Geek-to-Guru Guide:

ELIMINATING NETWORK BLIND SPOTS

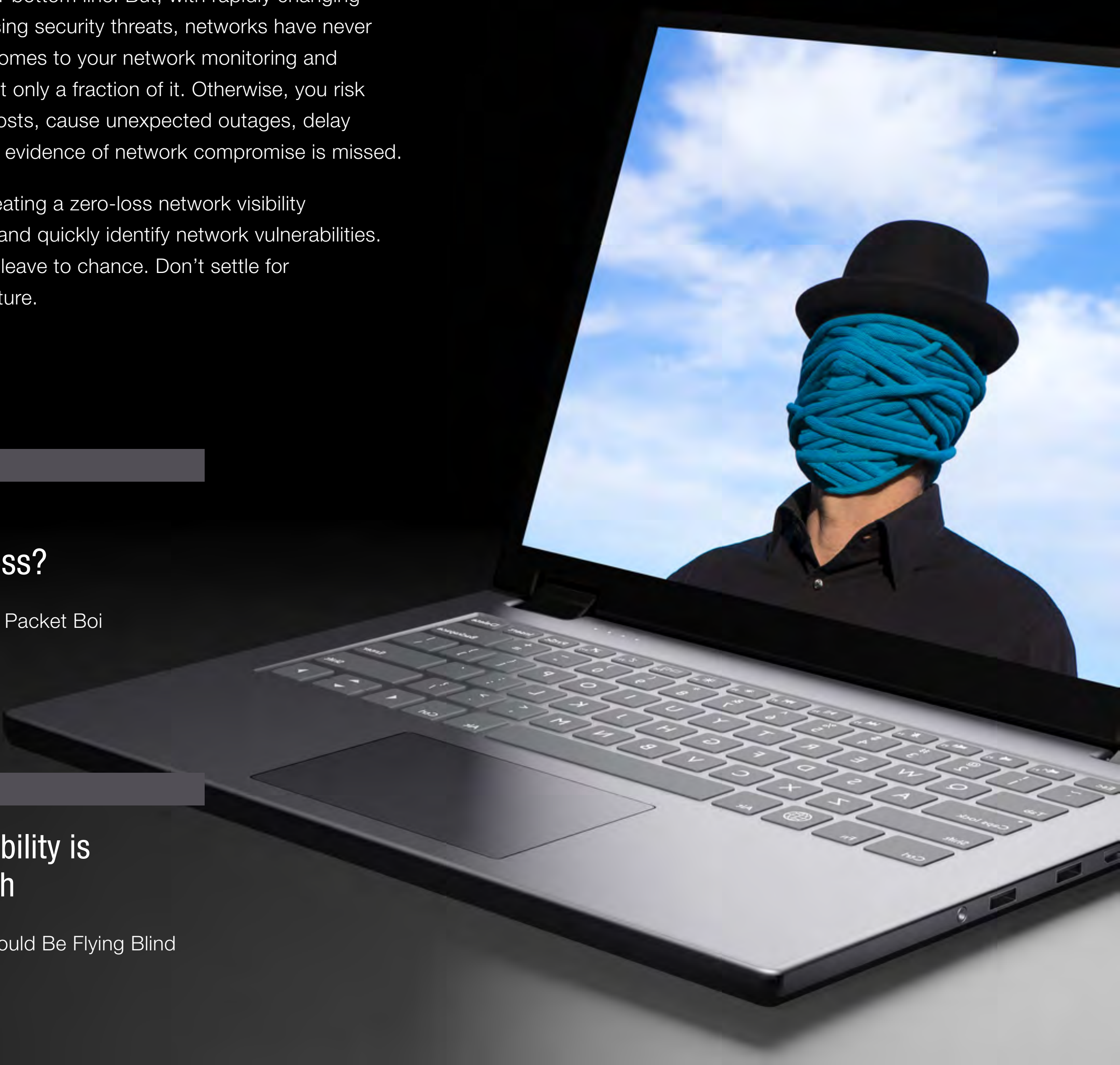
KEYSIGHT
TECHNOLOGIES

INTRODUCTION

Partial Visibility is Not Enough

Your network, applications, and data are critical to your bottom line. But, with rapidly changing technologies, an expanding network edge, and increasing security threats, networks have never been so challenging to manage and protect. When it comes to your network monitoring and security tools, you need to see the whole picture — not only a fraction of it. Otherwise, you risk potentially disastrous consequences that can run up costs, cause unexpected outages, delay network troubleshooting, and result in data breaches if evidence of network compromise is missed.

As you read through this guide, you'll discover how creating a zero-loss network visibility architecture will help you avoid dangerous blind spots and quickly identify network vulnerabilities. Your network, users, and security are too important to leave to chance. Don't settle for compromised visibility or anything less than the full picture.



CHAPTER 1

Leave No Packet Behind

The Dangers of Network Blind Spots

Your network tools are only as good as the data they see. When packets are dropped or lost entirely, having only partial visibility causes dangerous blind spots and network vulnerabilities.

CHAPTER 1

Leave No Packet Behind

The Dangers of Network Blind Spots

It's a brave new world for your network. New technologies, applications, and faster network speeds, along with more sophisticated cybercriminals, are transforming the way you do business. But they're also making your network more complex. The larger and more complex your network, the greater the chance your security and monitoring tools will miss critical information. Your tools are only as good as the data they see. Packets can be missing, corrupted or dropped entirely. Blind spots may lurk unseen. When your business depends on the integrity of your network, you can't afford to see anything less than the complete picture.

Network vulnerabilities can be hard to pinpoint and security breaches are increasingly more difficult to detect, which often creates dangerous blind spots. Blind spots directly correlate to network problems and outages, inefficient troubleshooting, and increased security risks.

A visible network is a secure network

You've got massive volumes of data and traffic flowing in and out, plus numerous applications to keep running. While that stream of traffic carries the lifeblood of your organization, it's also a potential vehicle for attacks and errors. How do you know if your network is performing as well as possible? Or if it's as secure as you think?

The best way to ensure the security and performance of your network is by monitoring the traffic entering and leaving the network. It is essential that your monitoring tools capture all the information you need without missing critical clues that could identify potential network breaches. Missing data is a big concern because so many breaches go undetected. In fact, encrypted data that protects at risk information on your network also helps hackers cover their tracks.

Cybercriminals know that many enterprises cannot effectively monitor and inspect all SSL traffic, especially at scale as traffic increases. They find your vulnerable blind spots and treat them as open doors. They exploit encrypted SSL data to sneak ransomware, malware, viruses, and trojans into your network, undetected by your security tools.

And what's even worse than missing data? Not knowing that it's missing. When it comes to your network, incomplete knowledge is definitely a dangerous thing. If your security and monitoring tools are overloaded and not as high performing as your network, they are likely missing critical data. Packets dropped before they even reach your tools results in network blind spots. It's like putting out a welcome mat for the bad actors looking to do you harm. The results are network outages, degraded performance, security breaches, loss of sensitive data—and unhappy customers.

To see it is to secure it

To secure your network and ensure that it's performing at its peak, you need a visibility architecture that's lossless, holistic, and capable of quickly and thoroughly inspecting the massive amounts of data crossing your network with zero packet loss. A well-designed visibility architecture gives you end-to-end visibility into traffic across all network links, including virtual and encrypted traffic—without dropping data packets or creating dangerous blind spots. Such a solution consists of network taps, bypass switches, and network packet brokers (NPBs) that intelligently filter and load balance data to get it to the right tools.

Total visibility, because "good enough" is not enough

Complete network visibility gives you critical insight into your entire network so you can see every packet, eliminate your blind spots, pinpoint performance drags, and more quickly identify network vulnerabilities and security risks.

Total end-to-end network visibility provides the following key advantages:

- improved network performance
- continuous network security
- efficient troubleshooting and faster mean time to repair (MTTR)

Intelligently process data with contextual awareness

NPBs and their accompanying software stacks are absolutely vital components of a network visibility architecture. Keysight's Vision Series NPBs process and deliver data based upon context. They automate the data inspection process and respond to network incidents by taking action in near real-time, dramatically boosting monitoring response times. Having the ability to simultaneously support multiple filters and functions on a single platform while running at line rate is a must for any NPB. This includes deduplication, load balancing, SSL decryption, data masking, packet trimming, header stripping, geo-location and tagging, among others.

By creating a resilient and scalable visibility architecture that spans every corner of your network, you'll expose your blind spots, experience better network performance, and minimize security risks. That's real peace of mind.

CHAPTER 2

What is Packet Loss?

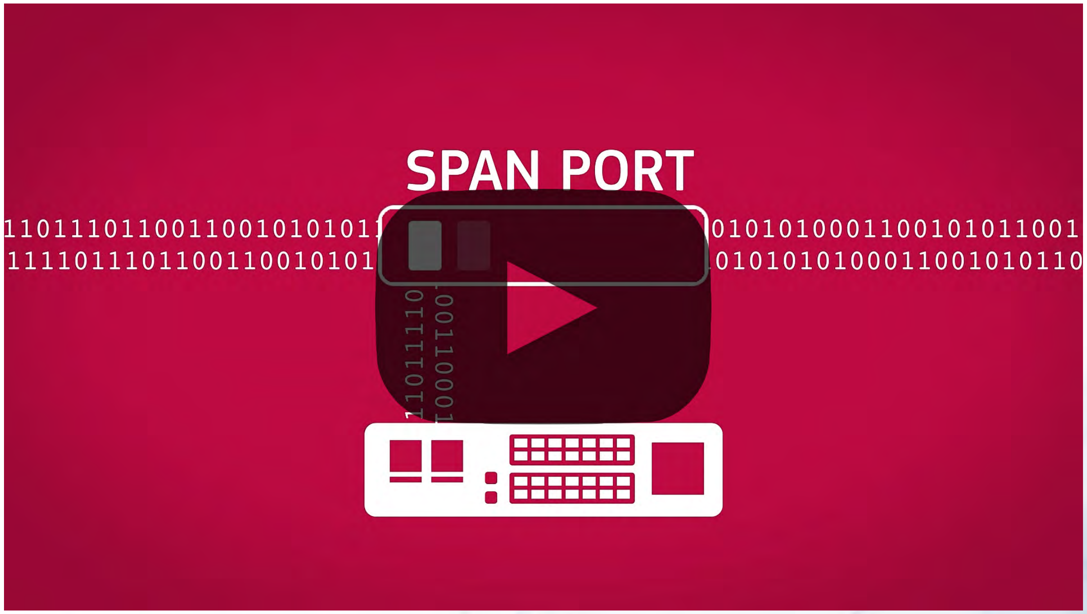
Tech Tips with Packet Boi

> A visibility architecture should eliminate blind spots, not create them. Understand the impact of packet loss from performance issues, data breaches, and even network outages.

CHAPTER 2

What is Packet Loss?

Tech Tips with Packet Boi



Source: https://youtu.be/uK9oBnA51no

CHAPTER 3

Take Five

Keysight’s President of Network Applications and Security Discusses Preventing Blind Spots for Improved Security and Performance

Mark Pierpoint, Keysight’s president of network applications and security, discusses the importance of a secure network visibility architecture and how blind spots impact enterprises beyond IT.

CHAPTER 3

Take Five

Keysight’s President of Network Applications and Security Discusses Preventing Blind Spots for Improved Security and Performance

With massive volumes of network data, a plethora of applications to maintain, and rapidly evolving technologies, networks are growing more complex. Cybercriminals are also constantly evolving their techniques to take advantage of network vulnerabilities. Seeing all network traffic is the best way to ensure high security and performance. Partial visibility is not good enough. Encrypted, missing, or corrupt data can lead to blind spots that open the door to performance issues and security risks. We sat down with Mark Pierpoint, Keysight’s president of network applications and security, to discuss why implementing a network visibility architecture is critical when it comes to uncovering and preventing dangerous blind spots that can wreak havoc on even well-established businesses.

Mark Pierpoint
President of Network
Applications and Security

1 How does having blind spots and network vulnerabilities impact a business beyond the network?

With digital transformation, it is very difficult to separate the network from the business itself because, almost by definition, everybody is using data in some form to improve their processes, performance, and customer satisfaction. Just four years ago, McKinsey published a study pointing to only 40% of businesses having embraced digital transformation. But today it is obviously much higher, especially as a result of the pandemic.

In more tech-based companies, you've got everything from mobile networks that form a significant business for providers like Verizon and others but also more operational technology (OT) networks that extend far beyond traditional IT. These could be to control a factory, the HVAC in an office building, or something very critical to the water or fuel supply. The world has really changed in the past 12 months and across all businesses, with more employees working from home and many more electronic engagements across partners, suppliers, and customers. So, I think it is clear that the network is very tightly linked with any business, and how this network operates directly impacts the business.

When blind spots and vulnerabilities cause a breach, it has a wide-ranging impact on customers, employees, and so on. Just last week it was a meatpacking plant that was breached, a few weeks before that, the Colonial Pipeline, and before that it was SolarWinds. We still don't know the full impact of the SolarWinds breach. Cognizant issued a press release in May 2020 about the breach they had experienced the previous month, saying they expected a $50 million to $70 million impact to their business in just that quarter.

But obviously, it's about more than dollars. On average, it takes 200 days to know you have a breach and find out exactly what happened and about another 80 days to remediate the impacts of that breach. Beyond that, there is brand reputation to consider and loss of customers. Lost customer data could potentially have an even bigger impact and take longer to resolve, so it's important to get a clear view into the network and understand your risks and vulnerabilities. It's why this is such a big issue for most company boards these days.

2 What does it mean to send the right data to the right tools at the right time, and how does this impact the bottom line and operational efficiency of a business?

This is no different than going to your doctor. It would be a terrible day if they took blood work and sent it to your radiologist, or maybe they took an X-ray or CT scan and sent it to your dermatologist. Sending the wrong information to the wrong place is obviously not a sensible thing to do. That may sound simplistic, but too often, network monitoring and security tools receive too much, too little, or not the right data, and it's costly not to address this.

When used properly, there are many effective tools these days, but they can be expensive. It's important to not just send the right data but to send the right rate of data so that tools are not overwhelmed. Say you've got a voice-over-IP tool. It would know nothing about video and would be absolutely useless if you were trying to get any video analytics out of it. At the heart of any effective visibility architecture is optimizing the number of tools you have, especially the more expensive ones. The right visibility solution has been shown to save more than 3x in terms of deployment costs. But you also need to make those tools more effective and getting the right data to the right places at the right time really helps accomplish this.

3 How do organizations benefit when IT has the insight to proactively resolve problems faster?

We typically talk about IT, but I've also mentioned OT, whether in smart buildings or something like manufacturing, utilities, or transportation. We've always considered IT as being separate from the business. But again, I don't think IT is simply a supportive activity these days, and it's inherently integral to driving the businesses forward in many cases.

If I consider our own business, not understanding who we've sold to, or where and when, would make a huge difference in how we put products together and go to market or solve problems in different ways. If a company can troubleshoot faster because they have a visibility architecture that provides insight into all network traffic, they can more quickly identify these issues. So, we're talking about a shift in mean time to repair (MTTR) from what is typically hours of response time down to only minutes. Ultimately this means a much better outcome for our customers and our customer's customers — the end users.

It's also important to realize that in a modern IT network, perhaps as much as 30% or more of the traffic in the network is "management" related — in other words, handling backups, dealing with configuration changes and copies of traffic being used to gain visibility. Implementing these systems optimally can help with overall network performance as well.

4 To expand on that, how do end users benefit when enterprises have a network visibility strategy?

End users are ultimately interested in continuously accessing the services or types of capabilities they're used to having, whether it be as simple as walking into a store and paying with a credit card to streaming a video and not seeing the picture break up. Fundamentally, the value of a well-architected visibility solution allows those services and capabilities to have an increased uptime.

So, yes, sure, we can reduce vulnerabilities. But ultimately, it's a bit like a burglar alarm in that it won't stop the most determined thief from getting in, but it will give you an early warning. It will allow you to deploy the right resources at the right time so you can respond rapidly and minimize the damage. I think of it like a thermal camera pointed at your house — you can see the hot spots, the cold spots, and so on. It makes sense to spend some money to address the hot spots, the lossy areas, knowing full well you can never stop heat loss 100%. It is about enabling businesses to make proactive decisions, deploy capital more effectively, and do all of that based on real data.

5 What do you think the biggest continuing network security threats will be, and how can a visibility architecture help companies stay ahead of new threats?

I would start out by saying that inevitably — and maybe this isn't a surprise to anybody — but the weakest link in any of the systems we have is always human. No matter how a breach occurs, most breaches require some information and an entry point to be enabled. We see that manifested through phishing and other scams that attempt to use social engineering to collect vital information. Ultimately, I think this will continue to be one of the biggest challenges in this cybersecurity world. Education and continual awareness are critical to addressing this and making progress.

Beyond that, I think we'll continue to see hackers targeting nontraditional areas. With SolarWinds, we saw the first major supply chain hack. We forecasted that type of vulnerability in one of our forward-thinking security threat reports published in 2019. I don't know whether that's a good thing or not. It's never good to be right about something bad. And I would anticipate that's going to continue impacting some nontraditional areas because, ultimately, ransomware and other attacks are designed to cripple businesses with a view to extracting money. As I mentioned before, just last week it was a meatpacking facility that was targeted. Today cybercrime exceeds $6 trillion a year, and its rate of growth is not slowing yet. The percentage of hackers that are caught and brought to justice remains a very small number. In terms of a crime, it's probably viewed as one of the lowest-risk ventures since nobody actually has to be physically present and may even be locally supported, so they tend to get away with it. If a company is not prepared, the remediation is very drastic and very costly in many ways.

One interesting program to note that I think points the way to the future is Cyber Catalyst by Marsh, a program that Keysight joined last year. It helps insurance providers who offer coverage against things like ransomware and other security breaches to evaluate network and security products that help to reduce risk for their clients. The program offers training materials and access to best practices. When companies follow these best practices or use specific certified products, they receive reduced insurance rates. This helps everyone become more aware of best practices that reduce the risk of breaches and how to promptly take remedial action if a breach should occur.

CHAPTER 4

Partial Visibility is Not Enough

5 Signs You Could Be Flying Blind

Complete network visibility is vital in identifying hidden threats. Discover five common causes of network blind spots and tips on how to eliminate them.

CHAPTER 4

Partial Visibility is Not Enough

5 Signs You Could Be Flying Blind

If you're an airline pilot flying at 500 miles an hour with hundreds of lives in your hands, you better see everything around you clearly. When it comes to keeping a critical enterprise network performing securely at its peak, visibility is just as important. The life of your business depends on it.

Network visibility goes beyond simple monitoring. A pilot without 20/20 vision has blind spots. Anything less than perfect 20/20 vision into all network traffic could create blind spots that jeopardize your entire business and its reputation. Security breaches are also becoming more challenging to detect. What's worse, these vulnerabilities frequently go undetected, creating network blind spots that impact application reliability, performance, and security. Blind spots lead to network problems and outages, increased security risks, and potential regulatory compliance issues. Partial network visibility is simply not good enough.

Network complexity also continues to grow with the proliferation of bring your own device (BYOD), globalization, virtualization, the IoT, cloud, software as a service (SaaS), and evolving wireless standards, including 5G. Meanwhile, companies are opening more offices and links as their employees connect to more and more mobile devices. Companies must extend their network edge — often into places where they cannot easily gain visibility.

End-to-end network visibility is vital in identifying hidden threats. If you want to avoid blind spots in today's fast-paced IT environment, there are a few key areas to watch.

Five Signs You're Flying Blind: Common causes of network blind spots and how to eliminate them.

1. Dropped or missing data packets

Businesses count on a secure, reliable network. They can't risk serious disruptions that impact security and network performance. Complete network visibility requires quick and easy access to all data traffic – not only some or even most data. Capturing the wrong data and dropping packets that contain critical data and user authentication information opens the door to costly cyberattacks.

Security issues, tool and network incompatibility, and bandwidth congestion can lead to corrupted data and packet loss. When packets are missing or dropped, troubleshooting inevitably slows down, another cost that most businesses can't afford. Let's take a closer look at some of these serious implications.

Network cyberattacks often alter databases and how they behave. In a distributed-denial-of-service (DDoS) attack, cybercriminals flood the network with too much traffic. This deluge of traffic often causes significant packet loss, degrades network performance, and in many cases, a total network outage.

Today, Secure Sockets Layer (SSL) attacks are more common than DDoS attacks. Organizations encrypt sensitive network data, such as credit card and Social Security numbers, to protect themselves and their users. The Transport Layer Security (TLS) 1.3 protocol brings enhanced security to help prevent security breaches and data leaks. However, it also makes it more challenging to gain visibility into all encrypted traffic.

Cybercriminals hide malware, ransomware, and viruses within encrypted data packets, sneaking them into networks on the tails of "safe" encrypted data much like a trojan horse. As most traffic becomes encrypted, IT needs to retain the benefits of TLS 1.3 while also inspecting all traffic for threats and malware to protect their networks and users.

By the time a security breach is discovered, it is often too late, and the damage is done. Many breaches go undetected for weeks or even months, so having full visibility of all data — both unencrypted and encrypted — is critical.

ProTip

Choose the right network packet broker

Many businesses rely on their security tools to perform decryption, but this can easily overload tools, especially in heavy traffic situations, requiring you to invest in more tools. One way to address this challenge is to centrally manage and offload TLS / SSL decryption so you decrypt once and optimize security and monitoring tool performance. It's important to choose a network packet broker (NPB) with the capability to perform SSL decryption. Keysight's SecureStack, an advanced NPB software module performs inline decryption without impacting other NPB features or capabilities. Keysight NPBs can deploy both inline and out-of-band (OOB) or simultaneous inline and OOB tool configurations using other capabilities of the NPB for ultimate flexibility. This solution allows you to see into both outbound and inbound traffic to inspect downloads and quickly detect server attacks.

2. SPAN port overload

Your choice of network monitoring equipment affects the complexity and effectiveness of your entire visibility strategy. Two primary ways of accessing and capturing network data are through a switched port analyzer (SPAN) port or a test access port (tap). SPAN ports, also called a mirroring port, take up a physical port on a network switch as an active device. SPAN ports create a copy of specific network data but have no filtering capabilities.

Although a SPAN port has a buffer, the buffer is not infinite, and SPAN ports cannot scale for high bandwidth requirements without dropping packets or causing network delays. When a SPAN port reaches capacity, it stops capturing data. When using SPAN ports to pass data to monitoring and security tools, be aware that they can easily get overloaded and drop data, opening the door to security threats and performance issues.

What's more, the SPAN port is a low priority resource. Since the data traveling through the network switch often exceeds what the SPAN port can support, when the switch CPU becomes overloaded, the switch drops monitoring data on the SPAN port. Because SPAN requires a dedicated port on the switch, you must re-configure the switch(s) every time you need to make a change.

ProTip

Choose network taps over SPAN ports

Security and monitoring tools are only as good as the data they receive. SPAN ports can drop important troubleshooting data, such as malformed, corrupt, or missing packets. The solution is to use network taps for data capture and an NPB to intelligently filter the data to prevent SPAN port overload and packet loss.

A tap is a purpose-built device that passively makes a copy of network data but does not alter the data. Network taps are installed between any two network devices to passively monitor all network data. These devices can include switches, routers, and firewalls. Taps are easily deployable anywhere across your network, without the need to disrupt live network traffic. Any monitoring device connected to a tap receives all inline traffic. The tap duplicates all traffic on the link and forwards it to the monitoring and security tools — without introducing delay or altering the content or structure of the data in any way.

Keysight's broad selection of network taps capture all network data providing the assurance you need for exposing and preventing blind spots.

The following are key differences between network taps and SPAN ports.

Network Taps	SPAN/Port Mirroring
Captures all network traffic including errors without corrupting or dropping packets.	When SPAN port reaches capacity, it stops capturing full data. It can also drop error packets or corrupt data.
No impact on network with bandwidth saturation. No dropped packets or network delay.	Cannot scale for high bandwidth requirements without dropping packets or causing network delays.
Simple to install. Plug and play technology with no hands-on management required.	Require engineering to configure switch. Not plug and play so it is a more costly and complex option.
Highly secure and cannot be hacked since taps are not addressable network devices	Vulnerable to security threats and attacks.
Does not require a dedicated switch port for monitoring which frees up a port for switching traffic.	SPAN requires a dedicated port on the switch.

Visit the Keysight Taps versus SPAN Port Monitoring resource page for more details

3. Underperforming security and monitoring tools

Most businesses use several network monitoring and security tools. As traffic volume and security threats continue to rise each year, so do the number of performance and security monitoring tools needed.

Unfortunately, as the number of tools increases, so does the operational complexity and cost of managing tools. The costs can quickly add up. Tools from different vendors run on different operating platforms with varying management interfaces.

Underperforming security and monitoring tools are often a sign of network blind spots. When blind spots are present, tools may not receive all the data they need, or specific tools may not get the right data. It cannot be stressed enough that the right data must be sent to the right tools at the right time to prevent overloading or underloading for optimized tool performance and security. You need to see all data packets flowing through your network, without blind spots.

Increased monitoring activity results in more alerts that require follow-up and investigation. This troubleshooting process is time-consuming and requires experienced technicians. Many alerts may even go unnoticed without any further action since alert fatigue is a common occurrence. If this happens, an enterprise may suffer through a breach or other completely preventable disruption that went unresolved primarily because of security tool overload.

When tools are not performing optimally, troubleshooting network issues is also more difficult. Mean time to repair (MTTR) increases when blind spots are present because tools are working overtime. Longer MTTR not only increases costs — time is money, but it also negatively impacts the user experience.

ProTip

Work smarter, not harder

A well-designed network visibility architecture enables you and your tools to work smarter, not harder.

If you collect the right data, zero in on issues more quickly, avoid duplicating data, and reduce the workload on your tools, monitoring is less costly and more accurate. You may not be able to avoid network complexity completely but working smarter will help you manage this complexity and keep blind spots under control.

Be systematic about how you process and filter data. When you deploy a high-performing, intelligent packet broker between your data collection devices and security and monitoring tools, you reduce the burden on your tools, avoiding unnecessary and costly upgrades as traffic increases.

Be careful about how you move data. Look for an NPB that allows you to control and customize the path data takes. Sending data only in a serial path increases latency and delays the resolution of issues or breaches. With a drag-and-drop graphical user interface like those used to manage Keysight NPBs, you have complete control over data movement and delivery.

Be selective when choosing an NPB. With the right visibility architecture, you can perform intelligent data filtering with contextual awareness. Keysight's AppStack software filters specific applications and send that traffic to specific tools for greater efficiency. AppStack provides a comprehensive view of which applications are running in your network, the bandwidth they are consuming, and where they are running geographically. For example, you can select Netflix and drill down even further to subclasses that identify various types of Netflix videos, such as animation or documentaries. Filter flexibility allows you to filter data combinations that are uniquely important to your business - by application, geography, or both, and by specific actions in the application, including region and email address. This process identifies a subset of traffic and sends it to your security tools via packet data or metadata. AppStack software generates enriched NetFlow metadata called IxFlow from your network traffic. IxFlow provides detailed data about applications, devices, known threats, and geolocation that security tools can then analyze in real time to identify potential security threats to the network.

Some network packet brokers cannot support running all features together — much less at full line rate. That's why it's critical to verify that the features you need will all work together without complex workarounds, like daisy-chaining multiple appliances. Keysight's Vision NPBs provide intelligent visibility and data filtering capabilities like deduplication, packet trimming, data masking, time stamping, SSL decryption, geolocation and tagging, and more. All of these features can operate simultaneously on one platform.

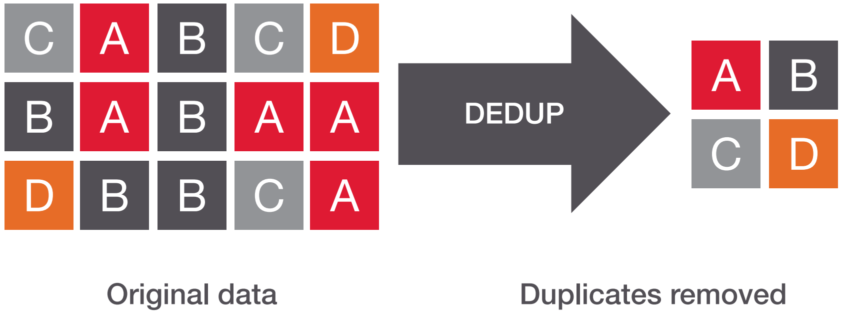


Figure 1. Example illustration of data deduplication

4. Network upgrades and tool incompatibility

As technology continues to advance at a breakneck pace, most businesses plan to upgrade to faster Ethernet and Wi-Fi in the near future. There is also a shift towards more high-bandwidth, low-latency networking technologies.

A network upgrade impacts more than your IT department. It also affects your employees and customers. Network upgrades are complex, so it's important to plan ahead, using industry best practices to design a visibility architecture that minimizes disruption, controls blind spots, and keeps the potential for security breaches and performance issues at bay.

There are many factors to consider when upgrading a network or adding new applications. Several factors also come into play regarding network upgrades and blind spots. Let's touch on the benefits of load balancing.

If you upgrade your network core from 40 Gbps to 100 Gbps, your tools need to operate and support these higher speeds. However, there may be few comparable security and monitoring tools available that support those data rates, and those that do are expensive.

Network packet brokers provide aggregation and load balancing that break down incoming segmented data into lower-rate data streams and send it to the proper monitoring tools. For example, load balancing of 40 Gbps data enables you to spread the monitoring traffic across multiple 10 Gbps tools. Centralizing and pooling your tools extends their life until you have the budget and resources to buy additional tools that support higher data rates. Some NPBs also offer context aware load balancing. As an example, data sent from VIP subscribers or specific accounts or social security numbers can be sent to specific tools at certain times or based on other parameters.

ProTip

Simplify your upgrades with taps and NPBs

When you upgrade your network or add new equipment and applications, it's critical not to overlook your visibility architecture. The stakes are simply too high for you not to have full end-to-end visibility into all traffic, data, and applications running across your network.

Network taps connect to a network link anytime, and you can connect a monitoring tool after deploying a network tap without disrupting network operation.

NPBs like Keysight's Vision X performs load-balancing to extend the life of your tools which optimizes tool performance and security after a network upgrade. Figure 2 is a simple example of NPB load balancing.

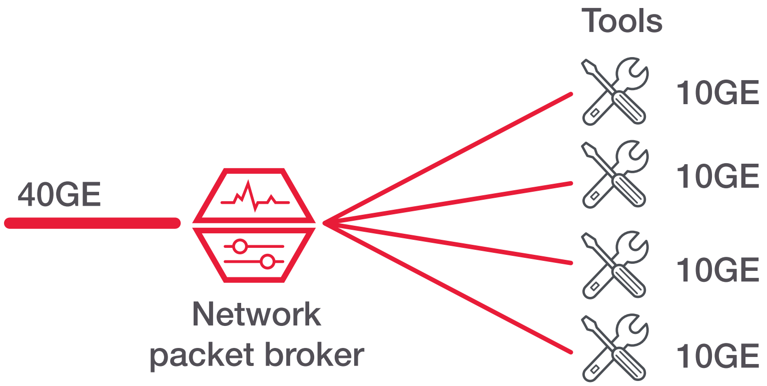


Figure 1. Example illustration of data deduplication

5. Increased adoption of cloud-based technology and virtualization

Most organizations use cloud networks in some way, shape, or form. While the cloud offers unparalleled flexibility, agility, and scale, it is not without its challenges. The cloud delivers many new innovations, but network and security teams continue to struggle to keep up with the constant changes in cloud technology. Some of their biggest challenges involve network visibility.

Monitoring east-west traffic with traditional monitoring components is complex, if not impossible, leaving you open to dangerous blind spots that can be catastrophic. As network perimeters vanish and attackers grow in sophistication, a lack of cloud visibility hampers your ability to monitor network security, compliance, and performance. It can also leave you exposed to data breaches and other costly security vulnerabilities.

As you design your network visibility architecture, consider a hybrid or cloud-based visibility solution to capture monitored data for distribution to both physical and virtual tools. Choose a vendor with a broad portfolio of products that support traditional enterprise networks, multisite campus networks, virtualized, and cloud environments.

ProTip

Select a robust cloud-based visibility platform

Look for a cloud-based visibility platform that monitors and protects network data on public, private, and hybrid clouds. A robust cloud-based visibility platform will deliver wide-ranging, actionable intelligence to the right tools at the right time. Keysight CloudLens, for instance, gives you complete security with platform-agnostic architecture and containers / Kubernetes compatibility. The solution also provides turnkey integration with leading security application performance management (APM) and network performance monitoring tools.

Visibility without compromise

You’ve got massive volumes of data and traffic flowing in and out, plus numerous applications to keep running. As networks increase in complexity, you may contend with SPAN port overload, inconsistent data collection and monitoring policies, new equipment, security issues, a growing remote workforce, and many other factors. The number of blind spots can begin to multiply if you’re not careful. A lossless network visibility architecture will help ensure that blind spots don’t wreak total havoc on your network.

This visibility architecture includes network taps that access network data where and when you need it. Packet brokers intelligently filter and aggregate data while both bypass switches and NPBs help increase network reliability, security, and uptime.

Having a complete picture of your entire network means you won’t be flying blind. A Keysight visibility architecture enables you to see every packet, eliminate blind spots, send the right data to the right tools, and pinpoint performance drags so you can identify and address vulnerabilities. Because, after all, a visible network is a secured network.

KEYSIGHT
TECHNOLOGIES

Information is subject to change without notice. | 7121-1100.EN © Keysight Technologies, 2020 - 2021 | Published in USA, June 30, 2021 | keysight.com