5 WAYS TO IMPROVE ROI WITH

Network Packet Brokers

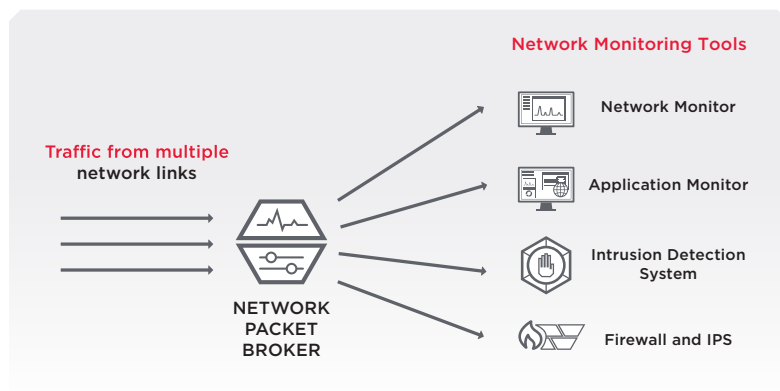**ixia**

A Keysight Business

Introduction

A compelling ROI analysis is the difference between a successfully funded IT project, and one that gets canceled. This is especially true for relatively new technologies that are not well understood by IT management.

The ROI of your network infrastructure is based on two pillars: performance and effectiveness. Network packet brokers (NPBs) offer direct benefits to network operations and security in both areas.

By reading this eBook, you will learn five different ways you can use NPBs to improve your network architecture ROI:

1. Expedite troubleshooting

2. Detect breaches faster

3. Reduce the processing burden on your existing tools

4. Extend tool life after a network upgrade

5. Streamline regulatory compliance

What is an NPB?

A network packet broker is a device that aggregates data flows from across the network, manipulates the data as configured by the user, and delivers it to security and monitoring tools. It acts as an abstraction layer, extracting data from the network, and as a "broker", or "dealer", distributing the relevant data to the relevant tools.

NPBs can deal data from:

- one network link, to one tool
- one network link, to multiple tools
- multiple network links, to one tool
- multiple network links, to multiple tools

Ultimately, NPBs make monitoring and security tools more effective, by giving them access to a range of data across the entire network. By using NPBs, you can reduce blind spots and offer tools the visibility they need to identify and tackle performance and security threats.

Read this brochure to find out more about network packet brokers and why you need one.

# Contents

CHAPTER 1

Expedite Troubleshooting

CHAPTER 1
Expedite Troubleshooting

Unplanned network downtime is expensive, and the cost only increases with each passing minute — by $8,851 to be exact.1 The average unplanned outage lasts 95 minutes, so expediting troubleshooting and reducing mean time to resolution (MTTR) helps save time and money.2

NPBs speed troubleshooting and improve MTTR by filtering data. This helps pinpoint the cause of the problem: Is it a specific device type, a particular application, or is something else causing the outage? Intelligent NPBs filter packet data at layers 2 through 7 — by geolocation, operating system, device type, application type, IP address, browser, carrier, and more. Having this context helps you to pinpoint network issues and resolve them quickly.
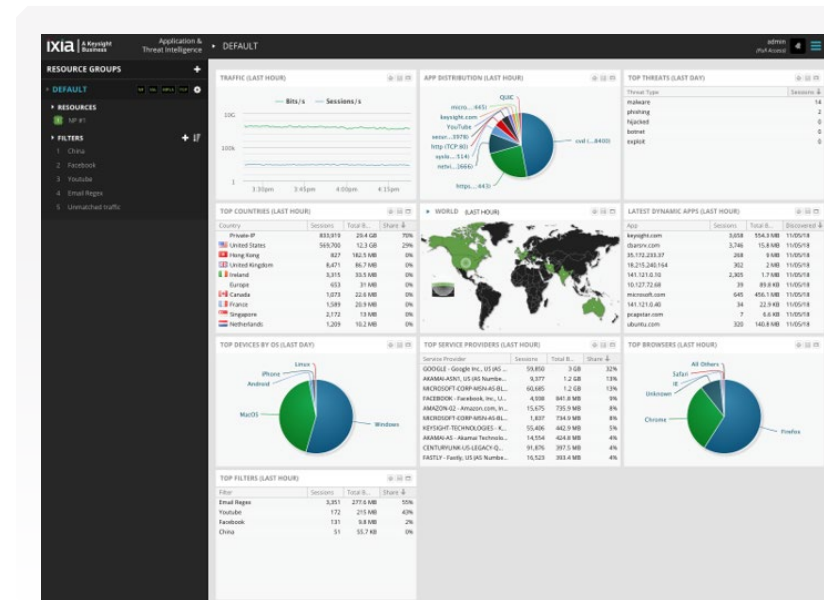
Learn how Ixia's application intelligent filtering solution, AppStack, reduces troubleshooting time and MTTR.

---

1 "Cost of Data Center Outages," Data Center Performance Benchmark Series, Ponemon Institute, January 2016, pg. 14.

2 "Cost of Data Center Outages," pg. 7.

NPBs also reduce MTTR by eliminating IT change board approvals. Change boards are common in large enterprises and approvals are often tedious. Members of the board must discuss and decide whether to implement a change to the production network, as such changes may cause a disruption or an outage.

A change board meeting is no longer needed since NPBs are already installed and running on the network. There is no risk of a disruption or outage from equipment installation, and analysis and troubleshooting happen immediately. The reduction in MTTR easily offsets the initial cost of purchasing and installing the NPB and provides a strong ROI.

CHAPTER 2

Detect Breaches Faster

CHAPTER 2

Detect Breaches Faster

IT teams face an average of over 174,000 alerts per week.[1] The deluge of alerts and false alarms often leads to alert fatigue and creates the risk of serious network threats going uninvestigated. Not investigating a single serious threat is costly. In 2018, the average cost to discover, mitigate, and recover from a breach was $3.86 million.[2]

NPBs help mitigate alert fatigue and lessen the alert burden on security teams, both of which help teams and tools detect breaches faster. This translates to increased team productivity, driving ROI for the solution. NPBs provide several capabilities which help IT teams decrease breach detection time and drive ROI for the NPB solution.

They include:

- Traffic decryption
- NetFlow metadata generation
- Threat intelligence feed integration

1 "The State of SOAR Report, 2018," Demisto, pg. 4.
2 "2018 Cost of a Data Breach Study: Global Overview," IBM Security and Ponemon Institute, July 2018, pg. 3.

Over half of all internet traffic is encrypted, and encrypted attacks are on the rise, too.1 SonicWall reported that encrypted attacks increased by 27% from 2017 to 2018 and show no signs of slowing down in the future.2 Not all security tools can decrypt traffic for inspection. In other instances, data privacy requirements prohibit IT from decrypting and storing personal data embedded in encrypted traffic. And finally, some security tools suffer performance degradation when decryption is turned on.

If these issues affect your organization, it is possible that encryption-cloaked malware is entering your network with a free pass. By deploying an NPB with decryption capabilities, you ensure encrypted malware does not sneak by with legitimate encrypted traffic. This drives ROI for your NPB and tool infrastructure.

When investigating a potential breach, you can greatly increase efficiency by configuring an NPB to generate detailed NetFlow metadata. Enriched NetFlow data can be used by your current security tools, so you can identify and categorize breaches faster.
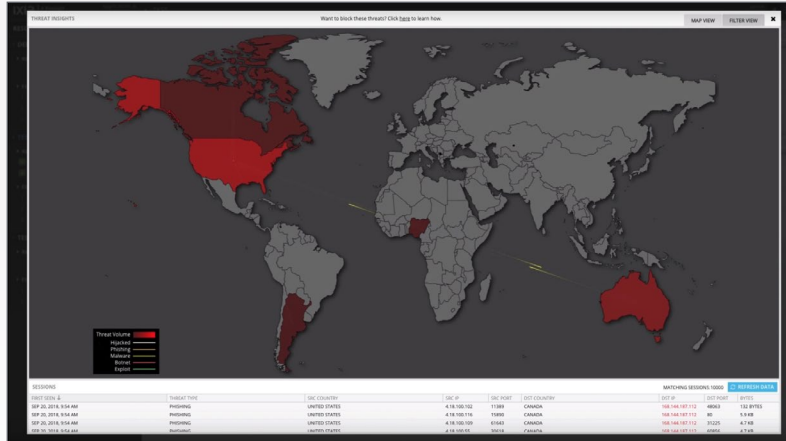
LEARN MORE

Read this case study to learn how a bank used SSL decryption to reduce security threats
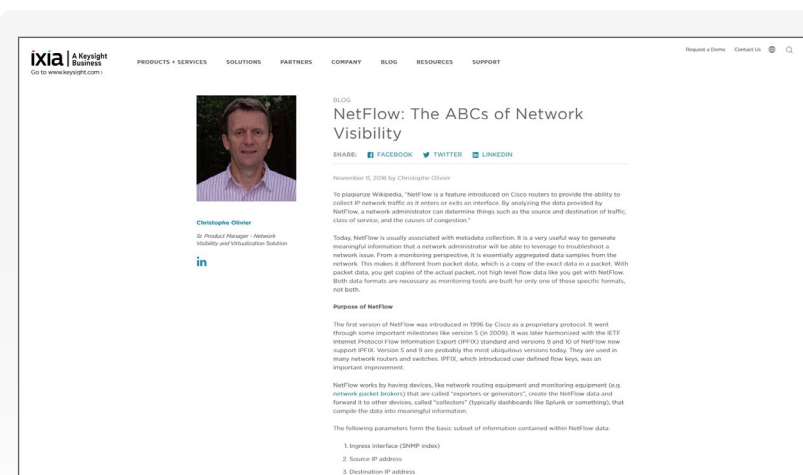
LEARN MORE

Learn more about Ixia's enriched and customizable NetFlow metadata generator, IxFlow, in this blog.

1 Finley, Klint, "Half the Web is Now Encrypted. That Makes Everyone Safer," Wired, January 30, 2017, https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/

2 "2019 Sonicwall Cyber Threat Report," Sonicwall, 2019, pg. 31.

Advanced NPBs deliver application awareness and threat intelligence. Ixia NPBs incorporate threat intelligence feeds into their data analysis process. This provides security teams with valuable information and additional control points for decision making, breach detection, and breach prevention.

Integrated threat intelligence enables the NPB to detect and filter certain types of threats. This allows the NPB to flag suspicious activity from untrusted users, so you can pinpoint where an attack originates. These capabilities reduce the load on other tools, minimize breach detection time, and drive ROI for your tool infrastructure.

LEARN MORE

Watch this video to learn more about Ixia's Threat Insights feature.
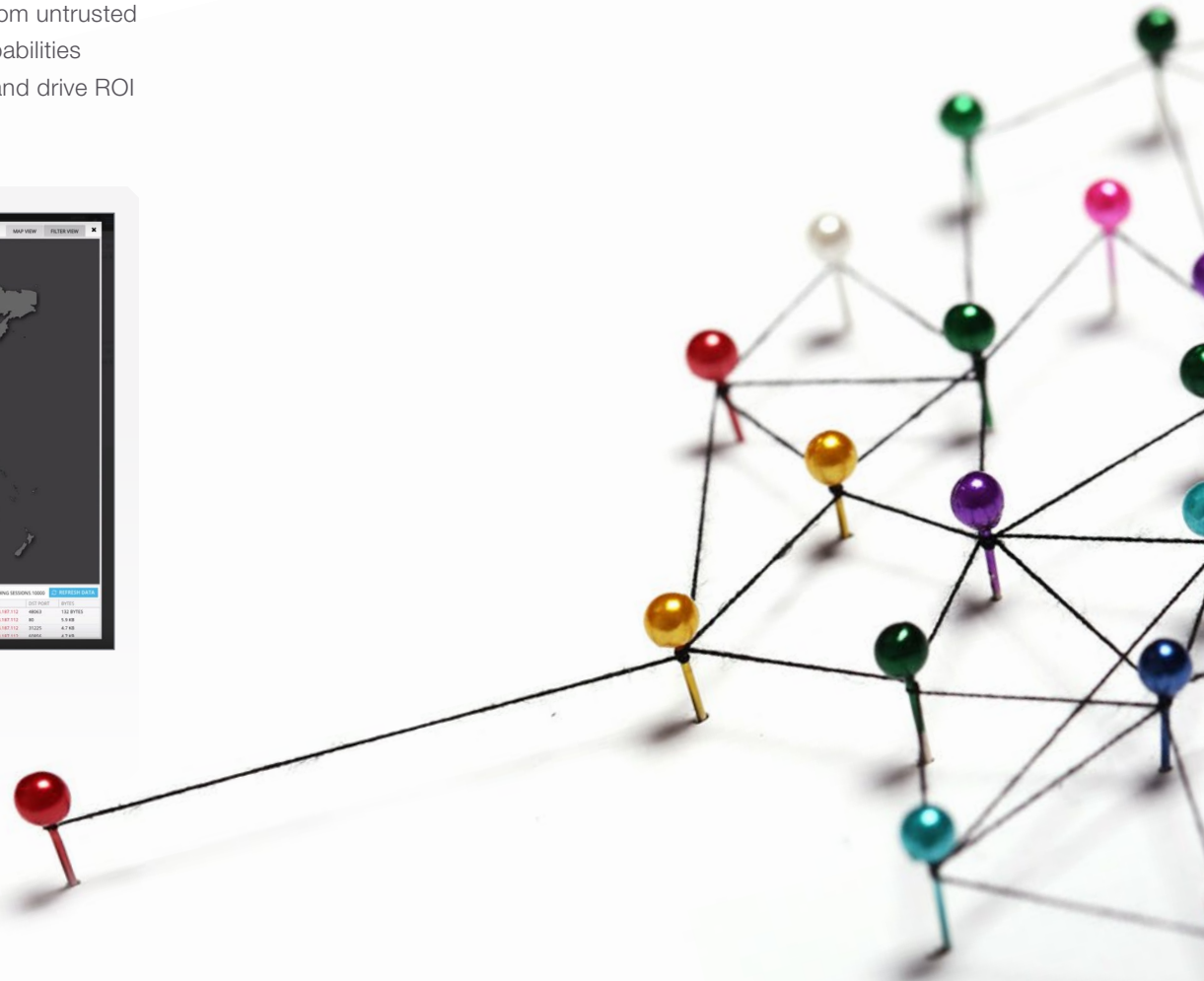
CHAPTER 3

Reduce the Burden on Your Tools

CHAPTER 3

Reduce the Burden on Your Tools

Global Internet Protocol (IP) traffic levels are expected to reach 4.8 ZB in 2022.1 That is more than triple the levels in 2017. Most organizations respond to traffic growth by purchasing and deploying more security and monitoring tools. But tripling your monitoring capacity every five years is an expensive proposition and increases to network complexity. An alternate way to deal with traffic growth is to route unthreatening traffic around your tools.

---

1 "Cisco Visual Networking Index: Forecast and Trends, 2017-2022," Cisco, 2019, pg. 1.

For example, if your Intrusion Detection System (IDS) operates at maximum capacity, it may cause slowdowns, or miss critical threats. Advanced NPBs are application-intelligent, which means they can identify and filter all, or specific, application data out of the data stream that flows to your IDS. This allows your IDS, or other tools, to work more efficiently, extends the deployment life of your IDS, and improves ROI.

The University of Texas at Austin reduced the load on its intrusion detection system (IDS) by 20-30% after implementing Ixia's data filtering solution.

LEARN MORE

Read the UT Austin case study here.

NPBs further reduce the load on tools by deduplicating and trimming traffic. Typically, you collect data from several places within the network, which often leads to the collection of duplicate data packets. If you aggregate the flows to an NPB, the NPB can deduplicate that data, so that your tools receive only one unique packet flow.

LEARN MORE

Learn more about Ixia's header stripping and packet trimming capabilities with PacketStack.

Furthermore, if a tool only needs the header of a packet or certain information in the middle of the packet for analysis, the NPB can send only that data. Instead of sending the entire packet, the NPB can strip the header or trim the packet and forward only the necessary information. This reduces the size of the packets delivered to the tools and the load on the tools. Such reductions directly increase the performance and longevity of those tools, improving the ROI of your NPB.

CHAPTER 4

Extend Tool Life After a Network Upgrade

CHAPTER 4

Extend Tool Life After a Network Upgrade

Cloud computing and the Internet of Things are driving massive growth in enterprise traffic, especially at the network edge. By 2025, IDC predicts that 150 billion connected devices will exist globally.[1] Users will expect exceptional speed, reliability, and quality of service. This will require you to upgrade your network, which you cannot do all at once.

After a network upgrade, existing tools may quickly get overloaded. NPBs load balance high-volume traffic to multiple tools, so you can scale your infrastructure without replacing it. As the core network speed continues to increase and as your tools age, NPBs also load balance higher–data rate traffic across lower–data rate tools. This extends the life of your existing security and monitoring tools.

LEARN MORE

Learn how you can get more value from your existing security and monitoring tools in this solution brief.

---

1 David Reinsel, John Gantz, John Rydning, "The Digitization of the World – From Edge to Core," Data Age 2025, IDC, pg. 13

A high-density, high-availability, modular NPB chassis provides long-term protection. It allows your monitoring infrastructure to scale and maximizes your network uptime over time. This reduces the need for maintenance windows to upgrade the hardware as traffic volumes increase.

Like a high-performance network switch, a modular NPB consolidates many traffic flows in one place. This results in fewer consoles to manage, less tools to purchase, and a more efficient use of rack space, all of which contribute to the ROI of the solution.

LEARN MORE

Learn more about Ixia's solution for large and growing data centers, Vision X.

CHAPTER 5

Streamline Regulatory Compliance

CHAPTER 5

Streamline Regulatory Compliance

If personal data or financial data traverses your network, regulatory compliance standards require you to protect that information while remaining transparent. Local, federal, and international laws may require proof of compliance. Two ways in which NPBs streamline regulatory compliance audits are data masking and traffic encryption. NPBs can perform both, at the same time.

Phone numbers, email addresses, credit card numbers, and social security numbers circulate our networks around the clock. It is crucial to keep sensitive personally identifiable information (PII) safe and secure.

Hackers can easily exploit cleartext data. Because of this, regulations often require encryption when data is in motion. By keeping data encrypted and using the latest encryption standards, you make it harder for hackers to attack your network.

NPBs can decrypt traffic and send it to security tools for analysis. If you deploy them inline, NPBs can also re-encrypt traffic before sending it onward through the network.

Decrypting data creates the risk of exposing sensitive PII when passing data to tools. You can mitigate this risk by masking sensitive information before passing it to other tools. Advanced NPBs can mask the sensitive data that a hacker seeks.
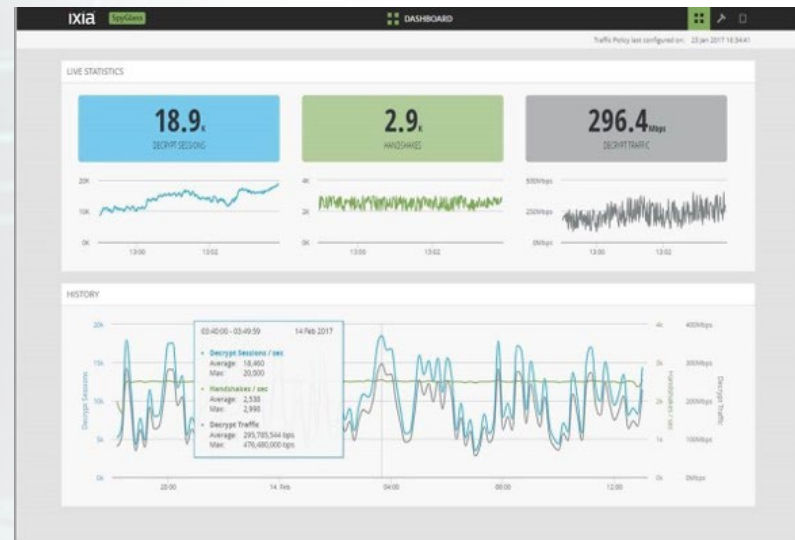
LEARN MORE

Learn more about the new TLS 1.3 encryption standards and Ixia's Active SSL encryption in this webinar.

Data masking occurs when pre-defined patterns or configurable offsets are used to mask specific information in a data packet. The NPB decrypts the incoming data, masks the important stuff (which the tools do not need to see anyway), sends the data to the tools for analysis, receives the data back from the tools, re-encrypts the data, and forwards it on through the network.

Using your NPB for encryption and data masking means you do not need to spend money on additional tools with those capabilities. Furthermore, it decreases the work load on your tools that can decrypt, encrypt, and mask data. This lets your tools focus on the tasks they were meant to do, like intrusion prevention and performance monitoring. The NPB provides encryption and data masking which improves overall ROI.

LEARN MORE

Read this application note for quick tips to improve network compliance with a visibility architecture.

CHAPTER 6

Summary

CHAPTER 6

Summary

A network packet broker is central to your network visibility strategy. Without an NPB, your network coverage is only as robust as your tools. How long will it take you to troubleshoot an outage, identify a performance problem, or detect a security breach?

NPBs give you visibility and over time, they pay for themselves many times over. They help on all network management fronts, including:

- Troubleshooting
- Breach detection
- Tool performance
- Tool longevity
- Regulatory compliance enforcement

Ixia's Vision X — A Network Packet Broker For Your Growing Data Center

- Expand your data center without losing visibility, and without replacing your legacy analysis and security tools.

- Monitor and aggregate up to 6 Tbps of total traffic from the edge to the core for analysis.

- Manage security and privacy compliance, while maintaining a superior user experience.

- Process up to 2 Tbps of data, at speeds from 10 to 100GB, in 3 rack units.

- Future-proof your network for next-generation technology upgrades.

Visit the web page here.