Ixia Security Fabric™

Security Through Visibility, Context, and Simplicity

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Ixia

November 2016

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary 1

The Traditional Perimeter is Flawed 2

Detection Requires Rich Data 2

Analysis Requires Efficient Traffic Delivery 3

Timeliness: The Key to Reducing Breach Damage 3

Ixia Security Fabric: Providing Visibility, Context, and Performance 4

EMA Perspective 5

About Ixia 5

APPENDIX A: IPFIX NetFlow and Additional Metadata (IxFlow) Fields (as of October 2016) 6

- Standard Mandatory Fields 6
- Optional Fields 7

Appendix B: Ixia Applications and Application Families (as of October 2016) 8

- Appendix B: Ixia Applications and Application Families (Cont'd) 9

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Executive Summary

Security professionals are overwhelmed by data. There is an overload of information presented to people with limited time and bandwidth. Without context, this information can also overwhelm tools, making security analysts' lives more difficult rather than hastening a path to incident response and resolution. When early detection and discovery fails, advanced persistent threats remain.

With dozens of disparate and often overlapping data sources, early warnings are frequently missed. Security monitoring solutions trigger alerts without adequate context for identification and categorization. In order to be most effective, security intelligence must be coupled with automation and orchestration tools designed specifically for enhanced protection, using information across multiple silos.

This is where Ixia® Security Fabric™ comes in. It facilitates security operations and analysis, acting as an intelligent traffic manager with the ability to direct packets based on numerous administrator-defined criteria and augmenting that traffic with additional data and metadata through network and application protocol analysis. All of this is done to deliver greater context around incidents in a shorter period of time so analysts can achieve results faster. This allows them higher efficiency in operations and gives them time to address other operational issues in a proactive manner.

While this concept originated in network operations, its benefits have much further-reaching effects in the security world. The top four value drivers for Security Fabric include:

- **Visibility** – Illuminating and overseeing network traffic originating from various input sources, including contextual intelligence using both data and metadata
- **Context –** Understanding the information provided by various sources through situational, protocol, behavioral, and time awareness
- **Performance –** Maximizing resources by intelligently routing packets to the tool most appropriate to analyze them, thus protecting tools from unnecessary processing burdens
- **Resilience** – Ensuring continuous function when a link or tool within the chain is overwhelmed or broken

Many point solutions have attempted to solve the context and automation problem using log file aggregation and flow analysis. Unfortunately, these disparate parts do not overcome the most critical shortcomings, notably intelligent traffic management and contextual analysis coupled with a smart console.

The Ixia Security Fabric offers simplicity and performance—a recipe for success!

Many point solutions have attempted to solve the context and automation problem using log file aggregation and flow analysis. Unfortunately, these disparate parts do not overcome the most critical shortcomings.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

The Traditional Perimeter is Flawed

The traditional perimeter no longer provides adequate protection. With a highly remote workforce, an explosion in public cloud services, and a plethora of mobile devices, discovery at the edge has become far less effective than it was five years ago. To make it worse, even those workers and applications previously secure behind the perimeter are now in jeopardy from phishing, drive-by downloads, watering holes, and other social engineering and malware attacks.

In short, there is no longer a traditional boundary. The technologies previously used as staples in perimeter security are not sufficient, so organizations bolster them with more advanced tools that require more data to provide advanced analysis for detection and prevention.

Effective detection and prevention require more data of a better quality delivered in context. There are many tools that need this data to operate effectively. These tools include security incident and event management (SIEM), identity and access management (IAM), security and network analytics, forensics, and remediation platforms.

Detection Requires Rich Data

Gaining ample data and total visibility is critical to making good security decisions. Protection is predicated on adequate detection by downstream resources, while prevention requires ample context by target and upstream resources. Better visibility is also a foundational aspect of achieving early identification of indicators of attack and indicators of compromise that might have otherwise gone unnoticed until much further in the kill chain. Ixia's ability to identify applications and correctly target security devices improves analysis of data, which reduces attacker dwell time and the related financial and reputational impact to the customer. Without ample context, reporting also becomes inaccurate. The Ixia Security Fabric provides real value in several areas.

Ixia's ability to identify applications and correctly target security devices improves analysis of data, which reduces attacker dwell time and the related financial and reputational impact to the customer.

1. Security Fabric supports a broad and rich set of data from hardware, software, and a wide variety of partner solutions. Data ingestion is possible from anywhere in the environment, including virtual and physical systems, either on-premises or in the cloud, and can be distributed to any target security device.
2. Ixia enhances standard Internet Protocol Information Export (IPFIX) NetFlow data with additional data and metadata, providing security operations staff with a deeper understanding of networked communications regardless of physical or logical directionality. There is a large variety of metadata available in the packet and protocol stream, which varies based on the application and protocol. Some examples of metadata are included at the end of the paper.
3. Both physical and virtual traffic can be managed from the logical perspective, "north–south" (client–server) and "east–west" (server–server) traffic. This level of enhanced visibility aids with everything from early detection and incident response through post-incident root cause analysis and, with the right tools, can be used to provide information necessary for operation personnel to proactively identify preventative maintenance needs, further reducing unplanned outages and maintenance costs.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

4. Security Fabric offers highly resilient inline architectures to remove single points and paths of failure, maintaining data flow in an "always available" state for the solutions that need it. For inline security appliances, the Security Fabric architecture leverages a smart bypass switch that can automatically forward traffic around security tools experiencing congestion or that have failed. Paths and devices are monitored through both positive and negative heartbeat injection. Positive heartbeats are added to the packet stream to track path and device health, while negative heartbeats are injected to ensure that security gateways are properly filtering traffic. Security Fabric supports high availability using both serial and parallel network traffic architectures and load balancing to ensure fully redundant packet delivery with near instant failover.

Analysis Requires Efficient Traffic Delivery

Security Fabric delivers traffic optimally to the appropriate security and network monitoring tools, creating enriched data for analysis and action. This creates optimal security tool performance by providing contextual analysis on flows, streams, headers, and packet data with virtually no added network latency. The Security Fabric appliance also provides top-of-the-industry performance using separate and dedicated processors. At a minimum, it can have dedicated, line-rate advanced processing at each of its output ports by leveraging additional accelerator technology (field-programmable gate array (FPGA)) solely for deterministic packet processing. The offload of packet processing from the central processing unit (CPU) allows for faster policy management, while the FPGA is optimized specifically for the packet processing task, which increases throughput. This allows the Security Fabric to maintain all packets in the flows, even at high speed flow under continuous heavy loads.

Ixia identifies traffic type to efficiently deliver information only to the security tools that need it. The context-aware data processing engine passes—or filters—traffic by numerous criteria, including Open Systems Interconnection (OSI) Layers 2 through 4 and very critical, but often unleveraged, Layer 7 application visibility. The Layer 7 application visibility is coupled with real-time geographic filtering, packet type, and device information, quickly turning virtually any data stream into actionable insight. Ixia identifies applications and locations to add intelligence for how to best manage traffic.

Timeliness: The Key to Reducing Breach Damage

Response timeliness requires both speed and focus. Time savings can be realized through both the simple and intuitive front-end graphical user interface (GUI) and the powerful backend processing engine.

Ixia Security Fabric provides simplicity in its modern, drag-and-drop interface and powerful policy editor, overcoming the labor-intensive scripting found in other security traffic delivery packages. This integrated policy management environment is loaded with easy-to-understand checkbox fields to create the Layer 2 through 7 filters quickly and easily.

Ixia's support for over 200 application families[1] out of the box removes the need for analysts to pre-analyze packet flows and create their own application signatures, thus spending more of their valuable time threat hunting, rather than programming. These predefined application signatures, combined with an ability to operate at line speeds, puts both Ixia's Security Fabric and security operations ahead of the game.

[1] Example: Netflix has multiple content families like comedy, horror, drama, etc. These would count as one family rather than multiple application protocols. A list of application families supported at the time of publication is in the appendix.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

For applications not supported out of the box, Security Fabric uses contextual analysis to automatically build profiles for web-based applications. It uses numerous characteristics from URL and port numbers to digital certificates to continuously learn about the application traffic. These profiles are easily editable and can be used as a guide to build custom application signatures. Regular expressions can also be used to identify packets, or specific data within a packet, such as an email address you may want to filter to a recording device.

Security Fabric uses contextual analysis to automatically build profiles for web-based applications.

Developing application signature "recipes" from scratch by capturing and analyzing packets using external applications and writing regular expressions (regex) takes precious time. Also, validating recipes can often be tricky, akin to creating intrusion detection system (IDS) or antivirus signatures, and ultimately, this procedure is prone to errors. Even small errors or variations can cause traffic to be misidentified or missed altogether. As applications are updated or added to the business portfolio, organizations must also maintain those recipes in some sort of application catalog to stay current, further increasing overhead on the already burdened staff.

In addition to filtering, deduplication services are also provided. As a packet traverses multiple monitored links, several copies of the same packet appear. Deduplication removes packets identical to those previously processed, so there are fewer packets to forward to the relevant security tools.[2]

Deduplication is one of the high system utilization functions. Utilizing both the output port processor and the FPGA technology tuned for packet processing drastically increases performance over competing products. The internal architecture provides Ixia's Security Fabric with a stronger foundation for inline and out-of-band security deployments. In testing performed by Tolly, the Security Fabric delivered a steady traffic rate with variable packet sizes and content while performing deduplication and packet brokering services. In some scenarios, traffic rates were more than four times the advertised throughput of a similar competing product without packet loss or significant latency.[3]

Deduplication and filtering can also significantly reduce costs for security tools that license based on ingested or indexed data volumes.

Ixia Security Fabric: Providing Visibility, Context, and Performance

The last benefit of Ixia Security Fabric to call out is its unification, aggregation, and forwarding of traffic, triggering actions to further investigate and remediate threats.

Using the Security Fabric's application intelligence console, powered by the context-aware data processing engine, analysts can quickly create actionable insight into network communications. The Security Fabric's context-aware data processing engine identifies both known and unknown network applications, providing rich data on application behavior and the location of users, mitigating security threats, and identifying trends in application usage.

Network administrators only need to specify the characteristics of traffic they are interested in finding and how that traffic should be presented, even if it is encrypted, provided the administrator can ensure Security Fabric access to the proper encryption keys. Cryptographic processing in hardware rather than software allows greater throughput of application traffic without negative performance impacts. Analysts choose the fields they wish to monitor, and begin realizing value from the Security Fabric in minutes or hours rather than days.

[2] The volume of reduction is highly dependent on the types of traffic in the environment.
[3] http://tolly.com/Docdetail.aspx?Docnumber=216100

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

EMA Perspective

Ultimately, the amount of manual effort a security solution removes from workflows determines its value. Though no single solution solves all security issues, any security solution must minimize the time required to collect, process, and interpret data.

Simple delivery of network traffic to analysis tools is not sufficient. The value is in the ability to bring context and prioritization to change data into useful information. Without delivery precision and context, organizations will continue to overburden security personnel and tools with noise, similar to putting them in a rock concert and telling them to isolate one person's cheers.

Network operations and security operations are collaborating to mitigate security threats—and this is becoming more and more critical to business survival.

By directing traffic to the correct analysis tool with context provided at the time of delivery, organizations gain tremendous speed in their never-ending challenge to focus on the most appropriate/greatest threats. This offers more time to act while avoiding "alert fatigue" and ultimately providing security systems greater leverage and response automation.

Gaining more value from less work, Ixia's Security Fabric offers a better recipe for success. This unique solution unites visibility, context, performance, and resilience in a single network-aware solution. The high-performance, context-aware, security intelligence data processing engine achieves truly loss-less visibility.

The Security Fabric maximizes the use of security analysts' scarce time while protecting environments from known and unknown threats, including advanced persistent threats. In a crowded security marketplace occupied with a variety of point solutions, only Ixia's Security Fabric unites these various activities under a single umbrella.

To locate root cause and resolve problems faster, Ixia's Security Fabric enhances the data and, therefore, the value of existing security tool infrastructure. This goes beyond a simple security delivery platform by directing and augmenting data to the tools that can use it to create actionable threat intelligence specific to the organization.

The Ixia Security Fabric creates context-aware security intelligence then delivers de-duplicated and highly relevant traffic to both inline and out-of-band security tools. It provides data resilience and intelligent processing, creating virtual conduits to ensure that only relevant data is forwarded to each security tool, even at high speeds.

About Ixia

Ixia provides testing, visibility, and security solutions, strengthening applications across physical and virtual networks for enterprises, service providers, and network equipment manufacturers. Ixia offers companies trusted environments in which to develop, deploy, and operate. Customers worldwide rely on Ixia to verify their designs, optimize their performance, and ensure protection of their networks to make their applications stronger. To learn more about Ixia Security Fabric, please visit http://www.ixiacom.com/securityfabric.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

APPENDIX A: IPFIX NetFlow and Additional Metadata (IxFlow) Fields (as of October 2016)

Standard Mandatory Fields

NetFlow Field Name	IPFIX ID	Version	Data Type	Length	Description
Octets	1	9	UINT64	8	Number of Octets for a flow
Packets	2	9	UINT64	8	Number of Packets for a flow
Protocol	4	9	UINT8	1	Protocol
SrcPort	7	9	UINT16	2	Source Port
SrcAddr	8	9	UINT32	4	Source Address
InputInt	10	9	UINT32	4	Ingress Interface
DstPort	11	9	UINT16	2	Destination Port
DstAddr	12	9	UINT32	4	Destination Address
OutputInt	14	9	UINT32	4	Egress Interface
SrcAS	16	9	UINT32	4	BGP Source AS Number
DstAS	17	9	UINT32	4	BGP Destination AS Number
Flow End Reason	136	10	UINT8	1	Reason for Flow Termination
flowStartMilliseconds	152	10	UINT64	8	The Absolute timestamp of the First Packet of This Flow
flowEndMilliseconds	153	10	UINT64	8	The Absolute Timestamp of the Last Packet of this Flow

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Optional Fields

Ixia IxFlow Field	IXIA-IPFIX ID	Data Type	Length	Description
L7 Application ID	110	UINT32	4	Application Identification Number Note: since applications are dynamically detected, this ID is unique to each exporter
L7 Application Name	111	STRING	Variable	Application Name, truncated at 128 characters
Source IP Country Code	120	STRING	4	Two Letter Country Code for the Source IP Address
Source IP Country Name	121	STRING	Variable	Country Name for the Source IP Address, truncated at 128 characters
Source IP Region Code	122	STRING	4	Two Letter Region Code for the Source IP Address
Source IP Region Name	123	STRING	Variable	Region Name for the Source IP Address, truncated at 128 characters
Source IP City Name	125	STRING	Variable	City Name for the Source IP Address, truncated at 128 characters
Source IP Latitude	126	FLOAT32	4	Latitude for the Source IP Address
Source IP Longitude	127	FLOAT32	4	Longitude for the Source IP Address
Destination IP Country Code	140	STRING	4	Two Letter Country Code for the Destination IP Address, truncated at 128 characters
Destination IP Country Name	141	STRING	Variable	Country Name for the Destination IP Address, truncated at 128 characters
Destination IP Region Code	142	STRING	4	Two Letter Region Code for the Destination IP Address, truncated at 128 characters
Destination IP Region Name	143	STRING	Variable	Region Name for the Destination IP Address, truncated at 128 characters
Destination IP City Name	145	STRING	Variable	City Name for the Destination IP Address, truncated at 128 characters
Destination IP Latitude	146	FLOAT32	4	Latitude for the Destination IP Address
Destination IP Longitude	147	FLOAT32	4	Longitude for the Destination IP Address
OS Device ID	160	UINT8	1	Unique ID for Each OS
OS Device Name	161	STRING	Variable	String Containing OS Name, truncated at 128 characters
Browser ID	162	UINT8	1	Unique ID for Each Browser Type
Browser Name	163	STRING	Variable	Unique Name for Each Browser Type
Reverse Octet Delta Count	176	UINT64	8	Byte Count for Server to Client when Exporting Bidirectional Flows
Reverse Packet Delta Count	177	UINT64	8	Packet Count for Server to Client when Exporting Bidirectional Flows
SSL Connection Encryption Type	178	STRING	Variable	When SSL decryption is enabled, the encryption type: 'Encrypted' - flow encrypted and was not decrypted 'Decrypted' - flow encrypted and was decrypted by ATIP 'Cleartext' - flow not encrypted
SSL Encryption Cipher Name	179	STRING	Variable	The Name of the Decryption Cipher Used for Decrypted Flows, truncated at 128 characters
SSL Encryption Key Length	180	UINT16	2	The Bit Length of the Key Used for Decrypted Flows
User Agent	182	STRING	Variable	The User Agent Sent in the Request HTTP Header, truncated at 128 characters
Host Name	183	STRING	Variable	The Hostname Field Sent in the Request HTTP Header, truncated at 128 characters
URI	184	STRING	Variable	The URI Sent in the Request HTTP Header, truncated at 128 characters
DNS	185	STRING	Variable	The DNS TXT Field Sent as Part of a DNS Request/Response, truncated at 128 characters

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Appendix B: Ixia Applications and Application Families (as of October 2016)

050plus	Concur Technologies	Gmail	ipp	MSN
4shared	ConnectBot	Gnutella	iTunes	MSN Messenger Service
9GAG	Coursera Mobile	Goodreads	KakaoTalk	mypeople
AIM	Daily Mail	Google	KakaoTalk Mobile	Netflix
AirDroid	Dailymotion	Google Analytics	Kaspersky Lab	Nico Nico Douga
Al Jazeera	DCE/RPC	Google Cloud Storage	Kik	Nimbuzz
Amazon	DCE/RPC-EPM	Google Earth	Kismet	NNTP
Amazon EC2	Deezer	Google Keep	KLM	ocsp
Amazon Kindle	DepositFiles	Google Maps	KPASSWD	Odnoklassniki
Amazon S3	Desktop Notification	Google Now	La Poste	Office 365
Amazon Video	DICOM	Google Talk	LDAP	Okazii
AOL	Dropbox	Gopher	League of Legends	OpenTable
AOL Mail	eBay	Grooveshark	LINE App	Outlook Web Access
Apache ZooKeeper	EPMD	Gryphon	LinkedIn	PANA
Apple	ESPN	GStatic	LiveScore Mobile	Pandora Media
Ask.com	Eventbrite	Hangouts	LLRP	PayPal
Ask.fm	Evernote	HBO	LPD/LPR	Photobucket
Badoo	Facebook	HDFS	Maaii Mobile	Pinterest
Baidu	Facebook Mobile	HDFS JobTracker	Mail.ru	Plurk
Baidu Tieba	Facetime/iMessage	Hightail	Manolito	Pocket
BBC	FCIP	hike	MessageMe	Pokemon GO
BBC iPlayer	Feedly	HLS	MGCP	POP3
BGP	Fitocracy	hulu	Microsoft Excel	Portmap
Bing	FIX	iCloud Web	Microsoft PowerPoint	PPS
BitTorrent	Flickr	Ident	Microsoft Silverlight	PPTP
Blogger	Flipboard Mobile	IMAP	Microsoft SkyDrive	Profinet/PNIO-CM
Booking.com	Fox News Channel	IMDB	Microsoft Word	PVFS
Box	FTP	iMesh	MiTalk	QQ
CNET	Gadu Gadu	Instagram	MOUNT	QUIC
CNN	GitHub	Internet Relay Chat	MPEG-TS	Continued Next Page

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Appendix B: Ixia Applications and Application Families (Cont'd)

QuizUp	Skype	Tango	Ustream	WordPress.com
Quora	SMPP	TED	Viber Media	Workday
Reddit	SMTP	TFTP	Vimeo	Xunlei
Rediffmail	SMTPS	Tor	Vine	Yahoo!
RPCAP	Snapchat	TPNCP	VNC	Yahoo! Mail
RQUOTA	SNMP	TripAdvisor	Vudu	Yahoo! Messenger
RTMP	SoundCloud	TripAdvisor City Guides Catalog	We Heart It	Yammer
RTPS	SoundHound Mobile	TS2	WebEx	Yelp
Salesforce	SpeedTest Mobile	Tumblr	WeChat	YouTube
Salesforce AppExchange	Spotify	TV4 Play (Sweden)	WhatsApp	YouTube Remote
Salesforce Desk	SRVLOC	Twitch	WikiLeaks	ZDNet
Shazam Entertainment	STAT	TwitPic	Wikipedia	Zendesk
SIP Call	Steam	Twitter Mobile	Windows Live Hotmail	

©2016 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3475.111016