NEXT COMPUTING

Cost Effective, Scalable Packet Capture and Cyber Analytics Cluster for Low Bandwidth Enterprise Customers

The Enterprise Lite Packet Capture Cluster Platform is a complete solution based on NextComputing's unique Packet Continuum capture and storage architecture. The system platform is a 2U rackmount, which offers high-speed packet recording with real-time analytics and visualization. With optional 2U cluster nodes, packet processing may be distributed to a cluster network of rackmount nodes with massive high-speed storage. 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.

FEATURES INCLUDE:

- Lossless packet capture, with deterministic performance, up to 2Gbps aggregate capture rate
- Extended forensic timeline and storage features, starting with 40TB physical storage in a stand-alone capture node, up to max amplified storage 400TB in a cluster system
- Log Manager: HTTP, files, DNS, email, user agents, NetFlow, TLS/SSL and VOIP
- Actionable search of all logs, cross-correlated with PCAP & NetFlow
- Active Triggers: real-time, dynamic, user-defined
- Open data access: view PCAPs & NetFlow records in Wireshark, view log data as CSV
- Open PCAP workflows: playback output to any 3rd party forensic capture tool
- Open remote access: web GUI and RESTful interface
- Scalable, lightweight, MapReduce cluster architecture

Lossless capture to 2Gbps

2 capture interfaces (1G)

100 Active Triggers

2U capture node

100TB physical capture store

Scalable to 4 cluster nodes

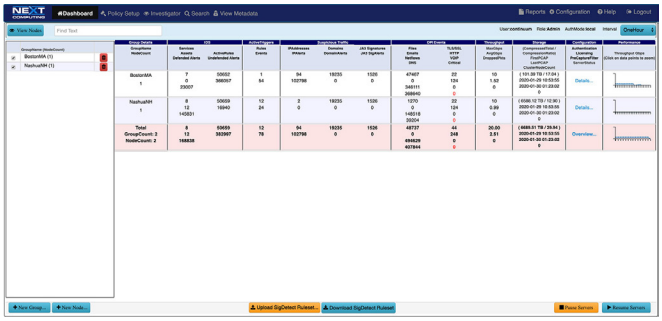
Simultaneous search

Federated search

Very fast query response

Streaming PCAP playback to 3rd party tools

NEXT COMPUTING



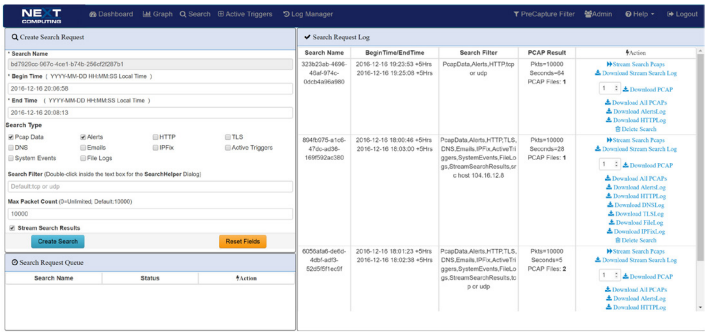
LOSSLESS PACKET CAPTURE & LOG MANAGER, WITH DETERMINISTIC PERFORMANCE

Packet Continuum provides a performance guarantee of sustained lossless capture rate, for a set of real-time packet analytics (Log Manager) functions, and a specified number of Packet Continuum cluster nodes. This means a deterministic guarantee to capture every packet under real world conditions, not just a "best effort" attempt.

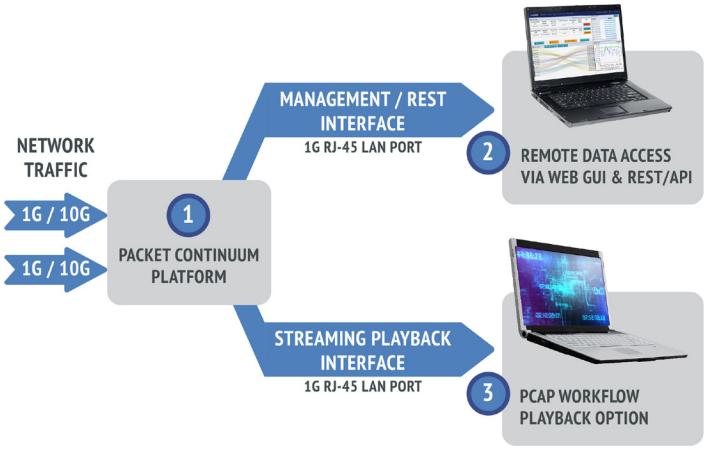
- Real-time indexing, for efficient query and retrieval of retrospective PCAP data or NetFlow records
- Log Manager advanced packet analytics options include real-time event logging & cross-correlation:
  - Logs for HTTP, files, DNS, email, user agents, NetFlow, TLS/SSL, and VOIP
  - Active Triggers (BPF signature)
  - Snort rules (emerging-DNS, emerging-ftp, and files)
  - System events
- Log Manager search actions:
  - All logs are time-correlated with PCAPs, NetFlow data
  - Text string search of logs
  - NetFlow record logging and search

FIND CRITICAL EVENT INFORMATION FAST!

- Fast, Streamed Query Results: Every query has the option to return PCAP files, NetFlow records, and/or any log files. Especially valuable for PCAP queries, all results are streamed in "chunks", allowing partial results to be analyzed while the remaining query is completed, the first of which appear almost immediately after the query initiates.
- "One-Click" searches directly from Sankey Relationship Diagrams, Time Graph or Critical Alerts Log.
- Historical "look-back" queries based on standard Berkeley Packet Filter (BPF) within a time period. Users can setup multiple BPF-based
- Active Trigger "look-forward" alerts, BPF-based and user-defined, will generate alerts whenever the target condition occurs. Dozens can be active simultaneously.
- Pre-capture filters, also BPF-based, can be changed on-the-fly during capture operations.
- All historical logs are searchable by text string
- Cluster systems may be globally federated for unified search/retrieval, or locally aggregated for lossless capture in excess of 100+Gbps.



NEXT COMPUTING



STREAMING PLAYBACK FEATURE

- PCAPs that have been searched/filtered/extracted with the Packet Continuum UI may be regenerated out a 1G copper RJ45 interface to an external device.

OPEN DATA ACCESS

- Open file formats and data viewers: standard PCAP-NG file and NetFlow record extractions are viewable in Wireshark or TShark. All log files and alerts are viewable as CSV or text files in any compatible application such as MSFT Office.

REAL-TIME LOG MANAGER / DATA RECORDER

- Packet Continuum is a lossless, time-based data recorder of PCAP files, IPIX flow records, Log files and Alerts. All data is searchable, with actionable correlations. All data is accessible via an open REST/API.

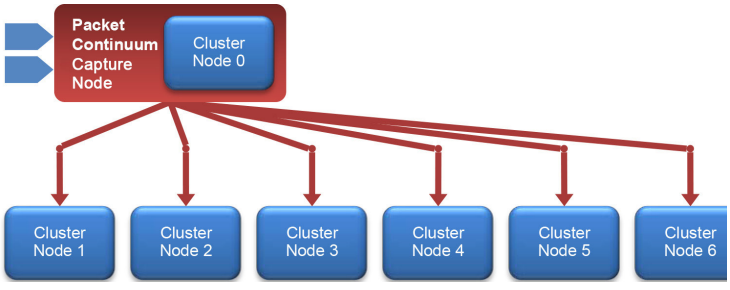
FOR END USERS

This "Open PCAP Infrastructure" has multiple use cases across the enterprise:

- **SOC & Cyber Security** teams need access to PCAPs for Incident Response (IR) investigations.
- **IT/Operations** needs fast IR access regarding uptime and performance problems.
- **Compliance, Audit and Legal** teams increasingly have their own IR requirements for the same ground truth for critical network events.

FOR OEMS

You can further differentiate yourself with the Packet Continuum through private label branding, customer-specific features, and application integration, as well as additional OEM appliance services offered by NextComputing.
We can help you productize your innovation with first to market advantage for a specific service solution or product appliance.

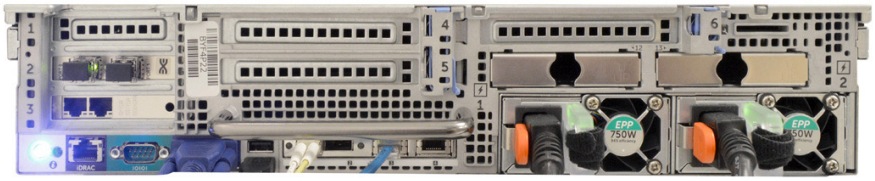


Rev 1.8b—10/18

PACKET CONTINUUM ENTERPRISE LITE

SYSTEM SPECS

Capture Interface Options	2 x 1G interfaces
Capture Rate	• Up to 2Gbps aggregate lossless capture rate with packet analytics enabled *Additional cluster nodes increase: capture rate, forensics timeline, and/or advanced packet analytics*
Time Stamp	150 nanoseconds
Pre-Capture Filter	BPF (dynamically adjustable)
Active Triggers	BPF (100 simultaneous)
Management Interface	1G RJ-45 LAN port, to an external host for Web GUI and REST/API. Automation via REST API and shell scripts to assist with automated workflows.
Playback Interface	PCAP Streaming / Playback Interface: Playback of filtered packets from historical searches via 1G RJ-45 LAN port, to an external traffic/ PCAP analyzer
Encryption	Optional AES256 encryption on OS/application and data arrays. *Note:* Capture Store capacity reduced by 20%, per each Capture Node and/or Cluster Node
Device Control	IPMI Interface
Operating System	CentOS or RedHat
Forensic Timeline - Capture Node	• 100TB PCAP storage • Capture timeline: 4-20 days, assuming 2Gbps average capture rate
Forensic Timeline - Cluster Node	• 100TB PCAP storage • Capture timeline: 4-20 days, assuming 2Gbps average capture rate
Forensic Timeline - Max System Capacity	• Up to 4 cluster nodes • For more capacity, “clusters of clusters” may be configured A single “Federation” may include up to 100 Capture Nodes (or Capture Clusters), where the remote user interface (and REST/API access) provides a unified view of all PCAP/log data and allows federated data queries. For additional capacity, “federations of federations” may be configured.
Support	Global hardware support direct from the enterprise-grade computer vendor, with software support from NextComputing
Physical	• Capture Node: 2U rackmount, 26.92”(683.77mm) depth • Cluster Node: 2U rackmount, 26.92” (683.77mm) depth
OEM Services	• Front bezel branding, soft bag branding, GUI branding, and customization services • Packet Continuum RESTful interface for network-based laptop or remote client access • OEM/solution provider-specific analytics, visualization and cyber solutions • Other OEM/solution provider services available to help you create your cyber appliance solution

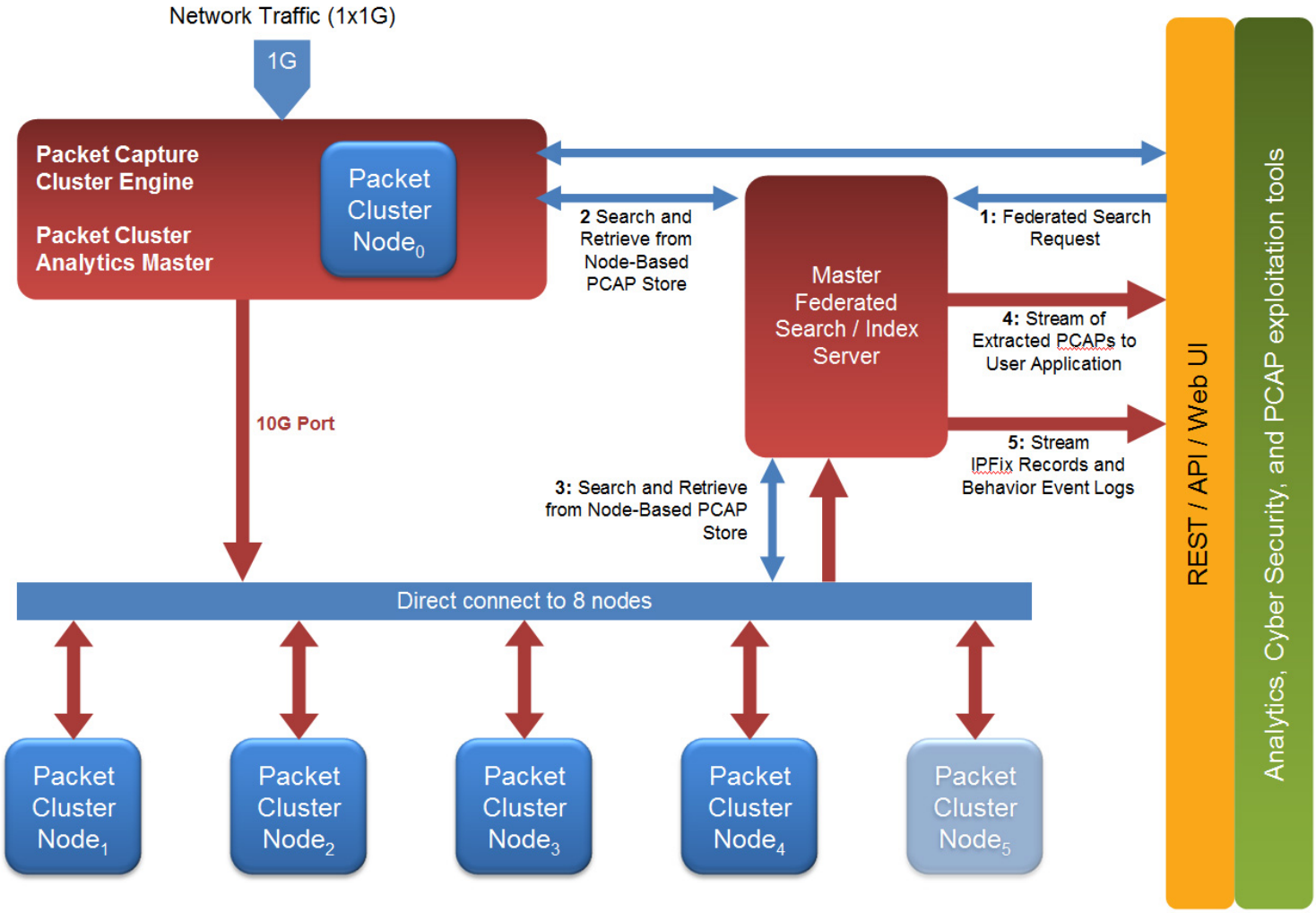


NEXT COMPUTING

4 TOWNSEND WEST, BUILDING 17, NASHUA, NH 03063
PHONE: 1 (603) 886-3874 • FAX: 1 (603) 886-1736
WWW.NEXTCOMPUTING.COM • SALES@NEXTCOMPUTING.COM

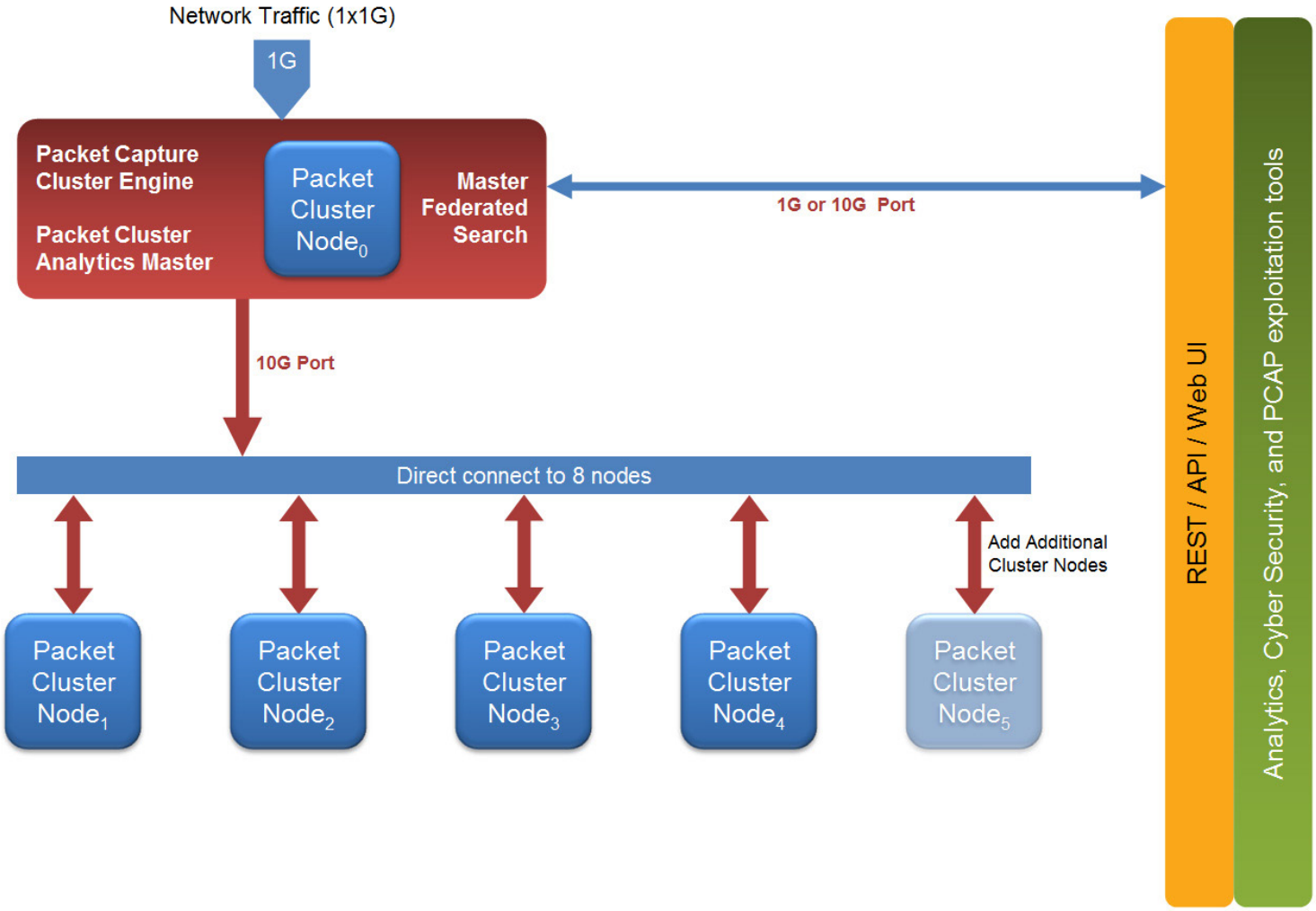
NEXT COMPUTING

CAPTURE, INDEXING, AND SEARCH EXTRACTION



NEXT COMPUTING

CAPTURE, INDEXING, AND DISTRIBUTED SEARCH EXTRACTION



Rev 1.8b—10/18