NIAGARA NETWORKS

WHITE PAPER

Unified Visibility for Hybrid and Multi-Cloud Environments Using the Cloud Intelligence Platform

Extending Cloud Visibility Through an Intelligent Cloud Packet Broker Architecture

The Modern Visibility Gap: Why Cloud Adoption Breaks Traditional Network Monitoring?

The widespread enterprise adoption of hybrid and multi-cloud environments represents a fundamental shift in IT strategy. Organizations are increasingly leveraging the cloud to enable innovative business models and execute efficient digital transformation strategies. However, this transition introduces significant challenges for maintaining network visibility, a critical component of effective security and performance management. As applications and data move from centralized data centers to distributed cloud infrastructures, the methods used to monitor them must also evolve.

The core of the problem lies in the architectural differences between legacy and cloud networks. Traditional monitoring tools were engineered for a world of predictable, box-based networks, where physical infrastructure was the norm. In contrast, modern cloud environments are dynamic, on-demand, and highly abstracted. Traffic flows are now API-driven and follow service-to-service communication patterns rather than predictable north-south paths. This new paradigm creates a significant visibility gap, rendering legacy tools incapable of providing the deep, packet-level insight that NetOps & SecOps teams rely on. This gap not only complicates troubleshooting but also creates dangerous blind spots that can be exploited by threat actors. To successfully navigate this transformation, organizations must address the specific technical challenges that make cloud traffic so difficult to see.

Deconstructing the Challenge: Technical Barriers to Visibility in Cloud Architectures

The visibility gap in cloud environments is not a single issue but rather a collection of distinct technical hurdles inherent to modern cloud design. For NetOps & SecOps teams, understanding these architectural barriers is the first step toward selecting a solution that can effectively restore control and insight. Without a purpose-built approach, teams are left struggling to adapt tools that were never designed for the scale, complexity, and abstraction of the cloud.

The primary technical barriers that prevent traditional monitoring tools from operating effectively in hybrid and multi-cloud architectures include:

- Distributed and on-demand non-deterministic Workloads: In the cloud, traffic is highly distributed across availability zones, subnets, and geographic regions. Furthermore, workloads such as virtual machines (VMs) and containers have short lifecycles, spinning up and down on demand. This constant change makes it incredibly difficult to establish and maintain a consistent monitoring posture.

- Opaque East-West Traffic: The rise of microservices architecture has led to an exponential growth in East-West traffic (communication between servers within the cloud). Unlike traditional North-South traffic, this internal traffic is much harder to tap and inspect. This creates an unmonitored highway for lateral movement by threat actors, a common tactic in advanced persistent threat (APT) campaigns.

- Pervasive Encapsulation: Cloud providers use overlay tunneling protocols, such as VPC/VNet, VXLAN, GENEVE, and GRE to create virtual networks. These overlays wrap the original L2-L4 packet, hiding the very headers that traditional monitoring tools rely on for analysis and filtering, rendering the traffic flow effectively "opaque."

- Limited Access to Raw Packets: Cloud Service Providers (CSPs) deliberately limit or block direct access to the raw packet plane. This is a fundamental design choice to enforce their multi-tenant security and abstraction models, making traditional packet acquisition methods like physical TAPs and SPAN ports obsolete within the cloud fabric.

- Tool Overload and Inefficiency: Sending raw, unfiltered packet streams from the cloud to monitoring tools is both cost-prohibitive and operationally inefficient. To function correctly and avoid being overwhelmed, security and performance tools must ingest only the "right traffic, not full packet copies."

These challenges collectively demonstrate that a fundamentally new architectural approach is required. A modern visibility solution must be designed from the ground up to overcome these exact barriers.

The Solution: Introducing the Niagara Networks Cloud Intelligence Platform (CIP)

To close the visibility gap in modern hybrid and multi-cloud environments, a new architectural layer is required. The Niagara Networks Cloud Intelligence Platform (CIP) provides this foundational layer, operating as a cloud-native virtual packet broker designed to deliver deep, packet-level visibility and provide optimized, filtered data to SOC and NOC tools across public, private, and hybrid clouds.
By bridging public clouds and private on-premises virtualization, CIP restores the deep, packet-level insight that enables a coherent, secure, and improved user experience.

Traditional Monitoring vs. CIP: Challenges and Benefits

Challenge	Traditional Monitoring Limitations	CIP Solution	Benefit
Distributed Workloads	Static tools can't handle dynamic VMs/containers across regions.	Adaptive scaling with auto-spin-up/down.	Consistent monitoring posture, reduced manual intervention.
Opaque East-West Traffic	No access to internal service-to-service flows	Full tunnel termination (e.g., VXLAN, GRE).	Eliminates blind spots for lateral threat movement.
Pervasive Encapsulation	Headers hidden, rendering tools ineffective.	Strips overlays like MPLS, VLAN, FabricPath.	Delivers clean, inspectable packets to tools.
Limited Raw Packet Access	CSP blocks TAPs/SPAN in multi-tenant setups.	Cloud-native virtual packet broker within boundaries.	Maintains compliance and zero-trust segmentation.
Tool Overload	Unfiltered traffic causes high costs/noise.	Deduplication, slicing, NetFlow generation.	Smarter data delivery, up to 50% cost savings.

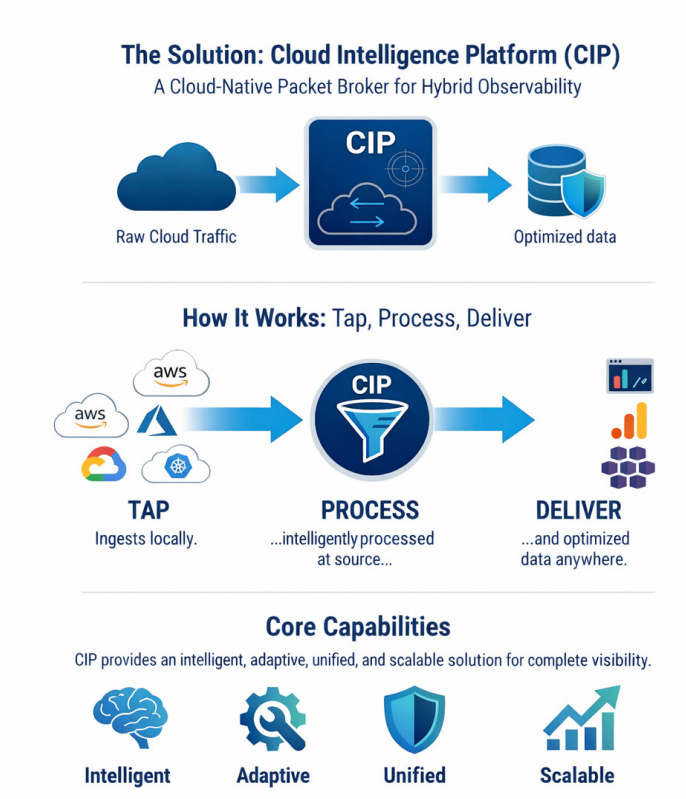
Core Architectural Pillars - The CIP architecture is built on four key attributes that enable it to meet the demands of dynamic cloud infrastructures:

- Intelligent: Delivers application-aware filtering and Layer-7 enrichment to provide deep context and precision traffic delivery.
- Adaptive: Automatically scales with cloud workloads and is architecturally flexible to fit any public, private, or hybrid cloud design.
- Unified: Provides a single control layer and flexible policy profiles for managing visibility across AWS, Azure, GCP, and private virtualized environments.
- Scalable: Employs a high-throughput virtual architecture designed for multi-region visibility and effective tool load optimization.

CIP Core Architectural Pillars

Pillar	Description	Key Features	Value to Users
Intelligent	Context-aware traffic delivery, regex filtering.	Context-aware traffic delivery, regex filtering.	Precision insights, reduced false positives.
Adaptive	Auto-scales with workloads.	Flexible for AWS, Azure, GCP, hybrid.	Handles spikes without overprovisioning.
Unified	Single control layer across clouds.	Policy profiles for multi-cloud management.	Simplified operations, coherent visibility.
Scalable	High-throughput virtual architecture.	DPDK/SR-IOV for line-rate processing.	Multi-region support, elastic TCO.

With these pillars as its foundation, the Cloud Intelligence Platform provides a robust and agile architecture for regaining control over network traffic in the cloud.



Architectural Value Proposition: How CIP Delivers Cloud-Native Visibility

The effectiveness of the Niagara Networks Cloud Intelligence Platform stems from its purpose-built, cloud-native architecture. Unlike legacy hardware-based solutions retrofitted for virtualization, CIP was architected from first principles to embrace the unique constraints and leverage the opportunities of cloud-native design patterns. This section deconstructs the key architectural principles that allow the platform to deliver comprehensive, efficient, and scalable visibility.

CIP Architecture - Operational Impact Highlights

Architectural Principle	Operational Impact
Built for Cloud-Native Overlay	Designed specifically for the speed, scale, and elasticity of modern cloud environments that utilize encapsulation.
Proximity to Workloads	CIP engines run close to workloads, applying L2–L7 processing locally to avoid costly and inefficient traffic backhauling.
Intelligent Traffic Reduction	Eliminates duplicates, irrelevant packets, and unnecessary tunnels before sending data to tools, resulting in lower tool overhead, reduced cloud compute costs, and faster investigation times.
Elastic, Event-Driven Scaling	Automatically scales processing engines up during traffic spikes and down when idle, ensuring an agile and cost-effective Total Cost of Ownership (TCO).
Unified Centralized Management	The CIP Controller provides a single web UI to discover, manage, and apply policies across all instances, simplifying operations in multi-cloud and multi-region deployments.
Cloud-Native Compliance & Segmentation	The visibility toolkit operates within the same trust boundary as the cloud application, ensuring raw traffic is not exported across accounts unless explicitly approved by policy.

By adhering to these principles, CIP provides a visibility fabric that is as dynamic and scalable as the cloud infrastructures it is designed to monitor.

Architectural Value Proposition: How CIP Delivers Cloud-Native Visibility

The cloud-native architecture of the Niagara Networks Cloud Intelligence Platform translates directly into a comprehensive feature set designed to empower both Network Operations (NetOps) and Security Operations (SecOps) teams. This is not merely a list of features, but a complete visibility toolkit that allows architects to surgically extract, process, and deliver the exact packet data required by any tool, under any condition. These capabilities are the essential building blocks for creating an agile and complete visibility fabric:

Traffic Aggregation and Distribution

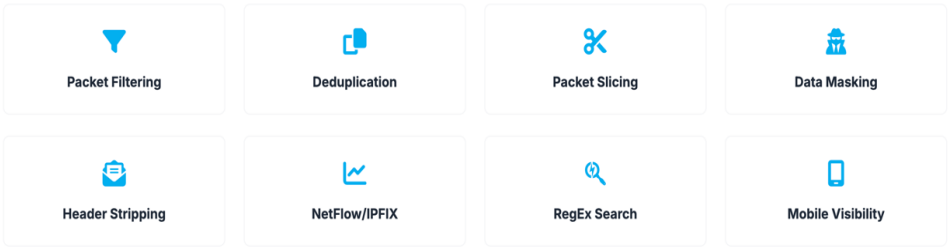
- Packet filtering (IPv4 and IPv6), aggregation, replication, and intelligent, flow-based load balancing
- Full tunnel termination for GRE, VXLAN, NVGRE, GENEVE & ERSPAN
- Header stripping for protocols including VNTag, VLAN/QinQ, FabricPath, MPLS, PPPoE, GTP-U & ERSPAN

Traffic Optimization and Reduction

- Packet and flow slicing to reduce load on downstream tools
- Deduplication to eliminate redundant packets and reduce false positives
- NetFlow/IPFIX generation for efficient flow-level analytics
- Collectively, these functions dramatically lower the Total Cost of Ownership (TCO) for the entire security and monitoring stack by reducing data transport costs, tool licensing fees, and storage requirements

Advanced Layer-7 Network Intelligence (adding the vPacketron engine)

- Application-aware filtering for precise traffic delivery
- Regular expression (RegEx) filtering for deep content matching
- Data masking to protect sensitive information
- Subscriber-aware mobile visibility for 3G/4G/5G environments
- TLS decryption & packet capture - a future software release



Platform Support and Integration

- Public Clouds: AWS, Azure, GCP
- Private Clouds: VMware ESXi, KVM, OpenStack
- Traffic Ingestion: CIP can ingest tunneled traffic from remote on-premises physical TAPs or SPAN ports using standard tunneling protocols, as well as traffic mirrored from virtual TAP or cloud-native mirroring service
- Performance: High-throughput processing using DPDK/SR-IOV.

These granular features provide the control and flexibility needed to build a robust visibility strategy that spans the entire hybrid cloud ecosystem.

Strategic Use Cases and Operational Value

The true measure of a visibility platform is its ability to solve critical business and operational challenges for SOC and NOC teams. The Niagara Networks Cloud Intelligence Platform (CIP) translates its rich technical capabilities into tangible value by enabling a range of strategic use cases, from optimizing tool performance to strengthening an organization's overall cybersecurity posture:

1. Unified Hybrid Cloud Observability In a hybrid world, visibility cannot be siloed. CIP acts as the ultimate solution for hybrid cloud observability by creating a single, holistic platform to collect, aggregate, and forward packet flows. It seamlessly integrates traffic from on-premises data centers, private cloud deployments, and public cloud environments, sending a unified data stream to analysis tools, thereby eliminating the complexity of managing disparate monitoring systems.

2. SOC/NOC Tool Optimization and Cloud Ops effeciency - The economic and operational efficiency of the entire SOC/NOC toolchain depends on the quality of data it ingests. CIP's traffic reduction features - including deduplication, packet slicing, and application-aware filtering - deliver cleaner, more relevant traffic to security and performance tools. By removing redundant and irrelevant data before it reaches the analysis layer, CIP lowers tool processing and storage costs, accelerates threat detection, reduces fault positives and mean-time-to-resolution (MTTR), and maximizes the return on investment (ROI) for the entire analysis toolchain.

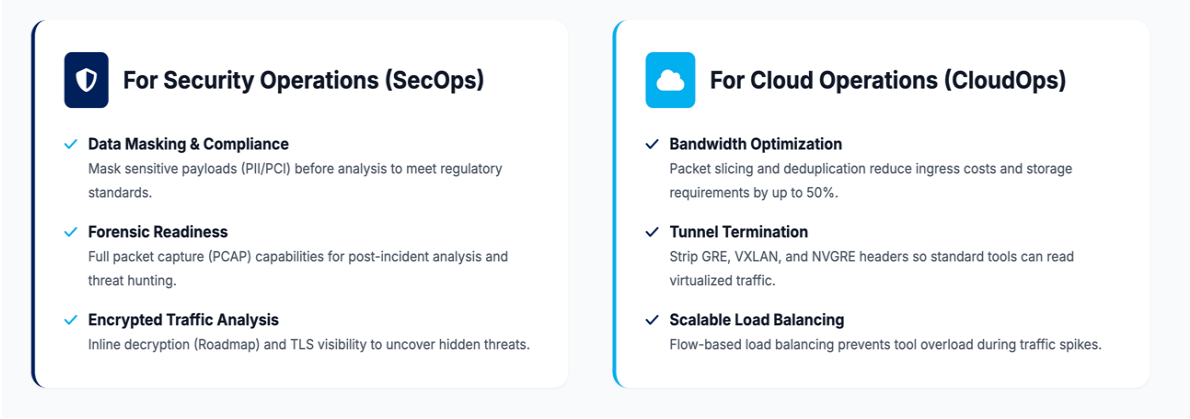
3. Strengthening Cybersecurity Posture Sophisticated threats like spyware and zero-day attacks are designed to remain hidden within network traffic. Comprehensive visibility is the first line of defense, and CIP helps unmask these hidden threats by eliminating blind spots in high-bandwidth and hybrid environments. This capability directly supports the continuous monitoring requirement (Detect DE.CM) of the NIST Cybersecurity Framework 2.0, ensuring that all traffic flows are available for inspection so anomalies can be detected before they escalate into major incidents.

4. Enabling Secure Cloud Migration Migrating applications to the cloud is a complex process where performance and security risks are high. CIP can be deployed to monitor application traffic before, during, and after a cloud migration. This allows teams to baseline performance, validate security policies, and troubleshoot any issues that arise during the transition, ensuring a smooth and secure migration process without compromising user experience or exposing the organization to new risks.

These use cases demonstrate how CIP moves beyond simple packet capture to provide strategic value, making the entire IT and security operation more efficient, effective, and secure.

Built for NetSecAppOps

Unified visibility for every team



Conclusion: Redefining Visibility for the Cloud Era

The migration to hybrid and multi-cloud architectures has created a new reality for enterprise IT. Traditional monitoring tools, built for a static and predictable physical world, are fundamentally incompatible with the dynamic, encapsulated, and distributed nature of modern cloud infrastructures. This has resulted in a critical visibility gap that exposes organizations to performance degradation, operational inefficiencies, and significant security risks.

The Niagara Networks Cloud Intelligence Platform (CIP) is the purpose-built, essential solution for closing this gap and regaining packet-level visibility across the entire hybrid ecosystem. As a cloud-native virtual packet broker, CIP is architecturally designed to handle the scale, complexity, and abstraction of the cloud. By providing intelligent filtering, advanced traffic optimization, and a unified management layer, it empowers NetOps and SecOps teams with the deep insight they need to protect and manage their digital assets effectively.

You can't secure, optimize, or monitor traffic you can't see. CIP gives cloud, NetOps, and SOC teams a virtual packet broker layer purpose-built for distributed cloud architectures, bringing packet intelligence back into environments where traditional solutions cannot reach.

Visit www.niagaranetworks.com to learn more and request a CIP demo for cloud visibility.

About Niagara Networks

Niagara Networks provides high performance network visibility solutions for seamless administration of security solutions, performance management and network monitoring. Niagara Networks products provide advantages in terms of network operation expenses, downtime, and total cost of ownership. A former division of Interface Masters, Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including TAPs, bypass elements, packet brokers and a unified management layer. Thanks to its integrated in-house capabilities and tailor-made development cycle, Niagara Networks is agile in responding to market trends and in meeting the customized needs of service providers, enterprises, data centers, and government agencies. For more information please visit us at www.niagaranetworks.com.

NIAGARA NETWORKS

48430 Lakeview Blvd,
Fremont, CA 94538, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529