Visibility Architecture – Eliminating Visibility and Security Blind Spots

Delivering an Amazing Customer Experience

From an information technology (IT) perspective, businesses are in the midst of a once in a generation change. The shift to public and private cloud computing, the shift to virtualized networking, and the growing number of connected devices are structurally changing IT. And within this increasingly complex environment, businesses depend on IT's ability to deliver an amazing customer experience.

Every business relies on critical applications that are connected in some way. Business customers and users simply expect anytime, anywhere access to all these applications. IT's challenge is to make sure the infrastructure that delivers these critical applications is reliable, fast and secure. But this level of reliability, performance, and security can be a real challenge. It requires changes to the way IT monitors, manages, and ultimately controls the infrastructure used in application delivery.

"Problem identification is it's biggest challenge."

Zeus Kerravala,
Principal Analyst

ZK Research

KEYSIGHT TECHNOLOGIES

Zeus Kerravala, Principal Analyst at ZK Research asserts that, “Problem identification is IT’s biggest challenge.”[1] He explains that 85% of the mean time to repair (MTTR) is the time taken to identify there is in fact, an issue. If IT can’t quickly identify problems, they will constantly hear about issues from unhappy customers. The MTTR clock starts ticking whether IT knows there is an issue or not.

79% of survey respondents report that they are not getting expected results from their APM investments.

Managing Fast, Reliable, and Secure

Companies try to ensure their networks are reliable, fast and secure through a number of teams that manage every aspect of the network. Examples include: Network Ops, Application Ops, Security Admins, Server Admins, Forensics, and Privacy and Audit teams.

And each of these IT teams buys their own set of analytics or monitoring tools. These include tools like:

- Network Performance Monitoring and Diagnostics (NPMD)
- Application Performance Monitoring (APM)
- Threat Intelligence Gateways
- Customer Experience Monitoring (CEM)
- Forensics Probes and/or Crash Carts
- Intrusion Detection Systems (IDS)
- Security Information and Event Management (SIEM)
- Firewalls and Next-Generation Firewalls
- Intrusion Prevention Systems (IPS)

Unfortunately for many organizations, these teams and their analytics tools have not solved the problem - blind spots still persist. A recent Keysight application performance monitoring survey proves the point. It shows that 79% of survey respondents report not getting expected results from their APM tools.[2] IT organizations continually report that monitoring efforts are complex, inefficient, and costly.

What Makes Good Visibility and Security?

Good visibility and security starts with the right analytics or tools. Jim Rapoza, Senior Research Analyst with Aberdeen Group previously stated that, “It’s imperative that IT professionals have the right tools to keep networks running securely.”[3] But the right tools are only a starting point, not the answer. Jim adds that, “Organizations must have visibility solutions that provide immediate insight into events.”

“Organizations must have visibility solutions that provide immediate insights into events.”

Jim Rapoza,
Senior Research Analyst

Aberdeen Group

[1] Application Drives the Need for Application Strengthening, Presented by Zeus Kerravala, January 2016.
[2] “The State of Application Performance Monitoring”, Keysight Inc., February 2016.
[3] “Keysight Brings Application and Threat Intelligence to Network Visibility”, Keysight press release, December 17, 2014.

This statement indicates a different model for visibility is needed. A model Keysight believes should include:

- The right analytics or monitoring and security tools
- Tool access to end-to-end network data
- Global application and threat intelligence
- Visibility solutions that tie it all together

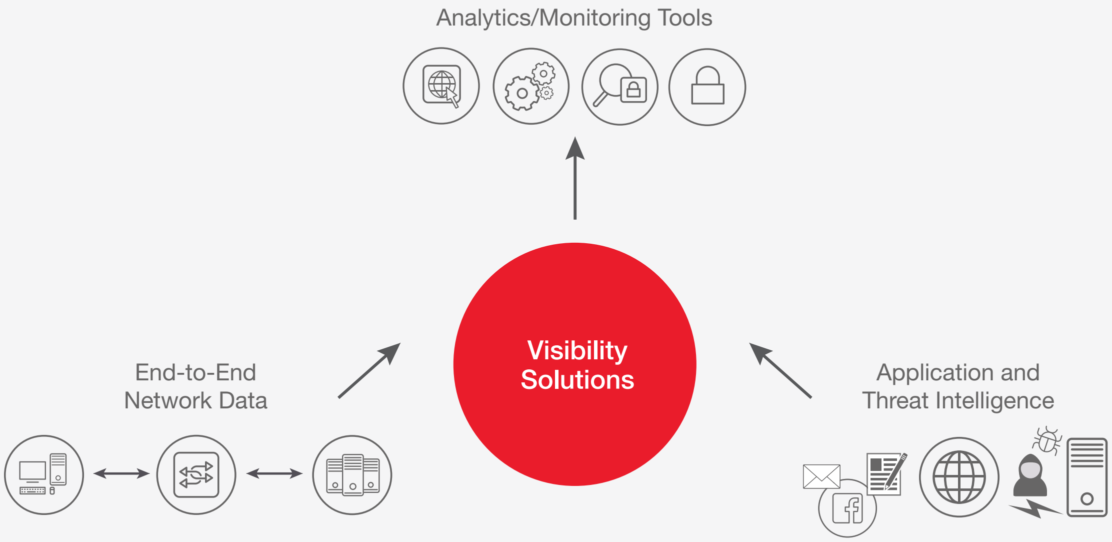
Analytics/Monitoring Tools
Visibility Solutions
End-to-End Network Data
Application and Threat Intelligence

Figure 1. A model to improve visibility.

Without these components, IT is hampered in its ability to deliver reliable, fast, and secure networks.

Keysight's Visibility Architecture

Enterprises, federal governments, and service providers use Keysight's Visibility Architecture to improve the insights they get from their out-of-band monitoring tools. They also use Visibility Architectures to ensure fail-safe deployments of inline security tools and to deliver proactive monitoring of SLA's and customer experiences.

Enterprises, federal governments, and service providers use Keysight's Visibility Architecture.

Further, a visibility architecture:

- Delivers a return on investment of 100% and more[4]
- Improves the speed and success of new service deployments
- Speeds problem identification, isolation, and repair times
- Increases the efficiency of network, application, and security monitoring tools
- Allows IT to effectively comply with many compliance mandates
- Provides end-to-end visibility into both physical and virtual networks
- Extends the life of existing tools when upgrading network speeds

At its core, a visibility architecture improves the effectiveness and efficiency of IT by giving its monitoring and security tools access to the right visibility data and intelligence at the right time. This visibility data includes end-to-end views of application traffic, and additional visibility intelligence from Keysight's AppStack solution.

Visibility Architecture – Visibility, Security, and Proactive Monitoring

Keysight offers the most expansive visibility product portfolio available. It is this innovative

set of visibility products and services that forms the foundation of three key Visibility Architecture solution frameworks.

- **Intelligent Visibility Framework** – Ensures the right data gets to the right tool at the right time
- **Resilient Security Framework** – Creates fail-safe inline security tool deployments
- **Proactive Monitoring Framework** – Validates active SLA and customer experience monitoring

Intelligent visibility framework: smarter monitoring and security tools

The Intelligent Visibility framework enables effective and efficient network, application, and security out-of-band monitoring. The goal is to give out-of-band monitoring tools a broader view of the network by providing easy access to both network traffic and external intelligence, and to conversely allow those same tools to efficiently focus on the details that matter most. It's about seeing everything so you can easily find a needle in the haystack.

Typical deployments consist of a variety of physical and virtual network taps, intelligent network packet brokers, external application and threat intelligence feeds, and IT monitoring and security tools. Once in place, it delivers reliable access to end-to-end network traffic, data filtering and grooming capabilities, decryption of SSL traffic for

[4] The University of Texas at Austin Case Study, Keysight, December 2015.

monitoring, NetFlow generation with extended contextual metadata, data masking of sensitive content like credit card numbers, and load balancing of traffic across monitoring tools as required.

Intelligent Visibility delivers numerous benefits including:

- Significant return on investment versus traditional monitoring deployments
- Reduced monitoring costs through more efficient use of tool resources

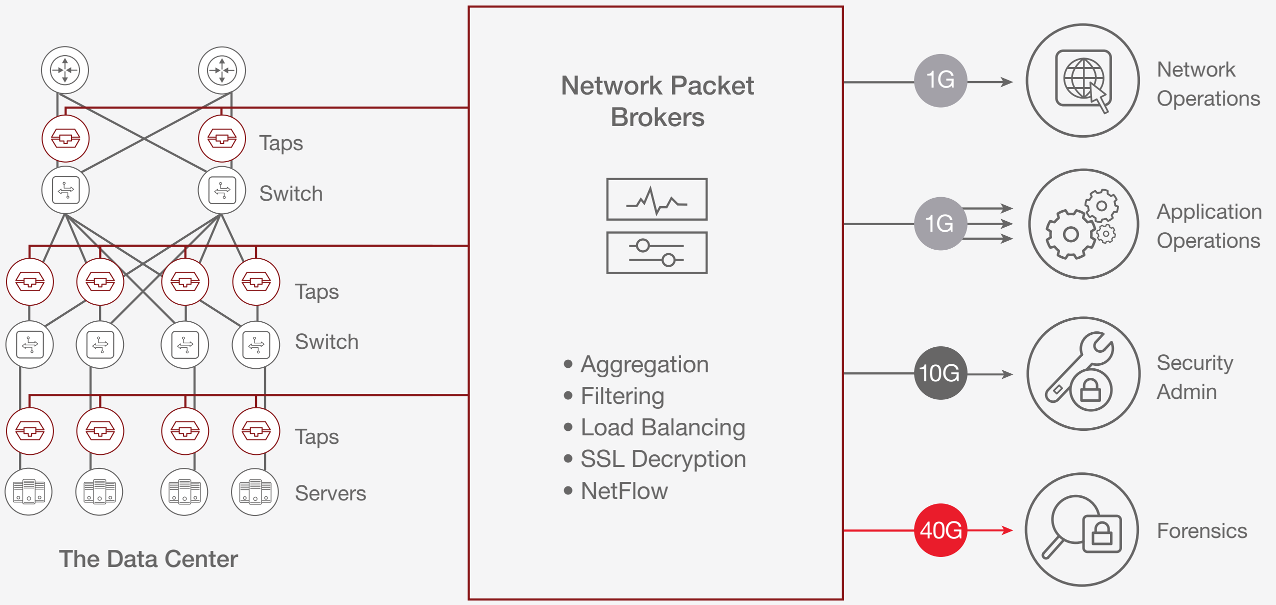

Figure 2. Intelligent security.

- Decreased troubleshooting and mean time to repair (MTTR)
- Increased reliability, performance, and security
- Expanded regulatory compliance for external audits
- Improved operations team efficiencies and harmony

Resilient security framework: fail-safe inline security deployments

The Resilient Security Framework eliminates the dangerous practice of installing multiple inline security tools directly in the network and provides fail-safe deployments for inline security tools that greatly reduces operational frictions between the networking and security teams. The aim is to harden network security deployments. It also aims to improve the efficiency of inline security tools and security operations teams ultimately freeing resources for even greater focus and investment. It's about doing more with less.

Typical deployments consist of inline bypass switches, intelligent network packet brokers, existing or new inline security tools, attack surface reduction appliances, and external threat intelligence feeds. Once in place, it delivers load balancing of traffic to inline security tools, security tool monitoring for health and performance impacting congestion, automated fail-over in the event of security tool outage or failure, manual security tool changes and upgrades without downtime, and selective traffic routing to and through the inline security tools

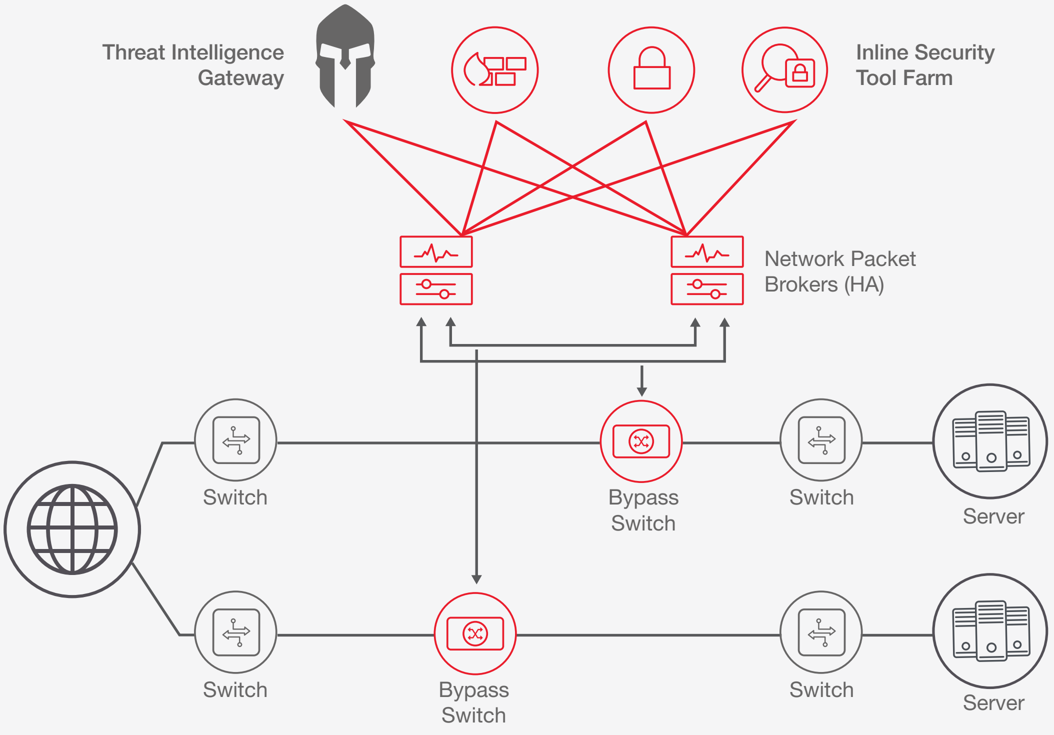
Threat Intelligence Gateway
Inline Security Tool Farm
Network Packet Brokers (HA)
Switch
Bypass Switch
Switch
Server
Switch
Bypass Switch
Switch
Server

Figure 3. Resilient security.

Resilient Security delivers numerous benefits including:

- Significant ROI versus traditional inline security tool deployments
- Reduced security costs through more efficient use of tool resources
- Zero downtime security tool configuration changes and upgrades
- Increased tool efficiency from the elimination of data from bad IP addresses
- No impact capacity additions or new security tool deployments
- Greater uptime for security resources protecting the network
- Improved security through automated event response
- Decreased troubleshooting and problem isolation time for networking teams
- Improved security and networking team efficiencies and harmony

Proactive monitoring framework: continuous SLA and experience validation

The Proactive Monitoring Framework provides simple SLA and customer experience monitoring for a wide range of applications including voice, video, web services, and critical enterprise applications. The goal is to ensure that the infrastructure is capable of delivering an amazing customer experience 24x7, even when there is no user traffic on the network to monitor.

Typical deployments consist of software and/or hardware active endpoints, emulated application traffic, and a simple web based management and monitoring interface. Once in place it delivers SLA and experience monitoring, site-to-site and site-to-datacenter reliability and performance monitoring, and proactive fault detection and isolation. It even lets IT conduct service readiness assessments and new service turn-up verifications.

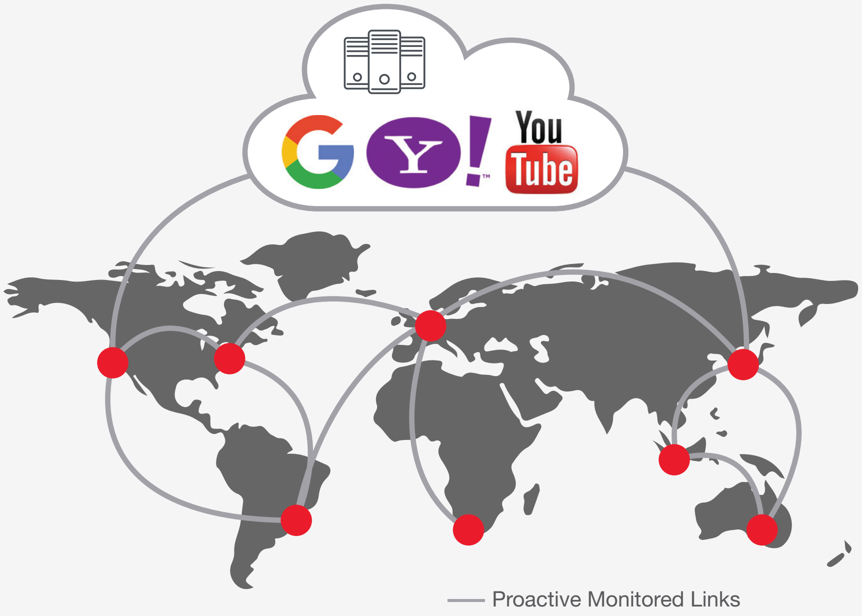

Figure 4. Proactive monitoring.

Proactive Monitoring delivers numerous benefits including:

- Quicker trouble identification and isolation times
- Reduced overall MTTR for customer / user impacting issues
- Increased network uptime and performance
- Improved overall service level agreement compliance
- Easier application, data center and cloud performance monitoring
- Smoother new service/application rollouts

Delivering on Today's Promises While Planning for Tomorrow's Innovations

In the short term, Visibility Architecture deployments are about quick returns on investments – 100% returns and more. It also improves overall application reliability, performance and security, and speeds trouble resolution. It is about accountability, delivering on SLA's, and meeting customer expectations. Improving the overall effectiveness and efficiency of monitoring tools and teams is the quickest way for IT organizations to demonstrate they are masters of their own domain, to accomplish more with less, and to free up both monetary and personnel resources.

In the long term, Visibility Architecture allows for increased investments in planning for tomorrow. It increases the life and capacity of existing investments, freeing up future budget dollars for new technologies. Once in place, teams will find they have fewer points of contention, greater flexibility, and independence. Teamwork and morale will improve as teams spend more time planning for tomorrow and less time chasing the problems of today.

Learn how you can easily start eliminating visibility and security blind spots and delivering an amazing customer experience today with Keysight's visibility architecture and solutions at https://www.keysight.com/us/en/solutions/network-visibility.html.

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