WHITE PAPER

# How to Create a Successful Visibility Architecture

## The Network Visibility Problem

The single most important activity an enterprise can do to protect itself from cybersecurity threats is to implement a visibility architecture. Shockingly, Enterprise Management Associates (EMA) found in a 2022 research report (Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise) that 66% of the companies surveyed failed in their attempts to implement a visibility architecture.

With the average cost of a security breach in 2022 exceeding $4M, failure is expensive. In addition to remediation costs, failure can impact profits through lost customers, cancelled cybersecurity insurance, and costly compliance fines. This can increase your total costs far beyond the $4 million average.

EMA attributed the 66% failure rate to the following issues:

- Lack of scalability
- Complex network architectures
- Poor data quality, through dropped packets or insufficient packet capture
- Inadequate staff training

But it doesn't have to be this way. The importance of visibility in the realm of physical security comes easy to most. Toddlers learn “Stranger Danger” defensive techniques before they can read. Five-year olds are told to keep their eyes open, to look both ways, and to watch for strangers bearing gifts.

The importance of visibility in the realm of digital security is no different, except that networks don't have eyes to see, and virtual strangers often masquerade as energy patterns transported through space. Security teams must add virtual sight to their networks. This is accomplished through what is referred to as a visibility architecture.

The following white paper provides an overview of a visibility architecture, a deeper dive into EMA's top four reasons for failure when implementing a visibility architecture, and the solution for implementing a successful visibility architecture.

## What is a Visibility Architecture?

The ultimate security challenge in the digital realm is how to protect yourself from danger that you can’t see. After all, hackers don’t knock at the door and wait. They breach, they hide, or worse, they masquerade in plain sight, pretending to be something they’re not.

Your analysis tools then must not only see packets inside the network, they must also recognize patterns of activity — good, bad, and unusual. But on-premises, cloud, hybrid, and multi-cloud networks are making visibility more difficult than ever. This is why you need a visibility architecture.

So, what is a visibility architecture?

### Three Layers to a Visibility Architecture

A visibility architecture consists of three fundamental sections:

- A data access layer
- A data control plane layer
- And a monitoring tool layer

Each layer consists of hardware and/or software dedicated to a specific set of functions. This is illustrated in Figure 1.

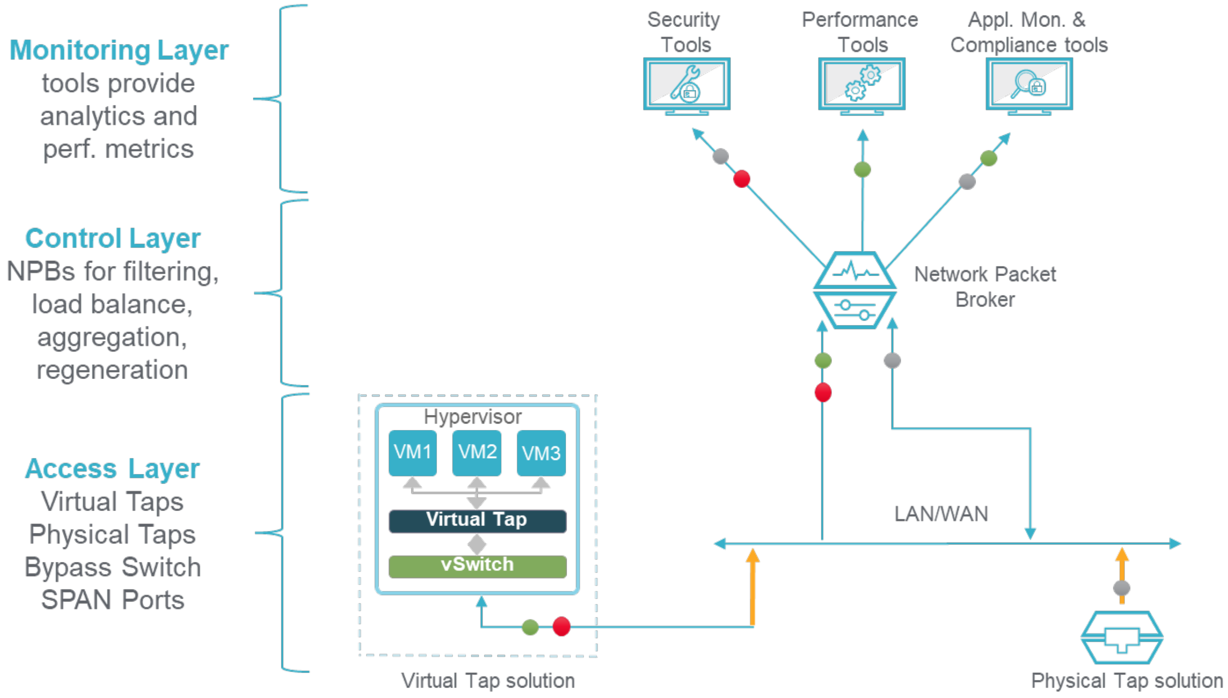

Figure 1: Three Layers of a Visibility Architecture

The first layer is the data access layer. This section splits off (or creates) copies of packets and then forwards them to the control plane layer. Within the access layer you will find taps, virtual taps (software taps for the cloud), SPAN ports, bypass switches, and aggregation taps.

Here are some important facts to consider about the access layer:

- Taps are dedicated devices that can't be hacked (because there is no IP address) and fail to wire (if power to the tap is lost, traffic continues to pass into the network)
- Taps can often be managed, making administration easier than SPANs
- Taps don't drop packets, making them the only viable solution to ensure your tools see 'all the packets'
- SPANs are often considered "free", but nothing in life is really free. SPANs must be programmed and reprogrammed as the network changes. And growing complexity increases the likelihood of not seeing all the packets

The control plane layer optimizes packets received from the access layer, and then forwards them to the tools within the monitor layer. Network packet brokers (NPB) are the main component of the control layer. The vendor and model of the packet broker chosen will have a significant impact on how well you can optimize your network data. For instance, packet brokers that support advanced features often yield the highest ROI.

Advanced packet broker features include the ability to:

- Aggregate packets from multiple sources
- Filter packets by OSI Layer and send packets to tools base on OSI Layer filtering
- Load balance packets sent to the analysis tools at the monitoring layer
- Regenerate traffic
- Remove duplicate packets
- Strip off unnecessary header information
- Perform SSL/TLS decryption
- Generate metadata using NetFlow

The monitoring layer is where threat analysis, network and application performance management, and network troubleshooting occur. In this layer you will see a vast array of specialized security analysis tools, like Security Information Monitoring (SIM), Security Event Monitoring (SEM), or a combination of both as in Security Information & Event Monitoring (SIEM).

Highly specialized in functionality, tools at the monitoring layer typically require skilled personnel to successfully operate. But even then, they're only as good as the data they receive from the network.

In the past, customers might have fed switch data directly into the monitoring layer, but this can introduce one of the four points of failure which will be discussed later.

## Two fundamental Visibility Architecture Use Cases -- Inline and Out of Band

There are two fundamental versions of a visibility architecture. A visibility architecture can be created directly in the path of live data (called Inline) or as a separate, overlay network (referred to as out of band).

Inline placement of your visibility architecture means it is directly in the path of real-time traffic. For instance, firewalls are inline, as they're typically located at the company's main network interface to the outside world and handle real-time live traffic. Figure 2 illustrates an inline visibility architecture.

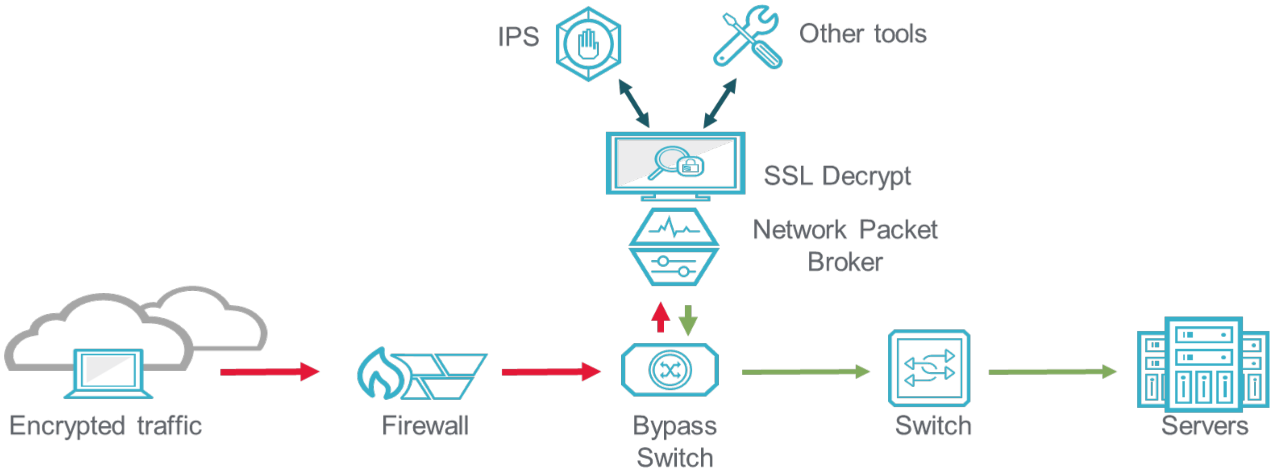

Figure 2: Inline Visibility Architecture Example

An inline visibility architecture is used for real-time data processing solutions to improve the efficiency of the:

- Security tools (like intrusion prevention systems (IPS) and web application firewalls (WAF)
- High availability options for your security architecture
- Data flow to security and monitoring tools

The inline architecture itself is accomplished by the following tasks:

- At the access layer, a special purpose device called a Bypass Switch is inserted to ensure network uptime. The bypass switch can detect problems in the both the network and equipment connected to it. If the bypass switch detects a problem (such as a planned or unplanned service outages), it reroutes traffic around the visibility architecture. Actions include routing data into the network to maintain business continuity or the halting of all traffic from entering the network to prevent infection by various types of malware.
- The packet broker then connects to the bypass switch and allows you to manipulate the data to maximize the efficiency of your security and monitoring architecture.
- Common use cases for an inline visibility architecture include:
  (1) High availability for mission critical deployments
  (2) Load balancing of data sent to inline tools
  (3) The serial chaining of data flows to multiple security tools
  (4) Centralized data decryption

The second type of visibility architecture is an out of band placement of your visibility architecture. This means that your security and monitoring tools are not fed by live, real-time data, but rather copies of network data produced by taps or SPAN ports. This is illustrated in Figure 3.

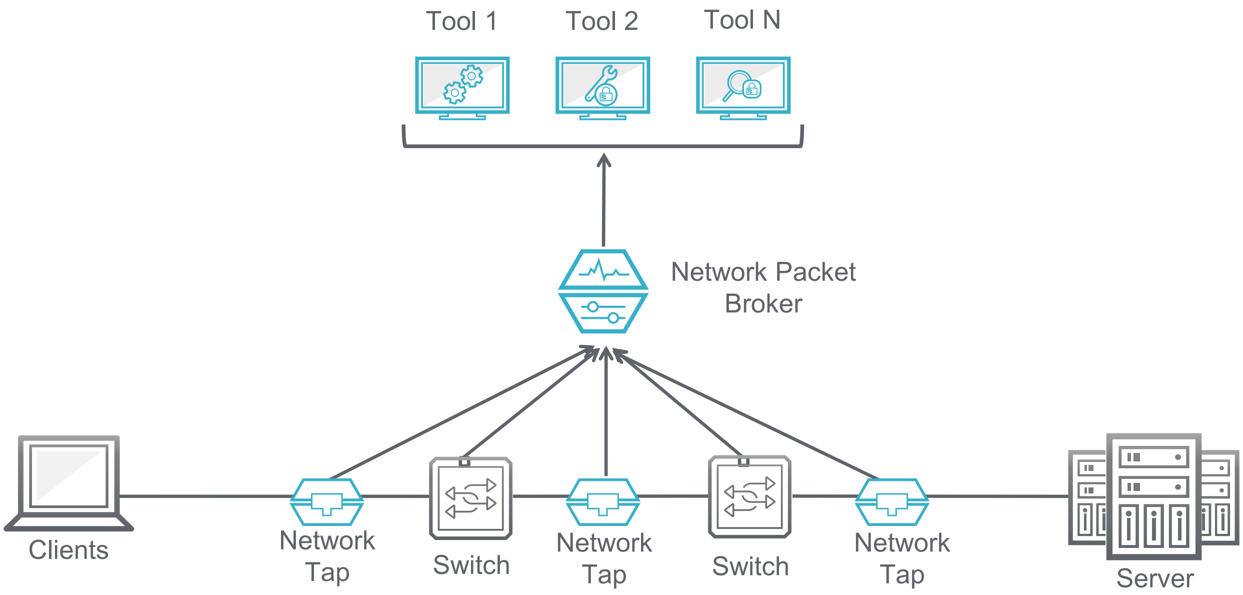

Figure 3: Out-of-band Visibility Architecture Example

The out of band architecture creates flexibility, as anything connected to a tap can be disconnected from the tap without impacting the network.

The out of band architecture itself is accomplished by the following tasks:

- Insert one or more taps into the network where you want to capture the type of data you are interested in. There will be a one-time network disturbance as each tap is inserted. After that, anything can be connected to the tap's monitoring port without affecting the live flow of traffic.
- In addition, or as an alternative, SPAN (mirroring) ports on a Layer 2 or 3 network switch can also be used to capture monitoring data. Unfortunately, SPAN ports have many inherent problems documented here that make them a poor choice for data collection. Adverse effects include missing data without any notification that the data was dropped and a low CPU service priority on the network switch.
- Common use cases for out of band visibility include the following:

  (1) Capture of relevant data for intrusion detection system (IDS) security screening and threat hunting

  (2) Capture of relevant data used to decrease Mean Time to Repair (MTTR) by up to 80% during troubleshooting activities

  (3) Capture of relevant data to optimize network and application performance

## Why Are so Many Visibility Architectures Unsuccessful?

Only 34% of companies surveyed in the 2022 EMA report on Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise believe they succeeded in building a successful network visibility architecture. Said another way, that's a 66% failure rate. The most obvious cost of failure is a security breach.

### Key Challenges of Visibility Architectures

Point solutions typically appear to be cost effective means to quickly resolve visibility problems. However, without the ability to grow and change along with the network, they quickly become ineffective. Some argue that partial visibility is not much better than zero visibility. As a result, scalability comes in as the #1 challenge.

As organizations move toward cloud and new on-premises solutions, such as network virtualization and cloud-native applications architectures, network and visibility complexity grow even more, making architectural complexity the number 2 challenge.

The EMA researchers also found that organizations struggled with two other challenges:

- Data quality issues, like blind spots, dropped packets, and inadequate visibility into east west traffic
- Skills gaps, poor leadership, and budget shortfalls.

Most would agree that these are not easy challenges to overcome. The next section will discuss how to avoid these common visibility architecture problems.

## How Do You Resolve Visibility Architecture Problems?

To effectively detect and isolate as many security threats as possible, you need an integrated visibility architecture. Data packets that traverse networks are the best source of truth about what is happening. Purchasing security tools is just the starting point. Taps and packet brokers can be used to capture all the packets and send them directly to your security and analysis tools. However, a better way is to insert a packet broker to refine and optimize the data being sent to those tools. This allows you to optimize tool performance and optimize the number of tools (and cost) that you will need.

According to the researchers at EMA, 78% of companies expect budgeting for visibility architecture projects to grow over the next two years, with 23% of companies expecting significant increases. The move to hybrid and multi-cloud networks are the biggest drivers, with 55% of companies expecting budget increases to support this move to more complex networks. Questions arise then, about how to create a successful visibility architecture.

For inline visibility architectures, well designed packet brokers feed network data to analysis tools for an extensive review of suspect packets before those packets are passed back to the packet broker for delivery to the next analysis tool that will also conduct an extensive analysis. Ultimately, all this analysis will reveal packets and patterns of bad actors that need to be quarantined or thoroughly investigated for the protection of the network.

For out of band architectures, well-designed packet brokers allow users to selectively screen packet data based on various criteria, like routing protocol, IP address, VLAN, or application type, and deliver those packets to the analysis tools for deep packet inspection.

## How to Overcome Scalability Issues

Deployment of a good packet broker will help eliminate scalability problems. Packet brokers ensure that every analysis tool sees exactly the data it needs to perform at the highest possible level. Depending upon your monitoring needs, it may be possible to remove up to 90% of the monitoring data quickly and efficiently to maximize monitoring tool efficiency and scale.

Some of the most relevant packet broker features include:

- Line rate processing – Packet processing is a resource intensive activity that can be outsourced to the packet broker. Packet brokers typically process packets via software running on the CPU, or hardware accelerated FPGA, that doesn't run on the CPU. Bake-off tests between FPGA and software, consistently show that FPGA processing is faster.
- Modular chassis with customizable bays – Scalability is all about the ability to customize your packet broker to handle network needs today, and seamlessly add functionality needed for tomorrow.
- The ability to downshift network speeds to the tools is another functionality of a packet broker, giving you the ability to increase network speed, while deferring associated costs of upgrading analysis tool speed.
- Powerful filtering – Since partial visibility leaves security holes where you can't see, you need to look for a zero-loss packet broker solution that can deliver 100% reliable data processing while performing load balancing, data filtration, deduplication, SSL/TLS decryption, and other processing-intensive functions.

## How to Overcome Architectural Complexity

There are four fundamental sources of complexity — the network, new equipment, monitoring tools used, and the network architectures. Network complexity grows when new links, new office locations, and mobile devices for remote workers are added. These can be set up with different VLANs, sub-nets, etc. to geographically segment them. There are also BYOD and Wi-Fi access issues to contend with, especially in a post-pandemic world.

A properly designed should include a visibility architecture with taps, bypass switches, and packet brokers. You should choose a packet broker that's easy to configure, but more importantly, is easy to modify as your network changes. You will want to evaluate your options carefully as everything can look easy to configure in a carefully scripted vendor demonstration.

Key relevant packet broker capabilities for this situation include:

- Ease of use – Configuring your packet broker to handle all your complex network needs has proven to be a serious challenge. With some packet broker models, configuration can be as simple as drag and drop that can be done by almost anyone, or as complicated as CLI or REGEX that requires a senior engineer to implement.
- Support for clouds environments – All physical packet brokers work on-premises, but not all of them can also support hybrid and multi-cloud environments.

## How to Overcome Data Quality Issues

A visibility architecture with blind spots is more than annoying. It can be dangerous if it impedes your ability to see hidden threats.

Blind spots arise for two main reasons:

- No available data
- Missing data

No available data is due to the lack of data capture for both physical and virtual environments. You are simply in the dark and have no idea what you could be missing. As many enterprises move operations from on-premises to the cloud, it is not uncommon to be missing key pieces of data from the virtual environment. Fortunately, a good visibility architecture can provide insight into your virtual network as well.

Missing data comes from the fact that either your intended data collection device (tap or SPAN port) or your packet broker choice (like a CPU-based packet broker instead of one that uses FPGA) dropped key data packets, often without alerting you. The missing data can lead to serious problems tools are searching for specific patterns. If a packet is dropped/missing, then a pattern might be missed, and a security attack could be successful. Note, while it not uncommon for SPAN ports to drop packets, a properly functioning tap should never do so.

Key relevant visibility capabilities for this situation include:

- Taps are dedicated devices that can't be hacked (no IP address), run at line rate (they don't slow down when traffic speeds up), and fail to wire (if power to the tap is lost, data still continues on into the network). For the most part, taps are "set and forget" technology.
- SPANs must be programmed and reprogrammed as the network changes.  Growing complexity increases the likelihood of not seeing "all the packets." Don't be fooled by an apparently free visibility solution offered by switch vendors. Nothing is free.
- Packet brokers that use FPGA-based acceleration are faster than CPU-based software solutions and are more likely to allow the packet broker to run at line rate.

- Zero-loss (no dropped packets) packet brokers can deliver 100% reliable data processing while performing load balancing, data filtration, deduplication, SSL decryption, and other processing-intensive functions.

For a deeper dive into these topics, see the following resources:

- The Importance of Lossless Visibility
- The Technical and Financial Impact of Ease of Use on Network Visibility Solutions
- Best Practices for Visibility Architecture Tap Planning
- Tolly Network Packet Broker Test Report

### How to Overcome Organizational Skills Gaps

Skills gaps are the difference between an employee's skills and the skills needed to effectively perform a particular job. While this can be a tricky problem, some packet brokers are easier to program than others and can help alleviate some of the skills gap problem.

Key relevant visibility capabilities for this situation include:

- A packet broker with a drag and drop or GUI based configurator, will significantly reduce the amount of training needed to setup and maintain a visibility architecture.
- A packet broker that allows you to create predefined filters (aka floating filters) which are created, saved, and reused as needed, can reduce troubleshooting time per occurrence, and reduce your MTTR.
- Unlike SPAN ports, taps are purpose-built devices that typically need no programming or ongoing programming updates as the network changes.

## Conclusion

The 2022 EMA Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise report found that the gold standard in network visibility is the use of packet brokers. Advanced features, such as packet filtering, manipulation, and metadata generation are the top characteristics of a network packet broker and return a higher ROI.

As with any IT solution, there will be challenges to adoption and implementation. Nonetheless, the benefits of reducing security risk far outweigh any potential disadvantages. Remediation involves more than just the cost of cleanup, and can impact profits through lost customers, cancelled cybersecurity insurance, and costly compliance fines.

Virtual visibility in your network is not optional. Failing to build a scalable visibility architecture to provide visibility for today and tomorrow, could ultimately result in limited visibility leaving you susceptible to security incidents.

The single most important activity an enterprise can do to protect itself from cybersecurity threats is to implement a visibility architecture — because breaches are inevitable. Use a visibility architecture to see virtual strangers in your midst before their breach leads to security incidents and a host of other nightmares.

Keysight Technologies offers a wide range of visibility solutions that can be used to augment any security and monitoring architecture. Examples include:

- Taps that include a vast array of interfaces including copper (10/100/1000 MB), optical (1/10/25/40/50/100/400 GE) and ruggedized to withstand industrial and harsh operating environments. Keysight also has a large portfolio of tap split ratios including 50/50, 60/40, 70/30, 80/20, and 90/10 splits.
- Vision series packet brokers that support zero packet loss for full featured, non-blocking monitoring up to 400GE. Keysight’s patented GUI interface is intuitive and easy to use which saves significant programming time and cost.
- Inline Vision series packet brokers that support internal high availability as well dynamic load balancing to create cyber resilience with security appliance survivability and self-healing architectures.
- SecureStack application provides integrated SSL/TLS decryption for the Vision series packet brokers. SecureStack exposes hidden security threats while offloading the inefficient and heavy decryption burden from your security tools.
- AppStack application provides high-value intelligence features for the Vision series packet broker that delivers empirical data to identify bandwidth usage by application type, flow data, geolocation, and various pieces of user data to look for indications of compromise.
- iBypass switches that increase your network reliability with superior fail-over and fail-back techniques.
- CloudLens which allows you to capture and filter packet data in public and private cloud networks.

Learn more at: www.getnetworkvisibility.com.