PACKET CONTINUUM

DEPLOYABLE ENTERPRISE PACKET CAPTURE PLATFORM

Innovative, High-Density Rackmount Appliance For Cyber Analytics OEMs and Solution Providers

Within a compact, short-depth rackmount footprint, the Packet Continuum Deployable Enterprise Packet Capture Platform is based on NextComputing's unique Packet Continuum capture and storage architecture. The system platform is a NextComputing 2U short-depth 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 10Gbps aggregate capture rate
- Extended forensic timeline and storage features, starting with 10TB physical storage in a stand-alone capture node, up to max amplified storage of 500TB 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 10Gbps

2 capture interfaces (10G each)

100 Active Triggers

2U capture node

10TB physical capture store

Scalable to 4 cluster nodes

Scalable to 500TB amplified capture store

Simultaneous search

Federated search

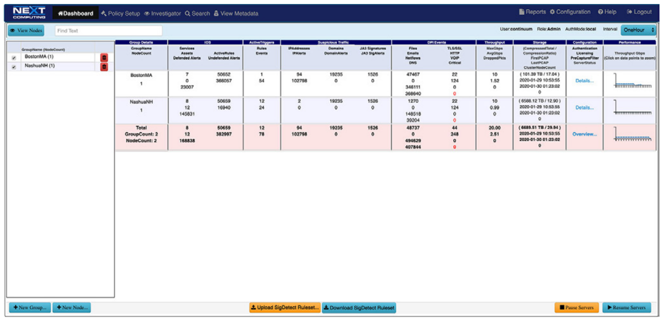
Very fast query response

Streaming PCAP playback to 3rd party tools

NEXT COMPUTING

PACKET CONTINUUM

DEPLOYABLE ENTERPRISE PACKET CAPTURE PLATFORM



User:continuum Role:Admin AuthMode:local Interval OneHour

GroupName (NodeCount)
☑ BostonMA (1)
☑ NashuaNH (1)

Group Details	IDS		ActiveTriggers	Suspicious Traffic			DPI Events		Throughput	Storage	Configuration	Performance
GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points to zoom)
BostonMA 1	7 0 23007	50652 366057	1 54	94 102798	19235 0	1526 0	47467 0 346111 368640	22 124 0 0	10 1.52 0	(101.39 TB / 17.04) 2020-01-29 10:53:55 2020-01-30 01:23:02 0	Details...	
NashuaNH 1	8 12 145831	50659 16940	12 24	2 0	19235 0	1526 0	1270 0 148518 39204	22 124 0 0	10 0.99 0	(6588.12 TB / 12.90) 2020-01-29 10:53:55 2020-01-30 01:23:02 0	Details...	
Total GroupCount: 2 NodeCount: 2	8 12 168838	50659 382997	12 78	94 102798	19235 0	1526 0	48737 0 494629 407844	44 248 0 0	20.00 2.51 0	(6689.51 TB / 29.94) 2020-01-29 10:53:55 2020-01-30 01:23:02 0	Overview...	

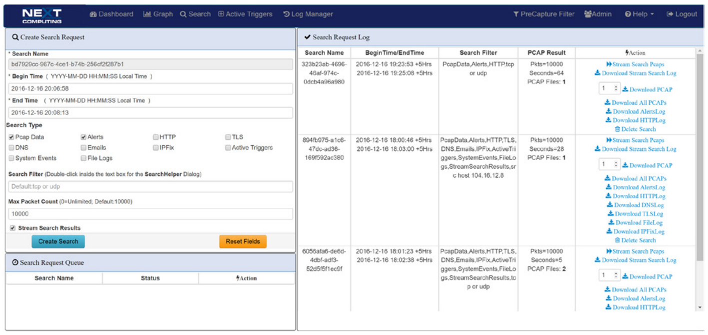
LOSSLESS PACKET CAPTURE & LOG MANAGER, WITH DETERMINISTIC PERFORMANCE

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.



Create Search Request

* Search Name
bd7929cc-967c-4ce1-b74b-256cf2f287b1
* Begin Time (YYYY-MM-DD HH:MM:SS Local Time)
2016-12-16 20:06:58
* End Time (YYYY-MM-DD HH:MM:SS Local Time)
2016-12-16 20:08:13

Search Type
☑ Pcap Data ☑ Alerts □ HTTP □ TLS
□ DNS □ Emails □ IPFix □ Active Triggers
□ System Events □ File Logs

Search Filter (Double-click inside the text box for the SearchHelper Dialog)
Default:tcp or udp
Max Packet Count (0=Unlimited; Default:10000)
10000
☑ Stream Search Results

Search Request Queue

Search Name	Status	Action

Search Request Log

Search Name	BeginTime/EndTime	Search Filter	PCAP Result	Action

323b23ab-4696-46af-974c-0dcb4a96a980	2016-12-16 19:23:53 +5Hrs
	2016-12-16 19:25:08 +5Hrs
		PcapData,Alerts,HTTP,tcp or udp	Pkts=10000
			Seconds=64
			PCAP Files: 1
				Stream Search Pcaps
				Download Stream Search Log
				1 Download PCAP
				Download All PCAPs
				Download AlertsLog
				Download HTTPLog
				Delete Search

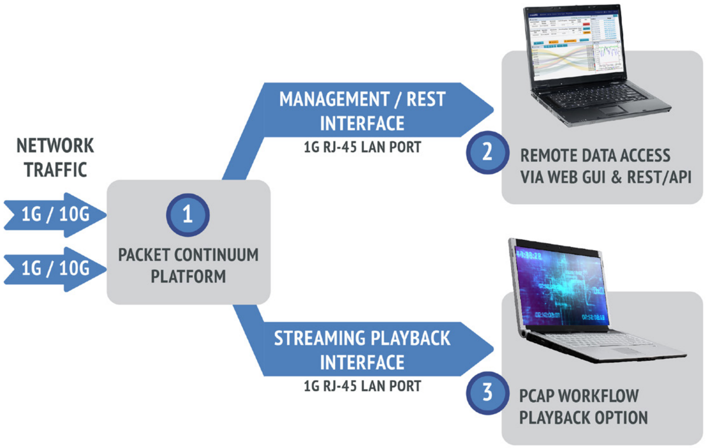
894fb975-a1c6-47dc-ad36-169f592ac380	2016-12-16 18:00:46 +5Hrs
	2016-12-16 18:03:00 +5Hrs
		PcapData,Alerts,HTTP,TLS,DNS,Emails,IPFix,ActiveTriggers,SystemEvents,FileLogs,StreamSearchResults,src host 104.16.12.8	Pkts=10000
			Seconds=28
			PCAP Files: 1
				Stream Search Pcaps
				Download Stream Search Log
				1 Download PCAP
				Download All PCAPs
				Download AlertsLog
				Download HTTPLog
				Download DNSLog
				Download TLSLog
				Download FileLog
				Download IPFixLog
				Delete Search

6056afa6-de6d-4dbf-adf3-52d5f5f1ec9f	2016-12-16 18:01:23 +5Hrs
	2016-12-16 18:02:38 +5Hrs
		PcapData,Alerts,HTTP,TLS,DNS,Emails,IPFix,ActiveTriggers,SystemEvents,FileLogs,StreamSearchResults,tcp or udp	Pkts=10000
			Seconds=5
			PCAP Files: 2
				Stream Search Pcaps
				Download Stream Search Log
				1 Download PCAP
				Download All PCAPs
				Download AlertsLog
				Download HTTPLog

NEXT COMPUTING

PACKET CONTINUUM

DEPLOYABLE ENTERPRISE PACKET CAPTURE PLATFORM


NETWORK TRAFFIC
1G / 10G
1G / 10G
1
PACKET CONTINUUM PLATFORM
MANAGEMENT / REST INTERFACE
1G RJ-45 LAN PORT
2
REMOTE DATA ACCESS VIA WEB GUI & REST/API
STREAMING PLAYBACK INTERFACE
1G RJ-45 LAN PORT
3
PCAP WORKFLOW PLAYBACK OPTION

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.

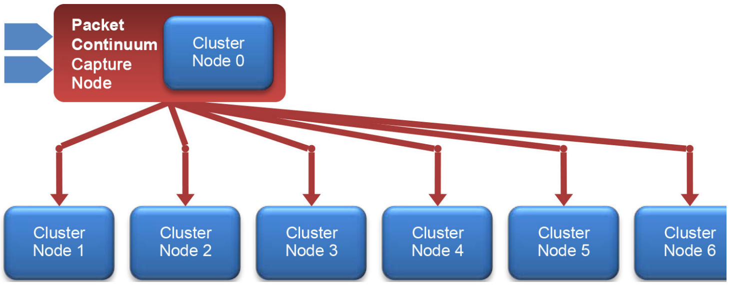
FOR END USERS

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.

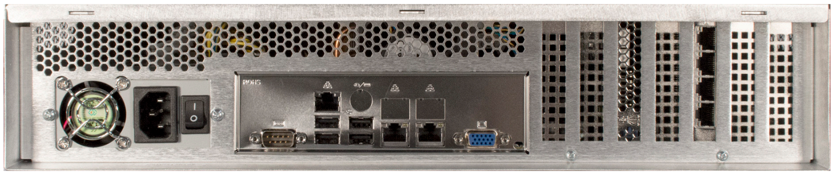
FOR OEMS

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.



PACKET CONTINUUM DEPLOYABLE ENTERPRISE SYSTEM SPECS

Capture Interfaces	2 capture interfaces up to 10Gbps aggregate (Includes 2 SFP+SR modules and 2 SFP RJ45 1G modules hot swappable)
Capture Rate	Up to 10Gbps aggregate lossless capture rate *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	• 20TB PCAP storage • Capture timeline: 2-16 hours, assuming 10Gbps average capture rate
Forensic Timeline - Cluster Node	• 20TB PCAP storage • Capture timeline: 2-16 hours, assuming 10Gbps 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	Full appliance support from NextComputing
Physical	Capture Node & Cluster Nodes: 2U rackmount, 17”(431.8mm) 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

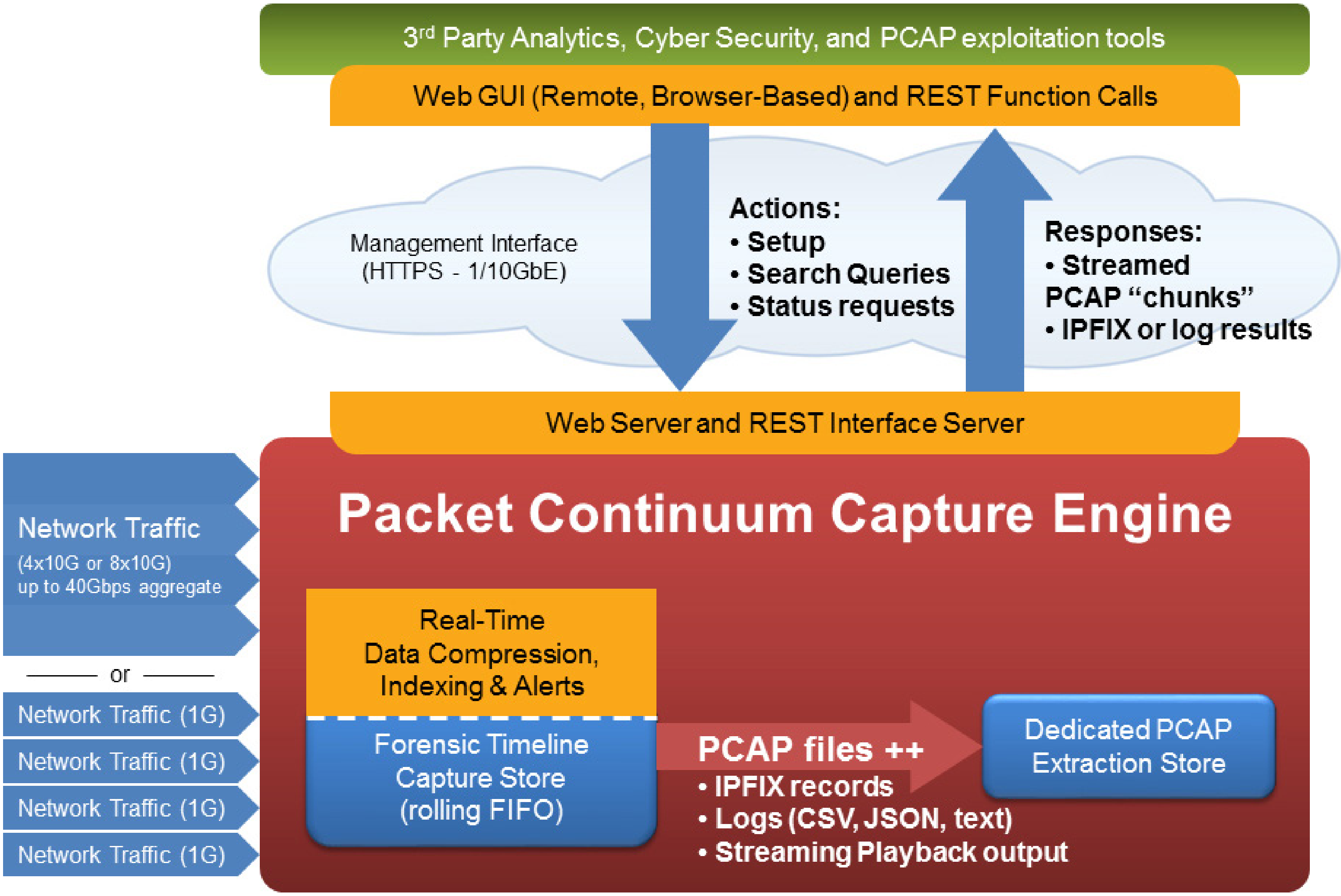


This document is for informational purposes only. Updates and changes can occur without notice. All logos, trademarks, and service marks are the property of their respective owners. Copyright © NextComputing all rights reserved.

NEXT COMPUTING

PACKET CONTINUUM

DEPLOYABLE ENTERPRISE PACKET CAPTURE PLATFORM



3rd Party Analytics, Cyber Security, and PCAP exploitation tools

Web GUI (Remote, Browser-Based) and REST Function Calls

Management Interface (HTTPS - 1/10GbE)

Actions:
- Setup
- Search Queries
- Status requests

Responses:
- Streamed PCAP "chunks"
- IPFIX or log results

Web Server and REST Interface Server

Network Traffic (4x10G or 8x10G) up to 40Gbps aggregate

or

Network Traffic (1G)

Network Traffic (1G)

Network Traffic (1G)

Network Traffic (1G)

Packet Continuum Capture Engine

Real-Time Data Compression, Indexing & Alerts

Forensic Timeline Capture Store (rolling FIFO)

PCAP files ++
- IPFIX records
- Logs (CSV, JSON, text)
- Streaming Playback output

Dedicated PCAP Extraction Store