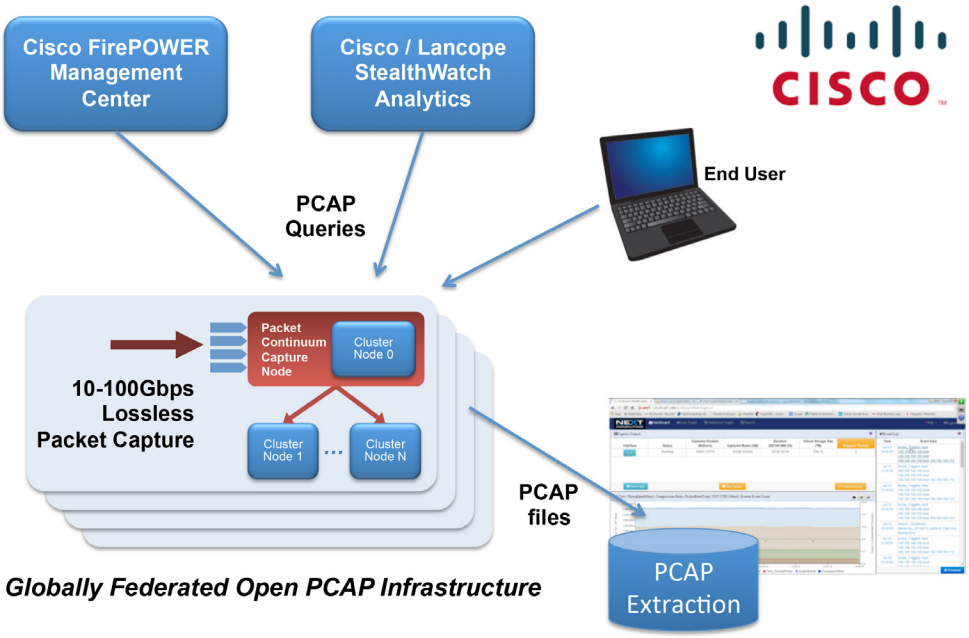
PACKET CONTINUUM FOR CISCO UCS

Packet Continuum UCS is a massively scalable, lossless packet capture solution on the open Cisco UCS computing infrastructure. Packet Continuum is designed to continuously capture live network traffic directly from a network tap, span/mirror, or packet broker. All captured traffic (in the form of PCAP files) is instantly searchable across very long capture timelines, with support for "federated" threat-hunting and fast PCAP search across up to 10,000 "Federated" capture points.

Packet Continuum UCS integrates with the Cisco suite of security solutions and with important Cisco partners. Users can quickly solve security or performance problems by drilling down into reported incidents directly from the application GUI screens of these products:

- **Cisco FirePOWER Management Center** (Sourcefire) analyzes network vulnerabilities, prioritizes any attacks, and recommends protections. Packet Continuum for Cisco UCS extends analysis of intrusion events with dynamic links to full-session data content.
- **Cisco StealthWatch** network visibility and security analytics for advanced protection. Packet Continuum for Cisco UCS allows quick pivot-to-PCAP for critical Incident Response.

Packet Continuum for Cisco UCS is a scalable sensor/recorder for enhanced network telemetry data, based on lossless PCAP that is cross-correlated with critical events. At line rate, in real-time, Packet Continuum for Cisco UCS executes over 50,000 Snort IDS rules, up to 1 Million ThreatIP alerts, and generates sessionized logs for critical security applications like file detection events, DNS, HTTP, Email, VOIP, SSL/TLS, etc.



Open PCAP and enriched telemetry for the Cisco Security ecosystem

Packet Continuum UCS solves these critical use cases for Cisco enterprise network customers:

Pre-wire global networks for continuous recording of network traffic, and for fast data retrieval only by proper authority

Cyber security Incident Response investigations, to greatly reduce the critical time-to-detect new and unknown threats

Network and IT Operations performance problem resolution

IT Compliance validation

Packet Continuum UCS Model	UCS Enterprise Capture Node Appliance	UCS Cluster Node Appliance
Hardware platform	Cisco UCS C240 M5 (LFF) Server - 2U Rackmount	Cisco UCS C240 M5 (LFF) Server - 2U Rackmount
Purchase Options	• Purchase the integrated capture appliance, with 1st year support/maintenance included • Services options for As-A-Service business model, and for extended support/maintenance	
Support	Full appliance support from NextComputing	

Capture Interfaces	2 x 10G/1G interfaces, with SFP+ SR and SFP RJ-45 transceiver modules	n/a
Capture Rate Options: Capture Node Stand Alone (no clusters)	• Up to 10Gbps sustained aggregate lossless capture rate, with packet analytics enabled and simultaneous search/retrieval • Additional cluster nodes increase: capture rate, forensics timeline, and/or advanced packet analytics	n/a
Forensic Timeline - Capture Node	• 100TB dedicated PCAP Capture Store • Worst case: 1 Day, with no compression and 10Gbps max capture rate • Best case: 10 Days, with 5:1 compression and 50% bandwidth	• Additional 100TB dedicated PCAP Capture Store per Cluster Node • Worst case: 1 Day, with no compression and 10Gbps max capture rate • Best case: 10 Days, with 5:1 compression and 50% bandwidth
Forensic Timeline - Max System Capacity	• Capture Node + up to 4 Cluster Nodes maximum, has a maximum of 465TB dedicated PCAP Capture Store • Worst case: 4.4 Days, assuming no compression and max capture rate • Best case: 44 Days, assuming 5:1 compression and 50% bandwidth • Note: There is no max limitation, because many systems may be Federated together for additional timeline capacity.	
Federation Manager	A single "Federation" may include up to 10,000 Capture Clusters (100 Federated "groups" of 100 each), where the remote user interface (and REST/API access) provides a unified view of all PCAP/log data and allows federated data queries.	

Time Stamp	150 nanoseconds	n/a
Pre-Capture Filter	BPF (dynamically adjustable)	n/a
Active Triggers	BPF (100 simultaneous)	n/a
IDS Alerts	Snort/Suricata rules (up to 50,000 simultaneous)	n/a
Threat-IP Alerts	IP Address lists (up to 1 Million simultaneous)	n/a

Operating System	CentOS v7.7, or optional upgrade to RedHat Enterprise License v7.7	
Threat-Hunting & Log Manager	Real-time logging/alerts for HTTP, Files, DNS, Email, User Agents, TLS/SSL, Active Triggers (BPF signature), System events, and Snort/Suricata rules (both user-defined & pre-packaged libraries). Log Manager events are actionable to search. All logs are time-correlated with PCAPs and NetFlow data. Text string search of logs. NetFlow record logging and search, when Log Manager Analytics enabled.	
Flow Record Recording	Flow record recording in NetFlow V9 record format with search & extraction of NetFlow data via timeline. UI-based NetFlow files downloadable and formatted for offline viewing in WireShark or tshark.	
REST & GUI Mgmt Interface	RJ-45 1G LAN port - For remote access by the Web-based User Interface and for programmatic access via the REST/API.	
Device Control Interface	RJ-45 1G LAN port - CIMC (Cisco Integrated Management Controller) Interface, for device control during "lights out" operation	
Output Options Interface	RJ-45 1G LAN port - For automated Active Defense Measures output, or alternatively for PCAP Replay output for offline traffic analysis	
Cluster Node Interfaces	Multiple 10G fiber SR LAN ports - for point-to-point fiber connection for up to (4) Cluster Nodes per capture node	Multiple 10G fiber SR LAN ports - for point-to-point connection with a Capture Node

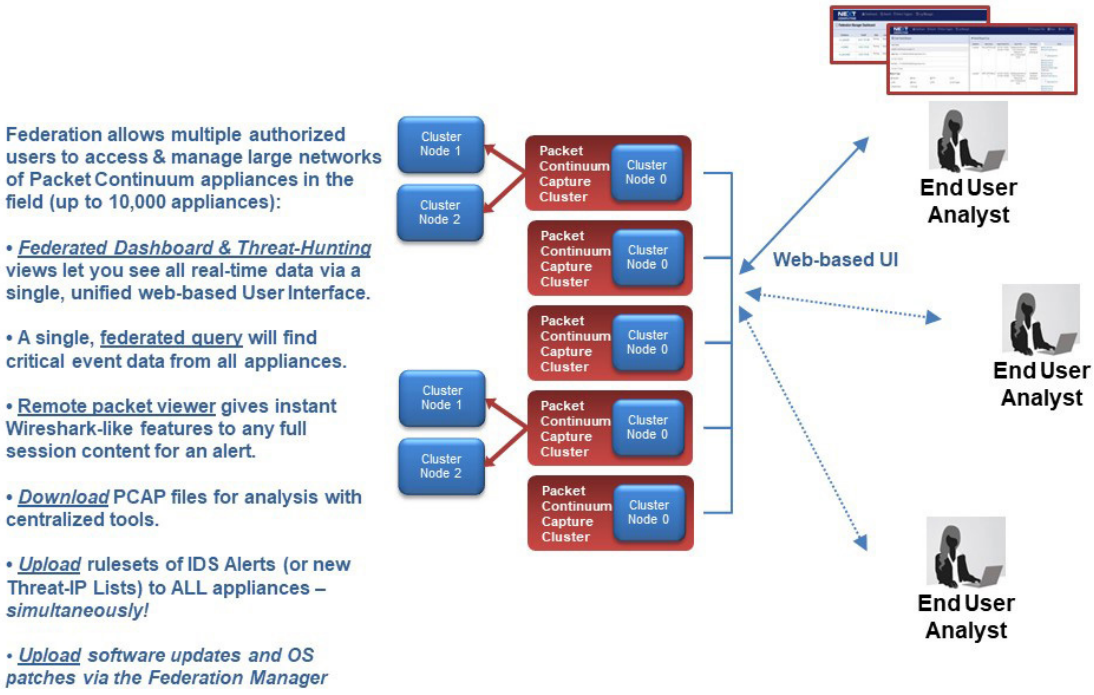
CARRIER-GRADE PACKET CAPTURE AND NETWORK EVENT LOGGING FOR SOC AND NOC TEAMS AND SERVICE PROVIDERS

Packet Continuum for Cisco UCS 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 for Cisco UCS 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



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

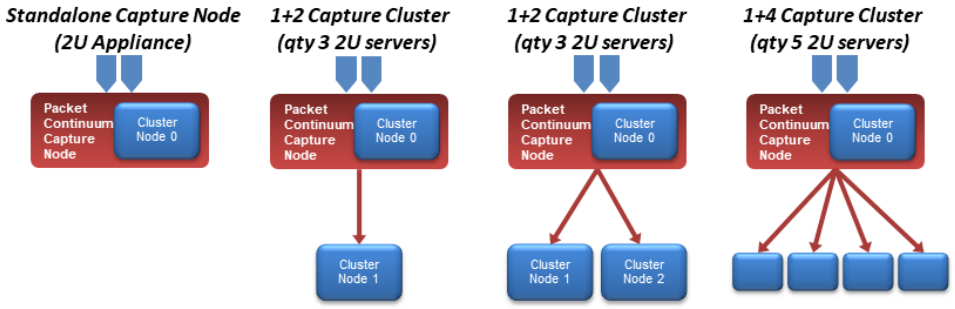
EXTREME SCALABILITY

Packet Continuum for Cisco UCS deploys on common enterprise-class UCS servers. It is uniquely cost-effective when deployed at scale. Examples of how Packet Continuum for Cisco UCS can scale include:

CAPTURE CLUSTERS

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.

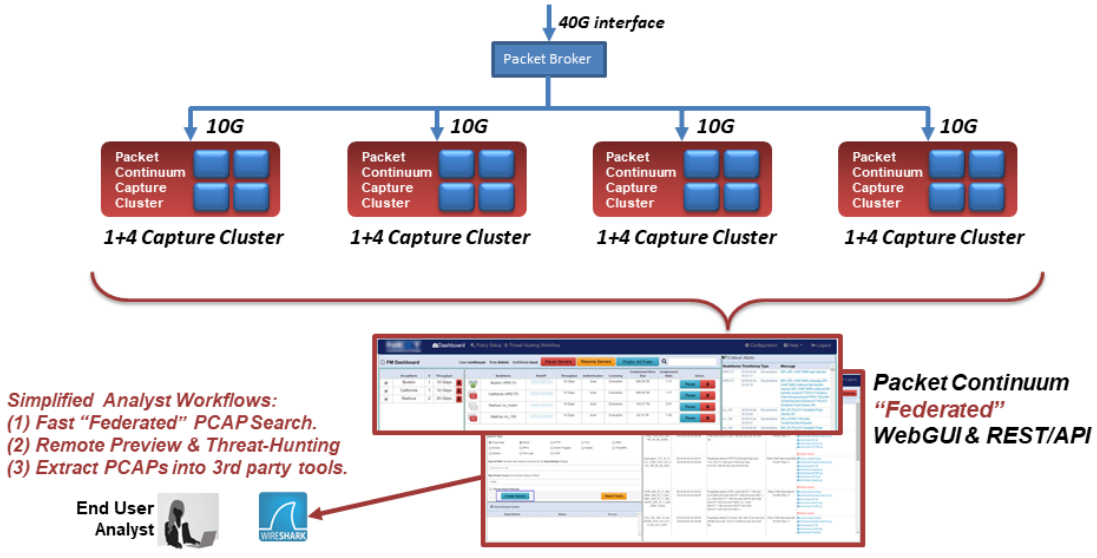
10G Capture Systems	*Capture Rate* PCAP + Logging	*Physical Storage* no compression	*"Amplified" Storage* 5:1 compression	*Forensic Timeline* Min - Max (50% usage)
Capture Node	10Gbps	100 TB	500 TB	1 Day – 10 Days
(1+1) Cluster	10Gbps	200 TB	1.0 PetaByte	2 Days – 20 Days
(1+2) Cluster	10Gbps	300 TB	1.5 PetaBytes	3 Days – 28 Days
(1+4) Cluster	10Gbps	500 TB	2.5 PetaBytes	5 Days – 48 Days



FEDERATION

High data-rate capture clusters (eg. 40Gbps, 100Gbps, and beyond) where a full feature set of real-time analytics functions must run at line rate with deterministic performance. Line-rate functions include continuous lossless full packet capture (PCAP), real-time IDS alerting and other user-defined Policy Management, with simultaneous search/ recall for Incident Response.

10G Capture Systems	*Capture Rate* PCAP + Logging	*Physical Storage* no compression	*"Amplified" Storage* 5:1 compression	*Forensic Timeline* Min - Max (50% usage)
4 x (1+4) Clusters	10Gbps	2 PetaBytes	10 PetaBytes	19 Days – 190 Days
4 x (1+4) Clusters	40Gbps	2 PetaBytes	10 PetaBytes	5 Days – 47 Days
10 x (1+4) Clusters	100Gbps	5 PetaBytes	25 PetaBytes	5 Days – 47 Days



POLICY-DRIVEN, AUTOMATED INCIDENT TRIAGE + WORKFLOW

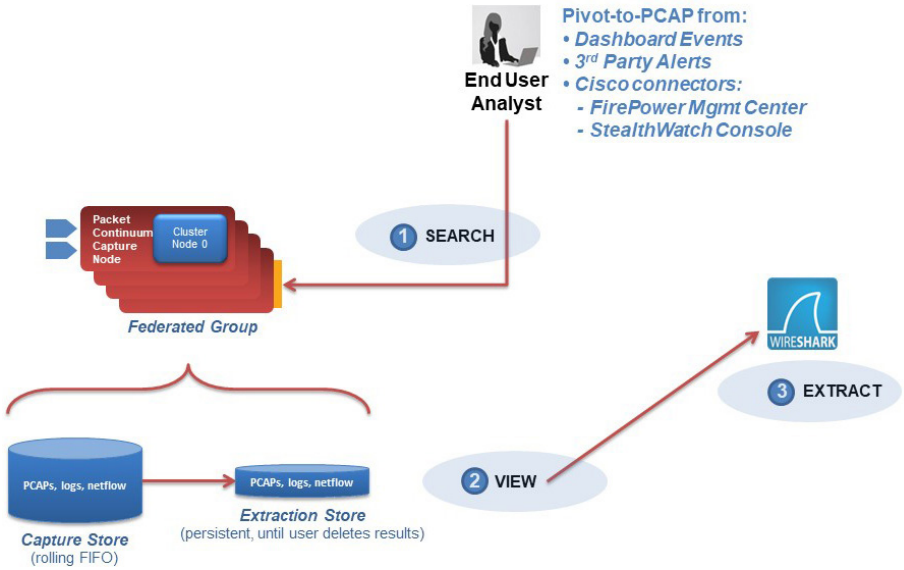
The Packet Continuum user interface (and programmatic REST/API) integrates Policy Management, Threat Hunting / Log Management, Forensic Investigation, and Open Data Access.

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

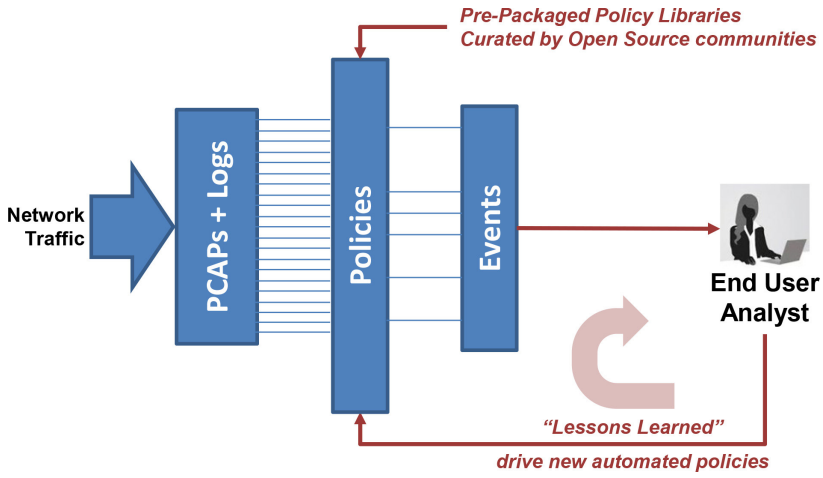
- IDS rulesets
- Malware rulesets
- ThreatIP lists
- Defended assets
- Defended services
- BPF-based Active Triggers

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 for Cisco UCS capture workflow is 1-2-3 simple: Search/View/Extract

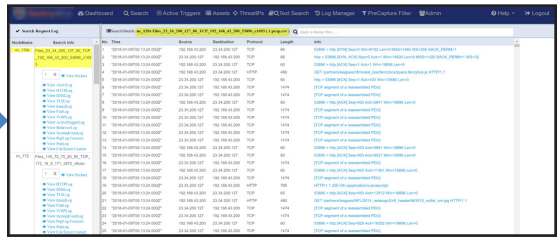


Packet Continuum for Cisco UCS facilitates the "Spiral-Model" methodology for effective forensic investigations.

SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS

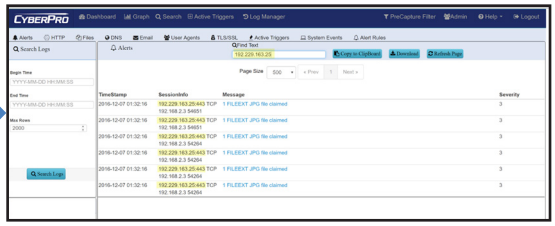
ANALYST OPERATIONS DASHBOARD

- 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



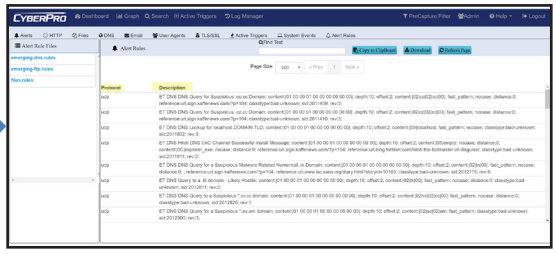
POLICY ALERTS DRIVES INCIDENT RESPONSE

- 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



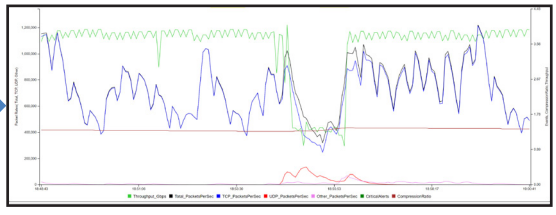
THREAT HUNTING - IOC POLICIES

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



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

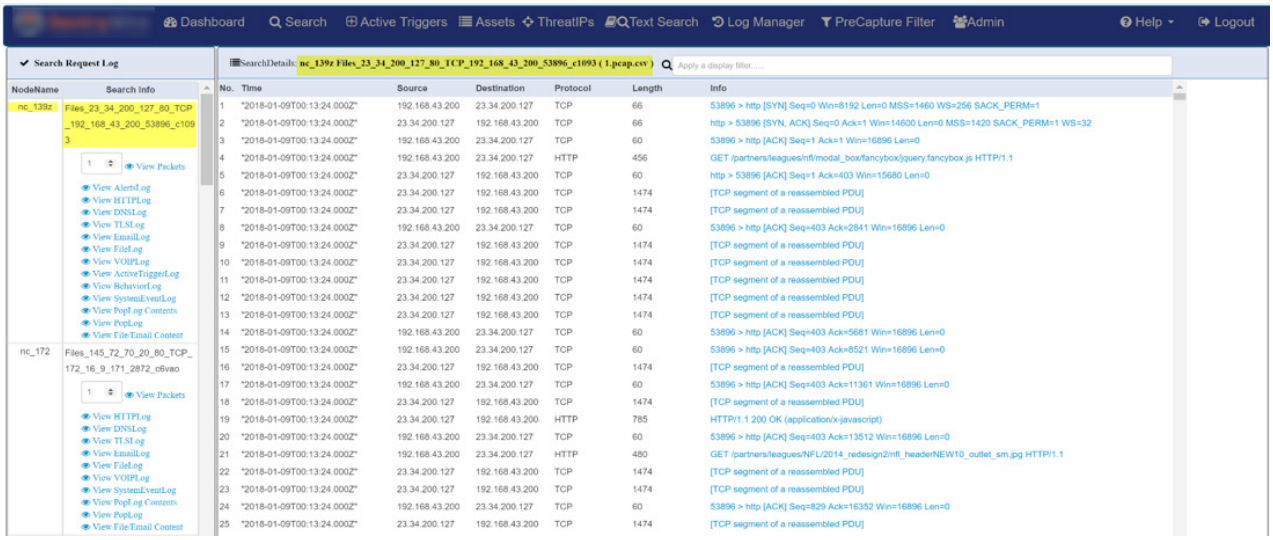


TIME-BASED DATA GRAPH

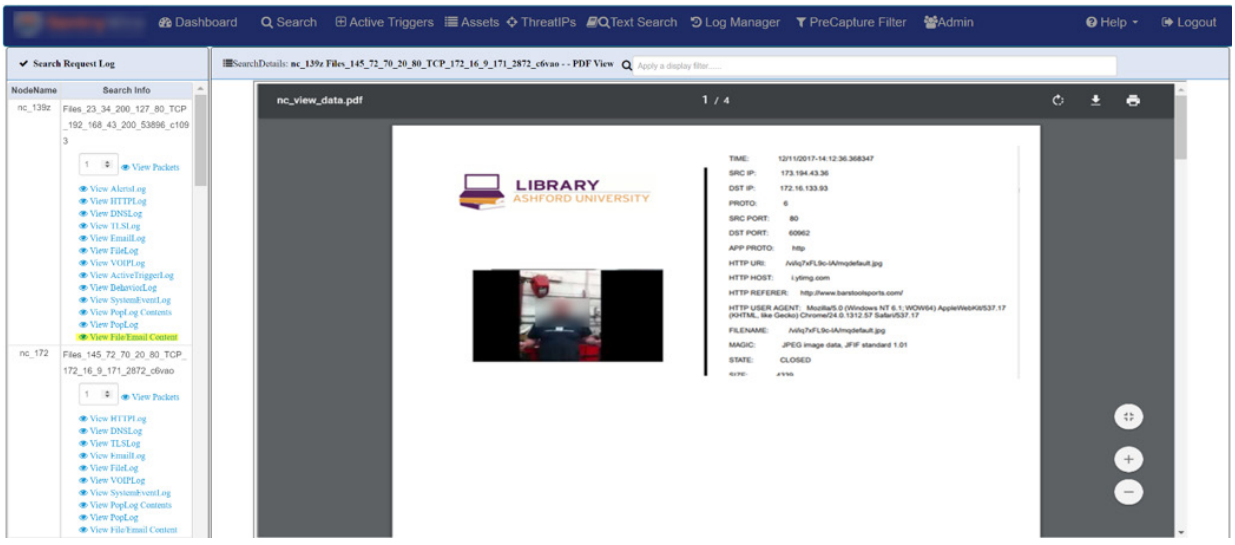
- With legends consisting of key packet capture and data compression statistics.
- One-Click search from any point in time, will automatically fill in a search request

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.



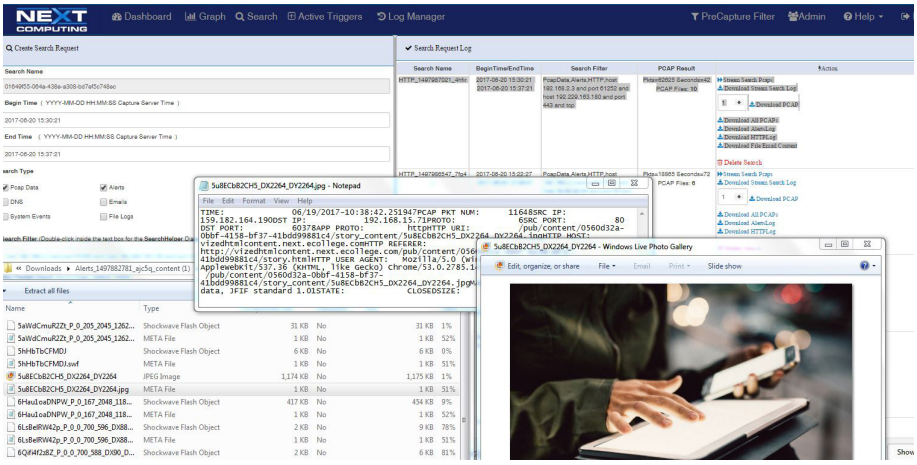
Clicking on search data or logs, displays the details on the right panel. For example, clicking "View Packets" shows an integrated web-based packet viewer has similar features to the Wireshark dashboard screen: the sequence of packets, each with timestamp, 5-tuple data, packet length, and the text-based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



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

SIMPLIFIED WORKFLOW

Packet Continuum for Cisco UCS 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.



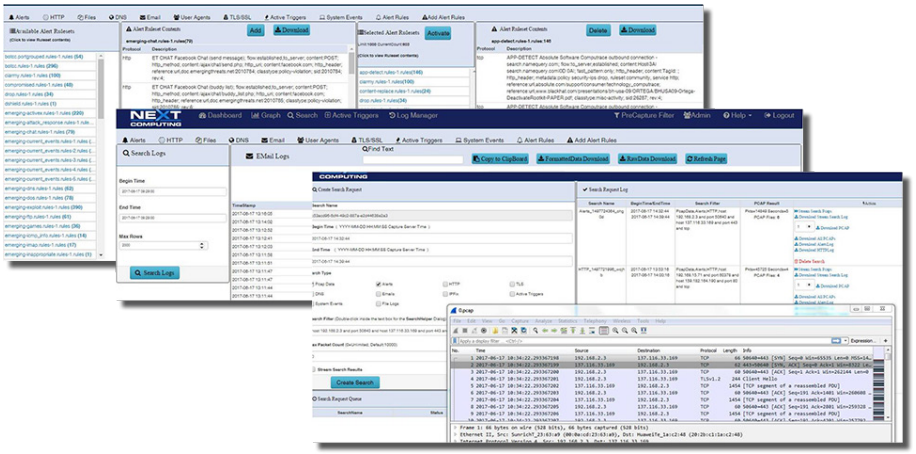
Log Manager showing HTTP log tab - HTTP session extraction and reconstruction of various files on the web page, including a JPG file showing the original content and metadata file breaking down the JPG file

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.

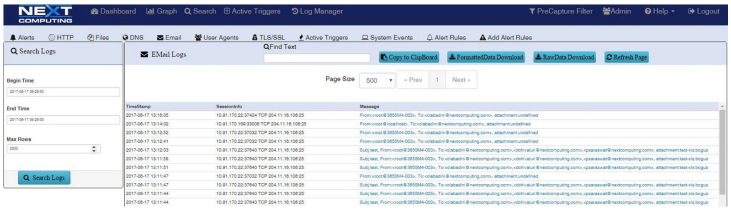
The real-time IDS alert configurator generates event logs for HTTP, Files, DNS, email, user agents, TLS/SSL, VOIP – all cross-correlated with PCAP & NetFlow V9 flow records.



EMAIL SEARCH / EXTRACTION

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

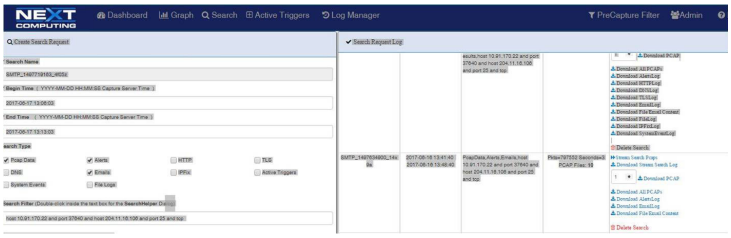
- SMTP email session logging with body text in HTMP format and file attachment reconstruction from original Mime format
- SMTP subject, send and receive email address logging



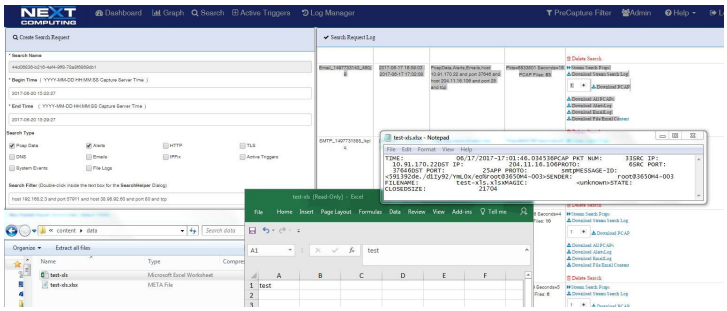
List of SMTP emails sessions searchable with time stamp, capture node location, session information and SMTP email address, sender/receiver. A user can click to get the full session packets, extract email subject/text and reconstruct file attachments in original mime format, PDF, doc, etc.

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

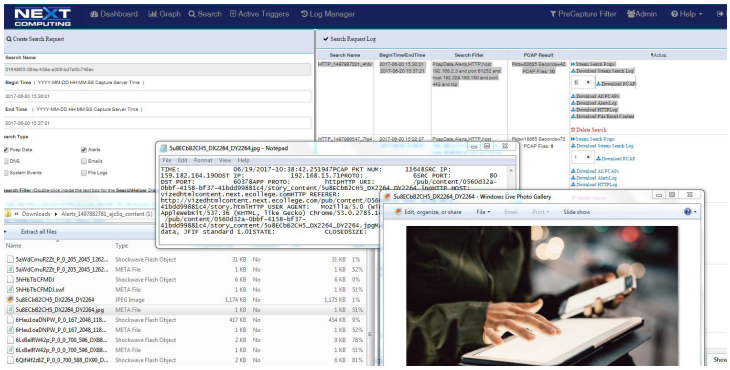
- Free form text search capability
- Clickable by event
- Second click initiates packet session recovery and file reconstruction
- Just two more clicks to the reconstructed file and meta data for that HTTP or SMTP email session
- All viewable and downloadable



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

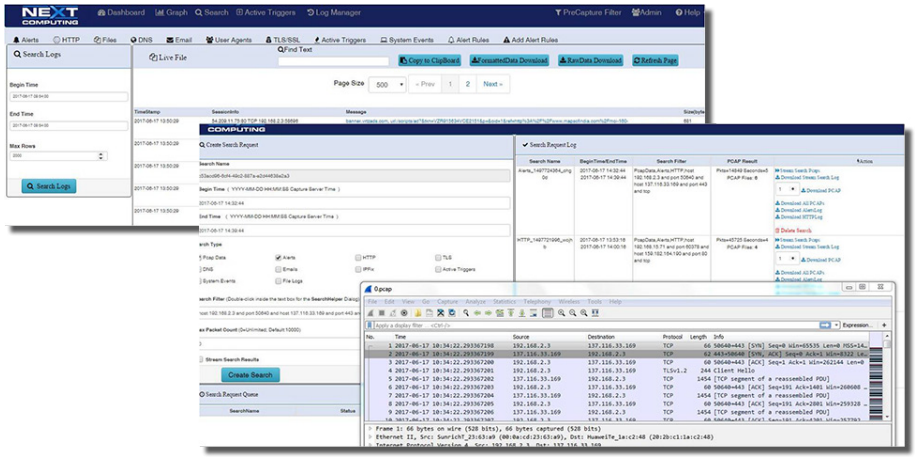


Reconstructed JPG file displayed with the metadata file associated with that graphic image

FILE LEAKAGE / EXFILTRATION

Packet Continuum for Cisco UCS enables

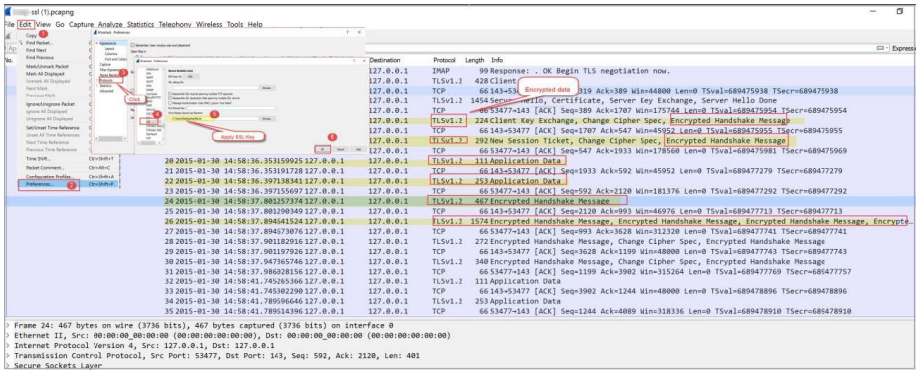
- HTTP, email and file transfer session logging and identification
- Reconstruction of files and associated metadata in original mime type for viewing and analysis



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

TLS / SSL VISIBILITY

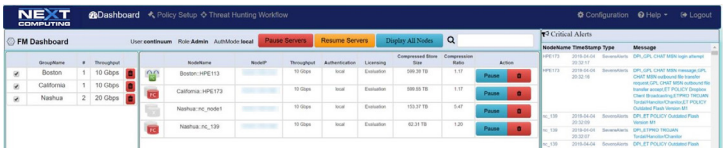
Gain visibility into TLS / SSL encrypted sessions. Log and extract sessionized PCAP data via timestamp, capture node and session information for recovery of sessionized packets, then offload them to WireShark using customer provided keys.



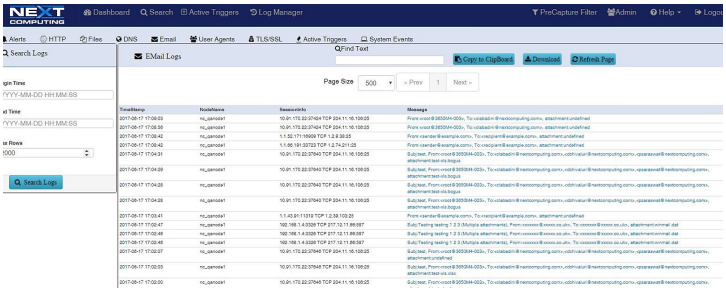
FEDERATION MANAGER

Packet Continuum for Cisco UCS's massively scalable Federation Manager allows you to federate multiple capture appliances in multiple locations.

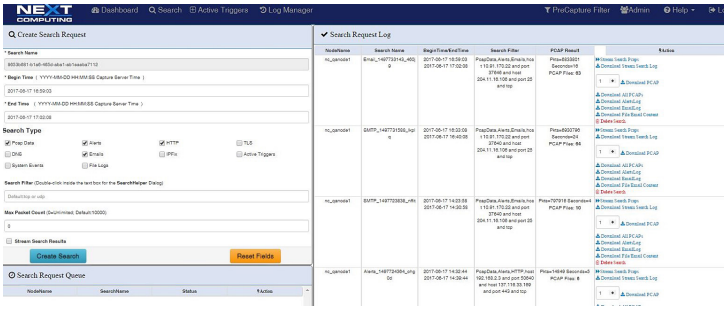
- Remote control capability via browser and REST API
- Federated View of all data
- Map-reduced framework to extract out packets, DPI data and logs across federation



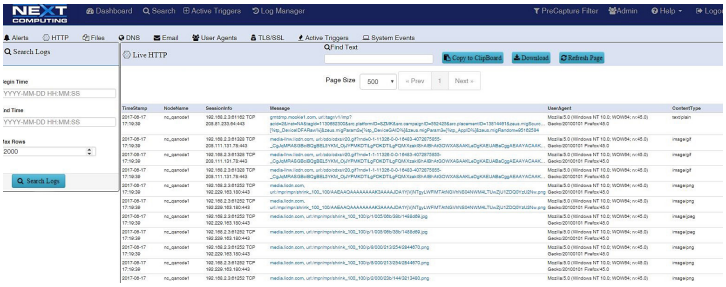
Federation manager dashboard for easy identification of Packet Continuum appliances/ clusters that can even be in different physical locations. Your enterprise network can identify the IP address of each appliance and federate together for a single pane of glass view of all network data.



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
- BPF — User-defined Active Trigger alerts
- Defended Assets/Services — Flexible user-defined lists
- TAXII/STIX — pre-packaged ThreatIPs and rulesets, supported via structured cyber threat information

OPEN DATA ACCESS, WITH STANDARD FILE FORMATS:

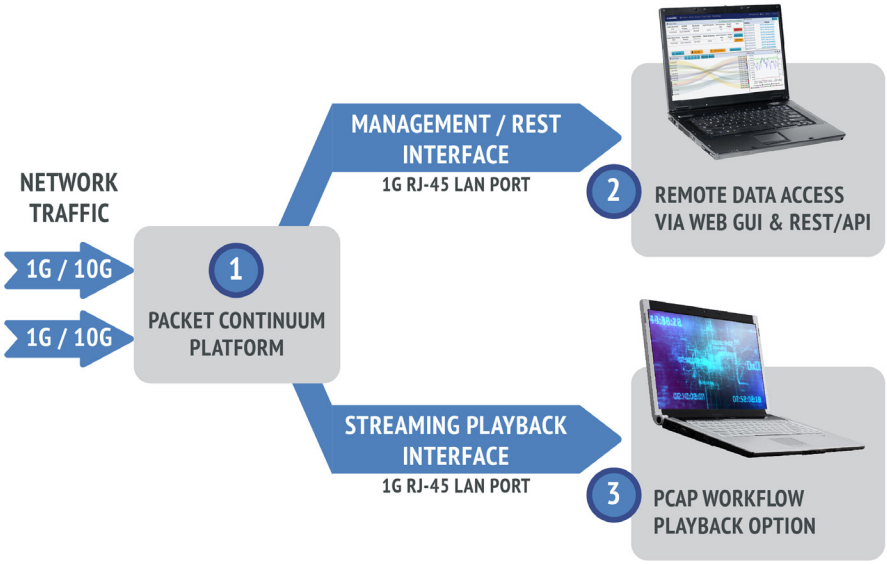
- PCAP-NG packet data
- NetFlow Version 9 flow records
- Text/CSV/syslog for enrichment log data

OPEN WORKFLOW AUTOMATION & ORCHESTRATION:

- Full-featured, mature REST/API
- Custom Workflow Scripting
- 3rd Party Event/Data/PCAP Correlation

STREAMING PLAYBACK FEATURE

- PCAPs searched / filtered / extracted with the Packet Continuum for Cisco UCS 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

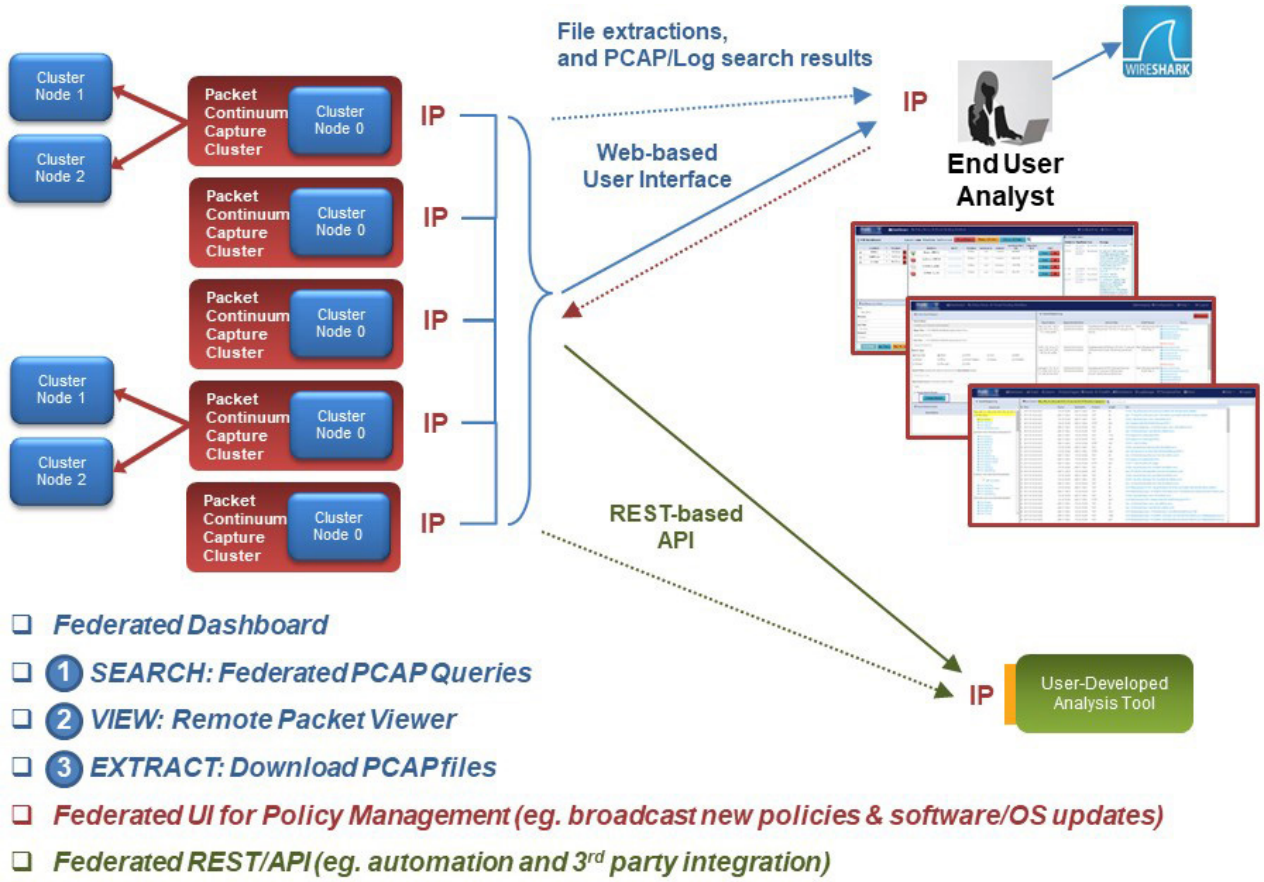


First, find the PCAP data you want, using Log Manager and Remote Packet Viewer, then you may use the Web-based UI to extract the PCAP file sequence via the Management Interface to an external system, for viewing in Wireshark – or another workflow. Alternatively, you may replay the PCAP out the Streaming 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

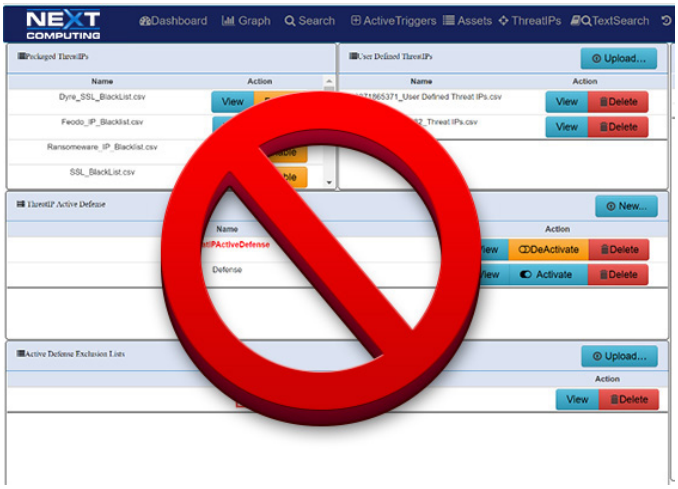
Packet Continuum for Cisco UCS's highly scalable, high performance network data recorder provides for forensics investigations based on breach detection and changed threats within a reasonable forensics timeline.

- 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



10,000s 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



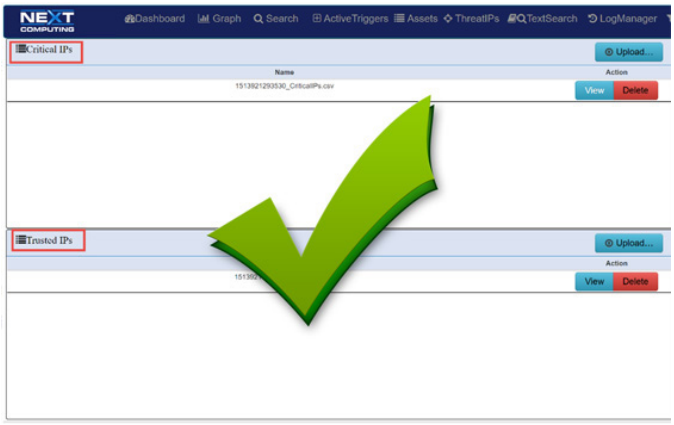
Packet Continuum for Cisco UCS enables identification, monitoring, viewing, and mitigation of pre-defined Threat IPs as well as user-defined IPs. Packet Continuum comes pre-loaded with a known list of Threat IPs; a number of malicious IPs previously identified by trusted sources such as US-CERT, for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

From the Packet Continuum for Cisco UCS 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 for Cisco UCS 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

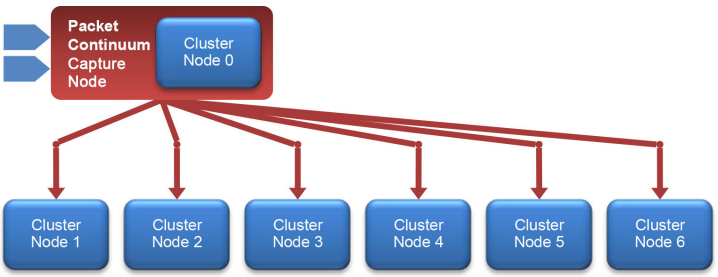
LABOR / COST REDUCTION

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/

WEB UI & 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