Executive Summary

Today's increasing network complexities require tools that offer detailed visibility into the network traffic. These tools enable the IT team to increase its awareness of the traffic characteristics and potential anomalies of their network. It is this awareness that provides network visibility and enables the IT team to make confident decisions in:

1. Planning for network and resources,
2. Mitigating network faults rapidly to reduce network downtime,
3. Ensuring proper performance of applications and maintain or exceed their consumer satisfaction, and
4. Fighting off unauthorized access to their networks.

Strong network visibility solutions also help extend the life and increase the efficiency of existing network monitoring and defense tools (hereinafter referred to analytical tools) such as Network and Application Monitors, IDS/IPS, and Firewall. They ensure that the network and business key performance indicators (KPI) remain at healthy levels.

ACG Research conducted an economic analysis of three separate scenarios (out-of-band, inline and data center virtualization) and used conservative assumptions in saving levels for deployment of Ixia's network visibility solutions, specifically Vision ONE. The analysis covered the reduction in cost-increase of the current network analytical tools, such as firewall, IDS/IPS, as well as cost savings in:

1. Lowering network downtime,
2. Mitigating network defects, that is, Mean-Time-To-Repair (MTTR)
3. Avoiding regulatory non-compliance, for example, HIPAA, inability to offer adequate lawful intercept, federal and state fines for lost records, and
4. Reducing costs of security breach, such as loss of revenue, post data-breach activities (such as legal and administrative activities), and cost of lost customer records.

The analysis was performed against "do-it-yourself" or "do-nothing" scenarios.

KEY FINDINGS

Ixia's suite of Network Visibility solutions enables the IT team to manage and run the company's network with deeper knowledge of the network traffic characteristics for out-of-band, inline and virtualized network infrastructures, while providing the following economic results over a three years, based on ACG Research's findings:

- Out-of-Band: ROI at 415%, IRR at 300% and a cumulative cash flow of $761.5 thousand
- Inline: ROI at 489%, IRR at 320% and a cumulative cash flow of $715 thousand
- Data center (virtualization): ROI at 108%, IRR of 173% and a cumulative cash flow of $1.7 million

Introduction

Today's increasing network complexities offer unprecedented challenges to IT teams. A major consequence of the complexity is that the network is now operating at unacceptable levels of risks and threats. Add the new mega-trend in cloud networking and the need to manage security becomes even more prevalent, especially, in a hybrid network architecture. This necessitates a solid plan to secure the network from attackers and their goals to disrupt business operations or attempting to gain access to vital information to conduct criminal activities, for example, ransom demands. Protection of an enterprise network from malicious intrusions is critical to the health and viability of that enterprise. Examples of cyber-attacks abound as they are used to exploit an enterprise for a variety of purposes, for example, theft of customer information. For example, global DDoS attacks continue to grow at the rate of data traffic growth. By 2020, it will grow 2.6X to 17 million. To further exacerbate the situation, as network security is improved, network functionality can become more complicated.

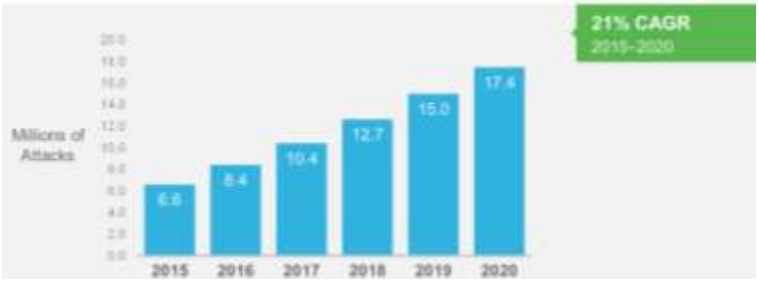

Figure 1. Global DDoS Attack Forecast[1]

Compounding the security issues, the IT personnel are faced with additional challenges in ensuring a smooth running network that delivers the network and application performance expectations of the enterprise. This is vital to ensure customers' satisfaction and maintain a competitive edge. Additionally, it helps IT with its forecast in resource and capacity planning to stay within the company's budgets. Clearly, tools are needed that can be used to objectively assess the security risk in an enterprise's network.

The trend to virtualization has created additional challenges for the IT team: virtual machines (VM) continuously travel from one server to another and the use of a simple "physical probe" from one server does not offer the full picture for a particular application. There is a need for analytical tools to travel with the VMs to make it easier for the IT team to analyze traffic patterns for the network and applications.

Currently, system administrators utilize their experience and "gut-feelings" to assess and mitigate security risks in a network. This is equivalent to throwing darts to make decisions when purchasing stocks and securities.

These challenges require proven solutions that enable the IT teams to rapidly integrate and use powerful tools to identify problems, get a clearer picture of the network operations and performance, and solve them with minimal or no impact on the company's daily business.

[1] Cisco VNI Global IP Traffic Forecast, 2015–2020.

A variety of network analytical tools are currently available to help monitor and protect the network: Firewall, IDS/IPS, Network and Application Performance Monitoring, and Threat Prevention platforms. These tools are invaluable to the IT team to protect their network, find faults, defend against malicious attacks and mitigate network defects. As the network grows, these tools will have to scale in size, capability and cost. It is, however, possible to manage and contain the growth in costs for these tools and create a network environment that:

1. Protects from threat vectors,
2. Monitors network/application performance, and
3. Assists the IT team to plan network resource and capacity with confidence.

These are achieved via network visibility solutions.

This paper focuses on the merits of visibility solutions for three different scenarios:

- Out-of-band: Collecting information in real time to be analyzed at a later time,
- Inline: Collecting information and acting upon the information in real time to ensure increased availability and performance of the network,
- Virtual data center: Collecting information from virtual machines, running virtualized applications, virtual network functions (VNF), as they may move from server to server for much better network visibility.

The business scenarios explore savings from a variety of network and business operations problems such as downtime, network defects, security breaches and noncompliance with regulatory requirements.

Ixia offers, IxVision, a visibility solution that covers these scenarios. This paper will provide ACG's KPI calculations for insertions of these tools in a network that demonstrates network visibility advantages over do-it-yourself or do-nothing scenarios.

Economics of Network Non/Low-Visibility

The increase in the level of awareness of the network traffic is a major goal for the IT team. It is this awareness that provides network visibility that enables the team to make confident decisions in:

1. Planning for networks and resource,
2. Mitigating network faults rapidly to reduce network downtime,
3. Ensuring proper performance of applications and maintain or exceed their consumers' satisfaction, and
4. Fighting off unauthorized access to their networks.

Various metrics have been offered by the industry and academia to quantify visibility, for example, Mean Time to Security Failure, Mean Effort to Security Failure, and Common Vulnerability Scoring System, which is an open framework used to address the different vulnerability of the different hardware and software components in a network. However, there are no published standards for these metrics, similar to, for example, five 9s high-availability requirements for service providers' network devices. Most companies have their own empirical data on these metrics and for business reasons are reluctant to make them public until they visibly affect their customers in a major way, for example,

cyber-attack against Sony Picture Entertainment in 2014 when private emails were released and employees were locked out of their accounts[2]. Other network issues such as down time can greatly affect a business KPI, resulting in lower revenue levels, damaging reputation and customer dissatisfaction/churn. This can especially be painful for companies in the Internet commerce business, for example, in 2013, the Amazon.com website went down for 30 to 40 minutes, costing the company between $3 and $4 million dollars[3].

As their existing network infrastructures pivot to virtualization and data centers, enterprises face new challenges that were not present in legacy networks, for example, having the same level of awareness for virtualized network functions and applications as they continuously move from server to server. This results in new challenges in network visibility for enterprises. How do you track and analyze a moving target? Low visibility in virtualized infrastructures has exacted a high cost on the owners. A recent report by the Ponemon Institute measured the cost of network down time due to unplanned data center outages[4]. According to the study, the average cost of a data center outage has steadily increased from $505,502 in 2010 to $740,357 in 2016 (or a 38% net change from the 2013 report). Other findings from the report include:

1. Down-time costs for the most data center-dependent businesses are rising faster than average.
2. Maximum downtime costs increased 32% since 2013 and 81% since 2010.
3. Maximum down-time costs for 2016 are $2,409,991.
4. Cybercrime represents the fastest growing cause of data center outages, rising from 2% of outages in 2010 to 18% in 2013 to 22% in the latest study.

These are especially problematic for financial institutions that saw a 43% rise in cyber-breaches from hacking or malware[5] in the first half of 2016.

A multitude of tools are available that help the network operator/IT team to combat these challenges. At the device level, these include firewalls, application and network performance monitors, intrusion detection and prevention systems, forensics, lawful intercept, etc. These are quite effective tools and greatly increase the network visibility for the IT team. The cost for deployment of these devices is directly related to the size of the network and as a network scales, so do these tools. Also, a failure in one piece of equipment can greatly reduce the visibility, albeit temporarily, until it is replaced. Meanwhile, as a matter of course, CFOs are always looking for cost containment strategies.

At the network device level, there are tools that increase visibility, as well. Switches and routers offer port mirroring (or SPAN ports) to intercept and record the data traffic within the network. The limitations of SPAN ports are well documented:

1. They need to be programmed and reprogrammed as the network changes and the network could potentially suffer from human errors,
2. The analysis of the data that they provide is time consuming and sometimes manual,

[2] https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack.

[3] http://www.fool.com/investing/general/2013/08/20/heres-how-much-yesterdays-outage-cost-amazon.aspx.

[4] http://www.emersonnetworkpower.com/en-US/Resources/Market/Data-Center/Latest-Thinking/Ponemon/Documents/2016-Cost-of-Data-Center-Outages-FINAL-2.pdf.

[5] http://www.wsj.com/articles/the-big-number-43-1468900861.

3. Usually, only a limited number (for example, two) of ports are free of charge. If more are needed, they cost the same as any other port on the switch or router.

The use of SPAN ports could potentially increase the mean-time-to-repair (MTTR) as network configuration changes could affect the data received by network monitoring tools and potential loss of corporate data. To account for these, additional time is spent to simply inform the higher management and receive confirmation to reconfigure SPAN ports. Finally, SPAN ports are not effective in a virtualized data center scenario as the traffic that goes through a specific port within a server can belong to different applications as the VNFs move from server to server.

A new set of capabilities are now available that address these issues to strongly increase network visibility in real time (inline) or out-of-band. Solutions are also available that greatly enhance data center visibility as they move with the virtual machines that carry the VNFs. These solutions also help contain the rise of costs in existing network analytic tools by lowering their scale.

Ixia offers the IxVision visibility architecture to help the IT team increase its network visibility and contain its cost levels. The economic advantage of this is discussed later in this paper. An examination of cost components of inadequate network visibility solutions is given next.

Cost Components of Inadequate Network Visibility

The cost components can be divided into two major categories: tangible costs and intangible costs. The former covers the increasing cost of the current network analytic tools, such as firewall, IDS/IPS. The latter covers cost factors such as:

1. Network downtime,
2. MTTR,
3. Regulatory noncompliance, for example, HIPAA, inability to offer adequate lawful intercept, federal and state fines for lost records,
4. Security breaches can be divided into sub-components such as loss of revenue, post data-breach activities (such as legal and administrative activities), and cost of lost customer records.

Ponemon Institute's research approach to "activity-based costing" utilized the following cost components, which are closely in line with the previously mentioned factors:

1. Damage to mission-critical data
2. Impact of downtime on organizational productivity
3. Damages to equipment and other assets
4. Cost to detect and remediate systems and core business processes
5. Legal and regulatory impact, including litigation defense cost
6. Lost confidence and trust among key stakeholders
7. Diminishment of marketplace brand and reputation[6]

These cost components are used to determine Ixia's IxVision value in the following sections.

[6] For additional information see: https://www.ixiacom.com/sites/default/files/2016-04/Ixia-360-Security.pdf.

Ixia's Network Visibility Solutions

IxVision enables maximization of network monitoring effectiveness. The solution consists of two basic elements: taps and network packet brokers (NPB). Taps are essentially data collection points for monitoring data and NPBs are used for data aggregation, filtering, load balancing, and packet manipulation before the data is passed on to special purpose monitoring tools. Taps and NPBs can be combined to cover three different solution sets: out-of-band, inline, and virtual data center.

The physical taps that are used for out-of-band scenario are similar to SPAN ports but are independent of network devices and are passive and do not affect network connectivity ports. They make complete copies of network traffic as they pass through regardless of the contents of the packets. They are superior to SPAN ports in that no programming is required and they are used as set-it and forget-it modes, for example, no (re)programming is needed.

For inline network traffic access, bypass switches (called iBpyass), are used in place of physical taps. No copies of the network traffic are made, instead all traffic is sent to an inline tool where it is analyzed and placed on the network path only if it is safe to do so. Because of its criticality, iBypass switches can be deployed in an active/active or active/standby redundancy mode to protect the mission-critical network traffic from bad or malicious packets. Additionally, Ixia's IxVision inline solution can reduce the cost of network tool ownership through reduction of scale and eliminate single points of failures. Figures 2 and 3 show the before and after diagrams of a network without and with visibility solutions. Figures 2 shows a network that has deployed network tools and depicts scale and equipment failure scenarios. Figure 3 shows the impact of introducing Ixia's IxVision inline solution, which will load balance inbound traffic. Its benefits include:

- Scale multiple network equipment tools for high bandwidth inspection
- Offer high availability with (active/active) or (active/standby) for mission-critical applications
- Load balancing capability ensures continuity with security appliances
- Security inspection at the high performance levels

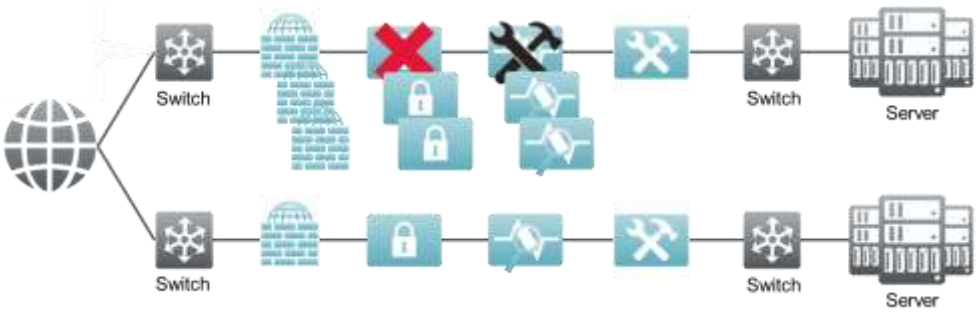

Figure 2. The Network with No Visibility Tools

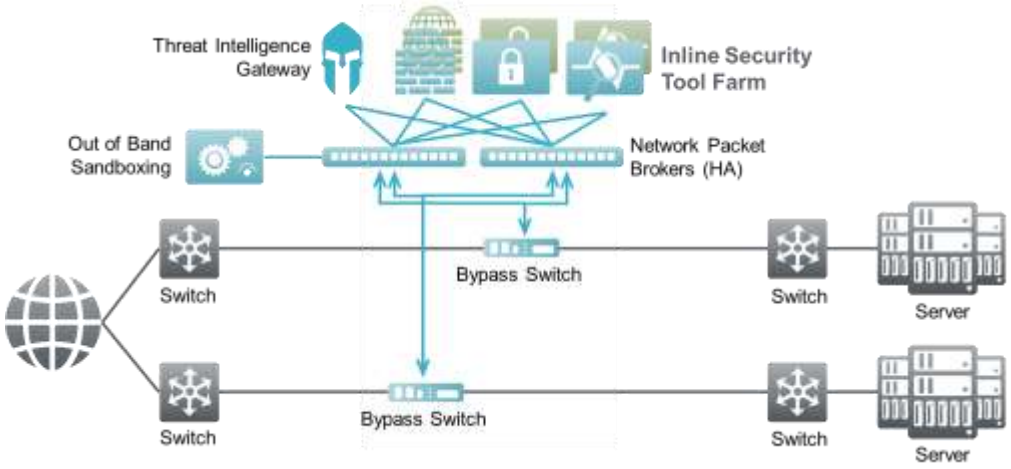

Figure 3. The Network with Visibility Tools

For data centers, Ixia offers its visibility solution with Vision ONE and its virtual tap (vTap) software product. vTaps are integrated within the Hypervisors (for example, VMware, KVM) that run the VMs hosting VNFs. vTaps travel with the VMs if they move from one server to another. They can monitor inter or intra VM traffic to continuously provide network traffic for specific applications (or VNFs) to Vision ONE.

For any of these cases, the main technical objective of visibility solutions is to ensure that the health and the viability of the network traffic are not compromised. Financially, they maximize the value of existing network analytical equipment in addition to reduction in noncompliance to regulatory requirements, security breaches, network downtime and rapid recovery from network defects. For additional information on Ixia's visibility solutions refer to this document[7].

Vision ONE advanced features are enhanced with its Advanced Application and Intelligent Processor (ATIP), which offers the ability to dynamically detect new and unknown applications. This processor also provides granular application behavior, user geo-location, mobile device identifier, SSL decryption, data masking, and browser information. It delivers real-time application data to monitoring tools[8].

Business Analysis Ixia's Network Visibility Solutions

To examine Ixia network visibility solutions' economic advantages, ACG Research conducted an analysis of three different network scenarios where these solutions were deployed: out-of-band, inline and virtualized network (data center). The economic advantages stem from different areas such as extension of life and efficiency of network analytic tools, resulting in lower investment levels in these expensive tools. ACG considered other areas of cost savings (security breaches, noncompliance, network down time and network defects) that result from deployment of IxVision solution. Each area was assigned a (conservative) probability of improvement when Ixia's solutions are integrated in the network.

[7] https://www.ixiacom.com/resources/white-paper-5-ways-maximize-value-security-and-monitoring-tools.
[8] https://www.ixiacom.com/resources/ixia-application-and-threat-intelligence-processor.

Ixia's breadth of products offers different solutions for different network sizes. The scenarios focused on different network sizes: small, medium and large based on the network traffic volume. For each scenario, ACG used the following Ixia products:

1. Out-of-band: Vision ONE plus Ixia's Flex Taps. Analysis was also conducted without the Taps using SPAN ports only
2. Inline: Vision ONE plus iBypass switches
3. Virtual networking, data center: Vision ONE plus virtual taps

The analyses were done against "do-it-yourself" or "do-nothing" scenarios. In both cases, ACG assumed the introduction of additional network analytic tools as the network expands and requires it. The do-it-yourself scenario (out-of-band) assumes that the IT team uses its own time to program SPAN ports and makes network changes as required.

Analysis of Ixia's Out-of-Band Visibility Solution

Table 1 summarizes the variables that were used for analysis and quantification of Ixia's visibility solution advantages. The analysis was done for Vision ONE with Flex Taps. The probability assigned for improvements in network issues are set to conservative levels.

Scenario Assumptions: Three Years	
Sustained network traffic volume (Year 1), Mbps	1000
CAGR in network traffic	60%
Number of customers, that is, customers of the enterprise	2500
Network segments	3
SPAN ports per switch	2
Probability in increasing network analytical tools life span	30%
Probability in reduction of security breaches	10%
Cost of lost record per customer	$225
Probability in reduction of network down time	30%
Probability in reduction of MTTR	25%
Probability of reduction in noncompliance fees	20%

Table 1. Out-Of-Band Scenario Assumptions

Out-of-Band: TCO Results and Cash Flow Analysis

TCO based IRR and ROI analyses were conducted over three years, and the study found a TCO based ROI level of **415%** and IRR of **300%** when Ixia solutions (Vision ONE plus Flex Taps) are introduced in the network. Figure 4 shows the TCO and cash flow advantages versus a do-it-yourself scenario.

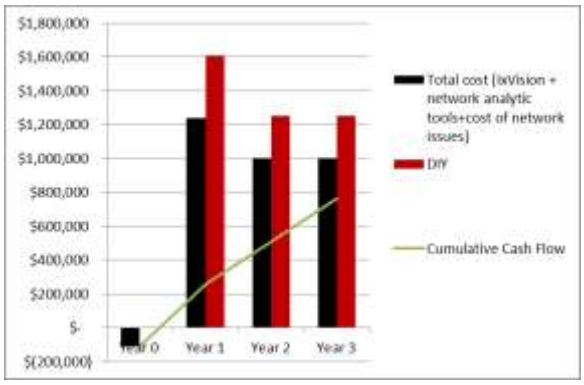

Figure 4. TCO & Cash Flow Comparison

Analysis of Ixia's Inline Visibility Solution

Table 2 summarizes the variables that were used for analysis and quantification of Ixia's visibility solution advantages. The analysis was done for the Vision ONE packet broker plus Ixia's iBypass switches.

Scenario Assumptions: Three Years	
Sustained network traffic volume (Year 1), Mbps	1000
CAGR in network traffic	60%
Number of customers, that is, customers of the enterprise	2500
Network segments	3
Probability in increasing network analytical tools life span	30%
Probability in reduction of security breaches	10%
Cost of lost record per customer	$225
Probability in reduction of network down time	30%
Probability in reduction of MTTR	25%
Probability of reduction in noncompliance fees	20%

Table 2. Inline Scenario Assumptions

Inline: TCO Results and Cash Flow Analysis

TCO based IRR and ROI analyses were conducted over three years; the study found a TCO based ROI level of **489%** and IRR of **320%** when Ixia solutions (Vision ONE plus iBypass switches) are introduced in the network. Figure 5 shows the TCO and cash flow advantages versus a do-nothing scenario.

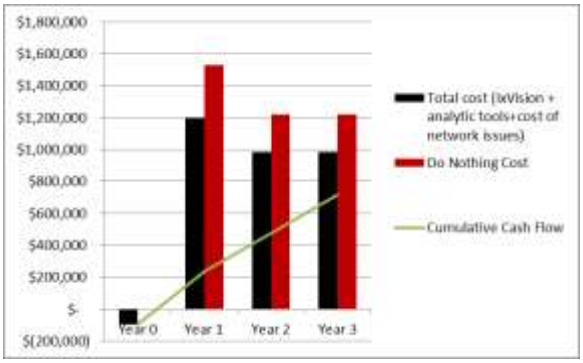

Figure 5. TCO & Cash Flow Comparison

Analysis of Ixia's Virtual Data Center Visibility Solution

Table 3 summarizes the variables that were used for analysis and quantification of Ixia's visibility tools advantages. The analysis was done using Vision ONE plus virtual taps.

Scenario Assumptions: Three Years	
Sustained network traffic volume (Year 1), Mbps	1000
CAGR in network traffic	60%
Number of customers	2500
Network data centers	3
Probability in increasing network analytical tools life span	50%
Probability in reduction of security breaches	10%
Cost of lost record per customer	$225
Probability in reduction of network downtime	30%
Probability of reduction in noncompliance fees	40%

Table 3. Data Center (Virtualization) Scenario Assumptions

Virtual Data Center: TCO Results and Cash Flow Analysis

TCO based IRR and ROI analyses were conducted over three years, and the study found a TCO based ROI level of **108%** and IRR of **173%** when Ixia solutions (Vision ONE plus virtual taps) are introduced in the network. Figure 6 shows the TCO and cash flow advantages versus a do-nothing scenario.

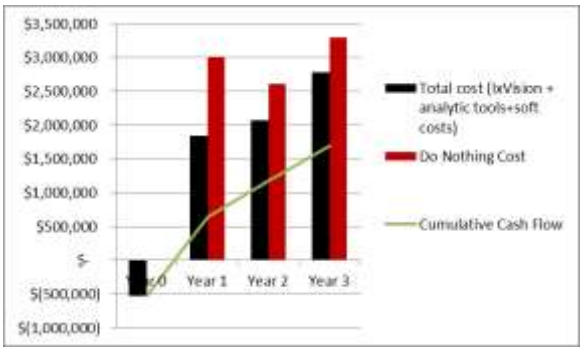

Figure 6. TCO & Cash Flow Comparison

Conclusion

Service continuity to customers, adherance to SLA clauses and having predictive key performance indicators for their network operations are important KPIs for any business. To satisfy these requirements, vendors must offer solutions that provide strong network visibility to minimize network down time and lower operational costs, such as costs stemming from network down time, security breaches and regulatory noncompliance. The solution must be flexible and powerful to give the ability of out-of-band, and inline network monitoring and managements. With the advent of virtualization, the need for strong visibility tools also becomes necessary.

Ixia offers a suite of network visibility solutions that are capable of addressing all of the visibility requirements of businesses. The solutions cover a varity of network sizes and capabilities.

ACG Research conducted its analysis of several Ixia visibility solutions for out-of-band, inline, and virtual data centers. Specifically for its Vision ONE product, which can be deployed for all scenarios, ACG found the following KPIs, calculated over three years and using conservative assumptions in savings levels:

1. Out-of-band: ROI at 415%, IRR at 300% and a cumulative cash flow of $761.5 K
2. Inline: ROI at 489%, IRR at 320% and a cumulative cash flow of $715 K
3. Data center (virtualization): ROI at 108%, IRR of 173% and a cumulative cash flow of $1.7 M

The calculations show that Ixia's network visibility tools enable the IT team to better manage the network and mitigate network issues with confidence. They also keep the CFOs content, offering excellent KPIs even with conservative assumptions.