



SentryWire - Sentry230 V7, 468 FC

Quick Facts

- Full Packet Capture
- Capture Speeds, 1Mbps - 10Gbps
- Powerful & Fast Search
- Extended Capture Timeline
- Intrusion Detection
- NetFlow Analytics
- Easy Integration/RESTfulAPI
- Advanced Filtering

Features

- Unlogged Activity Detection
- Lossless packet capture up to 10Gbps
- Simultaneous Search
- IPFix Record Generation
- HTTP Session Logging
- SMTP Email Event Logging
- SMTP and HTTP Protocol File Event Logging
- User Agent Event Logging
- TLS/SSL Session Event Logging
- File Carving and automated workflow to file inspection services/capability
- One (1) 2U Capture/Storage Node

Full Packet Capture with Cyber Analytics Cost Effective & Scalable

The Sentry230 V7, 468 FC Packet Capture Platform, is a complete solution based on a unique capture and storage architecture. The system is managed by One (1) 2U rackmount Capture/Storage Node which offers high-speed packet recording with real-time analytics and visualization. Data is stored within the capture device with massive high-speed storage. This model includes SentryWire's newest capability, File Carving.

This system is designed for applications that demand high-speed data recording and extensive storage, such as cyber forensics, cyber security, and big data analytics. The 2U Sentry230 V7, 468 FC Packet Capture Platform has a variety of powerful features:

Lossless Packet Capture

- Forensic retrospective functionality of lossless packet capture 1Mbps to 10Gbps
- Time stamping of 150 nanoseconds
- Expandable to 6 Nodes (2,808TB's raw storage capacity) without adding additional Capture Nodes.

Lightweight, MapReduce Architecture

- Scalable to hundreds of Cluster Nodes with federation manager
- Packet processing is distributed to cluster nodes
- Dynamic node management

OS

- CentOS or RHEL - customers choosing




**Hewlett Packard
Enterprise**

 **Red Hat**



Full Packet Capture

Capturing just Metadata does not produce a high fidelity record of Traffic.



Powerful & Fast Search

Search Petabytes of Network Traffic in Minutes.



Extended Timeline

Network Traffic Stored for Weeks, Months or Years.



Fast Capture Speeds

Capture speeds from 1Mbps to +1Tbps.



Intrusion Detection

Present Day intrusion detection limits breaches.



Visualization & Analytics

3D Visualization + Integrated Commercial, Open Source & Custom Analytics.



SentryWire - Sentry230 V7, 468 FC

Features

- Scalable to hundreds of clusters
- Scalable to Petabytes of Packet Store - Months or Years of Timeline
- Lightweight MapReduce architecture
- Real-time Analytics for any Volume
- Fast, Scalable, Distributed Search and Extract, even as Timelines Increase
- Federation of Multiple Clusters
- ThreatIP Session Matching/Logging and Ability to Load in User Defined Rules
- Snort/Suricata Rules and Ability to Load in User Defined Rules
- Role Based Access Control
- Integrated Browser and Session Based Packet Viewer, Alert Log Viewer and Extracted Files Viewer in PDF
- Format (All Within Our UI/ Browser)
- Place off a TAP location within a break and inspect zone for decoding encrypted traffic or the end-users can import and apply TLS/SSL certificates once a PCAP has been downloaded to enable the decryption of the packets.
- **Optional:** File Inspection capability either on premise or cloud based, automated and integrated with your workflow and SentryWire's user interface.
- File Inspection Service offered in conjunction with Trinity Cyber's "Deep Ocean".

Metadata Indexing & Logging System

- 5 tuple indexing — IP address source/destination, port source/destination, protocol (IP, UDP, ICMP)
- Indexing of MAC source/destination
- IPFix record generation NetFlow recording
- RFC anomaly logging
- Session and connection logging
- File exfiltration and infiltration has logging
- http, ftp, grid ftp logging
- UID event correlation
- RESTful search query access using easy BPF+ metadata descriptors

Data Storage & Forensic Timeline Features

- Includes 468TB's of raw storage, or 335TB's of available packet storage after RAID 5/6 and metadata overhead. Estimating compression at 1.5x will yield 503TB's of effective packet storage capacity. Additional capacity can be achieved by adding Capture/Cluster Nodes. Compression can vary greatly depending on data characteristics.
- Overall storage amplification up to 3x (depending on percentage of traffic with SSL encrypted or compressed packet payloads)
- Forensic timeline that is scalable, distributed, and searchable over days, weeks, months — even years!
- Queries respond with stream-based extracted packets, so analysis can occur in parallel with data retrieval
- Massive queries over large timelines respond quickly, even as the timeline increases
- Federated search — both within a cluster, and across multiple clusters

In-line File Carving (Two Methods)

- Live file carving that allows analysts to set specific file types to carve automatically.
- Search based / On-demand file carving where any files returned as part of a search are identified, viewable, and exportable as fully reconstructed files.
- In addition to the carved files SentryWire logs every file that is captured, he file logs included MIME type, hash, and rich contextual metadata.



SentryWire - Sentry230 V7, 468 FC

Metadata Indexing & Logging System

- 5 tuple indexing — IP address source/destination, port source/destination, protocol (IP, UDP, ICMP)
- Indexing of MAC source/destination
- IPFix record generation NetFlow recording
- RFC anomaly logging
- Session and connection logging
- File exfiltration and infiltration has logging
- http, ftp, grid ftp logging
- UID event correlation
- RESTful search query access using easy BPF+ metadata descriptors
- Includes 468TB's of raw storage, or 335TB's of available packet storage after RAID 5/6 and metadata overhead. Estimating compression at 1.5x will yield 503TB's of effective packet storage capacity. Additional capacity can be achieved by adding Capture/Cluster Nodes. Compression can vary greatly depending on data characteristics.
- Overall storage amplification up to 2.8:1x can be achieved (depending on percentage of traffic with SSL encrypted or compressed packet payloads)
- Forensic timeline that is scalable, distributed, and searchable over days, weeks, months — even years



**Hewlett Packard
Enterprise**



Federation Manager

- SentryWire Federation Manager allows analysts to search across multiple geographically disparate nodes and groups simultaneously.
- SentryWire Federation Manager provides a single pane of glass for the central configuration and management of administrative tasks such as authentication, policy, auditing, and updates for all federated nodes simultaneously. There can be several “layers” of federation, some variations involve an optional 1U Federation Node.

Web GUI & RESTful Interface

- Log and metadata information visualization, search, and packet viewing
- MapReduce support of multiple clusters
- Node management
- Remote access, automation, and control through your analytics application and framework

Session Reconstruction:

- SentryWire does not truncate or slice packets, this allows SentryWire to track session ‘flows’ by creating a flow hash when the first packet comes in; allowing the system to reconstruct sessions when packets are returned via search. The flow hash allows access to any data contained in the flow such as TCP session, app layer state data, protocol information, client/server byte transfers, etc. Once a search is completed, the analyst can view the returned packets in a lightweight packet viewer via SentryWire’s UI and additionally when a PCAP is downloaded and opened in a tool such as Wireshark; the packets are in order and protocol streams are reconstructed allowing an analyst to follow any available protocol stream. SentryWire will also reconstruct protocols that span multiple TCP segments such as TLS or HTTP and will attempt to reassemble out-of-order segments. SentryWire will also reconstruct protocols that span multiple TCP segments such as TLS or HTTP and will attempt to reassemble out-of-order segments.)

Drives

- Configuration flexibility with 14, 16, or 18TB SAS drives (optional FIPS 140-2 Validated™ Self-Encrypting Drives certified by the U.S. and Canadian govts to protect Sensitive but Unclassified and Protected class data)

System Specs

Packet Capture Interface & Capture Rate (With Simultaneous Search/Extract)	2 x10G or 4x10G Interfaces Licensed to 10Gbps of Aggregate Throughput
Timestamping	150 Nanoseconds
Total Timeline Capture Storage Capacity	Includes 468TB's of raw storage, or 335TB's of available packet storage after RAID 5/6 and metadata overhead. Estimating compression at 1.5x will yield 503TB's of effective packet storage capacity. Additional capacity can be achieved by adding Capture/Cluster Nodes. Compression can vary greatly depending on data characteristics usually 1.15:1 to 2.5:1.
Total Indexing & Metadata Storage Capacity	79TB's
RAID 5/6 & Hot Spare Overhead	54TB's
API/REST & Web GUI Control	R1 45-G LAN Port
Physical Dimensions - Capture/Storage Node x1 Node	2U: H 86.8mm (3.4") W 448.0mm (17.6") D 810.0mm (31.9") Weight: 40.0kg (88.2lbs)

Sentry230 V7, 468 FC



*Shown with One (1) 2U Capture/Storage Node, bezel design subject to change.

Security Ecosystem Segment-Specific Use Cases

Vulnerability & Incident Management

- Tenable, eEye Retina, RiskVision, Archer

Insider Threat

- RedOwl, DeviceLock

SIEM

- Q-Radar, ArcSight, LogRhythm, Splunk, Exabeam

NGFW/UTM

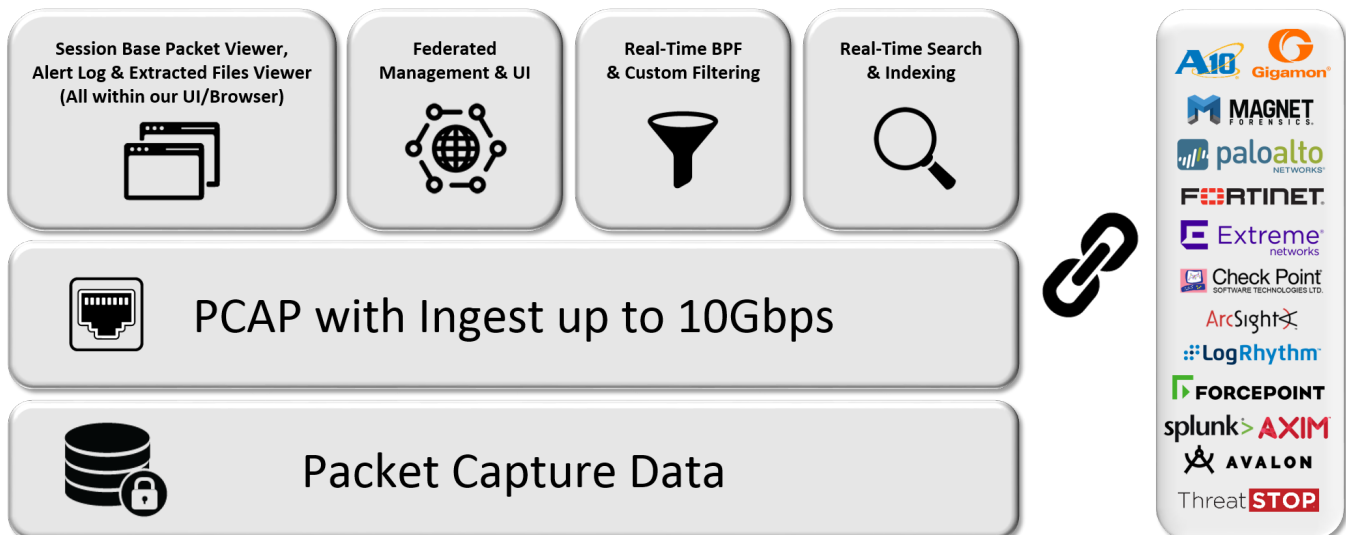
- Fortinet, Palo Alto Networks, CheckPoint

Cloud/SDP/SPB

- Zscaler, Avaya, Vidder

Threat Information & Intelligence

- All XX-ISAC feeds, IAVA, ISVM, ThreatStop and our RedForce offering, ETPro, Custom Intel



Logging & Filtering

Real-Time Log Manager:

- IPFIX Netflow Generator
- HTTP, Files, DNS, Email, User Agents, TLS/SSL
- Active Triggers (BPF)
- System Events
- Snort Rules (Emerging-DNS/FTP/files)
- Suricata Rules
- All Time-Correlated w/ PCAPs & IPFIX Data
- All Data Compressed



SentryWire Use Case: Incident Response

Data Exfiltration Detection

Log exfiltrated files with 5-Tuple indexing and hash details for comparing data, taking actions and retrieving sessionized PCAPs for forensics.

Unlogged Activity Detection

In conjunction with enterprise log correlation tools (Splunk, ELSA, LogRhythm, etc.), quickly detect and sessionize network activity that may have been removed from log buffers prior to being written to disk.

Malware Infiltration Detection

Detect, Classify and Extract objects (files, URLs, IP Addresses, etc.) in real-time to inspect and take appropriate actions to enrich cyber investigations and generate alerts.

Phishing Preparation Detection

Detect and log all URIs traversing the network, from targeted phishing emails to web traffic, and alert when internal traffic accesses those URIs, automatically sessionizing the corresponding traffic for human validation and remediation.

Indicators & Signatures Alerting

Multi-level signature and behavior event session search and logging, with visualization through DPI visualizer. Configure groupings of signature and unusual behavior alerts dynamically while in the fight, while real-time IDS alerting generates event logs for HTTP, Files, DNS, email, user agents, TLS/SSL, VOIP – all automatically correlated with PCAP and IPFIX flow records.

SentryWire Use Case: Network Troubleshooting

Network Access Control (NAC) Analysis

Receive real-time alerts of unauthorized network connectivity through 5-Tuple indexing and logging, allowing the security practitioner or network manager to compare the data to a known list of approved network access points.

User Anomalous Behavior

Identify employees using unapproved applications or using applications in ways that violate policies, correlating meta-data about users, files and sessions with real-time threat information and using the correlations to provide situational awareness and alerts.

Network Behavior Anomaly Detection (NBAD)

Detect anomalies from normal network traffic behavior and correlate to a 5-Tuple index for root cause review.

Various Forensic Traffic Analysis Applications

Analyze captured data for suspicious traffic (such as non-DNS traffic over port 53, encrypted traffic over port 80, etc.), alert the security practitioners of what they deem as suspicious user behavior, sessionizing the suspicious network traffic for view and analysis in the SentryWire UI.

Encryption Visibility

Gain visibility into TLS / SSL encrypted sessions. Log and extract sessionized network traffic via timestamp, capture node and session information to recover encrypted session, view in any packet viewer (e.g., Wireshark) using customer provided keys.



Hewlett Packard
Enterprise



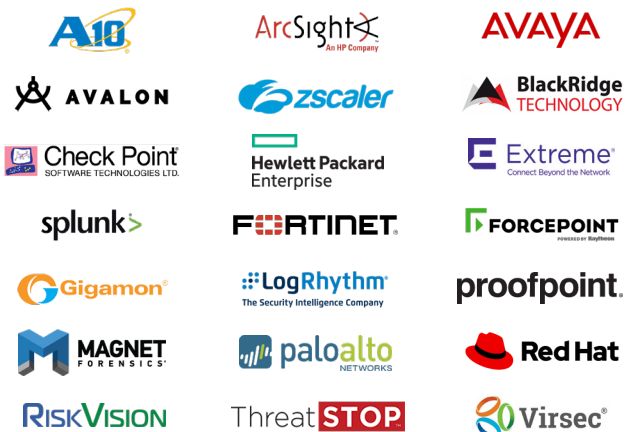
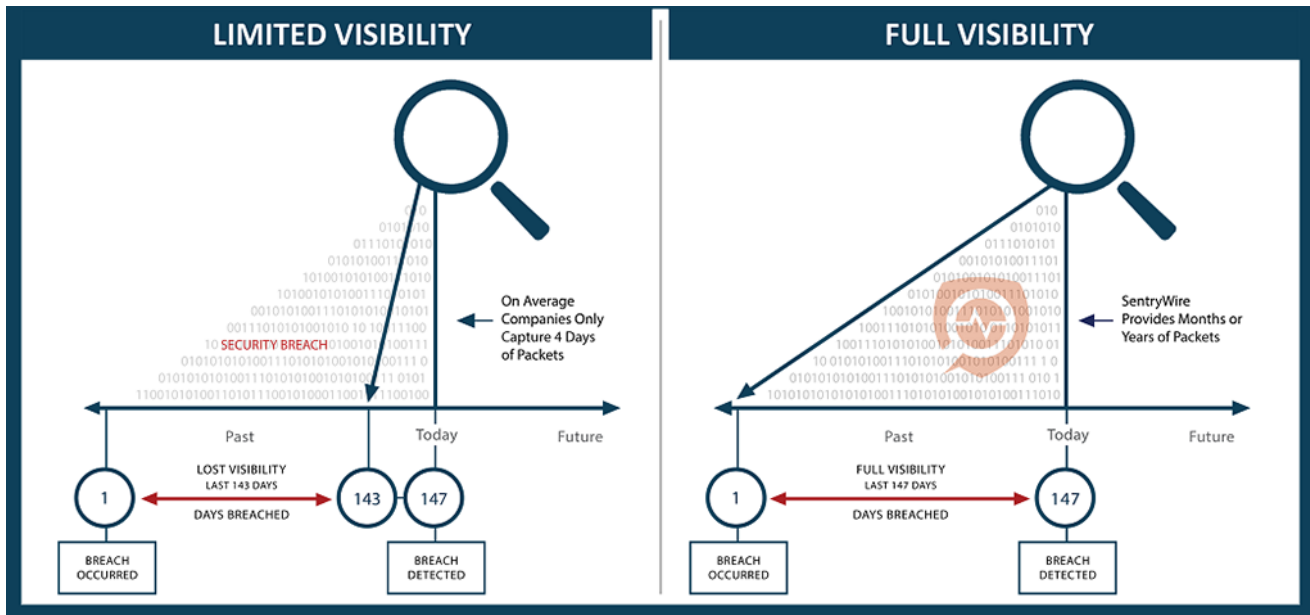
End Forklift Upgrades & Re-Buys

Imagine buying an IT solution once and upgrading it as needed, without losing a penny on your investment. Start small, SentryWire can grow with your enterprise. As your network throughput increases, simply add another cluster node. If you want to increase the amount of network traffic you retain simply add a storage node. You get uninterrupted value from your investment without ever re-buying storage or compute that you already own. Simply add capacity and throughput.



SentryWire, Gain Visibility

On average it takes 146 days to detect a breach in your network. Most companies only store 4 days of packets on average, that leaves you with 142 days of no visibility into what was happening on your network during the breach. The SentryWire Packet Capture Tool and Network Security Platform will provide you with visibility into your network and not leave you in the dark when a breach has occurred.



Technology Partners

SentryWire partners with the leading security solution providers to extend the power of our packet capture platform. This ecosystem of partner technologies includes governance, risk compliance management platforms, intrusion detection systems, behavior based solutions, hardware and OS providers, other security & industry solutions.