# Cloudifying Datacenter Monitoring with DANZ

The shift to a cloud networking approach driven by the emergence of massive scale cloud datacenters, rapidly evolving merchant silicon and software-driven operational models has opened a significant gulf between the ability to provision large, high throughput, highly shared networks and the ability to effectively monitor these networks at a reasonable cost point.

The Arista Visibility portfolio is designed to provide a feature-rich and more cost effective visibility architecture, all at a scale that has been previously unattainable. This is accomplished by natively integrating the advanced Data ANalyZer (DANZ) monitoring feature set into a common set of scalable switching platforms that leverage a single common Extensible Operating System (EOS) and a single CloudVision automation framework across both general compute and visibility network designs. This paper introduces a number of concepts that are unique to the Arista Visibility portfolio.

## Cloud Transition Needs New Visibility Architectures

Today's massive shift to virtualization, containerization and cloud-native applications is driving volumes of data, audio and video content. An insatiable demand for better visibility and telemetry in high-bandwidth and high-density cloud networking has grown exponentially. This is driven by the following technology transitions:

- Speed - now widely transitioning from 10G to 25G and from 40G to 100 Gigabits per second, and soon even faster.

- Scale - no longer a handful of links and devices but thousands of links, devices and services.

- Architectures - now evolved from legacy, hierarchical, oversubscribed models to non-blocking leaf and spine designs – even extending across multiple interconnected datacenters at hyper-scale.

With cloud datacenters on a path to higher performance and higher density at a global scale, visibility architectures have remained lacking, designed for an era of static and hierarchical network designs, with slower link speeds and limited points of access.

The challenge is caused by limitations in the available toolsets for monitoring:

- Reactive polling based approaches to network telemetry cannot provide real-time visibility at scale.

- Legacy packet brokers are limited by processor-bound filtering and cannot scale to cloud density with wire-rate performance
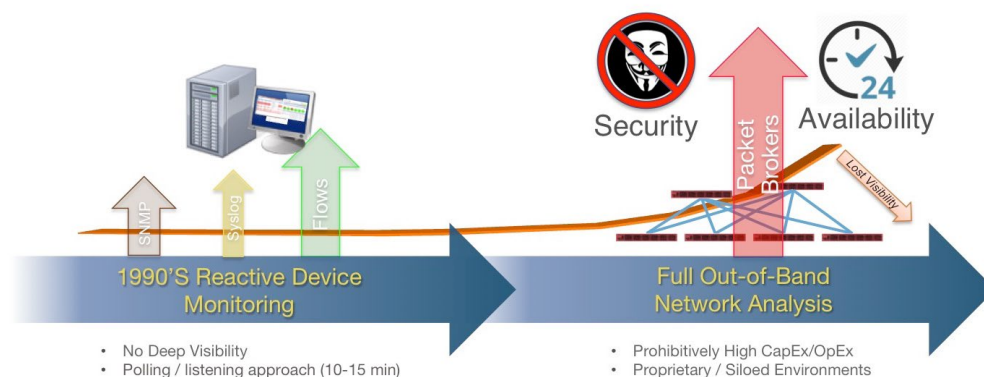


*Figure 1: Traditional overlay monitoring is disproportionately expensive*

Neither integrates well with cloud orchestration, network overlays and software-driven provisioning models. They do not provide any insight into real-time network state or even indicate packet loss within the monitored traffic and therefore have having a very limited scope for deployment at cloud scale. These solutions look increasingly arcane in the modern, cloud-centric world where agility, scale, economics and openness are the principles by which architectures are defined.

The result is a large-scale loss of visibility into the state of the network and communication within the network, an inability to precisely inspect traffic that may be threatening the security and availability of data and applications due to loss and obfuscation and extremely high costs to enable broad visibility because of the low density and high per port cost for speeds like 25 and 100 Gigabits per second. In effect, the outcome is a significant loss in the ability to detect anomalies and mitigate security threats and service outages – just as these have become foremost in enterprise and cloud operator's concerns.

## Cloudifying Data Center Monitoring

The requirement for ensuring cloud scale security and avoiding service outages depends upon the ability of security and network operations teams to respond quickly and efficiently, to take pro-active actions and to maintain total awareness. This translates to the following requirements:

- Insert next generation security tools in any flow either by flow, or on demand

- Maintain precise visibility, to see what happened, where, when and why

- Adhere to cloud principles including architecture, APIs and economics

- Scale to cloud dimensions with thousands of sources and terabits of data, and

- Automate to reduce operator workload, enable integration with orchestration and operations processes and implement instantaneous mediation in case of outages, threats or anomalies

Cloud architects are looking for modern analytical methods to gain visibility for thousands, even millions, of devices, workloads and events efficiently and consistently.

In this new era of visibility designed for the cloud, realizing that the legacy approach is no longer good enough. The Arista Visibility portfolio enables flexible security insertion and service monitoring at cloud scale.

### Arista: Delivering Holistic Visibility

Arista's visibility portfolio provides a unique set of integrated functionality, bringing advanced telemetry data and deep packet visibility with both in-band and out-of-band capabilities. The Arista approach is to deliver packet broker functionality on general purpose networking devices, leveraging the following components:

- Arista EOS, including the resilient, state-sharing architecture, open programmability, operational tools and full datacenter routing/switching feature set.

- Cloud-scale platforms, including the R-Series 7500R modular chassis and 7280R fixed configuration switch for dense 10/25/40/50/100G solutions. The low-latency 7150 is also a part of the visibility portfolio.

- DANZ feature set for TAP Aggregation, including precision filtering, packet slicing, source port labeling, tunneling, header stripping, time stamping, tunnel termination, tool load sharing and much more.

- CloudVision, for automation of network operations tasks, granular telemetry and analytics through the state streaming architecture, as well as services insertion with Macro-Segmentation Services (MSS). CloudVision also includes the TapAgg Manager integration.
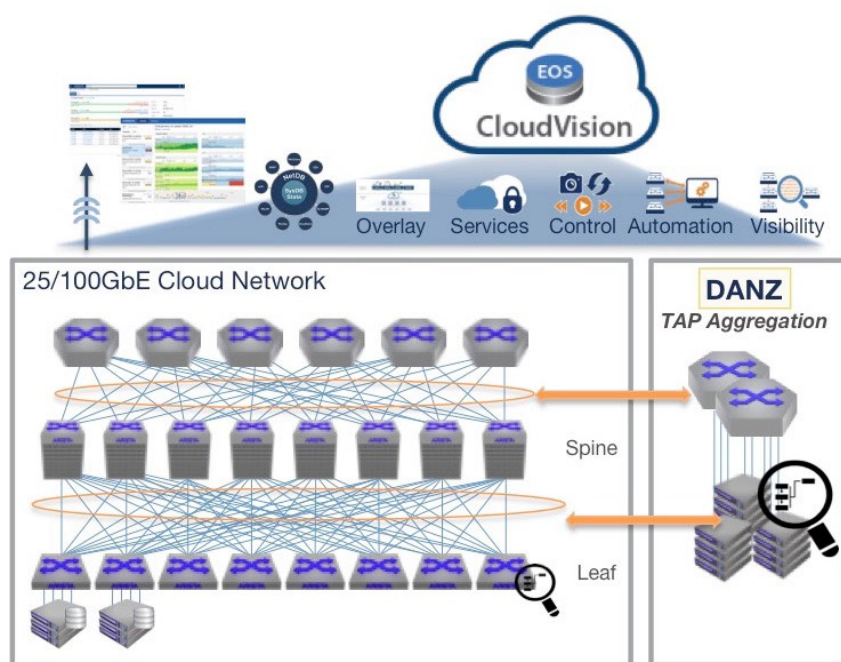


*Figure 2: The Arista Telemetry Approach*

## Universal Spine and Leaf Platforms for TAP Aggregation

Arista's popular 7150 and 7280R leaf switches and 7500R spine switches support DANZ functionality at densities and scales that allow a small number of visibility nodes to meet the needs of a large cloud datacenter without the expense and complexity of proprietary packet broker fabrics.



*Figure 3: The Arista platforms for TAP Aggregation*

DANZ is built upon the same premium datacenter switching platforms that Arista customers have dubbed our Universal Cloud Leaf and Spine. Backed by thousands of man-years of EOS software development and 10 million lines of code, DANZ on the Arista 7150-Series, 7280R-Series, and 7500R-series platforms delivers state-of-the art capabilities for monitoring real-time network telemetry and network traffic with unmatched precision and scale.

DANZ assures each packet and flow is consistently directed to the appropriate destination tool with perfect symmetry and reliability at a 10-60X advantage in bandwidth, density, footprint and power. DANZ is a compelling alternative to software or appliance based solutions like packet brokers.

In addition, DANZ capability is integrated in the Arista Extensible Operating System software on each of these platforms and does not require additional hardware or software. As a result, these common and widely used platforms are as interchangeable as production network infrastructure or out-of-band visibility infrastructure. Network administrators benefit from using consistent software images, platforms and reduced spares as well as a simple low-cost per-device licensing model.

The any-to-any mirroring and TAP Aggregation capacity of these platforms for network speeds from 10-to-25 and 40-50-to-100 gigabits per second are supported by non-blocking and lossless forwarding capacities ranging from 640 Gigabits per second up to 115 Terabits per second. Port densities are unmatched – up to 432 100 Gigabit ports to over a thousand 10-and-25 Gigabit ports.

Addressing the disparity between higher interface speeds and scaling up of production networks against monitoring/telemetry overlays is fundamental to removing the financial and practical barriers that create the visibility cliff. With market-leading density, a variety of form factors and simplified pricing, it is possible to support large numbers of TAP/mirror sources and tool-facing interfaces in a single unit.

## DANZ Feature Set

The DANZ feature set offer extensive functionality to combine and manipulate traffic including features such as:

- Packet filtering based on well-known L2,3,4 header fields

- Deep Packet Inspection (DPI) – user-customizable filters with the ability to inspect packet data beyond traditional headers

- Precision time stamping

- Packet truncation (slicing)

- Replication of traffic across multiple tools

- Load-sharing of traffic across a pool or cluster of tools

- Identity marking of traffic for the purposes of classification

- Removal of surplus headers to reduce processing load on tools

- Support multiple mixed interface speeds and transceiver types

- Support multiple sources (e.g. mirror ports and optical taps)

- CLI, API and Web-Based GUI

- CloudVision as a single point of control for automation, orchestration and real-time monitoring

## CloudVision

An automated network infrastructure can bring many efficiencies but often requires significant resources to develop custom automation software. Arista CloudVision addresses this by providing a purpose-built and turnkey solution for automating the otherwise manual and box-by-box network operations tasks.

Built on an innovative network-wide database architecture, CloudVision is an open, next-generation solution for cloud-like operations. With a focus on automating 3rd party orchestration, provisioning, change management, service insertion and telemetry and analytics, CloudVision provides the platform to allow an organization to start leveraging its network automation in ways it was never able to do before and drastically reduces OpEx costs to run the infrastructure.
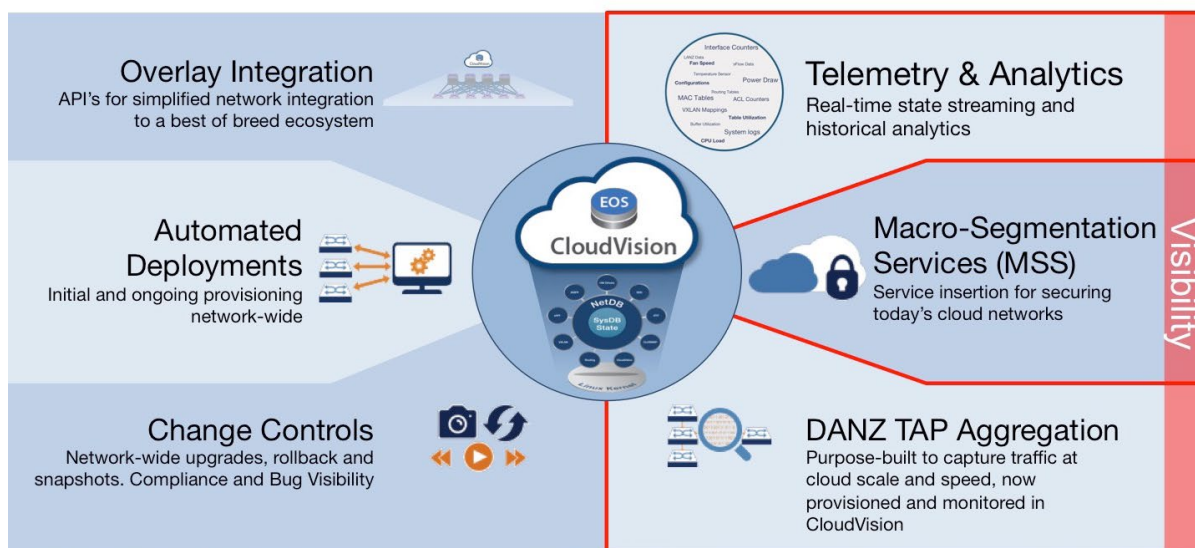


Figure 4: CloudVision, the multi-function platform focused on visibility

With CloudVision, network operators can leverage Zero-Touch Provisioning & Replacement (ZTP/ZTR) to manage the entire lifecycle of a fully-automated visibility network. Change control management provides powerful capabilities for managing and automating changes to configurations, software images and scripts across EOS devices in any network role. CloudVision also provides a central point of management to view, configure and monitor the Arista TAP Aggregation devices.

Arista's EOS streams the state of network events instantaneously to CloudVision's central state database for both the Universal Cloud Network and the Visibility Infrastructure. CloudVision provides real-time visibility into thousands of entities in a network, while Arista's DANZ provides precision visibility for selected traffic, to monitor and record in real-time and without packet loss, corruption or distortion.

In-band visibility capabilities for insertion of security platforms, such as next generation firewalls using CloudVision Macro Segmentation Service (MSS) and precision capture of traffic to tunnels for encapsulation to remote tool farms, optimize use of

multi-terabit cloud spines and do not add additional overhead. These unique capabilities provide an option for deep visibility where ample bandwidth is present, to capture events and traffic with zero additional cost.

## Flow Analysis

A key challenge in monitoring shared networks of scale carrying highly converged data is data overload - simply the inability to parse enough of the infrastructure at sensible cost and in appropriate timescales. One solution is to take a two-tier approach, separating detection and identification from full capture and forensic analysis. In this model, a wide-ranging and coarse level of visibility is used to drive trend, anomaly and threat detection across a topology. Once areas or patterns of interest are identified, deeper capture techniques can be initiated to deep dive and root cause the behavior. Achieving such goals requires three main capabilities:

- Ubiquitous flow export and analysis in-network

- The ability to retrofit matching flow analysis to non-capable devices or inspection points

- Open APIs to enable closed-loop transition from detection to full capture

The universal capability within all Arista switches of sFlow (RFC 3716) on all interfaces, including platforms operating in both full- or hybrid- aggregation modes, ensures the complete coverage of flow analysis under any network topology. EOS provides the stability, openness and rich API feature sets for integration with third party tools and orchestration platforms to aid in automation. EOS also allows for locally-deployed applications to take advantage of telemetry data, enabling autonomous identification and capturing of anomalous behaviors.



*Figure 5: Automated linkage of coarse and fine grained monitoring tamed modern traffic patterns*

### LANZ

Arista Latency ANalyZer, or LANZ, is an EOS device instrumentation feature that tracks sources of congestion and latency with real time reporting in microseconds. The visibility provided by LANZ of network hot-spots and microburst oversubscription gives the network operator greater insight into when problems are occurring in the network and why. With LANZ, one will know when congestion happened, track the sources of congestion and be able to export real-time events to external applications. LANZ also shows the effect of packet buffering on an application as well as monitors and records packet drops during network congestion. Coupled with DANZ, this enables the deeper visibility to both general purpose network and the visibility network designs.

### Visibility Use-Cases

Cloud security and availability assurance can be accomplished using a wide variety of Arista ecosystem partner tools from Threat Mitigation to Regulatory Compliance, Capacity Planning and Service Assurance. Many new applications are emerging that take advantage of the automation capabilities and visibility within the cloud network to help customers avoid the increasing threat of security breaches and service disruptions.
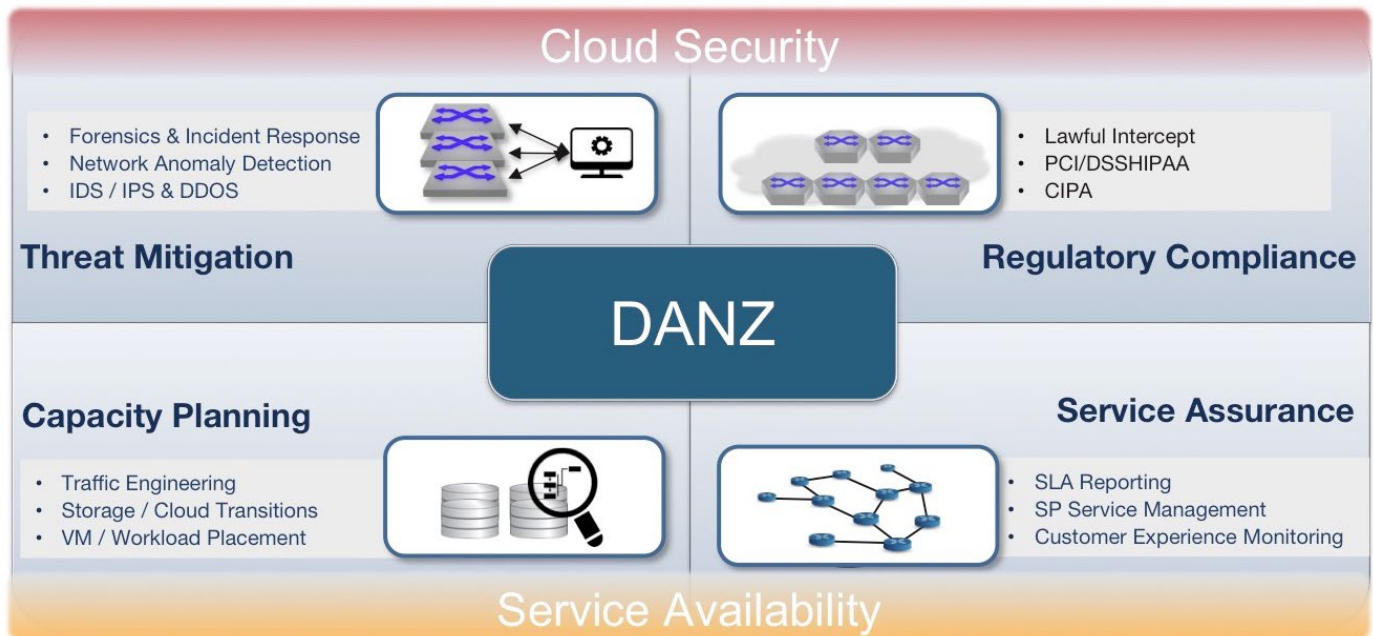


*Figure 6: Visibility Use-cases for DANZ*

**Summary**

To summarize, network visibility is not a singular problem that can be addressed by point solutions like network packet brokers or feature-starved white box solutions. End-to-end visibility for today's network starts with embedded instrumentation at the device level, extends visibility into workloads across hybrid environments at any scale and provides real-time monitoring and analytics for the entire cloud.

Arista's Visibility portfolio addresses each of these requirements with a comprehensive approach for cloud scale networks, providing end-to-end visibility for better security and availability. With the R-series as a DANZ visibility platform, users can insert security services cost-effectively, continuously conduct precision monitoring at scale and "design visibility", with the same capabilities of the cloud titans.

Providing better visibility and security with the dynamic nature of traffic and cloud workloads traversing private and public clouds is the challenge of legacy networks. Arista DANZ and CloudVision are the solution.

**Santa Clara—Corporate Headquarters**
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

**Ireland—International Headquarters**
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

**Vancouver—R&D Office**
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

**San Francisco—R&D and Sales Office**
1390 Market Street, Suite 800
San Francisco, CA 94102

**India—R&D Office**
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

**Singapore—APAC Administrative Office**
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

**Nashua—R&D Office**
10 Tara Boulevard
Nashua, NH 03062