WHITE PAPER

Five Steps to Building Visibility and Security Into Your Network

Introduction

As organizations seek to walk the networking tightrope between the demands of performance management and network investment, they clearly need something to hang on to, to help them keep their balance. Mature enterprises are increasingly turning to network visibility as that proverbial balancing pole.

Without visibility, it is difficult to manage operational variables to maintain high levels of network performance—and it is nearly impossible to understand the threats maligning the network in order to maintain security and control over network assets. But simply throwing money at network and security monitoring tools does not provide the kind of visibility necessary to balance performance and control. Organizations also need to employ best practices to ensure they are getting the most out of their network and security monitoring investments.

The following five-step approach can help IT keep its balance while gaining that crucial visibility into the network.

Without visibility, it is difficult to manage operational variables to maintain high levels of network performance.

KEYSIGHT TECHNOLOGIES

Step 1:

Do not let capacity limit access to monitoring information

In an ideal world, network monitoring offers a window into the infrastructure, allowing IT to make more informed decisions about how to configure the network for improved performance and respond rapidly to security incidents. But this paradigm depends on one assumption: You must have the capacity to support it. Without enough network connections available to plug in monitoring and security information and event management (SIEM) tools simultaneously, the organization effectively neutralizes the underlying assumption of visibility afforded by monitoring.

On a nontechnical level, you could compare it to plugging all of the lights in your house into a single power strip: If the strip can handle only seven lamps but the house needs 10 to keep all the rooms lit, then you are left with the prospect of unplugging three lamps to plug in three others. At any given time, some part of the house goes dark.

From a networking perspective, capacity restrictions that hamper full monitoring coverage make it difficult to gain a full understanding of how well the network is performing across all components of the infrastructure. These capacity limits can also prove a considerable security liability, as an organization that must ration monitoring will sometimes be unable to pinpoint risk indicators that crop up in those areas of the network that have gone “dark” due to disabled tools. This is why it is so critical to implement a monitoring solution like Keysight’s IxVision visibility architecture to help address your TAP and SPAN port shortages in a cost-efficient manner. Doing so makes it possible to engage all of the monitoring and SIEM tools required for maximum visibility without buying more hardware to support those tools.

Step 2:

Reduce unnecessary data and costs

Without a visibility architecture capable of removing duplicate traffic, monitoring and security tools may become clogged with redundant data.

Achieving comprehensive network and application monitoring on all network traffic can be a double-edged sword. On the plus side, a full slate of monitoring tools allows organizations to analyze all aspects of the network for clues to help fine-tune performance and protection. But on the flip side, those monitoring tools are looking at everything, including all of the redundant and extraneous packets streaming through the infrastructure.

Plain and simple, the more unnecessary packets cluttering network traffic, the harder it is to sift through the mound of data to find the relevant information necessary for maintaining solid performance and spotting security issues. Without a visibility architecture capable of removing duplicate traffic, monitoring and security tools may

become clogged with redundant data. It costs more to not only process all this data, but to also store duplicate data on the SAN.

In order to get the most from your monitoring investment, it is critical to find ways to strategically cut down on packet clutter. This kind of decluttering is something the Keysight's IxVision excels at—it cleans up the stream so that the data being monitored is the data that matters.

Step 3:

Get the ROI you want from your existing monitoring tools

Even after cleaning up a packet stream, it is still possible for organizations to be overwhelmed by the data fed to their monitoring tools. Depending on the legacy architecture, organizations could be faced with the prospect of drinking from the metaphorical data fire hose.

For instance, analysts at Enterprise Management Associates (EMA) found that at the University of Texas at Austin, IT teams responsible for protecting and monitoring the network were using traditional network switches to replicate production traffic back to the monitoring tools.[1]

"But we had a problem," the university's chief information security officer told EMA. "As [traffic] volumes grew, these mirrored flows were exhausting resources on the switches, causing packet drops. We had been doing this for years using old Cisco switches, so it was not costing us much, but volume was really becoming an issue and dropping packets was simply unacceptable."

This is where the strategy of segmenting packet information, filtering packets, and directing the filtered traffic to specialized monitoring tools can help IT teams manage and parse out that flow of information, to give organizations a better ROI from their existing monitoring investments.

Keysight believes that not only are these capabilities critical, but that they also need to be easy to control. Time is money, and the faster administrators can configure their tools and the data streams these tools rely on, the higher the ROI. That is why Keysight puts the power to distribute the correct information in administrators' hands, using a graphical user interface (GUI) to create out-of-band filters for monitoring data.

It is the solution that the University of Texas (UT) used, and as a result, the school reduced their intrusion detection system (IDS) capacity demands by 20-30%. UT expects the solution to pay for itself in one year. Review the UT case study here.

1 "ROI Experiences with Network Monitoring Switches—University of Texas at Austin," Enterprise Management Associates, 2012

Step 4:

Optimize incident response to reduce mean time to repair

Time is money, and the faster administrators can configure their tools and the data streams these tools rely on, the higher the ROI.

The longer it takes IT to actually respond to security or operational incidents, the more risk it incurs for the business and the more expensive such incidents become. This is where automating responses to incident triggers picked up in monitoring traffic is so crucial to gaining the most return on monitoring investments. Organizations that are able to optimize real-time reactions to performance issues or security problems tend to reap the most ROI—because the faster they respond, the more likely they are to reduce their mean time to repair.

Another benefit of adding a monitoring switch to the network infrastructure is that organizations can eliminate the need for crash carts and change board approval. Crash carts and change board procedures are put in place to deal with SPAN/TAP shortages and the risk of network disruptions or outages when any physical change is made to the IP network. History has repeatedly shown that when IT has to make network changes on the fly, it far too often results in additional—potentially worse—disruptions. With a monitoring switch installed, network disruptions are minimized. IT can connect and configure data streams through software filtering instead of making physical network changes, which has far fewer risks. Risks can be further minimized by testing configurations through a simulator first, before uploading any new configurations into the monitoring switch. Only a few monitoring switches, such as Keysight's network packet broker (NPB), offer this simulator functionality, but it can be a powerful tool for optimizing the data network.

While visibility solutions like the Keysight visibility architecture do not fix the problems themselves, they make it easier for an organization's expert problem solvers to take care of issues more quickly. Operations staff can be automatically apprised of issues that are hindering performance, greatly reducing troubleshooting time. And security personnel are tapped into information about where, when, and how attacks are occurring so they can more strategically plan for a proactive defense.

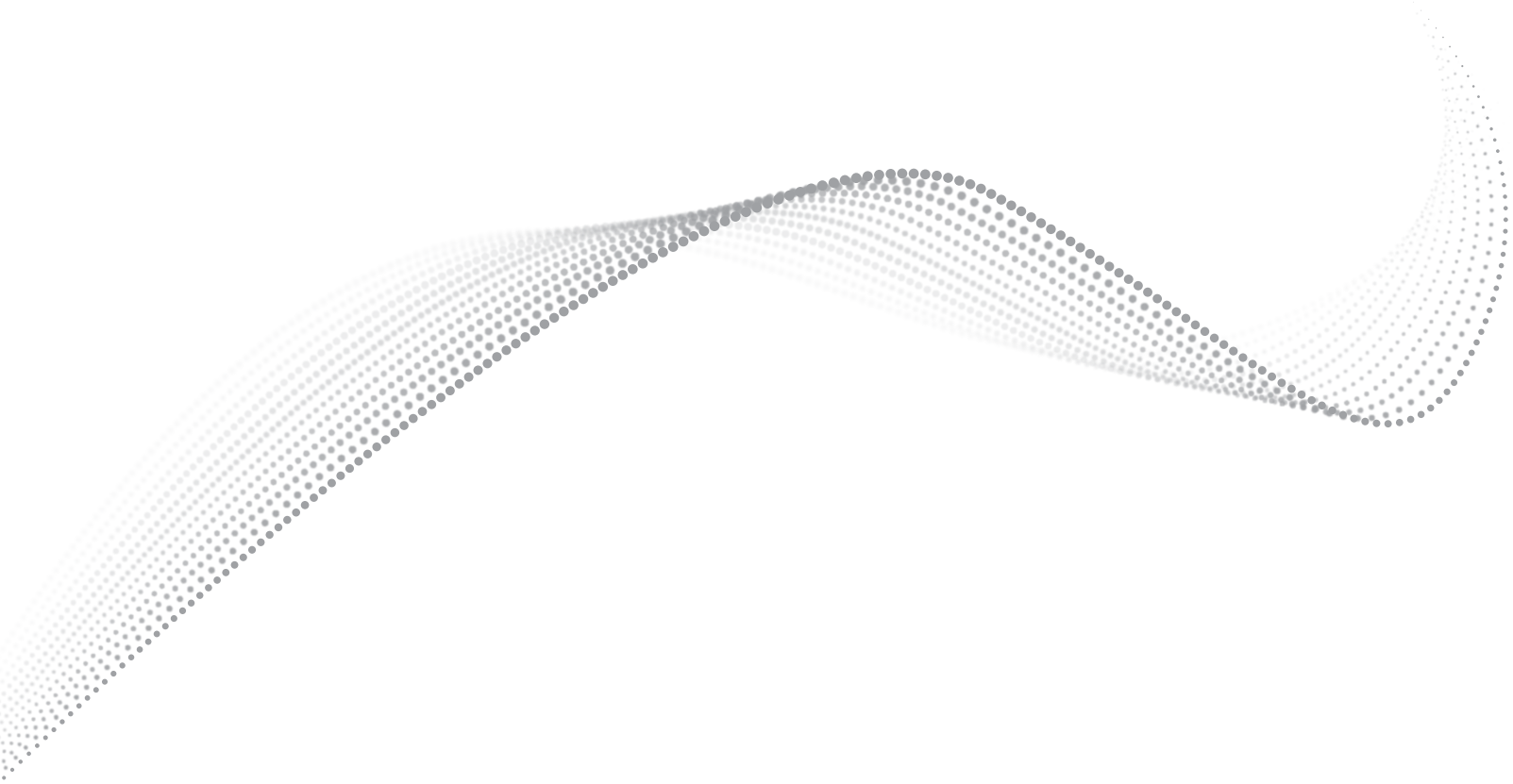
The idea is simple: By developing a set of trigger scripts, the monitoring switch can respond when problematic conditions are met. So, in the case of security, if network traffic is deemed suspicious by the security tool, it will be sent to the appropriate security tool or network recorder for analysis. At the same time, an alert can be sent to the incident response team, whose members will immediately have all the necessary information at their fingertips when they access the network to troubleshoot the incident. Keysight's IxVision offers an additional layer of security through integration with SIEM tools. This integration makes it possible to automatically send relevant information to these tools for better correlation of seemingly disparate events.

Step 5:

Optimize your network with trend analysis

Network planning requires long-term strategies that depend on business intelligence. Without a long history of network intelligence, it is difficult to devise a strategy based on anything other than guesswork.

Not only can a network visibility architecture help with immediate issues like distribution of data to monitoring tools and automated incident response, but it can also provide the capabilities needed to make decisions that feed into the organization's strategic vision. By using the historical trend data offered by the monitoring switch, organizations are better able to institute proactive network optimization on the operations side, rather than running the network reactively. Customers can watch trends and anticipate when network capacity will need to be added, rather than being surprised by network segments reaching capacity. Additionally, that same statistical information can be used to validate service-level agreements (SLAs).



Conclusion

All too often, organizations throw money and bandwidth at network performance and security problems without ever achieving the network intelligence to fix the root causes. In order to strike that perfect balance between secure performance and reasonable investment, it takes a visibility architecture to achieve the kind of visibility necessary for that intelligence. Keysight's network packet brokers help organizations filter unnecessary data packets and distribute data optimally to existing monitoring tools so that they are never overloaded by data that eventually could be lost.

Automatic trigger scripts help organizations get the most out of their monitoring investment by reducing mean time to repair. And all of that valuable trend data is made available so that organizations can be more proactive about their infrastructure decisions. Most important, it is all done in a way that reduces complexity, through a consistent management interface across all deployment scenarios. This power of simplicity drives more network monitoring ROI.

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