Cybersecurity's Cost-Cutting Secret: Network Visibility

KEYSIGHT

NETWORK VISIBILITY

It's a Superpower

Network visibility is like having a superpower that lets you see through walls and know exactly what's happening in your network. It's the all-seeing eye that can detect even the tiniest network anomalies.

It's like being a detective but for your network. You can see who's using the network, what they're doing, and where they're going.

From a **performance** perspective, you can identify bandwidth bottlenecks and adjust network resources accordingly. From a **security** perspective, you can detect threats and take steps to mitigate them to pre-empt damage.

It pays for itself

Network downtime can be costly in terms of lost productivity and lost revenue. Network visibility enables real-time network monitoring so businesses can detect potential issues before they become major problems and optimise network performance to ensure maximum efficiency. Network visibility tools can be used to identify and resolve issues more quickly, reducing downtime and minimising the impact on the bottom line.

Furthermore, network visibility helps businesses make informed decisions about network upgrades, resource allocation, and security measures, allowing for greater control over costs and more efficient use of resources. **Network visibility is a critical component of cost reduction** and should be a top priority for any business that values its network infrastructure and wants to remain competitive in today's fast-paced digital landscape.

GETTING IT RIGHT

Security and monitoring tool expenditures can be a large expense for enterprises. Cyber security risks are on the rise and organisations must modernise and fortify their security measures. As network bandwidth consumption demands increase to 40, 100, and even 400 GE, there is a corresponding need for bigger data pipes, along with newer and faster tools. This is where IT management gets caught in the middle. Without new technology investments, IT staff can't keep up with the needs of the business. At the same time, purchasing larger scale security and monitoring tools is expensive.

Network visibility solutions consisting of taps and packet brokers can help for both physical on-premises and cloud-based solutions. Not only can the right visibility solution lower some of your costs, but - under the right conditions - you also have the potential to achieve a 100% ROI. Not many solutions can boast an ROI like that.

3 USE CASES

Here are three fundamental network visibility use cases to consider:

1. Delay tool CAPEX expenditures as you upgrade the network to 40, 100 and 400 GE links
2. Simplify network and application troubleshooting to reduce mean time to repair
3. Implement n+1 load balancing to optimise business continuity

1. Network Visibility Can Delay and Reduce CAPEX

While network visibility components cost money, they are often less expensive than many of the security and monitoring tools on the market. In fact, a recent survey from Enterprise Management Associates (Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise) found that tool expense was still a prominent complaint for some, if not many, enterprises.

The solution is to optimise the flow of data to those tools. This is where you can use a packet broker with a load balancing feature to extend the life of your tools. Load balancing is the ability for a network packet broker to take incoming traffic and dynamically spread that traffic across multiple output ports. For instance, incoming traffic at 40 Gbps could be distributed to either one 40 Gbps device, two 20 Gbps devices, four 10 Gbps devices, or some other combination of devices to process the required data. By using this capability, you can utilise your existing, lower bit rate tools instead of immediately upgrading your tools to 40 Gbps as well.

Strained IT budgets are a common challenge. A delay in additional CAPEX spending can be a welcome relief.

In another example, two fundamental packet broker features (data filtration and data deduplication) can significantly reduce the size of your monitoring traffic and optimise data bandwidth. The data filtration feature can remove extraneous data by up to 80% or more. It is also common for enterprises to have 25 to 50% duplicate packets on their network. When the two features are put together, it is fairly common to reduce the amount of monitoring tools by 1 or more units, assuming you have multiple units of a particular tool type. Using a basic financial example, by spending $50K on a packet broker you may be able to eliminate the cost of at least one $100K tool. This could theoretically result in an ROI of 100%. Actual savings would obviously depend upon your specific network configuration.

2. Simplify and Reduce Remote Troubleshooting Time

Once taps are inserted into a network, they are essentially "set and forget." There is a one-time network disruption but no routine disruptions. This means that a packet broker and diagnostic (or security-related) tools can be connected at will to resolve incidences — often will little to no Change Board approvals required, since there is no disruption to the network. Once an enterprise implements this type of scenario, it is possible to see an up to 80% reduction in the time it takes to troubleshoot problems. This has been the case for several of Keysight's customers.

3. N+1 Survivability Optimises Business Continuity

The load balancing feature of packet brokers mentioned earlier can also be used to implement n+1 survivability and increase tool utilisation. If one extra tool is added, then the packet broker will dynamically balance traffic across the tools. Should a tool fail, the load is rebalanced to prevent a loss in monitoring or security functionality. Once the problematic tool recovers, the load is dynamically rebalanced again by the packet broker. This feature creates a cost-effective component redundancy solution while also inserting self-healing capabilities into the network.

Cybersecurity's Cost-Cutting Secret: Network Visibility

Reach out to **Keysight Technologies Australia** to find out how to save money by optimising your security and monitoring solutions with the best line of packet brokers and taps on the market.

Toll-free:
1800-629-485

Email:
tm_ap@keysight.com

Learn more at: www.getnetworkvisibility.com

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance, and network monitoring tools.

KEYSIGHT