



# Myricom nVoy Series 10 Gbit Packet Recorder

The **Myricom nVoy Series Packet Recorder** enables security operations engineers to not only build next-generation intrusion detection systems (IDS) but also isolate and record accesses to an organizations critical business data including personally identifiable information (PII), enterprise resource planning (ERP) and intellectual property (IP). The nVoy Packet Recorder makes it easy to droplessly record and index up to 10 Gbit network traffic. Users can take advantage of these recordings to address issues such as compliance, forensics, and reducing the duration of incident investigation. Additionally, the Packet Recorder is fully backed by a customer support team that specializes in cyber incident response technologies.

## Compliance

Some businesses demand an accurate, time-stamped record of specific conversations. Regulated industries, including financial, government, retail must meet compliance requirements, as well as provide detailed auditing outlining cyber breach details including such items as dates, times and extent of data loss. CSPI's nVoy Series Packet Recorder's timestamp accuracy meets strict MiFID II specifications for recording financial transactions in automated trading. With many other regulations in effect including HIPPA, SOX and PCI DSS organizations need to be prepared to support these and others as they come online such as the European Unions' 2018 GDPR data privacy regulation which specifies cyber breach notification within 72 hours of any suspected intrusion.

## Key Features

- Two capture ports, each supporting 1 or 10 Gbit
- 10 Gbit/s packet recording to disk, in pcap file format, with zero packet loss
- On-the-fly indexing and compression/decompression
- Web configuration and management
- Packet indexes accessed through a command line or an API
- Optional pcap re-injection into the network
- 24 x 1.2 TB of storage standard in 2U with options for much more
- Optional pcap analysis available using the web interface

S P E C S

## Effective, Efficient Rapid Incident Response

Every day, numerous alert logs are generated from firewalls or other security tools, such as Next generation IPS/IDS or SIEMs, highlighting suspicious activity. However, these alerts only provide basic metadata information. While this is a good starting point it doesn't give enough detail to perform efficient nor effective, incident investigation forensic analysis against. With the nVoy Packet Recorder, security teams are able to capture, index and timestamp all accesses to identified critical assets at the packet level. Having this detail at your disposal enables your forensic tools to report out on what the suspicious activity really is.

For example, perhaps you need to fill in the gap between two distinct incidents. You can use the meta data to determine the start and end points. However, it is the recorded data that will give you the details on what has actually transpired. Or, it may be the case that you want to take data provided from a current alert and search on whether this type of suspicious activity has occurred in the past. The alert log will allow you to isolate the search parameters and through the recorded data your forensic tools can identify any previous points in time.

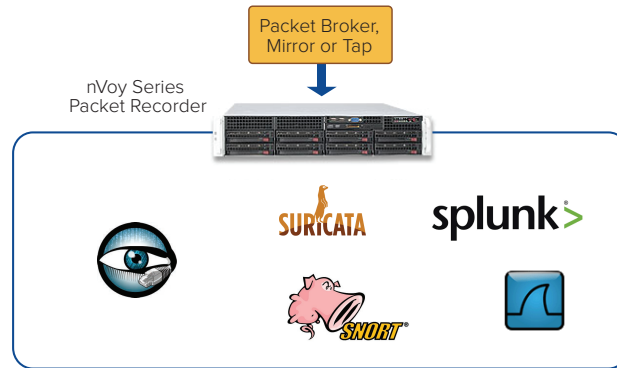
In addition, utilizing the optional nVoy AIR application, alerts targeting critical assets triggers the packet recorder to automatically generate an extraction file of all conversations associated with that alert. This streamlines the process and eliminates the need for manual efforts thus reducing the risk and cost associated with manual incident investigation.

## Performance

The nVoy packet recorder, built on the proven performance of CSPI's Myricom ARC Series network adapters, captures packets at 1 or 10G speeds without drops and with extremely accurate nanosecond timestamp capability. It runs on a server that CSPI has carefully tuned for optimal performance as a complete system (adapter, BIOS, operating system, and application software).

Of equal importance is the ability to locate and identify an area of interest quickly and effectively. Searching through large amounts of stored data for a pattern, session, or even IP addresses can present a significant challenge. The nVoy Packet Recorder creates on-the-fly index trees to retrieve packets in parallel while recording at line rate. You can search on a time basis or with an accelerated packet filter in BPF notation or a combination of both.

Extracted packets are formatted as pcap files for further analysis in your favorite tool. An API is also available to access the indexes, allowing advanced users to develop their own search and extraction tools.



The nVoy packet recorder has the capacity to host multiple analysis applications sharing the same packet stream.

### Real-time compression

Real-time pcap compression can be enabled upon packet capture to reduce the effective written data and extend the capture window within the same device. Certain network traffic patterns better lend themselves to compression, such as High Frequency Trading (HFT) related traffic.

### Web Interface

A powerful and easy-to-use, web-based interface is provided for capture and recording configuration, system management, and packet retrieval.

## Extract Packets

From

To

Filter  ☆  
BPF-Like filter for selecting packets (same format used by the popular [tcpdump](#) tool).

Output File   
Specify where the output file will be stored. If the path does not exist, it will be created.

NOTE: you can download the file via FTP or SSH. Please configure a login name and password in the Users Configuration web page.

●

The nVoy UI allows simple and powerful specification of packets to be extracted based on capture time and or BPF-like filtering.

## Myricom nVoy Series Packet Recorder Configurations

	nVoy Recorder 5 Gbit	nVoy Recorder 10 Gbit
Form Factor	1U Rackmount	2U Rackmount
Sustained Capture	Up to 7.44 Mpps	Up to 14.88 Mpps
Capture ports	2 x 1/10G SFP/SFP+ but the combined bandwidth to disk is limited to 5 Gb/Sec	2 x 1/10G SFP/SFP+ but the combined bandwidth to disk is limited to 10Gb/Sec
Standard Storage Capacity	8 x 1.2 = 9.6TB	24 x 1.2 = 28.8TB
Hardware	Single CPU with hardware RAID and Myricom ARC Series 2-port adapter	Dual CPU with hardware RAID and Myricom ARC Series 2-port adapter
Software	5G packet capture and recording license	10G packet capture and recording license
Timestamp Accuracy	± 50 ns	
Packet extraction Filtering	Allows filtering content by IP source address, IP destination address, protocol and or application.	
Management Port	RJ45 modular connector supporting up to 1 Gbit Ethernet	
Additional Storage Capacity	Drives larger than 1.2 TB are available. Or add additional drive-only storage expansion boxes.	
Configuration and Management	Web Interface	
Warranty	3 years hardware, 1 year software maintenance	

✉ Satisfy your packet recording needs. Contact us at [myricom.sales@cspi.com](mailto:myricom.sales@cspi.com).

## About CSPI

CSPI (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

### CSPI Corporate Headquarters

175 Cabot Street - Suite 210  
Lowell, MA 01854  
800.325.3110 (US & Canada)

### CSPI High Performance Products

800.325.3110 (US & Canada)  
[us-hpp-sales@cspi.com](mailto:us-hpp-sales@cspi.com)

### CSPI Technology Solutions

800.940.1111  
[us-ts-sales@cspi.com](mailto:us-ts-sales@cspi.com)



[www.linkedin.com/company/csp-inc](https://www.linkedin.com/company/csp-inc)



[@ThisIsCSPI](https://twitter.com/ThisIsCSPI)



[us-hpp-sales@cspi.com](mailto:us-hpp-sales@cspi.com)



[www.cspi.com](http://www.cspi.com)

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.