordinary cyber security application processing of the FlowIntelligence 6400 Series is achieved through BiviOS™, a patented packet processing, acceleration and application management ecosystem that is fully integrated with the standard Linux libraries.

Using this implementation, the application does not need to be modified with any system details – it only needs to invoke the standard Linux network traffic and packet handling mechanisms in the LibPcap API. This compatibility delivers significant improvements over server and packet capture card – combo appliances for the FlowIntelligence Cyber Sensor Suite of tools as well as open source, Linux applications such as Snort®, Suricata®, Zeek® NSM, Argus, YAF, nProbe, TCPDump and many other commercial or custom-proprietary software.

The system host applications run on a robust Red Hat® Enterprise Linux (RHEL) operating environment. In conjunction with the Linux operating environment, extremely efficient, high-speed network traffic processing is achieved through Bivio Networks' exclusive packet acceleration middleware that is fully integrated with the Linux packet capture (PCAP) libraries. The benefit for using this implementation is the application does not need to be modified with any systems details – it only needs to invoke the standard Linux network traffic and packet handling mechanisms. Consolidate your network traffic processing and cyber sensor operations with the FlowIntelligence 6400 Series. It is the only platform on the market today that can truly operate cyber sensors at full wire speed.

Transparent Operations

Network Interfaces on the FlowIntelligence 6400 platform are configured in transparent mode to support traditional “in-line” or passive “sniff” modes of operation. In this configuration, the interface(s) does not require an IP address for operation in the network. This enables the platform remains invisible to the infrastructure, or like a wire to network devices connected on either side.

Robust Operating Environment

The FlowIntelligence 6400 platform includes a robust and performance optimized Red Hat® Enterprise Linux (RHEL) distribution that provides a secure and reliable host environment for cyber security and network packet processing applications. The system combines the operating system with the power of Bivio Networks' BiviOS™ middleware which is exclusive packet processing, acceleration and management middleware technology. It provides “lockless queuing” to nearly eliminate internal packet handling latency and achieve an unmatched performance advantage for line-speed packet processing operations.

BiviOS middleware enables multi-application workloads with the ability to operate and manage simultaneous packet processing applications on the FlowIntelligence 6400 Series. All the while, it incorporates fault detection and recovery in the event of a hardware or software failure. BiviOS enables sensor applications to take actions such as blocking or passing traffic. An embedded management system handles dynamic flow load balancing for packet processing, fault detection and processor core re-allocation as well as alerts and actions.

The platform supports high-availability with redundant load-sharing power supplies, redundant cooling fans, redundant packet ingest interfaces, redundant data offload interfaces and redundant data storage. All modules and components are hot-swappable for non-stop operations. The system platform also contains dual M.2 480 GB, RAID-1 boot and system operating modules.

Enhancing the Defensive Cyber Operations Process

The FlowIntelligence 6400 platform hosts an advanced set of tools and features for enhancing the defensive cyber operations process and operating network sensors. Achieving speed-to-decision in mitigating cyber threats requires the ability to utilize an unparalleled combination of tools. The FlowIntelligence platform toolkit enables integrating real-time threat intelligence indicators with cyber sensors, automated workflow for security orchestration and decision-making response, share threat information with third-party systems as well as supports an integrated development environment (IDE) for customized cyber sensor implementations.

The platform incorporates a Trusted Automated eXchange of Indicator Information (TAXII) interface for enablement of the STIX, CYBOX and MAEC threat intelligence indicators in network-based cyber sensors. The platform also contains a visual workflow engine that aids in the security orchestration and automation response (SOAR) process with cyber sensor data. In addition, tools for sharing cyber sensor data is comprised of a Kafka message broker to allow cyber operators and analyst to move data from the platform to one or more external consumer systems. The Open Data eXchange Layer (OpenDXL) facilitates sharing data with McAfee® cyber security products and other third-party technologies that leverages this API. Other data sharing APIs are available through a custom API integration package for the platform.

The BiviOS™ Environment

FEATURE	BENEFIT
Network Performance	Exclusive packet acceleration software delivers the highest possible network throughput with minimal internal latency.
Multi-Application Support	Efficient and unique host infrastructure allows multiple applications to run in parallel, simultaneously seeing the same network traffic.
Ease of Use	Full performance and multi-application features are instantly available to any developer with basic proficiency in Linux. Rather than using custom APIs, all BiviOS networking details are hidden under the PCAP library making open source cyber applications and tools such as Zeek (formerly Bro), SNORT®, Suricata, YAF, nProbe, TCPdump, etc. ready to run with no changes at all.
Inline/Passive Modes	Bivio platforms support both inline and passive modes of operation, and when running multiple applications, some can be inline and some can be passive on the same platform.
Failure Detection and Recovery	In the event of a hardware or software failure, BiviOS can be configured to take actions such as blocking or passing through all traffic. An elaborate event management system handles fault detection, alerts and actions.
Application Management	Easy configuration of key application and interface parameters, application start/stop/restart control and extensive packet processing statistics simplify the complete cyber solution integration.
System Management	Comprehensive system status monitoring and reporting, including SNMP and hardware status, is provided through the BiviOS environment.

FlowIntelligence 6400 Specifications

Platform Features	FlowIntelligence 6425	FlowIntelligence 6425X
System Performance	25 Gbps	25 Gbps
Processing Cores	Quad Intel Xeon Gold 18 Core Processors	Quad Intel Xeon Platinum 28 Core Processors
Network Interfaces	2x Dual 25 Gb Interfaces (Packet Processing)	
Data Interfaces	2x 1/10 Gb Fiber SFP Data Offload Interfaces	
Management Interfaces	2x 1 Gb Copper RJ-45 Management Interfaces	
Local Technology Storage Capacity	M.2 480 GB (RAID-1) Boot and Operating System Storage Fast Read SSD - Up to 100 TB (RAID-5) Storage	
Cooling	6 Hot Swap fans	
Power	Dual 240 VAC 2000W Hot-Swappable PSUs	
Chassis Size	3.4" x 17.08" x 32.9" (2 Rack Units)	
System Weight	80.7 lbs	
Safety Compliance	USA/Canada: UL/CSA 60950-1	
Electromagnetic Compliance	USA/Canada: FCC Part 15 and GR-1089 Europe: EC Directive, EC Council Directive 2004/108/EC, ETSI EN300 386, EN55022, EN 55024 International: CISPR 22 Class A and CISPR 24	

About Bivio Networks

Bivio Networks is dedicated to providing leading networking products that enable government agencies and service providers to control, monitor and secure critical network infrastructure. A leader in cyber intelligence, cyber security and network control solutions, Bivio products are deployed in a wide range of environments by a global customer base including leading intelligence agencies, service providers and enterprises. Bivio is privately-held and is headquartered in the San Francisco Bay Area.

©2020 Bivio Networks, Inc. All rights reserved. The Bivio logo, BiviOS, FlowIntelligence and Cyber Mission Ready are trademarks or registered trademarks of Bivio Networks, Inc. All other company and product names may be trademarks of their respective owners. Bivio Networks may make changes to specifications and product descriptions at any time, without notice. P/N 62000-00041 Rev 1



Bivio Networks, Inc.
4457 Willow Road, Suite 240
Pleasanton, CA 94588
Tel: +1 925 924 8600
www.bivio.net