



WHITE PAPER

# IXVISION-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



Zeus Kerravala, Principal Analyst at ZK Research asserts that, “Problem identification is IT’s biggest challenge.”<sup>1</sup> 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.

## 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)
- 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 Ixia application performance monitoring survey proves the point. It shows that 79% of survey respondents report not getting expected results from their APM tools.<sup>2</sup> IT organizations continually report that monitoring efforts are complex, inefficient, and costly.

79% OF SURVEY  
RESPONDENTS  
REPORT THAT  
THEY ARE  
NOT GETTING  
EXPECTED  
RESULTS FROM  
THEIR APM  
INVESTMENTS.



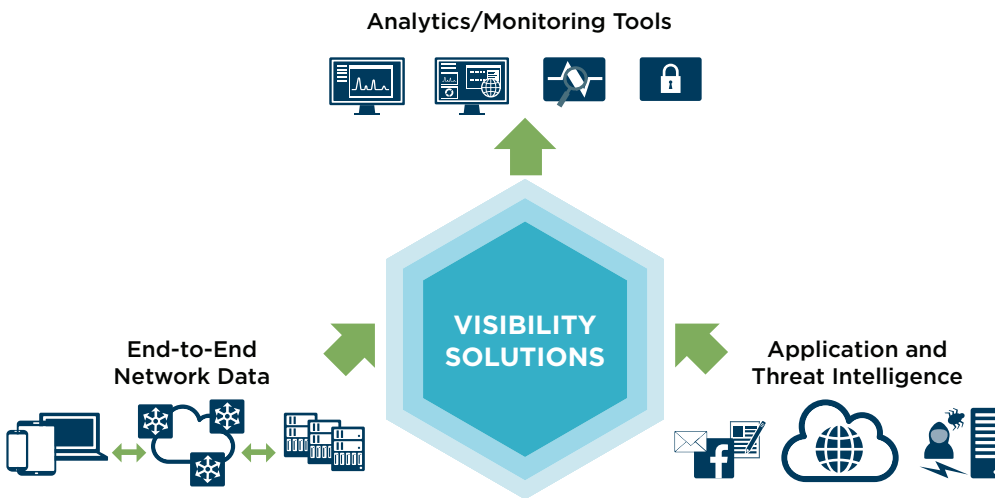
## WHAT MAKES GOOD VISIBILITY AND SECURITY?

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.”<sup>3</sup> 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.”

This statement indicates a different model for visibility is needed. A model Ixia 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

*Figure 1: A Model to Improve Visibility*



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

“ORGANIZATIONS  
MUST HAVE  
VISIBILITY  
SOLUTIONS  
THAT PROVIDE  
IMMEDIATE  
INSIGHTS INTO  
EVENTS.”

JIM RAPOZA  
SENIOR RESEARCH  
ANALYST  
ABERDEEN GROUP





## IXIA'S IXVISION VISIBILITY ARCHITECTURE

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

Further, IxVision:

- Delivers a return on investment of 100% and more<sup>4</sup>
- 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, IxVision 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 Ixia's Application and Threat Intelligence (ATI) Research Center.

The ATI Research Center lies behind many of the unique capabilities that IxVision delivers. It is through ATI that Ixia partners directly with customers instead of merely providing hardware solutions.

ENTERPRISES,  
FEDERAL  
GOVERNMENTS,  
AND SERVICE  
PROVIDERS USE  
IXIA'S IXVISION  
VISIBILITY  
ARCHITECTURE





## IXVISION – VISIBILITY, SECURITY, AND PROACTIVE MONITORING

Ixia 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 IxVision solution frameworks.

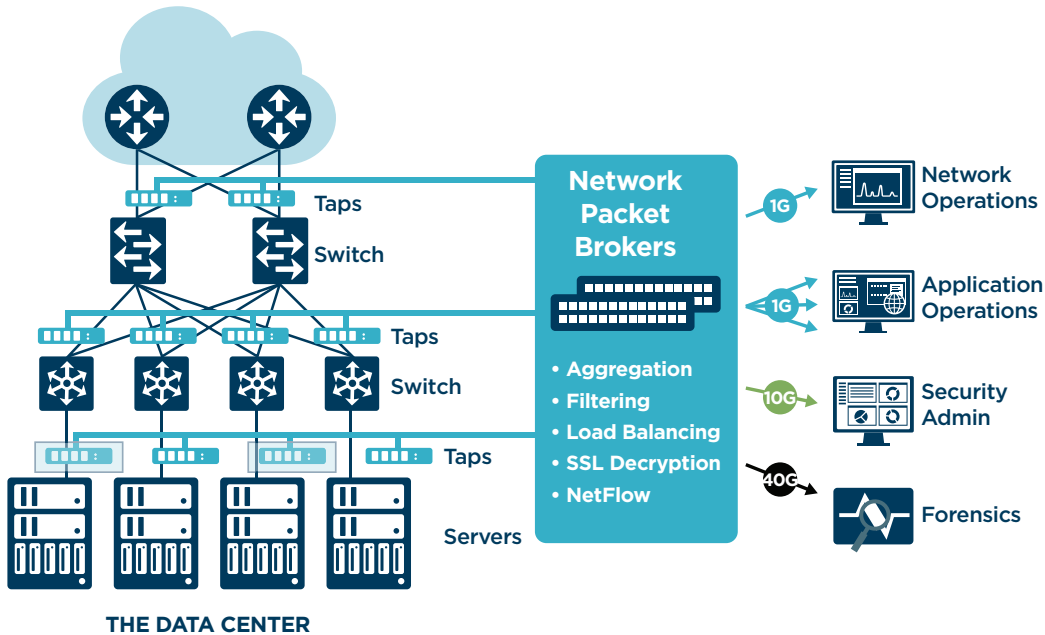
- **Intelligent Visibility Framework** – Ensures the right data gets to the right tool at the right time
- **Resilient Security Framework** – Creates fail-safe inline security tool deployments
- **Proactive Monitoring Framework** – Validates active SLA and customer experience monitoring

### ***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 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.

Figure 2: Intelligent Visibility



Intelligent Visibility delivers numerous benefits including:

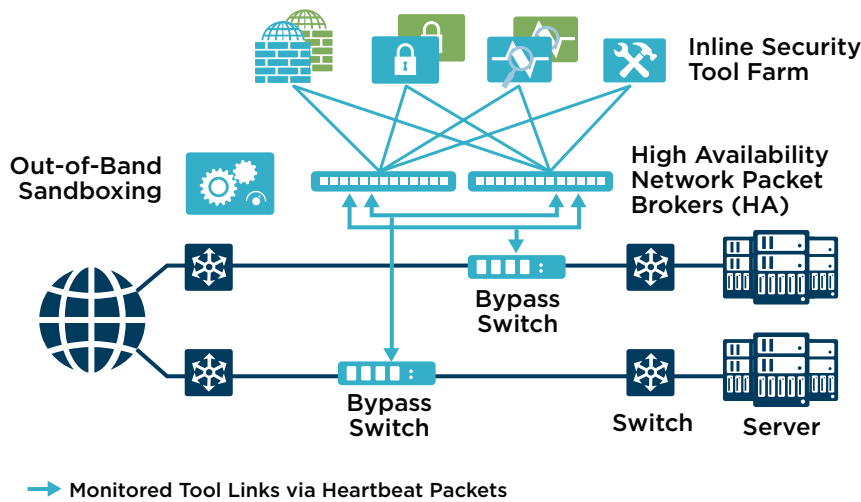
- Significant return on investment versus traditional monitoring deployments
- Reduced monitoring costs through more efficient use of tool resources
- Decreased troubleshooting and mean time to repair (MTTR)
- Increased reliability, performance, and security
- Expanded regulatory compliance for external 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, selective traffic routing to and through the inline security tools, and automated response or sandboxing in case of event detection.

*Figure 3: Resilient Security*



Resilient Security delivers numerous benefits including:

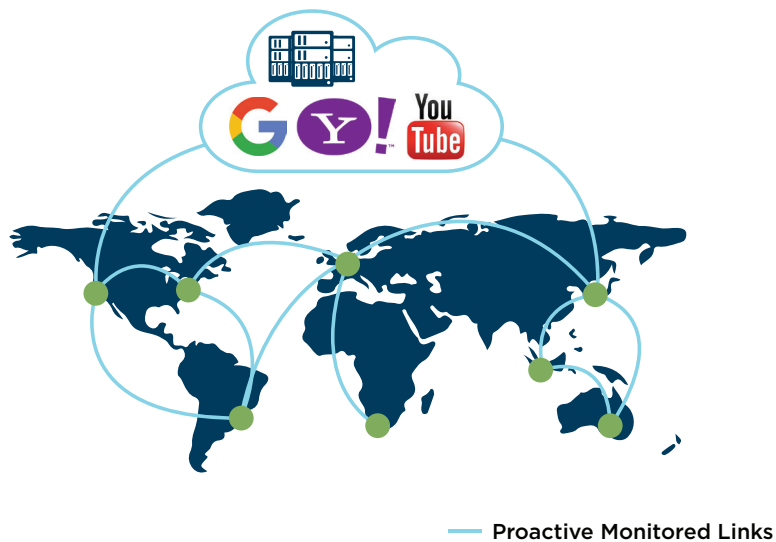
- Significant ROI versus traditional inline security tool deployments
- Reduced security costs through more efficient use of tool resources
- Zero downtime security tool configuration changes and upgrades
- No impact capacity additions or new security tool deployments
- Greater uptime for security resources 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, IxVision 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, IxVision 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 Ixia's visibility solutions and IxVision at <http://www.ixiacom.com/solutions/visibility>.

### END NOTES:

- Application Drives the Need for Application Strengthening, Presented by Zeus Kerravala, January 2016.
- "The State of Application Performance Monitoring", Ixia Inc., February 2016.
- "Ixia Brings Application and Threat Intelligence to Network Visibility", Ixia press release, December 17, 2014
- The University of Texas at Austin Case Study, Ixia, December 2015. [http://www.ixiacom.com/sites/default/files/resources/case-study/ut-success\\_stories.pdf](http://www.ixiacom.com/sites/default/files/resources/case-study/ut-success_stories.pdf)

### IXIA WORLDWIDE HEADQUARTERS

26601 AGOURA RD.  
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)  
1.877.367.4942

(OUTSIDE NORTH AMERICA)  
+1.818.871.1800  
(FAX) 1.818.871.1805

[WWW.IXIACOM.COM](http://WWW.IXIACOM.COM)

### IXIA EUROPEAN HEADQUARTERS

IXIA TECHNOLOGIES EUROPE LTD  
CLARION HOUSE, NORREYS DRIVE  
MAIDENHEAD SL6 4FL  
UNITED KINGDOM

SALES +44.1628.408750  
(FAX) +44.1628.639916

### IXIA ASIA PACIFIC HEADQUARTERS

101 THOMSON ROAD,  
#29-04/05 UNITED SQUARE,  
SINGAPORE 307591

SALES +65.6332.0125  
(FAX) +65.6332.0127