WHITE PAPER

Reduce Cost and Risk by Deploying Easy to Use Monitoring Solutions

The Benefit Of Ease Of Use

When trying to reduce the total cost of ownership (TCO) and the security risk associated with a network monitoring solution for government IP networks, there are two fundamental components that need to be thoroughly investigated.

The first component is to optimize agency processes. For instance, there are newer technologies, like network packet brokers, that IT teams can take advantage of. The second component is to make you sure choose the easiest to use monitoring solution available. While you need better data, you also need a system that is easy to install, easy to program, and easy to maintain.

There is a distinct need to control mission critical operations for government agencies. At the same time, you don't want to sabotage yourself with a solution that may appear to be low-cost initially, but be very expensive long-term. Simple choices, like using a graphical user interface (GUI), can cut your long-term operating costs by 75% or more. This is because a GUI creates higher productivity, while facilitating a lower cognitive load.

Simple choices, like using a graphical user interface (GUI), can reduce your long-term operating costs by 75% or more. This is because a GUI creates higher productivity, while facilitating a lower cognitive load

KEYSIGHT TECHNOLOGIES

Here are four actions to consider for increasing efficiency, reducing costs, and delaying the component obsolescence of critical infrastructure components:

- Update your processes to take advantage of the best data collection technologies
- Optimize the ease of use of your monitoring solution
- Understand the impacts and risk of a command line interface (CLI) based system choice
- Make sure your ease of use analysis includes all costs

Simply put, better monitoring data reduces your troubleshooting and forensic analysis costs, as well as the cost due to missed security threats.

Update Data Monitoring Processes

While government IT teams are under ever-increasing pressure to improve various responsibilities like: the performance and security of IT networks, monitoring for security, compliance mandates, and application and network performance, these initiatives require access to an increasingly large amount of network data. For security and monitoring solutions to perform optimally, they need full visibility into the network or there will be ramifications, such as extended analysis times, more false positives, inaccurate conclusions, and longer mean times to repair (MTTR). Simply put, better monitoring data reduces your troubleshooting and forensic analysis costs, as well as the cost due to missed security threats.

When it comes to data monitoring, ensuring proper access to network data is the most critical thing you can do. After that, data filtering and the conversion of data into actionable information can take place.

To accomplish these goals, there are two fundamental components required:

- Installation of test access ports (taps) to access the requisite network data
- Addition of a network packet broker (NPB) to filter and distribute that data to purpose-built devices for analysis

Proper visibility starts with proper data access. The first and easiest task is to install taps. Taps are passive devices that are typically “set and forget” devices. Once deployed, you never have to touch them again. This one step gets you better data to reduce your troubleshooting and forensic analysis costs.

Taps are an alternative to the use of switched port analyzer (SPAN) ports, which are now an outdated process, mainly because SPAN ports do not provide a complete copy of all network data and taps are so versatile that they can be deployed anywhere in the network. SPAN ports also have much higher long-term programming costs than taps.

In addition, you will want to add an NPB to optimize your filtering methodology. Powerful NPB features include: packet filtering, load balancing, packet deduplication, packet trimming and multiprotocol label switching stripping (MPLS).

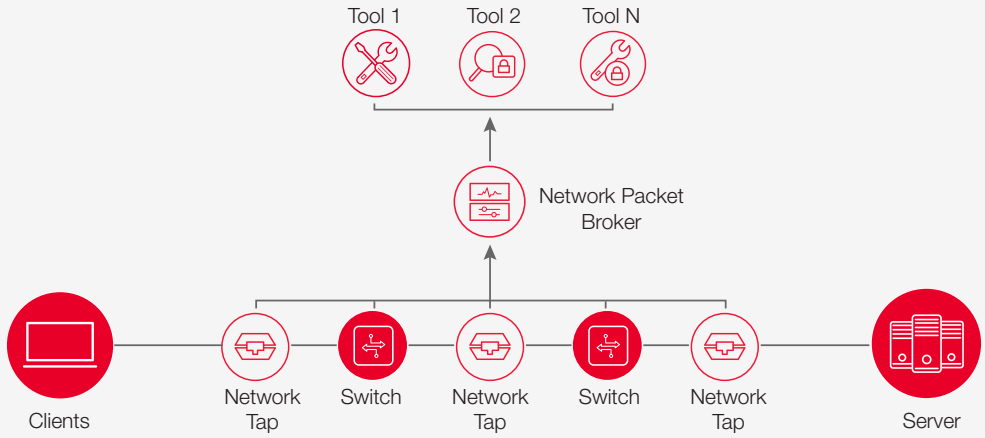


Figure 1. A network packet broker aggregates and filters data from tap and SPAN ports.

By filtering data within the NPB, the monitoring tool is freed to perform the work that it was purchased to do, resulting in more useful work being done by the monitoring tool. Since the tools are now as efficient as possible, less devices may be required to accomplish the same goals. In addition, the right choice of an NPB optimizes filter programming costs by removing the manual command line interface (CLI) process used in SPAN ports and some NPB models.

Understanding Ease Of Use

A fundamental component of the cost of ownership for any monitoring solution rests upon short-term and long-term usability costs. This is often referred to as the “ease of use” of the architecture. Specifically, ease of use for a monitoring solution includes initial installation, training, and day-to-day programming complexity.

A fundamental component of the cost of ownership for any monitoring solution rests upon short-term and long-term usability costs. This is often referred to as the “ease of use” of the architecture.

There are many factors that figure into these components, like whether taps or SPAN were deployed, the computer interface to the NPB, the specific capabilities of the NPB (e.g. remote access, automation, filtering engine, packet capture capability, NetFlow generation, etc.), and filter libraries.

A real GUI is where the commands (clicks) are hard coded into the machine’s operating system via hard ASIC routines. Once any variables are indicated, the system is already in action. GUI’s are much faster and the most repeatable methods for programming technical network equipment. In the early years, CLI was considered the most versatile

interface. However, today's GUI's are actually more flexible, more repeatable, and can be learned more simply and quickly. GUI programing does not require any retraining and can be used by the newest employee.

It should be noted that some vendors may make various claims that they have a GUI operating system. This concept should be investigated during the purchasing process. In actuality, some vendors use a combination of a CLI interface and a CLI translator to create data filters. This type of interface has quite a few drawbacks, not the least of which is complexity. As an example, the user interface for standard Layer 2 – 4 filter creation typically uses a menu driven interface for these vendors. Several steps are needed to create the filter. Then the filter needs to be tested. Finally, the filter has to be attached to an ingress or egress port.

The Keysight Vision series NPB has a built-in filter validation system, called the Dynamic Filter Engine, which validates the integrity of the filter created and prevents data clipping when multiple filter criteria are selected.

In contrast, other vendors use a complete GUI interface for everything — no CLI is required. A GUI is quicker, simpler, and more intuitive because no extensive filter rule programming is required. The NPB simply uses drag-and-drop, point-and-click technology to quickly create filters and activate them. This type of solution helps the user by eliminating the following: complex filter programming, the use of Boolean algebra, and filter validation. These steps have been automated, which is a huge benefit over any other state-based setup process. In addition, pre-configured, hard coded filters (also called floating filters) can be created and stored in the NPB for rapid deployment.

As an example, the Keysight Vision Series NPB has a built-in filter validation system, called the Dynamic Filter Engine, which validates the integrity of the filter created and prevents data clipping when multiple filter criteria are selected. The drag-and-drop interface is so intuitive to use and understand that no training courses are needed. This means your system is up and running in a minimal amount of time. In fact, several customers have installed the system and had it up and running in less than 30 minutes.

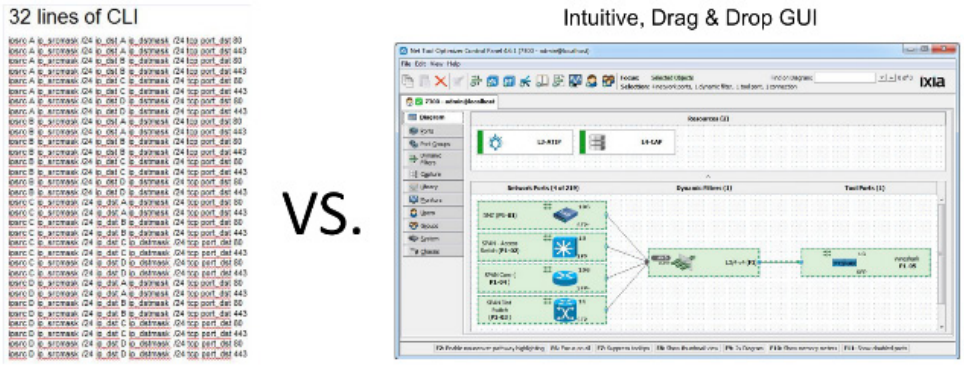


Figure 2. CLI vs GUI data filtering comparison

CLI is a risk

Another concept to understand is that the use of CLI increases organizational risk. This is for three good reasons:

- CLI created filters require validation
- More manual effort and time are involved which creates a lack of responsivity
- There is a higher personnel dependency risk for your agency

When examining CLI in more depth, the creation of a filter involves typing in multiple commands that define: the type of data to be captured, the ingress ports for data collection, and the egress (e.g. SPAN or NPB) port for filtered data. It should be noted for most solutions, especially SPAN ports, there is no filter validation within the routing switch. If the filter is programmed incorrectly, the wrong data will still be sent out the SPAN port and onto the monitoring tools.

It is important to understand that CLI filters are prone to errors, since they are often manually created. This creates a significant potential source of errors and debugging time required to troubleshoot those data filters. And while some errors are obvious upon review, others are not and may result in clipped data that delivers some of the data (but not all the requisite data) to the security or monitoring tool. This results in erroneous conclusions and delays in time to resolution. ZK Research estimates t monitoring filters which have been created by a CLI interface have errors in them at least 20% of the time. This is due to the complexity of the interface that uses a series of programmatic lines and Boolean algebra to accomplish filter creation. Separate test equipment should be used to validate the filter output every time a filter is created or modified. If not, simple mistakes can result in data clipping that is very hard to debug.

NPB's that have built-in filter creation engines can remove this issue for IT and security managers. Once the CLI-based filter is created, it needs to be validated. This can take over an hour to validate the filter. NPB's with built-in filter engines can often validate themselves. If not, a onetime validation process to prove the filter engine accuracy should be enough. Each individual filter doesn't need to be validated like it does when the filter is created through a CLI process.

GUI-based systems also decrease agency risk due to employee turnover. For instance, if CLI is the basis of the data filtering system, the loss of the CLI programmer can, and will, be a significant loss to the IT department if that individual retires, quits, or changes positions. By contrast, the use of a GUI-based system decreases this risk as most IT person can be brought up to speed in a matter of minutes. The existing filters can also be observed and reviewed within a few minutes time. There is no need to write the CLI command lines down and dissect their intention.

Once the CLI-based filter is created, it needs to be validated. This can take over an hour to validate the filter. NPB's with built-in filter engines can often validate themselves.

Cost Of Configuration Changes

If one is to perform a financial analysis of a monitoring solution, the analysis needs to accurately account for data filter programming and re-programming costs. Specifically, there are four components that should be investigated:

- Tap versus SPAN usage
- GUI versus CLI programming times
- Filter creation and validation costs
- Floating filter usage

As mentioned previously, taps are set and forget. There is a one-time installation cost. After that, no more configuration or reconfiguration is needed. If SPAN ports are used, there is a continual programming cost involved every time your data needs change, new tools are added or removed, and new data switches are added.

The next thing to consider is the length of time that it takes to create a "typical" filter. In an internal time trial at Keysight, it was found that a GUI interface was more than five times faster than a CLI interface. This analysis was based upon a Cisco Catalyst 6500 switch and an Keysight Vision ONE NPB. The time to setup and execute a filter using the Keysight interface was about 2 minutes versus about 15 minutes for the CLI interface on the Catalyst switch. As mentioned, a GUI all but eliminates filter errors due to the interface type.

In contrast, the CLI filter will require between 15 minutes to an hour to verify. The actual time depends upon the command line complexity and what test equipment is needed to validate the filter output. We will assume 30 minutes although this is probably a low estimate when the setup of the validating tool programming time is considered.

A third item to understand is how often data filter changes are needed. Research from the analyst group EMA shows that for the average enterprise (we will assume it is the same for a federal agency), 74% of the respondents move or change their tool connections two or more times per month. For 30% of the respondents, they change their tool connections five or more times per month. We should assume that each change will typically have some sort of programming modifications.

If CLI is the basis of the data filtering system, the loss of the CLI programmer can, and will, be a significant loss to the IT department if that individual retires, quits, or changes positions.

By contrast, the use of a GUI-based system decreases this risk as an IT person can be brought up to speed in a matter of minutes.

Another question in the EMA study clarified that for 27% of enterprises, IT engineers spend 1/4 of their time configuring monitoring tools. Another 28% of respondents spend up to 50% of their time configuring tools. And another 20% spend up to 75% of their time configuring tools. What this means is that the time it takes to program, or reprogram a monitoring filter, will directly affect your total cost of ownership. The programming of data filters is not a one time, or once a year, activity. It is an ongoing activity you will need to account for ahead of time when performing a TCO analysis. For this study, we will assume three new filters (or three modifications to existing filters are created per month.

Filter libraries are another important component. When a network issue or event arises, it takes less than a minute to attach a floating filter to a network port and also to a specialized tool to begin diagnostic capture and analysis. In contrast, additional time must be allocated for CLI-created filters and the validation time of those filters in this type of situation.

The GUI interface also delivers another benefit. Because of the intuitive interface, processing delays can be minimized, if not deleted. CLI-based configurations take four times longer than when using a GUI. This becomes significant because almost 50% of network managers spend more than half of their time configuring monitoring tools—leaving little time for innovation.

Using this input, you can perform a comparison between a CLI-based system and a GUI-based system for a typical year. For this analysis, let's assume that a command line interface is used to set up a simple data filter for deleting SSL encrypted data.

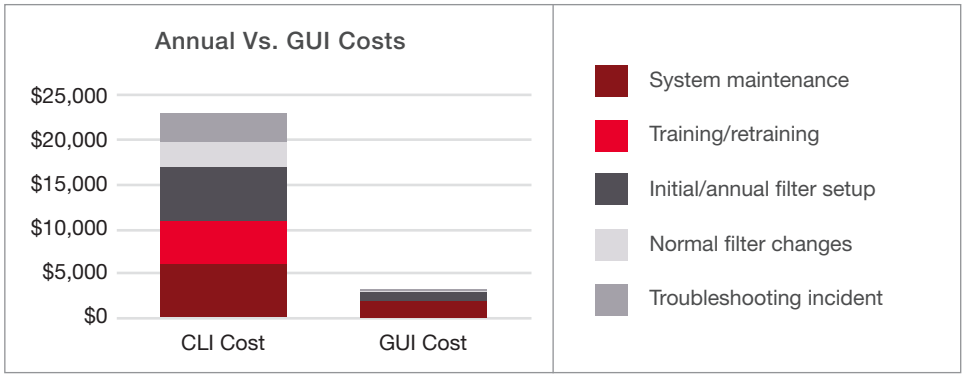
The GUI interface also delivers another benefit. Because of the intuitive interface, processing delays can be minimized, if not deleted. CLI-based configurations take four times longer than when using a GUI. This becomes significant because almost 50% of network managers spend more than half of their time configuring monitoring tools—leaving little time for innovation.

This data can be summarized in the following chart:

Cost Component	CLI	GUI	Frequency
System maintenance	$6,000	$2,000	Annual
Training/retraining	$5,000	$0	Annual
Initial/annual filter setup	$6,000	10 hours per year	Annual
Normal filter changes	15 mins per filter	2 mins per filter	3 times/month
Troubleshooting incident	4 hrs. per filter	15 mins per filter	4 times/month
Filter validation time	30 mins	0 mins per filter	Each filter
Labor rate	$100/hr	$100/hr	—

This data can be extrapolated to create a financial analysis of CLI versus a GUI. Here is a table with the detailed costs:

Cost Category	CLI Cost	GUI Cost
System maintenance	$6,000	$2,000
Training/retraining	$5,000	$0
Initial/annual filter setup	$6,000	$1,000
Normal filter changes	$2700	$120
Troubleshooting incident	$3400	$100
Total	$23,100	$3,220



Performing a side by side comparison of CLI costs versus GUI costs, a GUI-based solution could cut your long term operating costs by about 85%. Even being conservative, there is at least a 75% savings.

Also assume there is a creation/ modification of three filters per month for one year. In addition, assume that there will be four troubleshooting crises that would arise annually. Each of the four unplanned crises would mimic actual problems — so there is additional time needed to define the problem, determine a suspected cause, and to create a new filter to capture specific needed for debug purposes.

GUI vs CLI vs. menu driven summary

A final component to any cost study on ease of use would be to address installation and training costs for the solution. The initial setup and installation of a monitoring solution can take anywhere from a couple hours to a couple days, depending upon the features required. A CLI or CLI translator solution will naturally have higher costs than a GUI-based solution. Keysight research has found that a GUI creates higher productivity, while facilitating a lower cognitive load. This translated directly into a faster installation

Functionality	CLI	CLI Translator	GUI
L2-L4 filter creation capability	Yes	Yes	Yes
L7 filter creation capability	No	Medium	Extensive
Filter programming time	15 min	6 mins	2 mins
Installation time	24 hrs	120 mins	30 mins
Training time	8 hrs	8 hrs	N/A
Filter libraries	No	Yes	Yes
Role-based security	Yes	Yes	Yes
Filter validation testing	30 mins	Varies	None

Figure 3. GUI vs CLI vs. Menu Driven Summary.

and turn up time; and minimal to no training costs.

Once we have all the pieces, a comparison of the types of solution costs can be made. The following data shows a technical comparison of the three programming interfaces using the representative vendor data. The GUI is the winner of the analysis based upon filter creation time, installation time, and training time.

Conclusion

A fundamental question often asked is “how can I improve the short term and long term operating costs for my monitoring solution”? There are two easy steps: The first step is to update your processes to take advantage of the best technology. This means using taps instead of SPANs to access the proper monitoring data. This one step gets you better data. Better data reduces your troubleshooting and forensic analysis costs, as well as the cost due to missed security threats. Second step — you’ll want to add a network packet broker to optimize your filtering methodology and related filter programming costs to remove as many of the manual components as reasonably possible.

By combining both steps, you can effectively reduce your TCO and reuse the extra money to solve the additional needs that you have. When looking at the total cost of ownership of a visibility solution, an important aspect to investigate is the ease of use. While tool costs are an important part of the initial cost structure, long-term ease of use will figure in heavily to the total cost ownership. This comes about through the following direct and indirect costs:

- Data filter creation costs
- Data filter validation costs
- Salary/staff time costs for initial and ongoing training costs

Other indirect costs need to be factored in as well:

- Reducing the time to recognize and to fix issues — data leaks, attacks, etc.

When looking at the total cost of ownership of a visibility solution, an important aspect to investigate is the ease of use. While tool costs are an important part of the initial cost structure, long term ease of use will figure in heavily to the total cost ownership.

- Loss of network visibility during training courses
- Staff frustration and overtime to find and mitigate issues that were missed due to poorly configured data filters
- Minimizing, or avoiding, network outages by early recognition of issues before failure
- Reduction of support calls that reduce operational employee production downtime

Ease of use for a monitoring solution a is a crucial component of the TCO and the efficiency of the solution. The common practice of using a CLI has higher costs. For instance, the time to create a data filter within an NPB can be four to ten times faster than using a CLI. Simple choices, like using a graphical user interface (GUI), can cut your long term operating costs by 75% or more.

Keysight network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. For more information on network monitoring solutions, visit www.keysight.com/solutions/network-visibility.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES