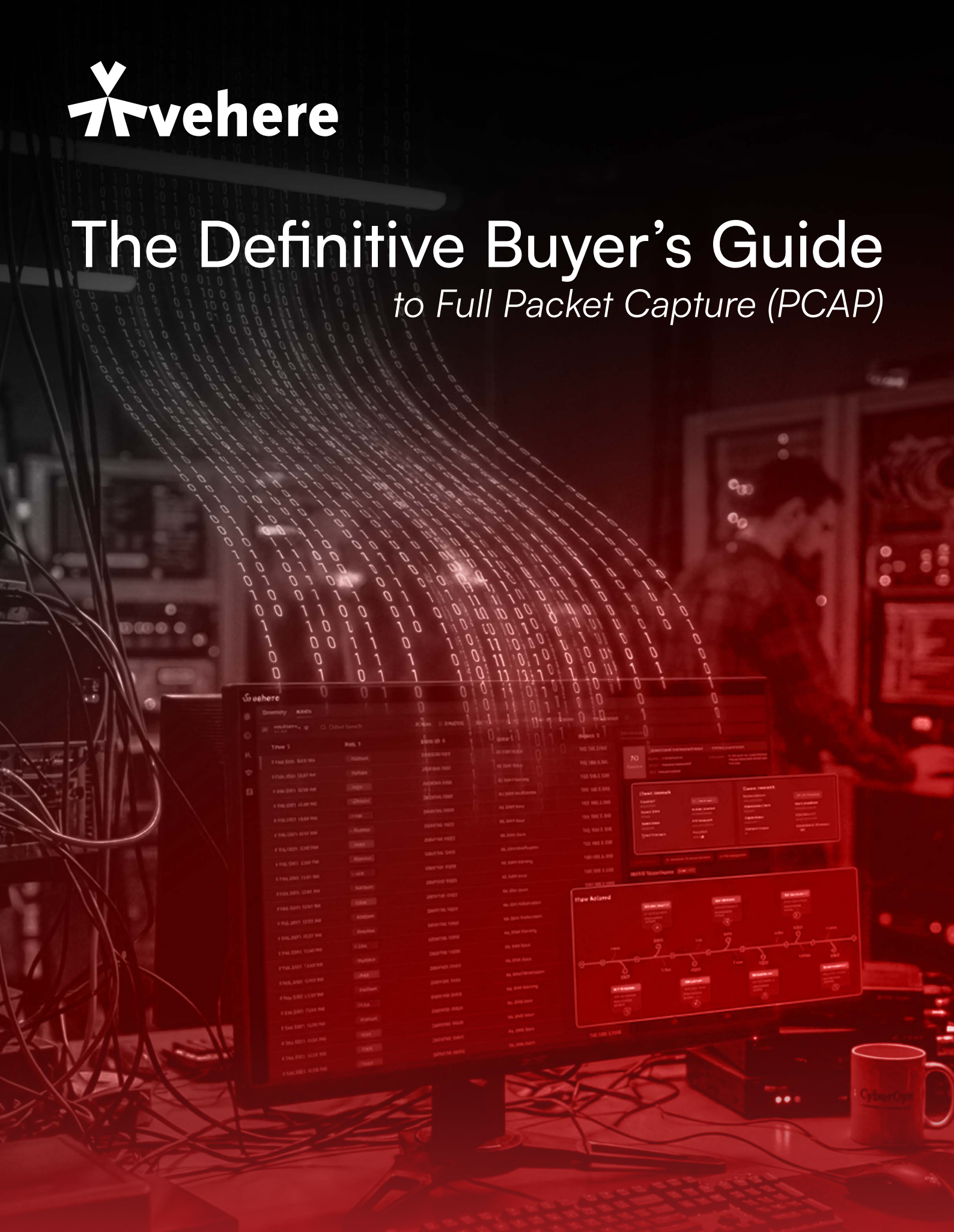
vehere

The Definitive Buyer's Guide

to Full Packet Capture (PCAP)



The Evaluation Matrix to Guide Cybersecurity Leaders towards a Modern Full Packet Capture Platform.

Executive Summary

Modern cyberattacks move faster than traditional security operations can investigate. Threat actors now operate within encrypted environments, move laterally in minutes, exploit east-west traffic blind spots, and often evade detection until after damage is done.

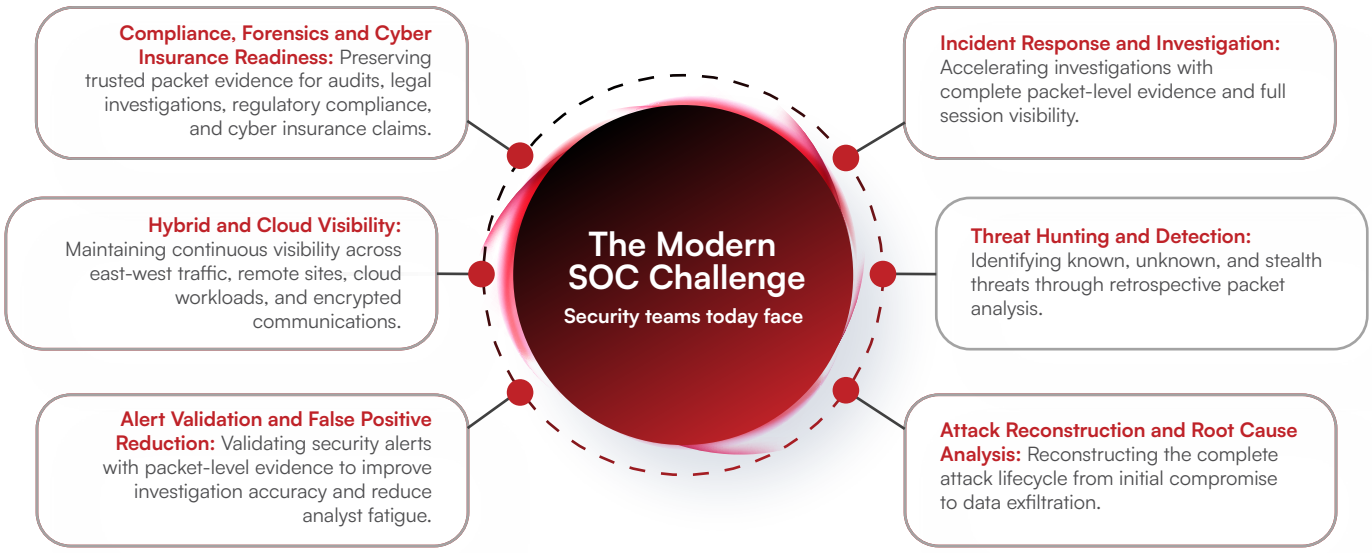
While SIEM, EDR, NDR, and XDR platforms generate alerts, they frequently fail to answer the most critical post-alert questions:

- What exactly happened?
- How did the attacker move?
- Was data exfiltrated?
- Which systems communicated with the threat actor?
- What is the full attack timeline?
- How long has the threat been present?

This is where Full Packet Capture becomes foundational. A modern Full Packet Capture platform provides continuous packet-level visibility, full session reconstruction, retrospective threat hunting, encrypted traffic intelligence, and forensic-ready evidence preservation.

This buyer's guide helps CISOs, SOC managers, incident responders, and cybersecurity architects evaluate the capabilities that truly matter while selecting a Full Packet Capture platform.

Why Full Packet Capture (PCAP) Has Become a Strategic Security Requirement

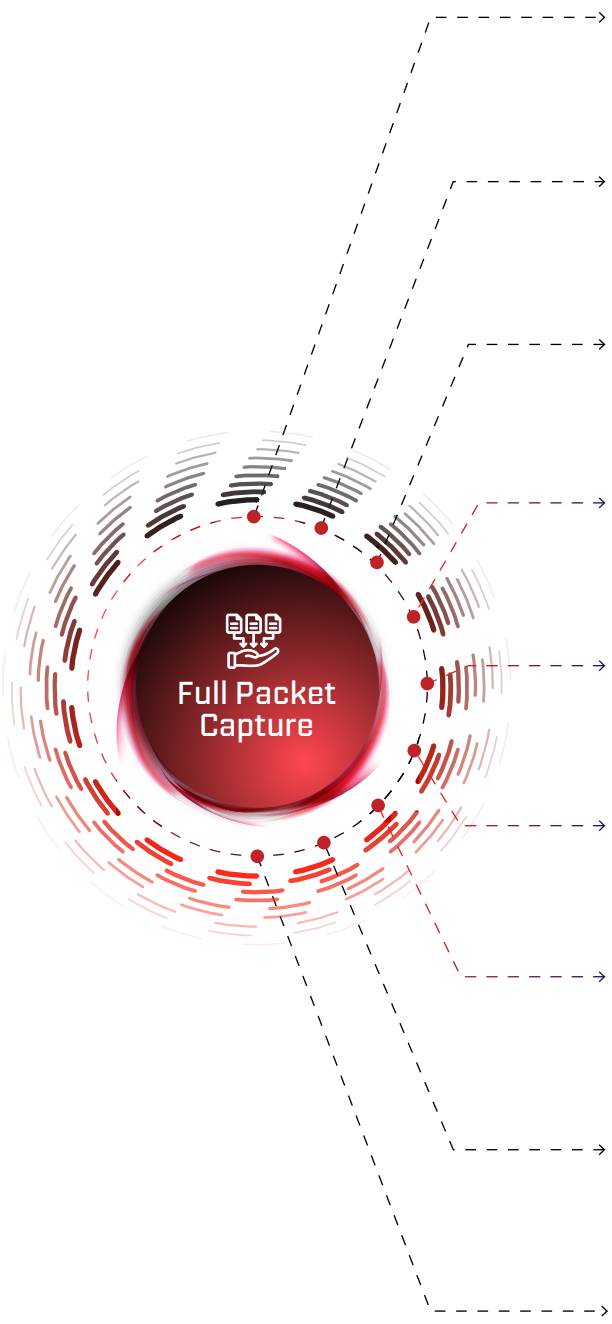


Traditional monitoring tools provide indicators. Full Packet Capture (PCAP) provides evidence. Unlike selective packet capture or alert-triggered logging, Full Packet Capture creates a continuously searchable record of network activity before, during, and after an attack.

What is Full Packet Capture (PCAP)?

Full Packet Capture also known as Packet Forensics or Network Forensics is the process of continuously capturing, indexing, reconstructing, analyzing, and investigating network traffic to:

- Detect malicious activity
- Reconstruct attacker behavior
- Validate alerts
- Hunt threats retrospectively
- Investigate unknown attacks
- Preserve legal-grade evidence
- Accelerate incident response



CONTINUOUS FULL PACKET CAPTURE (PCAP)
Capture every packet, at line rate, 24/7 across all network segments without loss.

DEEP PACKET INSPECTION (DPI)
Layer 2-7 inspection with protocol decoding for 1000+ protocols, files, and applications.

FULL SESSION RECONSTRUCTION
Rebuild complete sessions and attacker timelines with traffic replay and flow correlation.

METADATA EXTRACTION
Extract rich Layer 2-7 metadata from every session for faster context and analysis.

THREAT INTELLIGENCE CORRELATION
Correlate traffic and entities with global threat intel feeds, reputation scores, and adversary TTPs.

IOC-BASED HUNTING
Hunt across historical data using IPs, domains, hashes, JA3/JA3S, cert fingerprints and more.

ENCRYPTED TRAFFIC ANALYTICS
Gain visibility into encrypted traffic using TLS fingerprints, JA3/JA3S, SNI, certificates, and behavioral analytics-without decrypting payloads.

HISTORICAL SEARCH AND REPLAY
Search months of data in seconds, drill down to packets, and replay traffic to understand the full story of an incident.

REAL-TIME INDEXING
Index packets and metadata in real time for sub-second search, correlation, and investigation at scale.

The Business Outcomes Buyers Must Prioritize

A modern Full Packet Capture (PCAP) platform should serve as an operational force multiplier for the SOC - accelerating investigations, eliminating visibility gaps, improving threat detection, and strengthening security resilience. The following outcomes represent the key value drivers buyers should prioritize:

- **Faster Incident Investigation:** Reduce investigation cycles from days to minutes with indexed packet search and session reconstruction.
- **Reduced Mean Time to Detect (MTTD) and Respond (MTTR):** Enable analysts to pivot directly from alerts to packet-level evidence.
- **Elimination of Network Blind Spots:** Gain visibility into east-west traffic, encrypted sessions, remote locations, and cloud workloads.
- **Better SOC Efficiency:** Reduce dependence on multiple disconnected investigation tools.
- **Advanced Threat and Lateral Movement Detection Identify** lateral movement, beaconing, exfiltration attempts, stealth activity, and low-noise malicious behavior.
- **Improved Threat Hunting:** Enable retrospective investigation across historical traffic to uncover stealthy or previously unknown threats.
- **Compliance-Ready Forensic Evidence:** Preserve immutable evidence for legal, audit, and regulatory workflows.

Core Capabilities and Enterprise Evaluation Framework

The following framework combines the most critical technical capabilities, architectural requirements, operational outcomes, and evaluation criteria that modern enterprises should assess while selecting a Full Packet Capture platform.

- Align technical requirements with operational outcomes
- Evaluate platform maturity and scalability
- Assess investigative depth and visibility
- Compare vendor capabilities more effectively
- Accelerate vendor shortlisting and validation

Capability Group	Evaluation Criteria	Description	Vehere Full Packet Capture (PCAP) Capability
Packet Visibility	Continuous Full Packet Capture	Eliminates blind spots and preserves complete attack visibility	Continuous line-rate PCAP across 1G/10G/25G/40G/ 100G environments
	Lossless Capture and Burst Handling	Prevents packet drops during traffic spikes and attacks	Burst handling with packet loss prevention
	Multi-Environment Coverage	Supports hybrid, cloud, branch, and enterprise visibility	SPAN, TAP, ERSPAN, Cloud VPC support
	Traffic Integrity	Ensures trustworthy and accurate packet evidence	Hardware timestamping and evidence preservation

Deep Visibility	L2-L7 Protocol Intelligence	Provides application and protocol-level visibility	DPI across DNS, TLS, SMB, HTTP/2, SSH, VoIP
	Metadata Extraction	Accelerates investigations with rich telemetry	Real-time L2-L7 metadata extraction
	Traffic Classification	Detects anomalous application behavior	Automated traffic classification
Encrypted Traffic Intelligence	TLS Visibility	Improves visibility into encrypted communications	JA3/JA3S, SNI, cipher suite and TLS telemetry
	Behavioral Analytics	Detects suspicious encrypted activity	TLS behavior monitoring and anomaly detection
	Certificate Intelligence	Detects suspicious and malicious certificate usage	Expired, self-signed, and untrusted CA analysis
	Controlled TLS Inspection	Enables customer-governed decryption when required	On-demand TLS 1.2 decryption
Investigation and Forensics	Session Reconstruction	Rebuilds attacker timelines and activity chains	Full session reconstruction and traffic replay
	Packet Drill-Down	Enables analysts to pivot directly into evidence	Alert → Flow → Packet workflows
	Timeline Analysis	Improves understanding of attack progression	East-West and North-South correlation
	Evidence Preservation	Supports audit, IR, and legal workflows	Cryptographic hashing and legal hold support
Threat Hunting	Retrospective Hunting	Enables historical investigation across stored traffic	180-day retrospective hunting
	IOC-Based Investigation	Accelerates threat correlation and validation	IOC hunting across IPs, domains, hashes, JA3/JA3S
	Unknown Threat Discovery	Detects stealth and zero-day activity	Behavioral analytics and heuristic analysis
	Insider Threat Visibility	Detects slow-moving malicious behavior	Full packet retention and behavioral analytics
Search and Analytics	Ultra-Fast Search	Reduces investigation time and analyst fatigue	Indexed RAW packet storage
	Real-Time Indexing	Makes telemetry instantly searchable	Real-time session indexing
	Flexible Search Workflows	Supports advanced investigations and hunting	Session, flow, IOC, protocol, and attribute-based search
	Custom Queries	Enables tailored detection and investigation workflows	Custom query support

Scalability and Architecture	Enterprise Throughput	Supports high-speed enterprise traffic environments	Sustained capture up to 100 Gbps
	Petabyte-Scale Storage	Supports long-term retention and enterprise growth	Expandable petabyte-scale architecture
	Distributed Operations	Extends visibility across remote environments	Distributed probes and multi-site support
	Centralized Management	Simplifies enterprise operations	Unified centralized management plane
SOC Operations	Integrated Detection and Investigation	Reduces tool fragmentation and SOC fatigue	Integrated IDS and detection-to-forensics workflows
	Alert Validation	Enables evidence-based investigations	Packet-level evidence validation
	Reporting and Dashboards	Reporting and Dashboards	Built-in customizable reports and dashboards
Security and Compliance	Role-Based Access Control	Restricts unauthorized access to evidence	RBAC support
	Data Protection	Secures sensitive telemetry and evidence	End-to-end encryption
	Privacy Controls	Supports regulated and sensitive environments	PII/SPDI masking and selective filtering
	Auditability	Tracks analyst and administrative activity	Full audit logging
Integrations	SIEM and SOAR Integration	Streamlines SOC workflows and automation	Splunk, QRadar, Elastic, Cortex integration
	Threat Intelligence Integration	Improves external threat correlation	STIX/TAXII support
	API Integration	Enables automation and interoperability	REST APIs for search, export, and automation
Deployment Flexibility	Flexible Deployment Models	Supports enterprise infrastructure diversity	Physical, VM, and cloud deployment
	Air-Gapped Support	Critical for regulated and sensitive environments	Fully on-premises architecture
	Remote Site Visibility	Remote Site Visibility	Lightweight remote capture probes

Business Outcomes	Faster Investigations	Accelerates triage and incident response	Indexed search and rapid drill-down
	Reduced MTTR	Speeds containment and remediation	Unified forensic workflows
	Reduced Blind Spots	Improves encrypted and lateral traffic visibility	Continuous PCAP + ETI capabilities
	Compliance-Ready Forensic Evidence	Supports audit and legal preparedness	Long-term evidence preservation
	SOC Modernization	Consolidates investigative workflows	Integrated detection, hunting, and forensics

Questions Every Buyer Should Ask Vendors

The following evaluation checklist helps security leaders assess whether a Full Packet Capture (PCAP) platform can support modern enterprise investigation, threat hunting, scalability, compliance, and SOC operational requirements.

Evaluation Area	Questions Buyers Should Ask
Architecture and Performance	Can the platform sustain continuous line-rate packet capture?
	What throughput speeds are supported across enterprise environments?
	How does the platform prevent packet loss during traffic spikes?
	Is indexing performed in real time?
	What is the average search latency during investigations?
Visibility and Detection	Which protocols are decoded across L2-L7 visibility layers?
	Does the platform support encrypted traffic analytics and TLS intelligence?
	Can analysts investigate east-west and north-south traffic movement?
	Does the solution support historical and retrospective threat hunting?
	Can analysts conduct IOC-based investigations across stored traffic?
Storage and Retention	What is the maximum supported retention window?
	How is packet storage optimized for enterprise scalability?
	Does the architecture support petabyte-scale storage?
	Can storage expand as traffic grows?

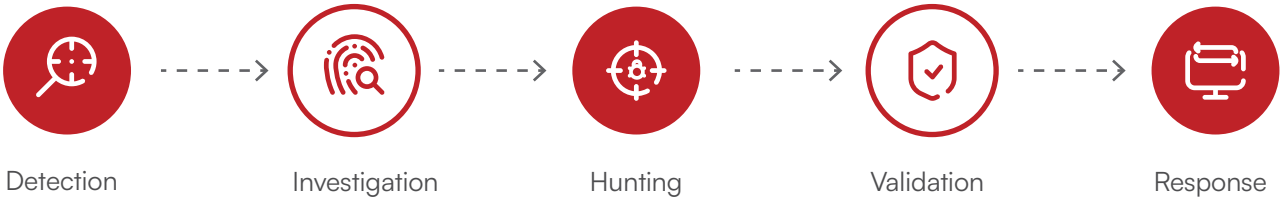
Investigation and Forensics	Does the platform support full session reconstruction and traffic replay?
	Can analysts pivot directly from alerts to packet-level evidence?
	Is evidence preserved using tamper-proof mechanisms?
Security and Compliance	Is RBAC supported for controlled access management?
	Are audit logs maintained for analysts and administrative activity?
	Does the solution support PII masking and privacy controls?`
	Is data encrypted both at rest and in transit?
Integration and Operations	Does the platform integrate with SIEM, SOAR, and NDR ecosystems?
	Are APIs available for automation and orchestration?
	Does the solution support on-premises, cloud, and hybrid deployments?
	Can distributed probes support branch and remote locations?

Common Mistakes Buyers Make

Prioritizing Detection Over Investigation	▪ Detection tools generate alerts. ▪ Forensics platforms validate and explain them. ▪ Organizations often over-invest in alerting tools while under-investing in investigative visibility. ▪ Need for zero downtime, where even minor disruptions impact customer trust.
Choosing Flow-Only Visibility	▪ Flow data lacks payload context. ▪ Without packet evidence, investigations become assumption driven.
Ignoring Encrypted Traffic Visibility	▪ Encrypted traffic is now the dominant attack surface. ▪ Ignoring ETI capabilities creates major blind spots.
Underestimating Storage and Scalability Needs	▪ As traffic grows, poorly designed architectures become operational bottlenecks.
Evaluating Features Instead of Outcomes	The right evaluation should focus on: ▪ Investigation speed ▪ Visibility depth ▪ Threat hunting capability ▪ Evidence integrity ▪ Analyst efficiency ▪ Operational scalability

Why Modern SOCs Are Moving Toward Unified Detection and Forensics

Security teams increasingly require integrated workflows that unify:



A disconnected SOC stack slows investigations and increases analyst fatigue. Modern Full Packet Capture (PCAP) platforms now act as the investigative backbone of the SOC by:

- Correlating alerts with packet evidence
- Enabling faster analyst pivots
- Reducing tool fragmentation
- Improving detection validation
- Supporting proactive threat hunting

What Differentiates Enterprise-Grade Full Packet Capture Platforms

The strongest platforms are engineered around:

- **High-Fidelity Visibility:** Complete packet-level evidence across the network.
- **Speed at Scale:** Fast indexing and searching across terabytes and petabytes of traffic.
- **Investigation Depth:** Session replay, protocol reconstruction, and attack timeline visibility.
- **Encrypted Traffic Intelligence:** Advanced analytics without operationally risky blanket decryption.
- **Operational Resilience:** Designed for mission-critical SOC environments.
- **On-Premises Data Control:** Critical for highly regulated and sensitive environments.

Why Enterprises Are Prioritizing On-Premises Full Packet Capture (PCAP)

Highly regulated industries increasingly prefer on-premises architectures because they provide:

- Full control over sensitive telemetry
- Data sovereignty compliance
- Better privacy assurance
- Air-gapped deployment support
- Reduced external data exposure
- Lower risk for critical infrastructure environments

Final Evaluation Framework for Buyers

Before selecting a Full Packet Capture platform, cybersecurity leaders should evaluate:

- **Visibility:** Can the platform capture everything continuously?
- **Intelligence:** Can the platform analyze encrypted traffic effectively?
- **Speed:** Can analysts search and investigate rapidly?
- **Integrity:** Can evidence withstand legal and compliance scrutiny?
- **Depth:** Can the platform reconstruct complete attack narratives?
- **Integration:** Can it operate seamlessly inside the SOC ecosystem?
- **Scale:** Can the architecture support enterprise traffic growth?
- **Operational Efficiency:** Will it reduce analyst fatigue and investigation time?

Conclusion

Modern cyber investigations require more than alerts. They require evidence. As attackers increasingly exploit encrypted traffic, move laterally across hybrid environments, and evade traditional defenses, Full Packet Capture has become a strategic security capability rather than an optional investigative tool. Organizations that invest in full-fidelity packet visibility, deep forensic workflows, encrypted traffic intelligence, and scalable retrospective hunting capabilities position themselves to:

- Investigate faster
- Hunt proactively
- Reduce blind spots
- Improve SOC efficiency
- Strengthen compliance readiness
- Accelerate incident response
- Defend against advanced threats with confidence

The future of cybersecurity investigations belongs to organizations that can reconstruct, validate, and understand every attack with precision. Full Packet Capture makes that possible.

About Vehere

Vehere is an AI cyber defense company operating at the intersection of national security and enterprise security. Our AI-powered Network Intelligence platform processes petabytes of network data at terabit speed, empowering government agencies with real-time intelligence, advanced analytics, and actionable insights. From preventing emerging threats to accelerating investigations, Vehere helps governments and law enforcement agencies protect national sovereignty and strengthen public safety.

Address:
1390 Market Street
Suite 200, San Francisco, CA 94102

Unit No. 5, 1st Floor, Andaz, Asset Area 1
Aerocity, New Delhi-110037

E: sales@vehere.com

W: www.vehere.com