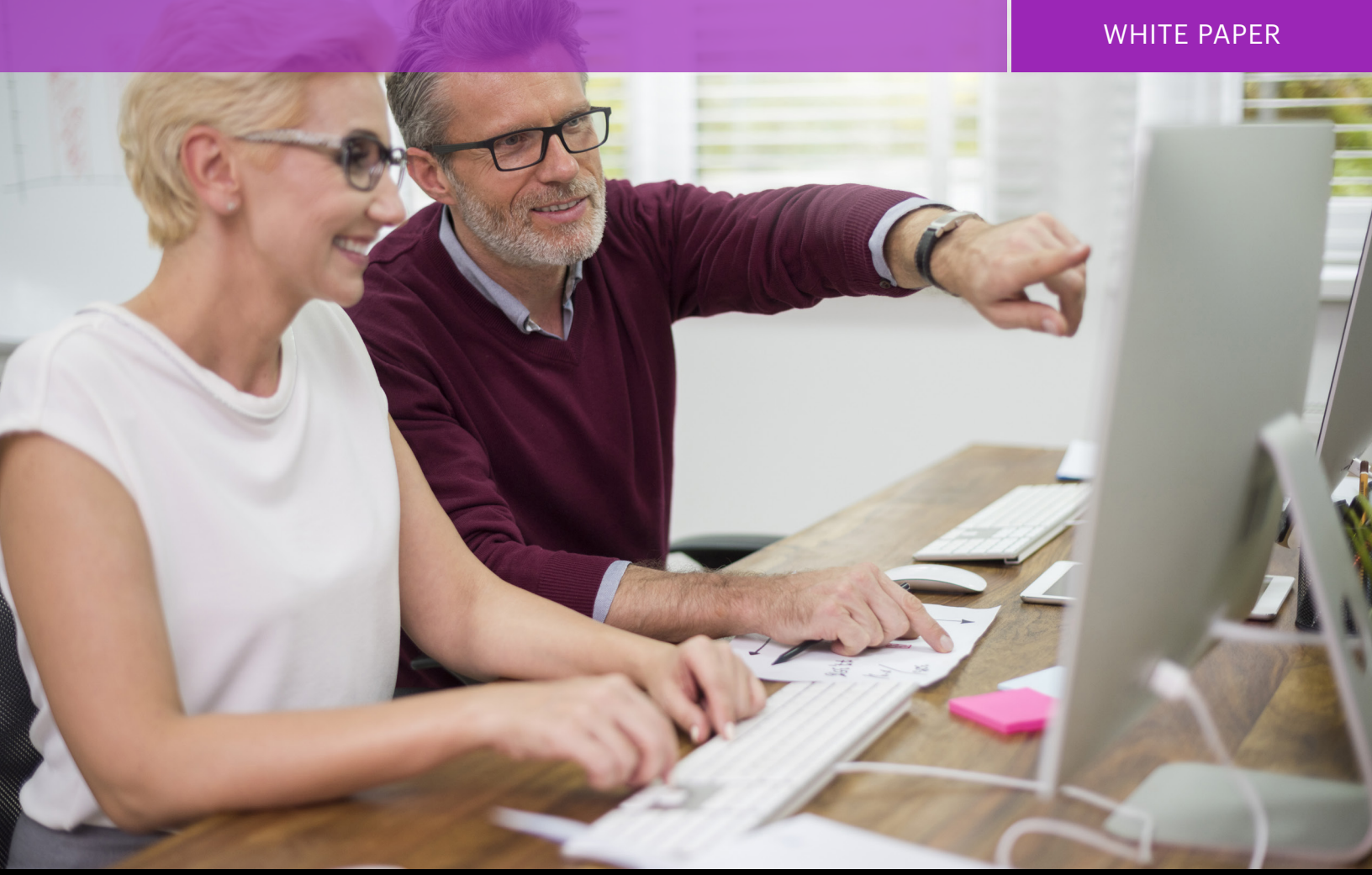
WHITE PAPER



5 Ways To Maximize the Value of Security and Monitoring Tools

KEYSIGHT

Deriving More Value from Your Tool Investments

Return on investment (ROI) is an important factor for new technology purchase decisions. However, having invested in many security and monitoring tools, what is the best way to maximize the value of your tools? Cost avoidance for new tool purchases is one way for IT to maximize this ROI and make your security and monitoring solutions stronger.

One way is to use the tool beyond its useful life. Another option is to place strict limits on tool usage and access which creates its own set of inefficiencies. A third option is to implement a visibility architecture to optimize data flows across your monitoring tools. This last option allows you to realize efficiency and performance benefits from architectural changes and incremental purchases. It can dramatically increase the usable life, and by association the ROI, of your monitoring and security tool(s).

It is important to understand the difference between cost elimination and cost avoidance though. Cost elimination means you decide not to make a purchase. This has an obvious financial benefit — no budgetary costs. However, technology is rapidly changing and a usable life of 3 years or less for equipment is the norm. So, cost elimination can save you money up front but could end up costing your business 3 to 4 times more in the long run due to costly network downtime, opportunity cost for using expensive level 3 engineers to fight fires, longer mean times to repair, inefficient processes, QoS and QoE issues for customers, and increased costs for mega breaches. Cost avoidance is different and focuses on the delay of large purchases, but not the elimination. Essentially it is about extending the life of your existing equipment — often with the addition of smaller equipment purchases that can extend those lifecycles.

For instance, you could spend $200K per tool for 6 monitoring or security tools for a total of $1.2M. Alternately, you could buy an equivalent capacity in 3 monitoring tools along with a $50K network packet broker to load balance across them for a total of $650K. In this case, using a network packet broker to load balance saves you $550K. Better still, if any of your 3 tools are pre-existing, then the packet broker allows you to continue using your existing tools for a longer period of time.

> Spending $50k on a network packet broker saves you $550k in CapEx. If you spend $200k on a security or monitoring tool, you want to get as much value as you can from it.

Monitoring Tool Challenges

Modern enterprise networks typically have four sets of common problems when it comes to getting the most value out of their monitoring tools. These include:

- Getting only the right data to each monitoring tool
- Managing the cost of monitoring tools
- Ensuring monitoring tool capabilities match network technology changes
- Maintaining optimum network security

Getting the right data to the right tool is a challenge because different tools need different types of data. Some need packet data while others need NetFlow data. In addition, some enterprises still use SPAN ports to feed data to the tools. As the network grows, SPAN port shortages often occur, resulting in tools that sit unused. Another issue is that if taps are used to directly feed monitoring tools, signal degradation issues can occur when too many taps are used between regenerators.

Virtual data centers pose another significant hurdle because up to 80% of the virtual traffic is east-west traffic. East-west traffic never reaches the top of the rack where it can be captured by physical tap and SPAN ports meaning that all that traffic sits in a network blind spot. This could lead to security and regulatory compliance issues that can be readily resolved by adding virtual tap to your physical tap architecture.

Controlling tool costs is another common issue as monitoring tools can become expensive. This is especially true if there are many links (both physical and virtual) where you need to collect data and insert tools. Some engineers dedicate specific tools to specific links which increases the number of tools required. Before too long, you have under-utilized (i.e. unnecessary) tools due to your architecture design.

Increases in network traffic is another very common issue for monitoring tools. For instance, if you upgrade your network core from 1 GE to 10GE, you will now need 10GE tools to properly monitor it. If you upgrade to 40 GE or 100GE, there may be few to no monitoring tools available at those data rates. Available tools at those data rates are very expensive.

In addition, every time network technologies change, interoperability with the tools needs to be reanalyzed and modified. For instance, if you implement encryption, VLAN tagging, firewall and IPS capabilities, you need programmatic changes for data filtering to the tools. New, special purpose, tools may also be required.

Maintaining optimum monitoring for network security is also a challenge. As an example, you might want to improve your security defenses by implementing high availability for your security tools, ensuring smooth failover in case of a tool outage. You may also need to analyze the same data with different tools. The serial chaining of this data can often be fairly difficult without the right data parsing architecture. Serial data chaining is where different tools are required to sequentially analyze suspicious/malicious traffic. Data masking is another common regulatory compliance requirement for sensitive and personally identifiable data such as credit card information and social security numbers. These data masking capabilities need to be applied before the data reaches the monitoring tool to maintain regulatory compliance.

A visibility architecture helps you maximize your monitoring capabilities.

What is the Solution?

The most cost effective solution to these issues is to include a visibility architecture in your network design. It helps maximize monitoring effectiveness by ensuring proper access to the data you need, when you need it.

A well-designed visibility architecture can do the following:

- Increase monitoring tool utilization and useful life
  - by removing unnecessary traffic to the monitoring tools
  - by pooling your monitoring tools instead of dedicating them to specific network links
- Increase monitoring tool efficiency
  - by offloading non-core functions to network packet brokers
- Increase monitoring utilization
  - by integrating virtual and physical data center monitoring strategies
- Increase monitoring effectiveness
  - by leveraging features such as high availability

All of these features help maximize the value of your existing monitoring tools. Common components of a visibility architecture include taps, packet brokers, application intelligence, and the monitoring tools themselves. Figure 1 shows one example of a visibility architecture implementation.

Gaining all of these benefits is not complicated or expensive. It involves adding two specific pieces of technology:

- Taps at key data access locations, and a
- Network packet broker

Increase monitoring tool utilization and useful life by removing unnecessary traffic.

There are different types of taps and network access (out-of-band tap, inline bypass switch, and virtual tap) that have different use cases. Out-of-band taps are the most common. These taps make a complete copy of the data (both good and bad packets) that passes the network at that point. The data is then sent on to the other components in the visibility architecture for processing. This type of tap can be used to replace SPAN ports with many benefits. For instance, taps are a "set and forget" type of device. So there is no programming required, which means no reprogramming are necessary for most network changes. The price points for taps are very cost effective circa $600 per port, which means they can be installed widely across the network — especially in places where SPAN ports are not available.

Inline security tool network access is accomplished by using bypass switches instead of a standard tap. In this case, a copy of the data is not made. The original data is actually diverted to an inline tool, analyzed by the tool, and then returned to the network to continue on to its destination if it is safe. The bypass switch has integrated fail-over and heartbeat messaging to the devices connected to it. This allows it to be used for high survivability and high availability solutions.

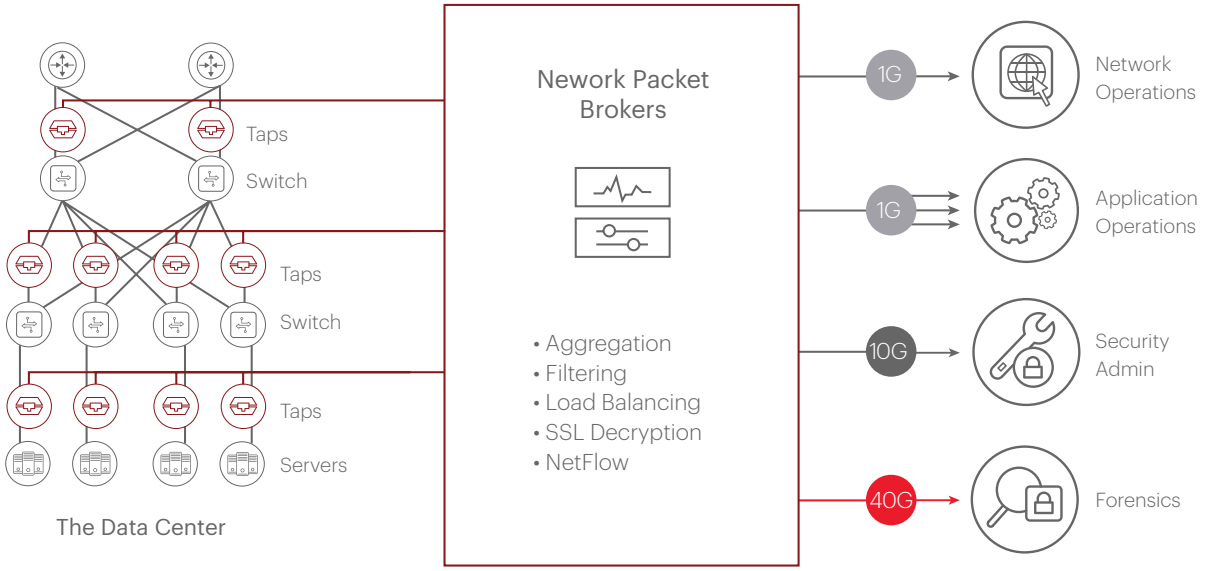


Figure 1. Visibility architecture example.

A typical rule of thumb is that the tool can become up to 60% more efficient once these functions are offloaded to an out-of-band packet broker.

A virtual tap is similar to the out-of-band tap except that it is software which is deployed in virtual environments, like VMware and KVM. The virtual tap can see all of the inter- and intra-VM traffic and forward that data out of the virtual data center.

The taps and bypass switches that are installed in your visibility architecture will send the monitoring data to a central collection point, called a network packet broker, for aggregation, out-of-band filtering, load balancing, and packet manipulation. Since the data coming in from the tap is a complete copy of all data, some of it will need to be filtered before being sent on to the appropriate monitoring tool. Other functions, such as deduplication, packet slicing, time stamping, data masking, etc., can be applied to the data as required to groom it. These features make the monitoring tools more efficient which means they can process more data than without the packet broker. A typical rule of thumb is that the tool can become up to 60% more efficient once these functions are offloaded to an out-of-band packet broker.

In addition, packet brokers provide aggregation and load balancing of information to the proper monitoring tools. This also makes the tools more efficient and can save you money in the short term. For instance, load balancing allows you to spread the monitoring traffic across multiple tools if you need to. One use case for this is to take faster 10 GE traffic and spread that traffic across multiple 1 GE tools, assuming you have enough 1 GE tools for the load. This allows you to extend the life of your 1 GE tools a little longer until you have enough budget to purchase more expensive tools that can handle the higher data rates. Another use case is to use a packet broker to remove low threat data (like Netflix, Hulu, and YouTube) from inspection by out-of-band tools, like an IDS. The packet broker simply routes this type of data back to the bypass switch so it can continue on into the network. Removing this unnecessary data for inspection can save up to 35% of the workload for an IDS. This allows those tools to be more efficient and can save you investment.

Application intelligence services provide an additional level of data monitoring and processing. Examples include filtering at the application level, the generation of NetFlow data, generation of geo-location of users and devices, and the capture of browser information. These features let you to extend the life of your existing monitoring tools by allowing them to focus on their core capabilities (i.e. not spend CPU cycles on decryption) and to receive the information in the form (data packets or NetFlow) that works best for the tool.

A good visibility architecture makes your applications and security stronger.

Conclusion

A properly constructed visibility architecture saves money in both the short and long run. Engage all the processing capacity of your tools and enable them to work for you longer. A good visibility architecture makes your applications and security stronger. It also provides all of the following benefits:

- Reduce tool costs by aggregating data streams and sending them to the appropriate tools
- Use network packet brokers to load balance higher data rate traffic across lower data rate tools to delay tool upgrade costs in a network upgrade
- Match the amount of tools to the amount of traffic to control costs
- Use network packet brokers to accommodate higher data rate traffic with lower data rate tools if high speed tools are unavailable or cost prohibitive
- Reduce your tool (and SPAN) port programming/reprogramming costs and effort simply by inserting taps and using the network packet broker GUI
- Increase the efficiency of your out-of-band tools up to 60% by using NPB filtering, deduplication, and packet grooming
- Make high availability for inline tools possible

Learn how you can easily start eliminating visibility and security blind spots and extend the life of your monitoring tools with Keysight's visibility solutions and visibility architecture at https://www.keysight.com/us/en/cmp/2020/network-visibility-network-test.html.