

Creating the Right Hybrid Cloud Visibility Solution

Improve performance, security, and ROI across your
cloud and on-premises networks

Adopting a hybrid cloud (physical on-premises + public / private cloud) infrastructure makes it easy to spin up high-performing new applications at will — if you stay in control throughout the whole process. Building the ideal hybrid cloud visibility architecture lets IT prevent blind spots that lead to risk, troubleshoot user experience (UX) with applications, and avoid costly rollbacks.

The right hybrid cloud visibility approach combines the scale and convenience of cloud with the tighter security controls and cost-efficiencies achieved within data centers. By ensuring you see everything as it happens, visibility lets you avoid complexity that adds to cost, particularly in multi-cloud environments.

Solutions components

- CloudLens cloud tap
- VisionONE Network Packet Brokers
- FLEX taps
- Hawkeye Active Monitoring

Solution Benefits

- Extend full visibility across hybrid cloud-plus-on-premises networks
- Proactively optimize UX with business applications
- Reduce cyber risk and maintain compliance throughout the migration life cycle
- Optimize network monitoring processes and day-to-day operations
- Achieve the greatest return on investments (ROI) from cloud and monitoring tools

Solution Overview

Hybrid cloud visibility requires three essential components:

- Reliable access to packet data in physical and virtual environments
- Physical and virtual pre-processing of data for use by monitoring tools
- Active monitoring to optimize performance throughout the deployment life cycle

The Value of Hybrid Cloud Visibility

Migrating workloads to public cloud environments can create blind spots that lead to increased security risk, user complaints about sluggish applications, and cost overruns that undercut the benefits of moving to cloud in the first place. Multi-cloud designs in which configurations get replicated across two or more vendor environments exponentially increase this risk and complexity.

An end-to-end hybrid visibility infrastructure gives your team full visibility to monitor, troubleshoot, and prevent performance and security issues — even when you don't own the cloud. A purpose-built visibility solution — using the right tool for the right job — lets you balance the processing of monitoring data in the cloud and on-premises to give your team the greatest control at a lower cost and with less ongoing effort.

Hybrid cloud visibility starts with establishing reliable access to packet-level data. Flexible deployment includes pre-processing traffic in the cloud or on-prem on an application-by-application basis. Ongoing proactive monitoring rounds out the solution with real-time insights to improve UX with business applications before, during, and after migration.

Reliable Access to Reliable Data

World-class visibility starts with accessing and capturing data, ideally without wasting valuable switched port analyzer (SPAN) ports on network switches. Keysight's physical and software-based virtual taps offer purpose-built, dedicated devices for capturing packets.

Like their physical counterparts, virtual taps can be inserted anywhere in a private or public cloud to extend full visibility across hybrid environments. These "Cloud" taps capture and replicate packet data that may be processed and analyzed by monitoring tools in the cloud or forwarded to tools in your data center.

Using taps to capture data delivers distinct advantages versus using high-cost SPAN ports:

- Resists hacking by not having assigned IP addresses
- Can be managed for easy, more holistic administration
- Captures 100% of packets to offer the only proven option for accessing data
- Works together with packet brokers to collect and direct packets to monitoring tools
- Handles encrypted data for added security while transiting to on-premises packet brokers

The Need for Packet Data

Less than half of companies rely on native traffic mirroring included with public cloud services to achieve visibility, and for good reason. Services hosted by cloud providers may be free, but of little use if they deliver limited insight, irreconcilable data, and fail to scale across hybrid or multi-cloud environments.

Along with log and flow data from providers that proves useful in analyzing trends, your IT and security experts need full packet data to spot hidden threats and performance problems. Packet-level visibility must extend to public clouds to collect reliable data (packets don't lie!) that can be filtered to provide actionable detail.

How To Process Monitoring Data: Send the Right Data to the Right Tool Every Time

Monitoring data must then be funneled to physical and virtual network packet brokers (NPBs) for processing to optimize performance and security monitoring. Here, physical and virtual packet brokers (NPBs and VPBs) feed specialized monitoring tools such as network and application performance monitoring (NPM and APM) solutions, Wireshark, next-gen firewalls, and intrusion detection systems (IDS) the right data at the right time.

Pre-processing by intelligent packet brokers plays a critical role in speeding incident resolution, shrinking your digital attack surface, and keeping projects on time and on budget.

Keysight's Vision ONE NPBs and CloudLens VPBs perform many advanced functions like:

- Aggregate packets from multiple sources
- Remove duplicates and unnecessary header information
- Perform SSL/TLS decryption to reveal hidden threats
- Filter and send packets to tools based on OSI Layer filtering
- Load balance traffic to optimize monitoring tool utilization
- Perform data decryption and re-encryption as needed to allow for the analysis and protection of monitoring data

The net result? As shown in Figure 1, each and every analysis tool sees all — and only — the data it needs at all times. Keysight packet brokers work across all provider environments so your teams can work efficiently without having to purchase, learn, and operate redundant tools that collect disparate information.

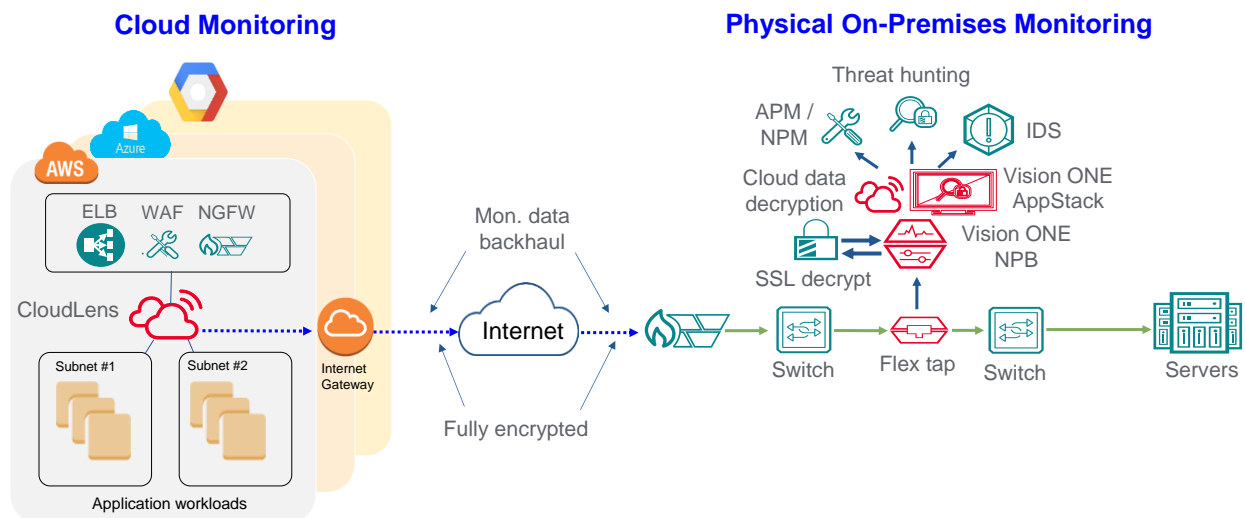


Figure 1. Hybrid cloud visibility delivers the right data to the right monitoring tools across your clouds and data centers.

Visibility-as-a-Service for Virtual Environments

CloudLens, Keysight's virtual visibility platform, gives IT granular access to traffic in any cloud environment. CloudLens visibility-as-a-service extends packet-level visibility to public cloud environments to complement incomplete log and flow data from providers.

Virtual sensors installed within workloads capture rich metadata and insight into where services are running, how well they're performing, and whether resources are fully cost-optimized. Data gets sent to physical or virtual packet brokers on an application-by-application basis for optimal bandwidth and cloud resource utilization. CloudLens deployments scale automatically and dynamically as instances are created or taken down, so you continually save time and money.

Deploy all the right tools in all the right places

CloudLens lets IT maximize the value of monitoring and analysis tools located in the cloud and running in physical data centers. Pre-processing traffic in the cloud reduces the volume of data transported to on-prem monitoring systems for inspection. With less to handle, your APM, NPM, NGFW, IDS and other systems work more efficiently, last longer, and achieve greater ROI.

Keysight's hybrid visibility architecture lets you choose the best place to monitor and analyze data — on prem or in the cloud — on an application-by-application basis. Flexibility to combine solutions optimizes total cost of ownership (TCO) at every turn by:

- Analyzing traffic on-prem aids in rationalizing and extending the value of security and monitoring tools located in your data centers
- Conducting analysis in the cloud conserves bandwidth and avoids costs associated with backhauling unnecessary traffic to data centers

As an example, virtual taps and packet brokers can capture and filter data in the cloud to remove duplicates, unnecessary headers, and other unwanted information. The smaller subset of data gets sent to your physical on-premises tools so that you can reduce backhauling costs without buying virtualized versions of tools you already own. The back-hauled data can be encrypted by CloudLens in the VPC and then decrypted at the NPB in the on-premises environment to protect your data.

Active Monitoring for Proactive Management Throughout the Hybrid Cloud Life Cycle

You should consider including active monitoring in your hybrid cloud visibility architecture to avoid unwelcome surprises as you migrate to and manage public cloud instances. The real-time insight provides an instant status of what's happening on the network so you can optimize rollouts, upgrades, and other ongoing changes as your network evolves.

Keysight's Hawkeye active monitoring solution lets you test cloud and on-premises performance at any time. Hawkeye uses software agents and probes deployed across a hybrid network infrastructure to collect monitoring data actively or passively.

Never stop monitoring

Proactive, ongoing assessment plays a vital role in demonstrating value to stakeholders and showing that goals for cloud migration have been met. Active monitoring lets your Network and DevOps teams:

- Create network and application performance baselines for on prem and cloud
- Proactively test performance and measure latency, throughput, and responsiveness on a per-hop basis
- Monitor and troubleshoot user experience with applications before, during, and following migration
- Validate cloud providers' conformance to SLAs to negotiate the best rates
- Isolate performance issues to the cloud or physical networks
- Optimize utilization of CPU, bandwidth, monitoring tools, and usage-based provider services

Hawkeye delivers customer experience data for a wide range of challenging applications like voice, video, web services, and critical enterprise applications. Using synthetic traffic to test performance enables administrators to synthesize "busy hour" conditions at any time. For example, engineers can simulate peak conditions during maintenance windows to assess real-world performance without impacting production traffic.

IT professionals use Hawkeye to test and ensure performance against:

- Large volumes of application traffic
- Limitless combinations of traffic types
- Mixes of protocols that could stress test the network

Figure 2 provides an example of a hybrid cloud network that has deployed the Hawkeye active monitoring solution to capture monitoring information across both the physical on-premises and multiple public cloud networks.

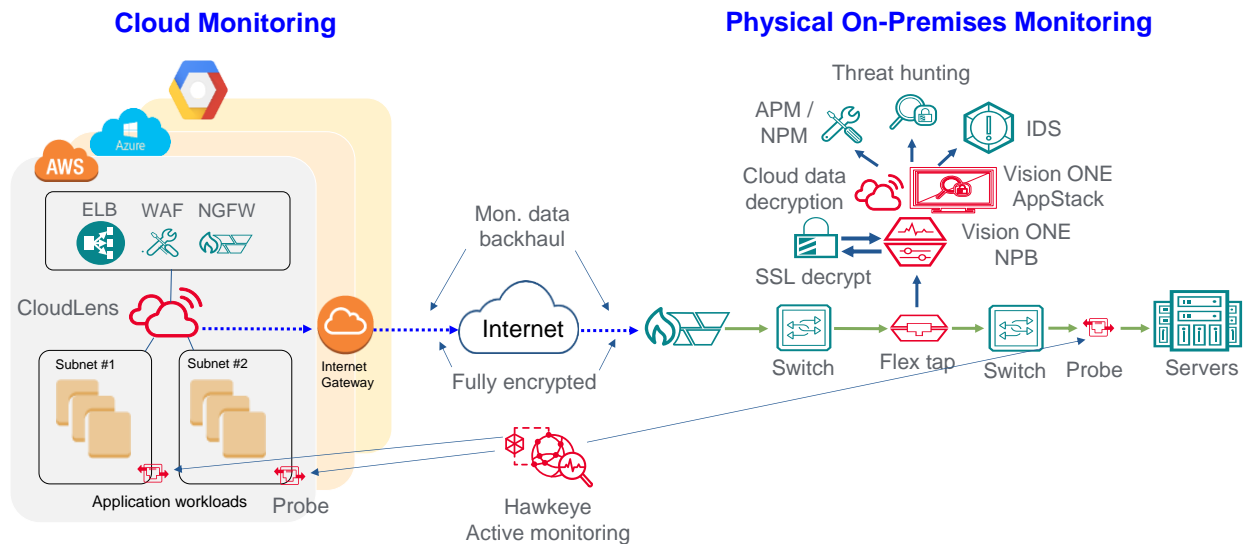


Figure 2. Active monitoring lets IT proactively test performance throughout migration of business services to the cloud, and as they troubleshoot users' experience with applications.

Conclusion

In today's highly digital workplace, a reliable, scalable visibility architecture is a must, not an option. Using a single purpose-built visibility architecture reconciles and homogenizes data to speed troubleshooting, incident resolution, and forensics efforts during and after migration.

Keysight solutions for hybrid visibility bridge the gap and leverage the best of public cloud and on-premises monitoring to improve your performance, security, and TCO at every turn. Unlike mirroring services from cloud providers, Keysight solutions operate smoothly across multiple vendor environments. Combine physical and virtual taps and packet brokers with active monitoring to ensure your teams see what they need to see — when and wherever it happens — so they can take the right action at the right time.

Reach out to Keysight Technologies and we can show you how to optimize your public cloud, physical on-premises, and hybrid cloud solutions to create one seamless solution.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.



This information is subject to change without notice. © Keysight Technologies, 2023, Published in USA, February 20, 2023, 3123-1079.EN