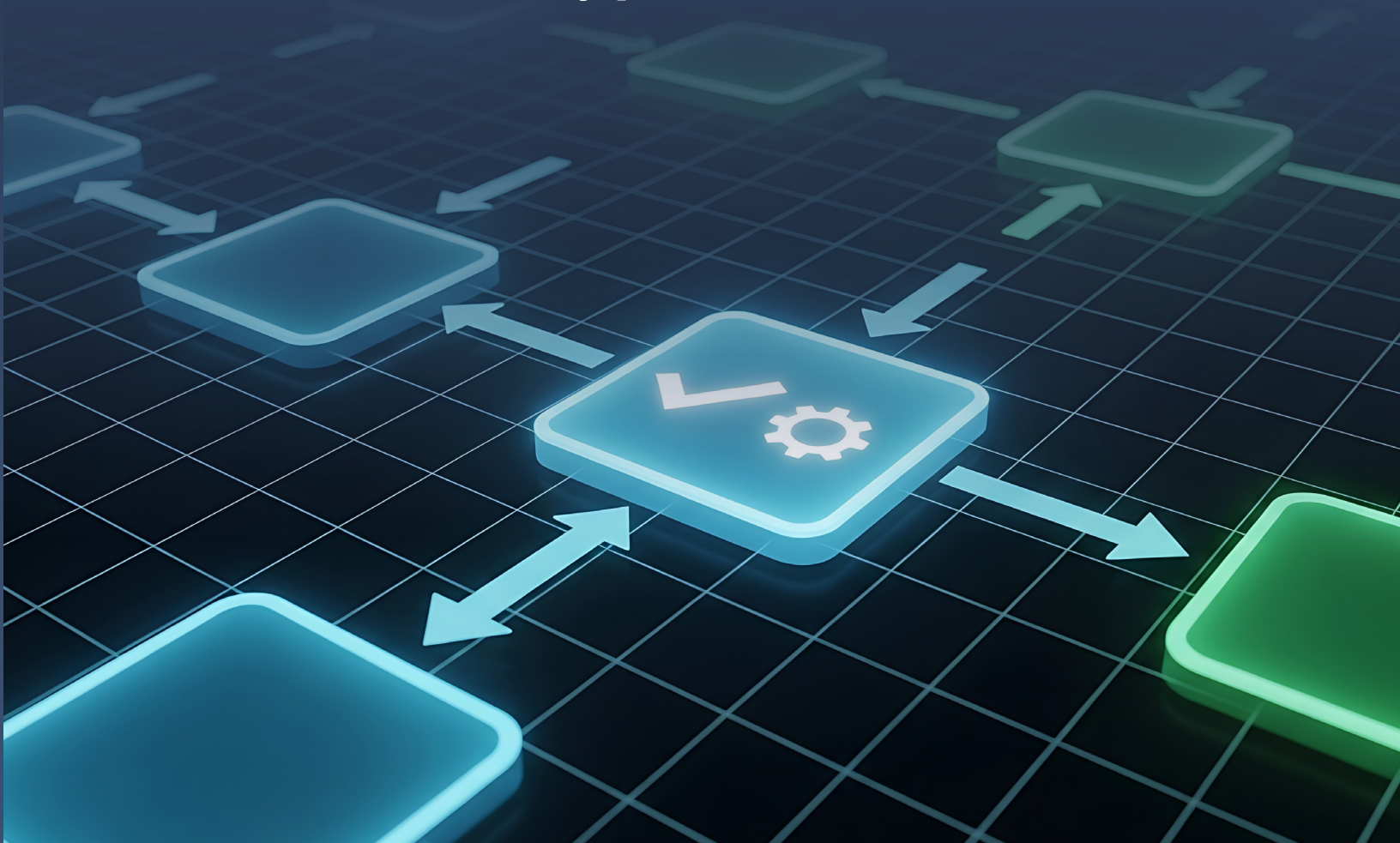


Network Observability Readiness Guide

**A practical framework for selecting,
justifying, and operationalizing a
Network Observability platform**





How To Use This Guide

This document is a companion to guide you through the network observability evaluation and planning process. Whether you're a network architect designing the solution, a security leader ensuring compliance requirements are met, or an IT director building the business case, this guide provides the frameworks and decision tools you need to succeed.

By answering a series of questions, you will:

- Identify key outcomes and targeted use cases for your business
- Assess your current network observability maturity and identify gaps
- Select the right architecture for your environment
- Plan a phased deployment that demonstrates quick wins
- Evaluate solutions systematically against your requirement

Introduction

Most IT organizations already have complex network observability stacks. The goal is not just to monitor network availability, performance, and traffic behavior, but to derive **actionable intelligence** that helps teams quickly detect, troubleshoot, and resolve issues, and when possible preempt them before they impact the business – which ultimately leads to fewer incidents, better decision making, and greater resilience.

AI-driven observability is likely the most effective means to achieve true network observability. But getting there requires a strategic approach to address foundational gaps to ensure the long-term value of future observability investments. These are gaps in how network behavior is captured, analyzed, presented, and acted upon.

Real operational improvement only happens when:

- The data reflects reality on the wire — not inferred, sampled, unverified or debatable
- The information scales across teams and workflows
- The conclusions are explainable — so engineers and leaders can make decisions with confidence

When those conditions are met, adopting AI-driven observability stops being a risk and starts adding real value – to your workflows, your stakeholders, and your business. So, let's get started!

1

SECTION 1:

Have Targeted Use Cases with Clear Outcomes

Prioritize Your Use Cases

Prioritizing use cases based on business impact — from foundational capabilities like application performance troubleshooting to strategic initiatives like AI-driven autonomous operations — is a proven best practice that ensures your observability investment delivers quick wins that build momentum while creating a clear roadmap toward transformational outcomes that justify enterprise-scale expansion.

Common Early Project Use Cases:

- Improve service quality (voice and video)
- Application performance troubleshooting
- Connectivity troubleshooting
- Security incident detection

Mid Cycle Project Use Cases:

- Improve network health and readiness for increased network traffic
- Capacity planning and optimization
- Multi-cloud visibility
- Security incident forensics and auditing

High Impact Targeted Project Use Cases:

- Predictive capacity management
- Proactive anomaly detection
- AI-driven autonomous operations
- Enterprise-wide integration

Set Your Outcomes Expectations

Before selecting technology or architecture, clearly articulate which specific business outcomes will define success for your observability initiative and secure ongoing executive support.

Defining written outcomes at the project's outset creates alignment across stakeholders, establishes measurable success criteria that justify your investment, and provides the clear benchmarks needed to demonstrate ROI and secure budget for future phases.

Here are some common customer outcomes that we often see in their projects:

Reduce network
"Mean Time to Innocence" (MTTI)
 and **"Mean Time to Resolve" (MTTR)**



Reduce ticket volume while
shortening incident duration
 (Enhance security and compliance/Other)



Improve tooling ROI
 (Return on Investment)



Improve staff efficiency
 (Hit your target SLAs and
 improve use experience)



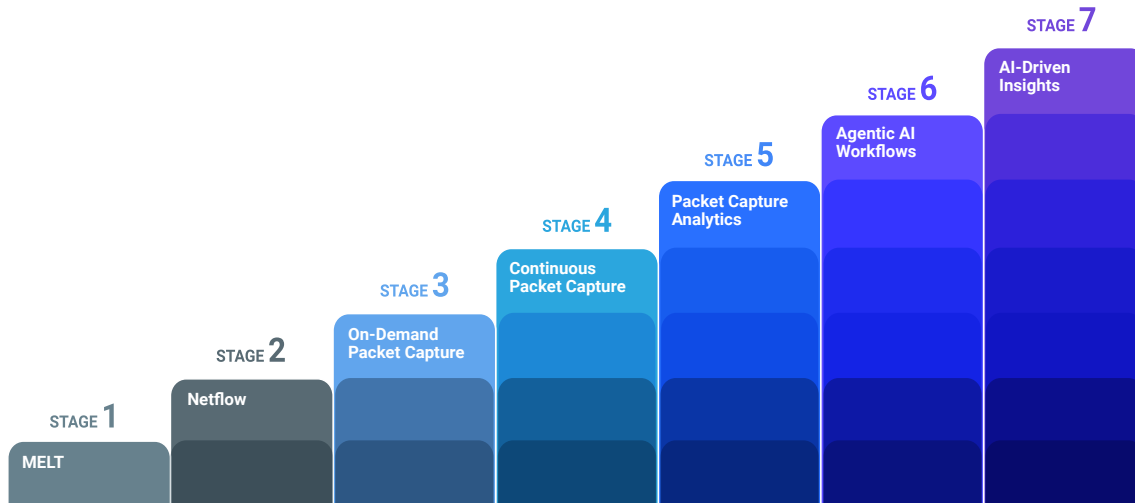
2

SECTION 2:

Assess Your Current State

Where Are You on the Network Observability Maturity Journey?

Understanding your current observability maturity is the foundation for planning your path forward. Most organizations operate at different maturity levels across their infrastructure. To help with this process, cPacket has built a maturity model with seven stages.

**Stage 1: MELT-Only Observability**

You rely entirely on metrics, events, logs, and traces from application monitoring tools. The network is a black box. When performance issues occur, you're left guessing whether the problem is in the application, server, or network.

Stage 2: Flow-Based Visibility

You've added NetFlow or IPFIX to understand "who's talking to whom." You can see traffic volumes and top talkers, but when applications slow down despite normal traffic patterns, you lack explanations.

Stage 3: On-Demand Packet Capture

You capture packets reactively when issues occur, either on hosts (tcpdump) or in the network (TAPs/SPAN). The challenge: by the time you set up capture, intermittent problems have often disappeared.

Stage 4: Continuous Packet Capture

Packets are captured 24/7 across critical paths. You never miss evidence, but manual analysis doesn't scale. Finding relevant packets in terabytes of data takes too long.

Stage 5: Packet Capture Analytics

Real-time analytics derived from packets enable proactive workflows. You detect rising retransmissions before users complain. Metrics-first investigation scopes issues quickly, then targeted packet retrieval provides proof.

Stage 6: Agentic AI Workflows

AI agents democratize packet intelligence. Application teams ask natural language questions and get answers backed by packet evidence. Cross-domain correlation eliminates war rooms and finger-pointing.

Stage 7: AI-Driven Insights

Autonomous systems learn normal behavior across what/when/where dimensions. Thousands of anomalies reduce to actionable insights. Issues are detected and often resolved before users are aware.

For more details on this model visit here:

➔ [MATURITY MODEL WHITEPAPER](#)



Quick Self-Assessment

Honestly assessing your current challenges provides the foundation for selecting your next logical steps, setting realistic project timelines, and building stakeholder alignment around the specific capabilities needed to advance your observability practice from reactive firefighting to proactive, AI-driven operations.

Current State Checklist – Check all that apply to your environment today:

Visibility Gaps

- ☐ We lack visibility in certain segments, ISP, or cloud provider networks
- ☐ Intermittent performance issues disappear before we can investigate
- ☐ We cannot see east-west traffic between internal applications
- ☐ We have blind spots in hybrid cloud environments

Operational Challenges

- ☐ Network issues are reported by users, not our monitoring tools
- ☐ We spend hours or days proving the network isn't at fault
- ☐ Root cause analysis takes days instead of hours
- ☐ Senior engineers are bottlenecks for packet analysis

Business Impact

- ☐ Prolonged outages directly impact revenue
- ☐ We can't confidently adopt new technologies (SD-WAN, cloud, AI workloads)
- ☐ Compliance audits require weeks of manual evidence gathering
- ☐ Security incidents lack definitive packet evidence

Skill Gaps

- ☐ Packet metadata analysis expertise
- ☐ Cloud and hybrid network troubleshooting
- ☐ AI/ML tool adoption for network observability
- ☐ Cross domain integration and workflow orchestration

Performance Visibility Gaps

- ☐ Can you detect microbursts causing packet loss?
- ☐ Can you measure hop-by-hop latency across paths?
- ☐ Can you identify TCP retransmissions in real-time?
- ☐ Can you baseline normal application behavior?

Security & Compliance Gaps:

- ☐ Can you reconstruct security incidents with packet evidence?
- ☐ Can you run forensics on historical packet data?
- ☐ Can you prove compliance with regulatory audits?

3

SECTION 3:

Select Your Architecture

Design Architectures Aligned to Maturity Stages

Your architecture should match your current capabilities while enabling growth to the next stage.

Architecture 1: Targeted Forensics (Stage 3-4)

Best for: Organizations making the leap from flow-based monitoring to packet-level evidence

Architecture Overview:

- Deploy packet brokers (cVu) at critical network aggregation points
- Implement continuous capture appliances (cStor) on high-priority segments
- Start with north-south traffic (perimeter, DMZ, internet edge)
- Feed packet data to existing security and analysis tools

Key Components:

- Network TAPs at aggregation layers
- Packet brokers (cVu) for traffic filtering and distribution
- Capture appliances (cStor) with 7-30 day retention
- Integration with Wireshark for expert analysis

When to Choose This Architecture:

- You're primarily reactive today (learning about issues from users)
- You need definitive evidence to end the "blame game"
- Security forensics and compliance are primary drivers

Quick Wins:

- Reduce MTTI (Mean Time to Innocence) from days to hours to minutes
- Solve intermittent issues with historical packet evidence
- Enable post-incident reconstruction weeks after events

Architecture 2: Continuous Operations (Stage 4-5)

Best for: Organizations moving from reactive forensics to proactive operations

Architecture Overview:

- Extend continuous capture across all critical network segments
- Deploy onboard analytics for real-time metrics extraction
- Implement centralized management across distributed sites (cClear)
- Add Grafana dashboards for metrics-first investigation

Key Components:

- Comprehensive TAP coverage (north-south, east-west, cloud)
- Packet brokers (cVu) with inline analytics
- Extended retention capture (cStor) appliances (30-90 days)
- Analytics and visualization layer
- Centralized management platform (cClear)

When to Choose This Architecture:

- You've proven packet capture value and are ready to scale
- You need proactive alerting, not just reactive investigation
- Multiple teams need concurrent access to observability data

Quick Wins:

- Detect microbursts and performance degradation before user impact
- Enable junior engineers to investigate using metrics dashboards
- Lower incident triage time with intelligent analytics

Architecture 3: Integrated Intelligence (Stage 5-6)

Best for: Organizations ready to democratize packet intelligence across teams

Architecture Overview:

- Unified observability platform spanning capture, analytics, and AI
- Deep integration with ITSM, NDR, and APM ecosystems
- AI agents providing natural language access to packet intelligence
- Cross-domain correlation eliminating operational silos

Key Components:

- Enterprise-wide packet fabric (cVu across all locations)
- Unified capture and analytics platform
- AI and MCP integration layer (cPacket AI)
- Bi-directional integrations (ServiceNow, Splunk, Datadog)
- RBAC and multi-tenancy for different teams

When to Choose This Architecture:

- You need to break down silos between NetOps, SecOps, and AppOps
- Application teams need self-service network intelligence
- You're ready to leverage AI for correlation and automation

Quick Wins:

- *Application owners investigate network issues without escalation*
- *Security incidents include network context automatically*
- *AI reduces thousands of alerts to actionable insights*

Architecture 4: Autonomous Operational Workflows (Stage 6-7)

Best for: Organizations pursuing AI-driven insights to automate network operations. Shift your workflows from Reactive to Proactive to Predictive

Architecture Overview:

- AI-driven baseline learning across what/when/where dimensions
- Autonomous topology discovery and correlation
- Predictive analytics forecasting issues before occurrence
- Closed-loop automation with human oversight

Key Components:

- Complete Pattern 3 foundation
- cPacket AI Insight Engine for autonomous baselining
- Predictive capacity and performance analytics
- Automated workflow execution with approval gates

When to Choose This Architecture:

- You operate at massive scale (multi-site, multi-cloud, 100G+ links)
- Zero-downtime requirements justify maximum investment
- You're ready for network observability as competitive advantage

Quick Wins:

- *Issues detected and resolved before users are impacted*
- *Demonstrate Predictive alerts*
- *Autonomous correlation: cPacket MCP data correlated with ecosystem data*

4

SECTION 4: Plan Your Integration Strategy

Integration by Workflow

NetOps Workflow: ITSM and AIOps Integration

When network issues are detected, automatic ticket creation with relevant context. Integrating packet-level insights into your AIOps platforms streamlines workflows and improves MTTR

ServiceNow Integration Pattern:

- cPacket detects anomaly (rising retransmissions, connection failures)
- Creates ServiceNow incident automatically with:
 - Affected services and time windows
 - Packet-derived metrics showing baseline vs. current state
 - Direct links to relevant packet captures
- Recommended next steps

Datadog/Dynatrace Integration Pattern:

- APM detects elevated application latency
- Events from cPacket provide additional context and insights
- Verdict delivered: network path health status

NDR Integration

- Integrated workflows between cPacket's full capture with NDR APIs providing security investigations with network context
- cPacket insights on security use cases provide additional data for SecOps

Splunk/Elastic Integration Pattern:

- Security alert fires in SIEM
- SIEM queries cPacket for network context via API
- Packet evidence retrieved for forensic analysis
- SOAR playbook executes automated response

Data Export Strategies

- **Metadata Only:** Session records, flow data, metrics (lightweight, real-time)
- **Enriched Flows:** Flow records with packet-derived intelligence
- **Targeted Packets:** Specific PCAP files for security tools
- **Full Replication:** Complete packet archive (regulatory requirements)

Authentication & Access Control:

- **Enterprise SSO/SAML** Integration for single sign-on
- **Role-Based Access Control (RBAC)** for different team permissions
- **Audit Logging** for compliance and forensic tracking

Common failure modes to avoid:

- Weak workflow integration and unclear ownership.
- Data distrust caused by inferred signals without explainable evidence.
- Skills bottlenecks where only a few specialists can use the platform.
- Pilot sprawl from proving too much without crisp success criteria.

5

SECTION 5:

Adoption Roadmap and Risk Management

Plan adoption like an operating model change. The platform becomes valuable when workflows are repeatable and teams trust the evidence.

30, 60, 90-Day Rollout	
Timeframe	Focus and Deliverables
First 30 Days	Deploy priority capture points, integrate with incident workflow, train core responders, publish initial runbooks. First "impossible to solve" issue resolved with packet evidence.
60 Days	MTTR consistently reduced 50%+, tool consolidation eliminates redundant platforms. Expand to additional segments, baseline packet-derived KPIs, reduce alert noise, establish governance for access and retention.
90-120 Days	Enable proactive detection and cross-domain correlation, publish executive reporting on MTTR and risk reduction. Proactive operations prevent issues before user impact; network becomes competitive advantage.

NEXT STEPS: Call to Action

Immediate Actions

1. Complete the self-assessment to determine your maturity stage
2. Identify your primary use case - Which problem causes the most pain?
3. Select your architecture pattern aligned to your maturity and goals
4. Engage with cPacket to validate your approach

Schedule a consultation with our cPacket solution architects or CTO team to:

1. Validate your maturity assessment and architecture selection
2. Review reference architectures from similar organizations
3. Discuss proof of value scope and success criteria
4. Plan your phased deployment roadmap

Planning Phase

1. Assemble your evaluation team - Network architect, security lead, operations manager
2. Document requirements using the checklists in Section 1
3. Draft your phased deployment plan using Section 4 framework
4. Validate with cPacket solution architects

Proof of Value / Concept

1. Deploy Phase 1 in your most critical environment
2. Validate success criteria - Measure MTTR reduction, document solved issues
3. Make Go/No-Go decision for Phase 2 based on quantified results

How cPacket Supports Your Journey

We Meet You Where You Are

Whether you're at Stage 1 (MELT-only) or Stage 5 (packet analytics deployed), cPacket provides a clear path forward. Our platform grows with you—add capabilities by enabling software features, not ripping out infrastructure.

Our Unique Approach

Unified Platform: One architecture spans packet brokering (cVu), continuous capture (cStor), analytics, and AI. No vendor sprawl, no integration nightmares.

Open Ecosystem: We integrate with your existing tools—ServiceNow, Splunk, Datadog, ExtraHop, Corelight, Grafana—through open APIs and MCP protocol.

AI at the Packet Source: Our AI operates on lossless, line-rate packet data. Every insight is backed by deterministic packet evidence, ensuring explainability and trust.

Customer-First Partnership: You get direct access to product, engineering, and executive leadership throughout your journey.

Proven Track Record

- Over 50% of global equity and exchange data flows through cPacket
- Morgan Stanley, Nasdaq, UPMC, Microsoft trust us for zero-downtime operations
- 95% improvement in triage times, 50% operational cost reduction

About cPacket

cPacket's Unified Observability Platform empowers organizations to deliver reliable, secure, and high-performing digital experiences. By uniting packet-level visibility with AI-driven insights, cPacket enables faster decisions, reduces risk, and improves operational resilience across hybrid and multi-cloud environments. Trusted by leaders in finance, healthcare, government, and technology. Visit www.cpacket.com to learn more.

