NEXT COMPUTING

PACKET CONTINUUM

CARRIER-GRADE PACKET CAPTURE AND NETWORK EVENT LOGGING FOR SOC AND NOC TEAMS AND SERVICE PROVIDERS

Packet Continuum is a powerful software architecture for continuous capture targeting. NextComputing offers a flexible business model for financial, technical and logistic support services. Core functions include:

- Advanced policy-driven threat-hunting
- Real-time alerting/detection of Indicators of Compromise (standards-based)
- Automated workflows, triggered by IoC or anomaly events, can extract critical PCAP files for forensic analysis
- Integrated Threat Hunting / Log Manager can prioritize Active Hunt analyst activity
- Fast search of lossless packet capture history, and correlation with events and logs

Packet Continuum targets SOC and IT Operations within Service Providers and End User Enterprises. Use cases include:

- Threat-Hunting and IoC Audit/Assessment
- SOC team Incident Response
- Network IT/Operations packet-based QoS troubleshooting

Federation allows multiple authorized users to access & manage large networks of Packet Continuum appliances in the field:

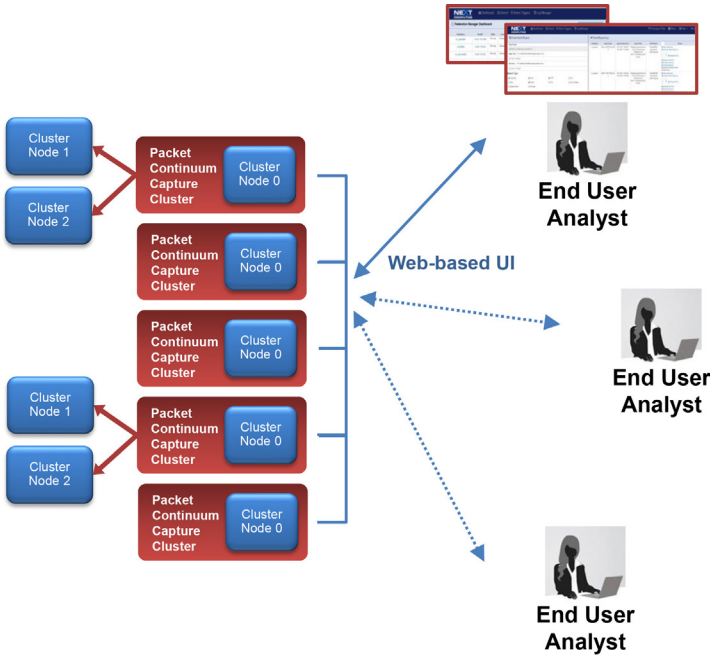
• *Federated Dashboard & Threat-Hunting* views let you see all real-time data via a single, unified web-based User Interface.

• A single, federated query will find critical event data from all appliances.

• Remote packet viewer gives instant Wireshark-like features to any full session content for an alert.

• *Download* PCAP files for analysis with centralized tools.

• *Upload* rulesets of IDS Alerts (or new Threat-IP Lists) to ALL appliances – *simultaneously!*



Numerous distributed sensor/recorders within a highly-scalable "Federated" network architecture, for close coordination with a central Security / Network Operations Center.

PCAP + IoC alerts, with deterministic performance

Labor / cost reduction for SOC teams

Simplified, open PCAP workflows

Behavior / signature visibility & logging

Scalable / federated

Email search / extraction

File leakage / exfiltration

TLS / SSL visibility

VOIP logging

Extended forensic timelines

Fast query / streaming

Open data interfaces

Web UI / REST API

Flexible subscription/ finance options

EXTREME SCALABILITY

Packet Continuum deploys on a wide range of rackmount and desktop common hardware platforms, from cost-effective sensor/recorders to enterprise-class servers (see Platforms Table on last page). It is uniquely cost-effective when deployed at scale. Examples of how Packet Continuum can scale include:

- Numerous distributed sensor/recorders within a highly-scalable "Federated" network architecture, for close coordination with a central Security / Network Operations Center.
- Long capture timelines for days, weeks, or months of lossless packet capture data history, when quick-response search is required. Added timeline features include in-line data compression and policy-driven data retention.
- High capture rate capture points (eg. 40Gbps, 100Gbps, and beyond) where a full feature set of real-time analytics functions must run at line rate with deterministic performance: Continuous lossless full packet capture (PCAP), real-time IDS alerting and other user-defined Policy Management, with simultaneous search/recall for Incident Response.

Packet Continuum is disrupting the market with open data access, smooth scale, and long timelines – at very low cost.

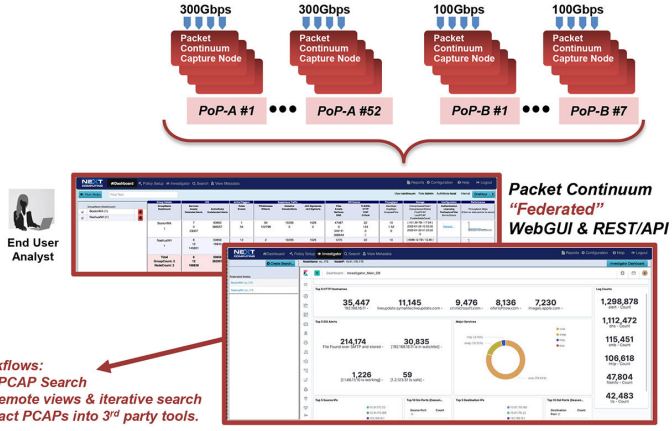
As an "Open PCAP Infrastructure", the Packet Continuum supports even the largest enterprise-scale users. Lossless packet capture is the immutable ground truth of any critical event – not merely an interpretation. Take direct ownership of your own critical network data resource.

TELCO EXAMPLE: 60 FEDERATED INTERNET POP SITES

System-wide Capture Rate:
52 PoP-A sites (300Gbps each)
+ 7 PoP-B sites (100Gbps each)
16.3 Tbps continuous lossless capture (aggregate)

System-wide Capture Timeline:
52 PoP-A sites (9.0PB each, for 6 Day timeline)
+ 7 PoP-B sites (7.5PB each, for 2 Weeks timeline)
520PB Capture Store

Rackspace:
52 PoP-A sites (15 x 4U servers each)
+ 7 PoP-B sites (12 x 4U servers each)
864 total # of 4U servers



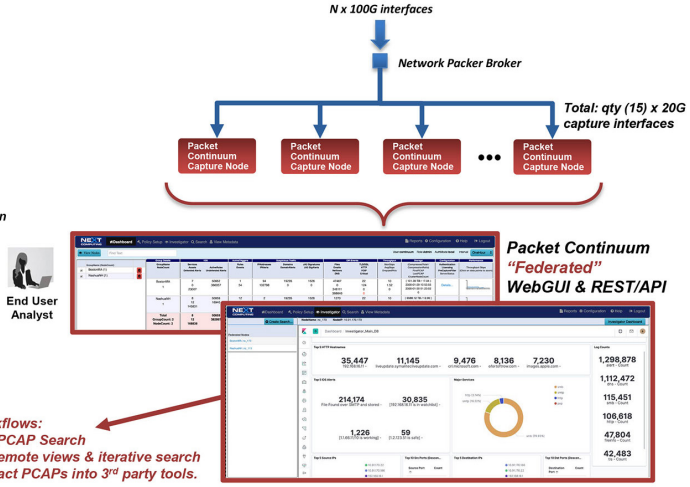
TELCO EXAMPLE: 300GBPS FOR 6 DAYS REQUIRED PER POP SITE

Capture Rate:
- *300Gbps PEAK continuous lossless capture*
- *IDS alerting at line rate*
- *Simultaneous PCAP search*
- *qty 15 Standalone Capture Nodes*

x 20 Gbps Average capture rate for 2 Days Timeline
300 Gbps Total aggregate capture rate

Capture Timeline:
- *6 Days, assuming 300Gbps AVERAGE rate, 2:1 data compression*
- *9.0PB Total Capture Store*

Rackspace:
- *qty 15 x 4U servers:*
  Up to 20Gbps lossless Capture Rate
  600TB Capture Store



POLICY-DRIVEN, AUTOMATED INCIDENT TRIAGE + WORKFLOW

The Packet Continuum user interface (and programmatic REST/API) integrates Policy Management, Threat Hunting / Log Management, Forensic Investigation, and Open Data Access.

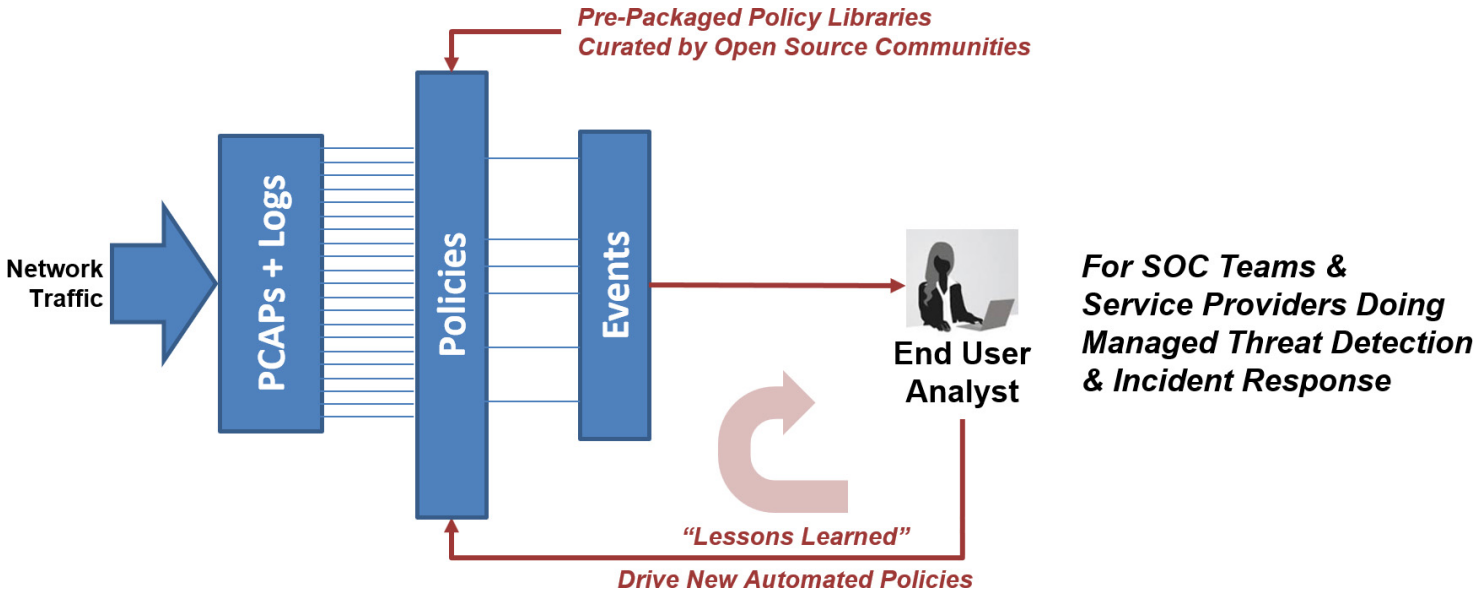
All policies generation logs/metadata which are compressed, correlated, and instantly searchable.

All policies integrate within a full-featured Threat Hunting / Log Management User Interface.

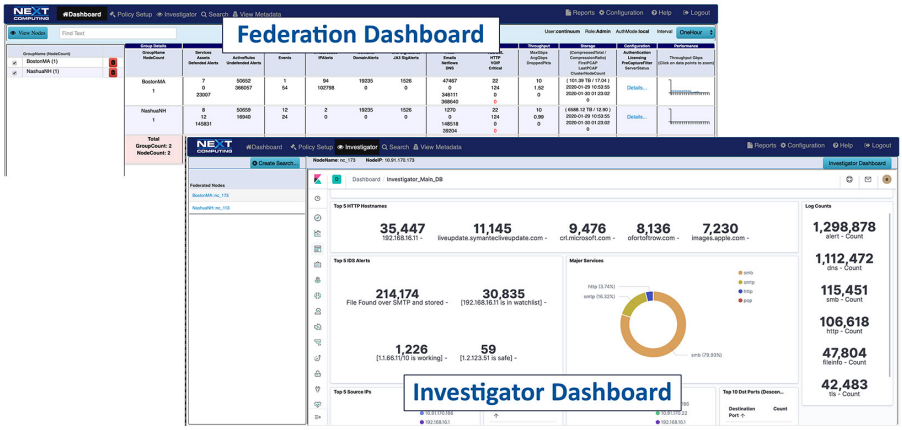
Packet Continuum facilitates the "Spiral-Model" methodology for effective forensic investigations.

An integrated Threat Hunting / Log Manager gives visibility to analysts about critical events, and allows quick drill-down to full session logs and full PCAP file content. Real-time IoC Policy Management comes with pre-packaged ruleset libraries, and allows SOC teams to design and upload their own rule sets, including

- IDS rulesets
- Malware rulesets
- ThreatIP lists
- Defended assets
- Defended services
- BPF-based Active Triggers
- Suspicious Domain lists
- Suspicious File Hash lists
- Suspicious TLS/SSL signatures (JA3)

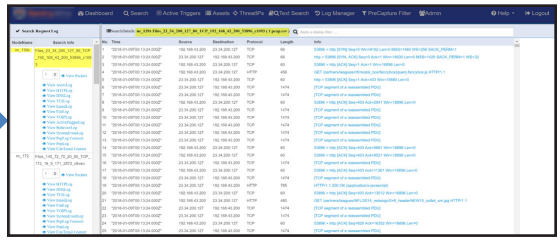


SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS



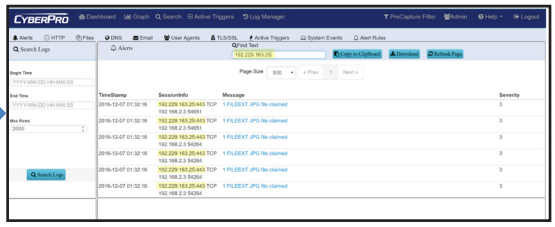
ANALYST OPERATIONS DASHBOARDS

- Prioritizes real-time Indicators of Compromise (IoC) & Incident Response actions
- Automated mapping of IoC events to adversary behavior in the Kill Chain
- One-click searches direct from the dashboard
- Live updates to the Capture Data Graph, and Critical Alerts List



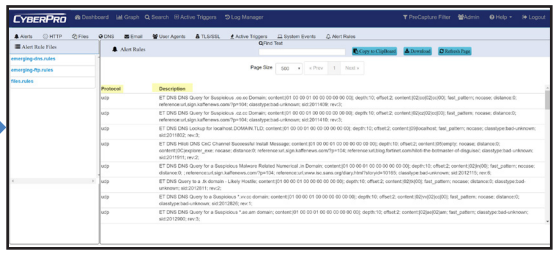
POLICY ALERTS DRIVES INCIDENT RESPONSE

- Start with red-flag behavior, like Exfiltration or suspect C&C activity
- One-click search to show IoCs for each step in the Kill Chain
- Then click to preview for all correlated PCAP data



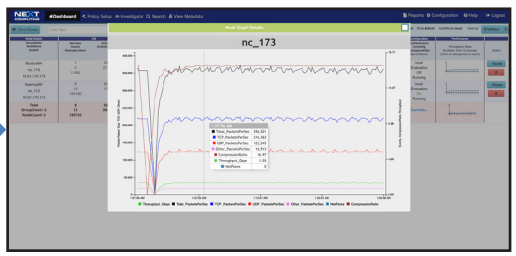
THREAT HUNTING - IOC POLICIES

- SNORT/SURICATA Rule Sets
- Threat IPs
- Defended Assets & Services
- Active Triggers (BPF-based)
- Threat IPs and Suspicious Traffic alerts



LOG MANAGER - EVENT SEARCH ACTIONS

- One-click time-based BPF search
- Text-based search of alerts
- All IoC events correlated with PCAPs, NetFlow records, and sessionized logs

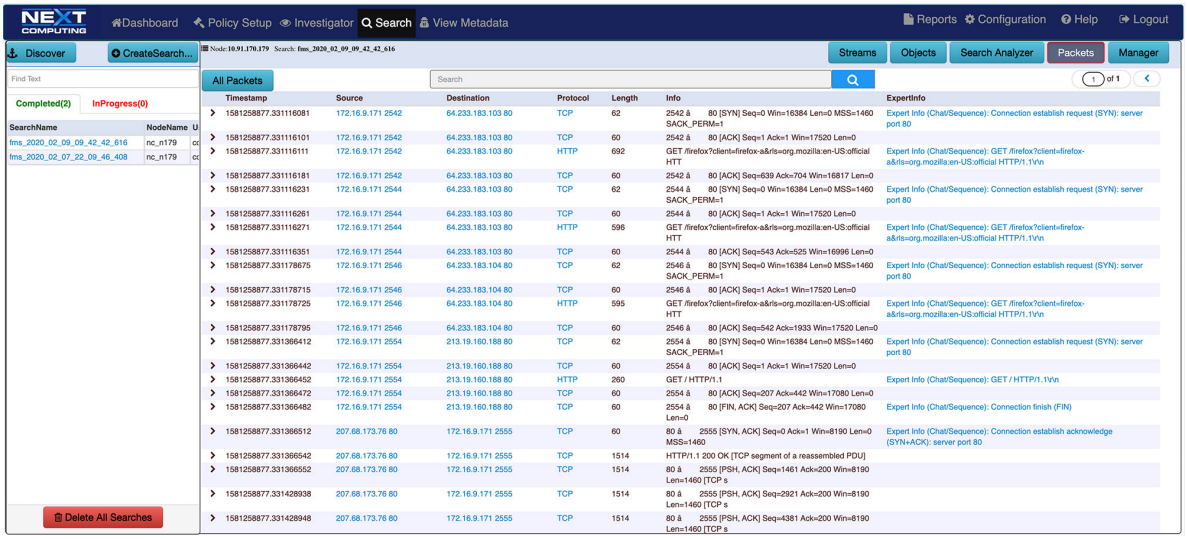


TIME-BASED DATA GRAPH

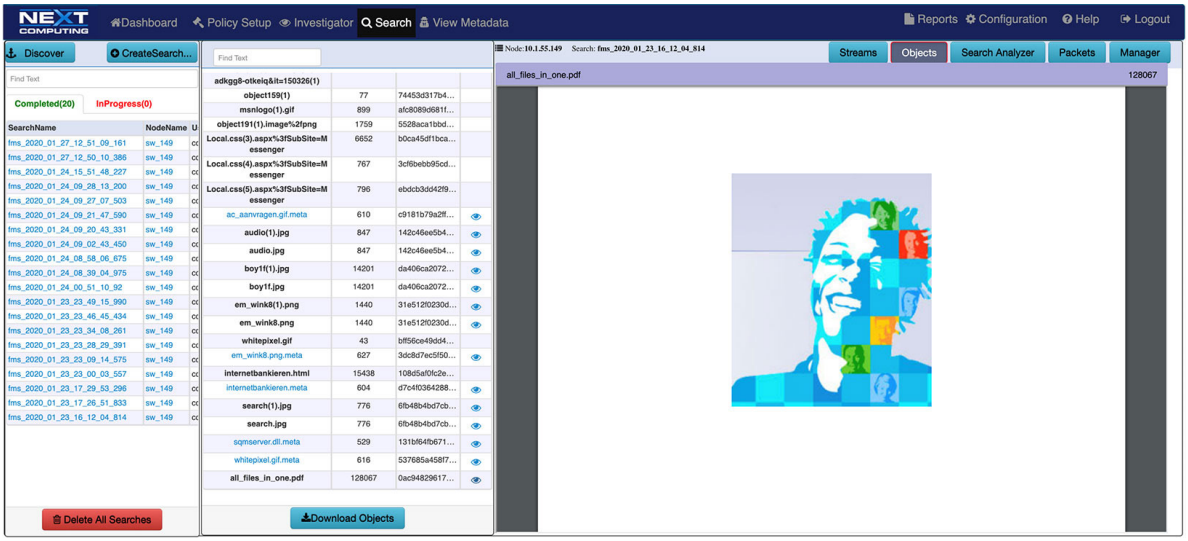
- With legends consisting of key packet capture and data compression statistics.
- One-Click search from any point in time, will automatically fill in a search request

INTEGRATED, WEB-BASED PACKET DATA VIEWERS

Users may view search results such as PCAP sessions, packets, log data and the content pdf, in-place on the appliance, without requiring any other external tools or downloading any files. Besides viewing, user also has the capability to create more concentrated and focused searches from the view data available – and to further target with a text-search of all content.



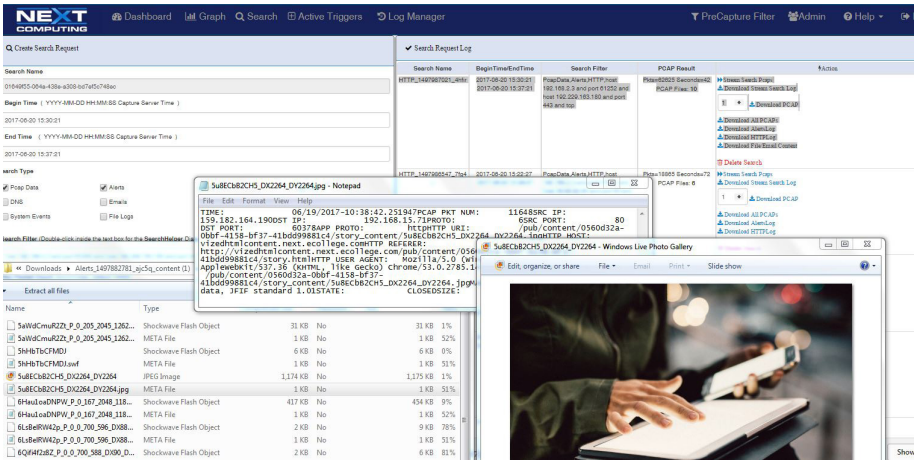
Clicking on search data or logs, displays the details on the right panel. For example, clicking "Packets View" shows an integrated web-based packet viewer has similar features to the Wireshark dashboard screen: the sequence of packets, each with timestamp, 5-tuple data, packet length, and the text-based "info column".



Clicking on "Objects View" data displays a pdf view of the content extracted during the search process.

SIMPLIFIED WORKFLOW

Packet Continuum simplifies your workflow by integrating endpoint behavior and network signature visibility and DPI with a simple pivot to the sessionized network data, enriched metadata and file recovery. Mitigate the nearly 2/3 of breaches per incident that are easy to catch, like administrative issues by implementing effective, basic cyber practice policies by tracking user agent signature characteristics, email and file exfiltration.



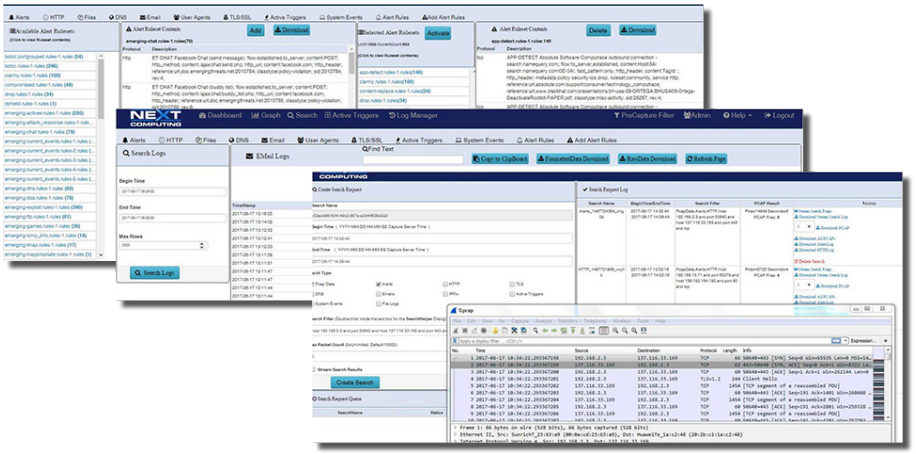
Log Manager showing HTTP log tab - HTTP session extraction and reconstruction of various files on the web page, including a JPG file showing the original content and metadata file breaking down the JPG file

BEHAVIOR / SIGNATURE VISIBILITY & LOGGING

The Threat Hunting / Log Manager's enhanced search capabilities allowing integrated pivot to PCAP and enriched metadata enables behavior and signature visibility.

The IDS Alert configurator and DPI Analyzer enable multi-level signature and behavior event session search and logging. This gives you the ability to configure groupings of signature and unusual behavior alerts dynamically from a grouping of 30,000.

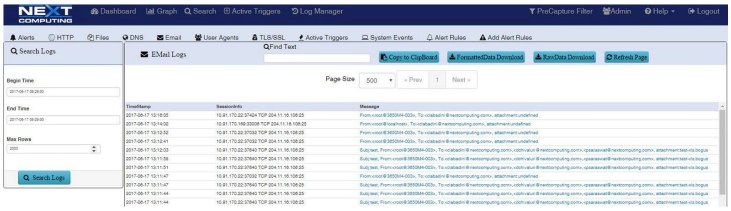
The real-time IDS alert configurator generates event logs for HTTP, Files, DNS, email, user agents, TLS/SSL, VOIP – all cross-correlated with PCAP & NetFlow V9 flow records.



EMAIL SEARCH / EXTRACTION

Identify and search email strings and subjects. Email extraction feature includes sender, receiver, subject line and text reconstruction.

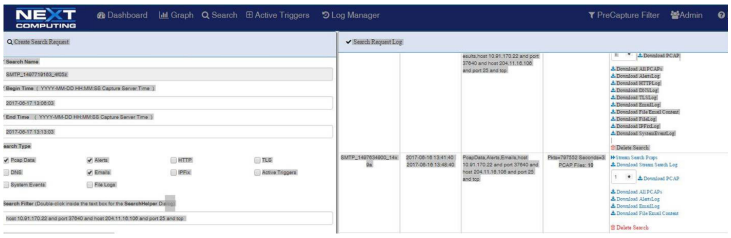
- SMTP email session logging with body text in HTMP format and file attachment reconstruction from original Mime format
- SMTP subject, send and receive email address logging



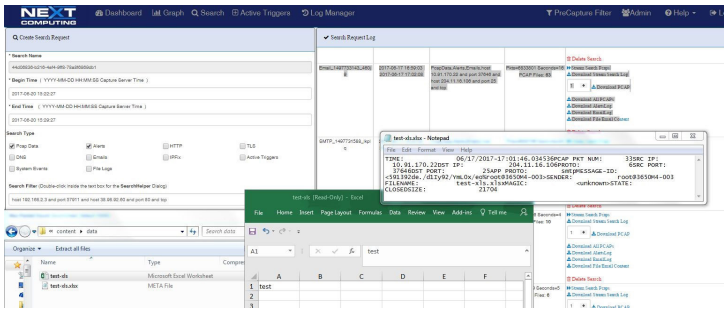
List of SMTP emails sessions searchable with time stamp, capture node location, session information and SMTP email address, sender/receiver. A user can click to get the full session packets, extract email subject/text and reconstruct file attachments in original mime format, PDF, doc, etc.

Packet Continuum simplifies the email session logging process with pivot to sessionized search and file recovery.

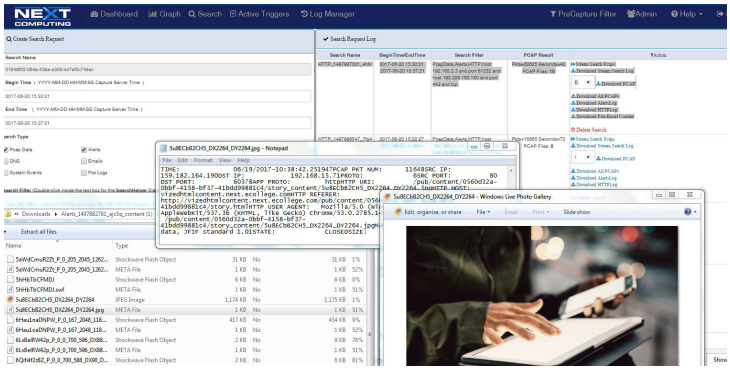
- Free form text search capability
- Clickable by event
- Second click initiates packet session recovery and file reconstruction
- Just two more clicks to the reconstructed file and meta data for that HTTP or SMTP email session
- All viewable and downloadable



Search window based on selected sessions



Log Manager email tab showing SMTP email session Extraction and Reconstruction of email attachment as Excel file with original content and metadata file

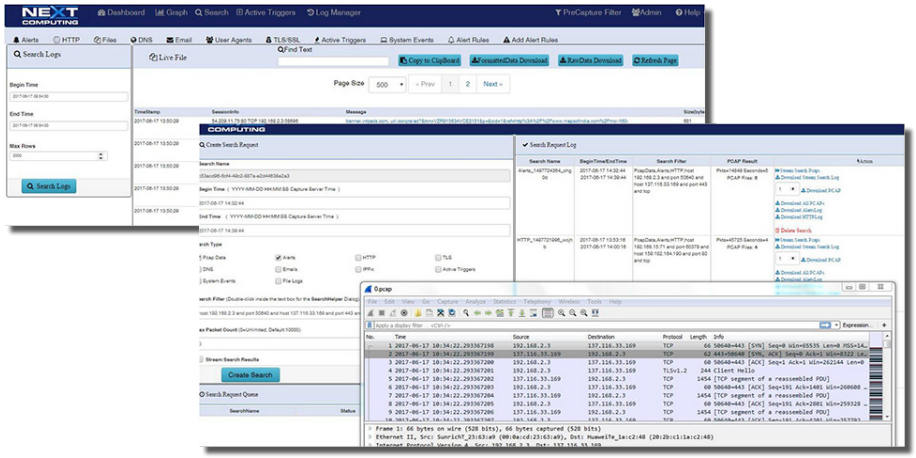


Reconstructed JPG file displayed with the metadata file associated with that graphic image

FILE LEAKAGE / EXFILTRATION

Packet Continuum enables

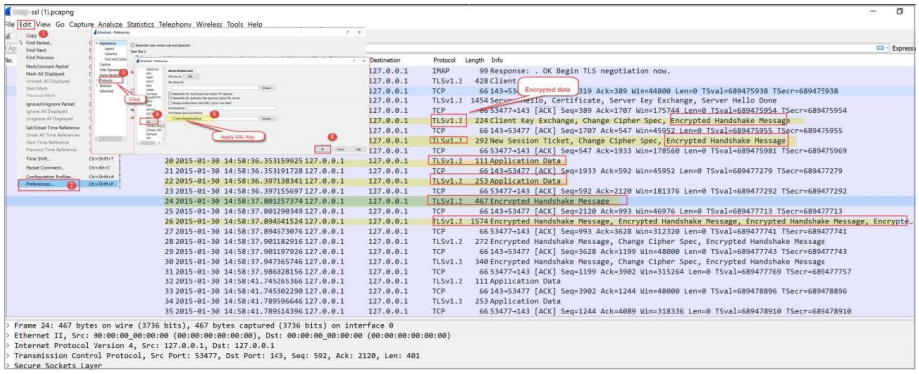
- HTTP, email and file transfer session logging and identification
- Reconstruction of files and associated metadata in original mime type for viewing and analysis



File Leakage Session showing logs and pivot to session search and file reconstruction with metadata

TLS / SSL VISIBILITY

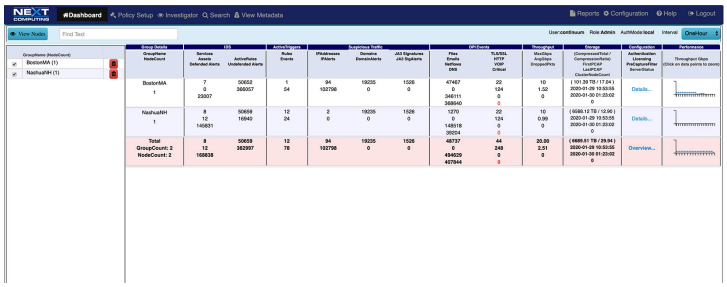
Gain visibility into TLS / SSL encrypted sessions. Log and extract sessionized PCAP data via timestamp, capture node and session information for recovery of sessionized packets, then offload them to WireShark using customer provided keys.



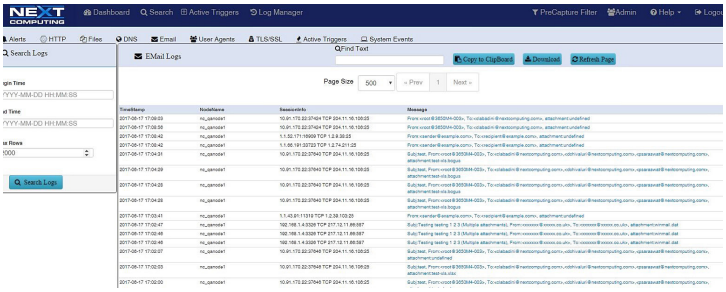
FEDERATION MANAGER

Packet Continuum massively scalable Federation Manager allows you to federate multiple capture appliances in multiple locations.

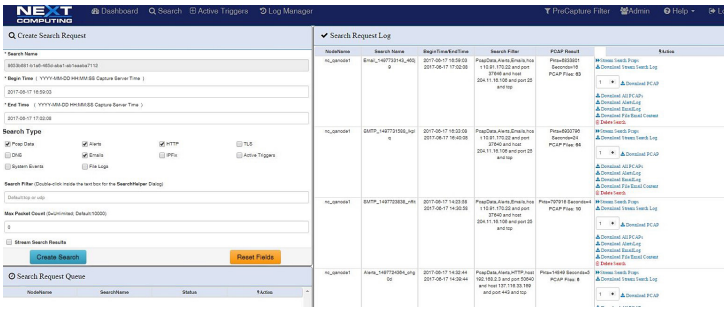
- Remote control capability via browser and REST API
- Federated View of all data
- Map-reduced framework to extract out packets, DPI data and logs across federation



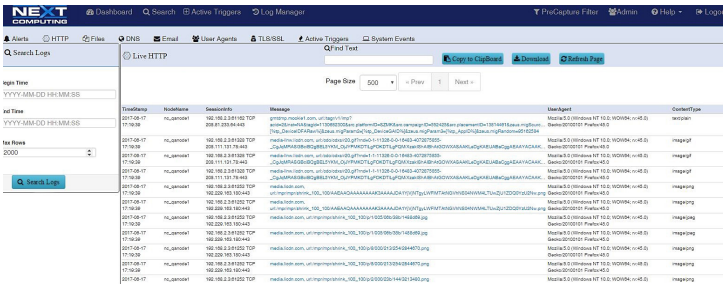
Federation manager dashboard for easy identification of Packet Continuum appliances/ clusters that can even be in different physical locations. Your enterprise network can identify the IP address of each appliance and federate together for a single pane of glass view of all network data.



Federated list of SMTP email sessions with time stamp, capture node location, session information, and SMTP email address, sender, and receiver. The user can click to obtain full session packets, extract email text, subject and reconstruct attachments in their original mime format, PDF, doc etc.



Federated search across PCAP data, DPI log data and flow records, as well as email text and files for reconstruction.



Federated list of HTTP sessions with time stamp, capture node location, session information, and HTTP link summary and files. The user can click to obtain full session packets, extract email text, subject and reconstruct attachments in their original format.

STANDARDS-BASED POLICIES, WITH OPEN DATA ACCESS

OPEN SOURCE RULESETS & DATA INTERFACES:

- Snort/Suricata — IDS alert rulesets
- Kibana – open data visualization, compatible with the Elastic ELK stack
- JSON – used for open data-interchange and PCAP search parameters
- JA3 – TLS/SSL encrypted traffic signatures
- MD5 – File Malware signatures
- BPF — used for Active Trigger alerts, PCAP search parameters, and pre-capture filtering
- Suspicious Alerts & Augmentation – Flexible user-defined lists
- Defended Assets/Services — Flexible user-defined lists
- TAXII/STIX — pre-packaged rulesets and Suspicious Alerts, supported via structured cyber threat information

OPEN DATA ACCESS, WITH STANDARD FILE FORMATS:

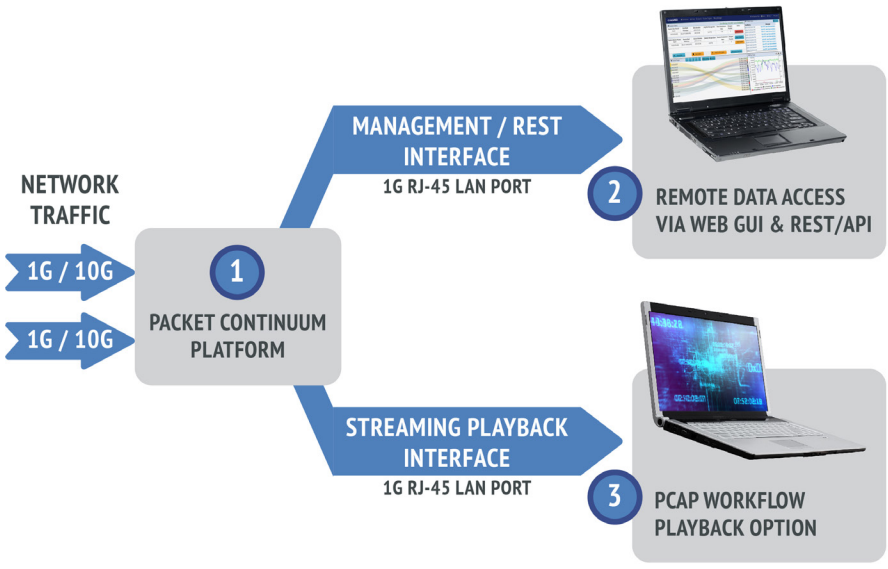
- PCAP-NG for packet data
- NetFlow Version 9 flow records
- Text/CSV/syslog for log enrichment data

OPEN WORKFLOW AUTOMATION & ORCHESTRATION:

- Simplified URL-based actions, via a full-featured, mature REST/API
- Unix Command Line Interface (CLI)
- Custom Workflow Scripting
- 3rd Party Event/Data/PCAP Correlation
- Role-Based Access Control

STREAMING PLAYBACK FEATURE

- PCAPs searched / filtered / extracted with the Packet Continuum UI may be regenerated out a 1G copper RJ45 interface to an external device
- Compatible with ANY 3rd party capture / analysis tool - just like a span / mirror port
- Perfect for recording, additional packet / signature analysis, or back-testing new firewall policies against real historical traffic

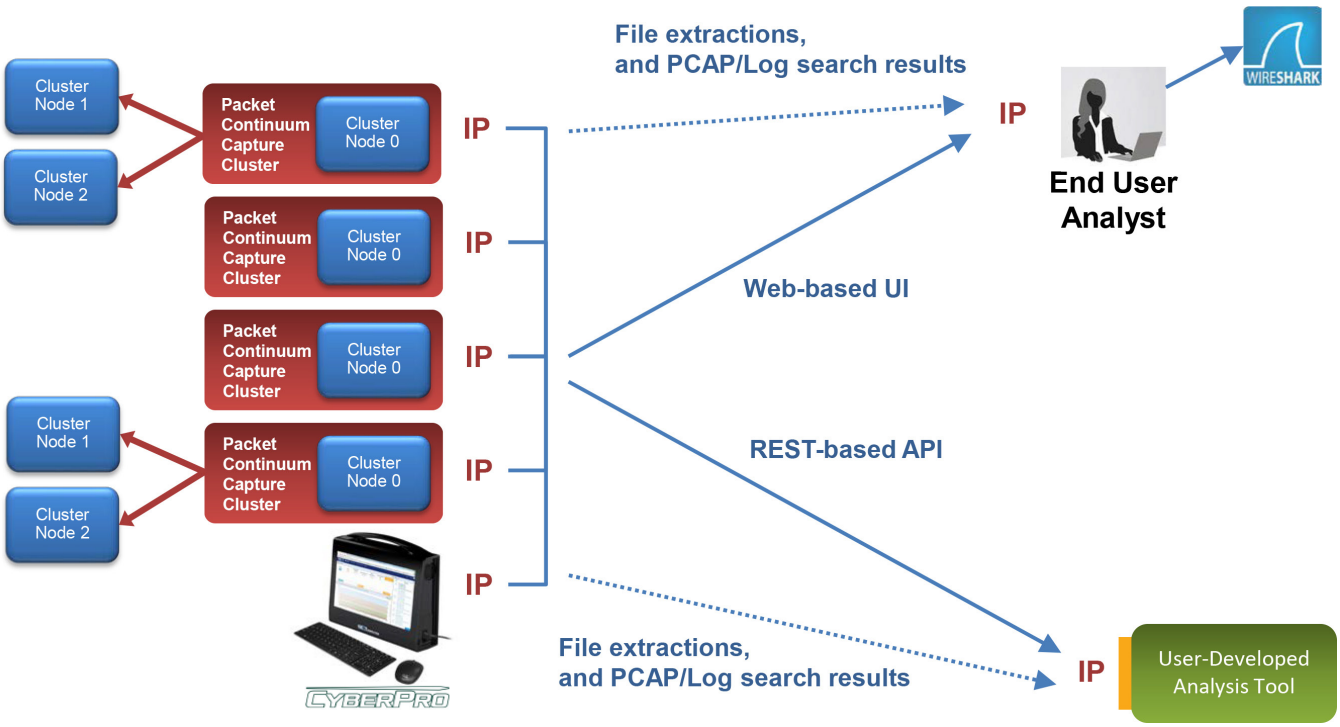


First, find the PCAP data you want, using Log Manager and Remote Packet Viewer, then you may use the Web-based UI to extract the PCAP file sequence via the Management Interface to an external system, for viewing in Wireshark – or another workflow. Alternatively, you may replay the PCAP out the Streaming Playback Interface, which looks like a SPAN port to 3rd party network tool. For example, a common use case for streaming playback is backtesting new IoC policies/rules against historical network traffic.

SCALABLE / FEDERATED

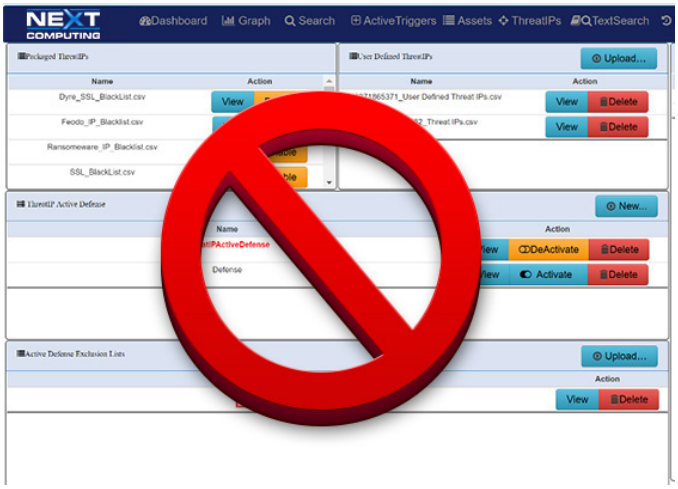
Packet Continuum's highly scalable, high performance network data recorder provides for forensics investigations based on breach detection and changed threats within a reasonable forensics timeline.

- Lightweight, federated control and off-load of data capability
- Scales up smoothly for any combination of desired goals for capture speed, IDS alerting, Threat Hunting / Log Manager functions and extended forensic capture timeline
- Scalable to multiple "cluster nodes"
  - Increased sustained capture rates
  - Increased packet analytics thruput
  - Extended storage timeline
- Capture nodes push packet processing operations to distributed Cluster Nodes enabling
  - PCAP storage, compression and indexing
  - Threat Hunting / Log Manager functions
- Federated search operates in parallel within the cluster enabling incredibly fast streaming results even with very large capture timelines
- Cluster ready for smooth scale up to very high performance
- Dynamic node management
  - Redundancy
  - Hot swap / expand



100s of "federated" capture appliances. Each Analyst has access to the federation via a web-based UI, without any need for intermediary data collectors or data concentrators.

THREAT-IP MONITORING



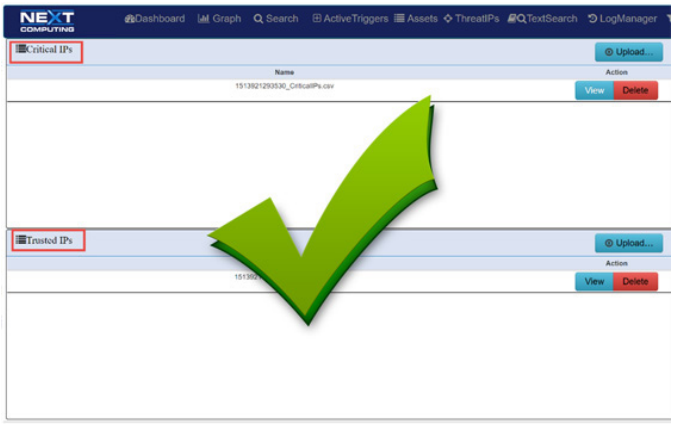
Packet Continuum enables identification, monitoring, viewing, and mitigation of pre-defined Threat IPs as well as user-defined IPs. Packet Continuum comes pre-loaded with a known list of Threat IPs; a number of malicious IPs previously identified by trusted sources such as US-CERT, for your protection.

From the Packet Continuum Threat Hunting / Log Manager, users can:

- Upload/enable, view or delete/disable lists of identified Threat IPs
- Set alerts based on identified Threat IPs
- Create Active Defense actions (via user criteria or Suricata rules) to be taken when a Threat IP is identified
- With one click, view detailed PCAP session information where a threat is identified

When a Threat IP is identified as present in a session, the system generates a severe alert and a pre-defined Active Defense action can be executed or, if one is not available, alert info can be sent to an external server.

PROTECTING DEFENDED ASSETS & DEFENDED SERVICES



You can specify “Defended” end points and services which are especially critical for your organization. This designation affects how information is displayed on the Dashboard screens, and how IoC policy events are tagged/escalated within the Threat Hunting / Log Manager. For example, an analyst can instantly filter out everything except information relevant to those special assets and activities.

From the Packet Continuum Threat Hunting / Log Manager or Operations Dashboard, users can:

- Upload, view or delete lists of identified Asset IPs
- Set alerts based on identified assets
- Monitor / view sessions containing specified assets as the source or destination
- With one click, view detailed PCAP session information where an asset is identified

TRADITIONAL FULL PACKET CAPTURE HAS THE REPUTATION TO BE PROHIBITIVELY EXPENSIVE. PACKET CONTINUUM CHANGES ALL THAT!

LOSSLESS PACKET CAPTURE WITH DATA ENRICHMENT

The immutable ground truth of any critical event – not merely an interpretation. Packet Continuum provides a performance guarantee of sustained lossless capture rate, for a set of real-time packet analytics (Threat Hunting / 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.

- Lossless packet capture from 1Gbps, to 40Gbps, to 100+Gbps telco interfaces
- Remote Packet Viewer for wireshark details about packets-in-place at remote sites
- Time stamping of 150 nanoseconds
- Real-time IDS alert configurator generates event logs for HTTP, Files, DNS, email, user agents, TLS/SSL, VOIP – all cross-correlated with PCAP & NetFlow V9 records
- Threat Hunting / Log Manager advanced packet analytics options include real-time event logging & cross-correlation
- 1000s of Snort/Suricate rules, from prepackaged libraries and user-defined rulesets
- Sessionaized logging for Email, HTTP, SMTP, Files, DNS, User Agents, TLS/SSL
- NetFlow Version 9 flow record logging and search
- Scalable architecture to meet your speed and/or analytics requirements
- Federate multiple cluster-based capture systems, for global visibility and PCAP retrieval

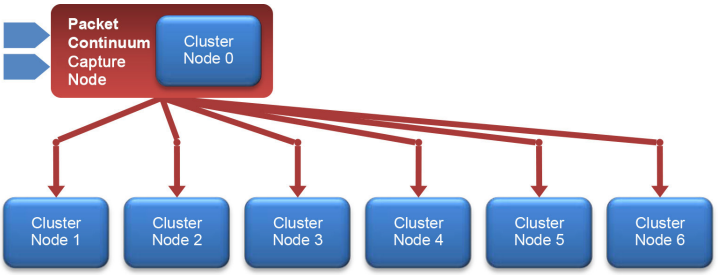
LABOR / COST REDUCTION

Combine zero day alerting and pivot for analysis/mitigation and historical post breach forensics analysis including "cyber-espionage," "point-of-sale intrusions," and "privilege misuse." Reduce the cost of network recording software and systems needed for medium and large networks.

Reduce labor needed for identification of indicators of compromise with an easy process to pivot to sessionized data / enriched meta data and reconstruct email and files for review.

Multiple features enable labor / cost reduction including:

- Low-cost, powerful sensor/recorder hardware platforms
- Real-time data compression: In-line packet/log compression is transparent to the user
- Cluster architecture enabling low-cost local-attached storage
- PCAP queries respond just as quickly over large timelines, by leveraging MapReduce CPU techniques.
- Federated search across multiple Packet Continuum appliances at diverse geographic locations, without any "data collectors/concentrators" required



CYBER INFRASTRUCTURE SERVICES CAPABILITY

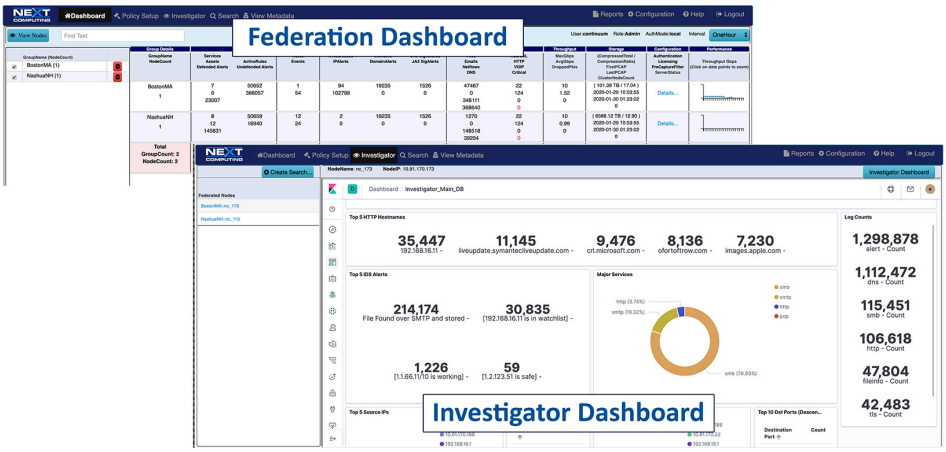
Packet Continuum includes comprehensive support services for long-term management of large numbers of sensors in the field. This is particularly valuable for Service Providers who can focus on optimizing their yber analytics and SOC procedures, while NextComputing manages a wide variety of hardware sensors, all with an identical software stack capable of field upgrades. The range of services includes:

- Flexible Pricing, including hardware financing and software subscription or site licensing
- Optimized Platform Specs
  - Based on requirements for Deterministic Real-Time Performance + Low Cost
  - OS, BIOS, Memory, CPU Cores, Hyper-Threads, RAID, Storage, Patch/Vulnerability Updates
- Common Architecture Flexibility
- Customer-branded hardware & UI software
- Customization / Integration
  - Software, Hardware, Cabling, Documentation, Packaging
  - Application Support
  - Example: Legacy Transition Support
- Configuration Management & Revision Control
- Sensor Refurbishment, QA, and Regression Testing
- Supply Chain Logistics
- Standards-Based Certification
  - Electrical, Vibration, etc
- Long Term Support Commitment
  - Tier 1/2/3 disciplined policies for ticket escalation/ resolution
  - End User Training + Innovative “Train-the-Trainer” techniques
- Full Cyber Infrastructure / OEM Services are detailed here:
  - https://solutions.nextcomputing.com/services/

FEDERATED WEB-BASED & REST API

An open REST/API for MSSPs and internal IT/security teams to customize their own workflows and tools for

- Event-to-PCAP Correlation
- Policy-Driven Packet Capture
- Automated File Detection
- Selective DPI Analytics
- Fast DPI Analytics
- Back-test FW polices
- Full Context PCAP Extraction
- Critical data retention policies



Type	Enterprise	Enterprise Lite	Short Rackmount	Deployable	Deployable
Hardware platform	Enterprise-class common platform server 2Ux27"	Enterprise-class common platform server 2Ux27"	NextComputing's Nucleus short-depth deployable 3Ux20"	NextComputing's NextServer-X short rack/ desktop, TSA-compliant carryon in transit case	NextComputing's Nucleus 1Ux17" short rack, or for desktop use
Purchase Options	• Options for monthly-based hardware financing and software subscription or site license terms • Or, purchase the integrated capture appliance, with 1st year support included and long-term support options				
Support	Full appliance support from NextComputing				
Capture Interfaces	2 or 4 x 10G interfaces	2 or 4 x 1G interfaces	2 or 4 x 10G interfaces	2 or 4 x 10G interfaces	2 or 4 x 1G interfaces
Capture Rate Options: Capture Node Stand Alone (no clusters)	Up to 10Gbps aggregate lossless capture rate with packet analytics enabled	Up to 2Gbps aggregate lossless capture rate with packet analytics enabled	Up to 10Gbps aggregate lossless capture rate with packet analytics enabled.	Up to 10Gbps aggregate lossless capture rate with packet analytics enabled.	Up to 1Gbps aggregate lossless capture rate with packet analytics enabled.
	Additional cluster nodes increase: capture rate, forensics timeline, and/or advanced packet analytics			*n/a*	*n/a*
Forensic Timeline - Capture Node	• 200TB PCAP storage • Capture timeline: 2-14 days, assuming 10Gbps average capture rate	• 100TB PCAP storage • Capture timeline: 4-20 days, assuming 2Gbps average capture rate	• 20TB PCAP storage • Capture timeline: 2-16 hours, assuming 10Gbps average capture rate	• From 1TB up to 200TB configurable PCAP storage • Capture Timeline: varies with storage	• 2TB PCAP storage • Capture timeline: 5-36 hours, assuming 1Gbps average capture rate
Forensic Timeline - Cluster Node	• 200TB PCAP storage • Capture Timeline: varies with storage	• 200TB PCAP storage • Capture Timeline: varies with storage	• 20TB PCAP storage • Capture Timeline: varies with storage	• From 1TB up to 200TB configurable PCAP storage • Capture Timeline: varies with storage	*n/a*
Forensic Timeline - Max System Capacity	• Up to 8 cluster nodes • For more capacity, federate multiple Capture Nodes	• Up to 4 cluster nodes • For more capacity, federate multiple Capture Nodes	• Up to 4 cluster nodes • For more capacity, federate multiple Capture Nodes	• Up to 4 cluster nodes • For more capacity, federate multiple Capture Nodes	*n/a*
	For more capacity, federate multiple Capture Nodes. A single "Federation" may include up to 10,000 Capture Nodes or Cluster systems (100 Federated Groups, with up to 100 nodes), where the remote user interface (and REST/API access) provides a unified view of all PCAP/log data and allows federated data queries.				
Management Interface	• For remote access by the Web-based User Interface • For programmatic access via the REST/API				
Stream Search Output Interface	• For streaming replay of PCAP search results. For example, for analysis by legacy tools. • For Alert/Event Log Forwarding. For example, selective log/metadata streaming to 3rd party systems. • For "Active Defense" messaging. For example, when Threat IP activity is detected.				
IPMI Platform Control Interface	For device control during "lights out" operation, server monitoring, remote re-boot, etc				
Cluster Node Interfaces	For point-to-point fiber connection for multiple Cluster Nodes for additional storage expansion that is actively-searchable				
Optional: Encryption	Optional AES256 encryption on OS/application and data arrays				
Operating System	CentOS or RedHat Enterprise License				
Physical	2U rackmount, 26.92" (683.77mm) depth	2U rackmount, 26.92" (683.77mm) depth	3U rackmount 20" (508 mm) depth	• 6.42" H x 17.65" W x 11.11" D • Includes TSA Carry-On compliant hard case	• Rackmount: 1U x 17" (431.8 mm) depth • Desktop: 17"x17"x1"

REAL-TIME PACKET ANALYTICS

Specification	Description
Time Stamp	• 150 nanoseconds
Pre-Capture Filter	• BPF (dynamically adjustable)
IDS Alerting	• Up to 50,000 active Snort/Suricata IDS rules, simultaneous with PCAP capture/search • Up to 1M Suspicious ThreatIP alerts • Defended Assets & Defended Services • User-defined, or select for pre-packaged libraries
IoC Alerting & Augmentation	• Up to 100 active BPF-based Active Triggers • Suspicious Domains & IP Addresses • Suspicious Files (eg. MD5 Hashes) • Suspicious SSL/TLS activity (eg. JA3 Signatures) • User-defined, or select from pre-packaged libraries
DPI Event Logging	• File Detection, Emails, DNS, SMB, SSL/TLS, VOIP, User-Agent – and NetFlow V9 generation
Retrospective Detection	• "SigDetect" feature to search-back over the entire timeline for emerging 0-Day threats, using Snort/Suricata rulesets and other Indicators of Compromise (IoC)

Rev 2.0b—12/20