SOLUTION BRIEF

Eastwind Powered by Ixia CloudLens:
Find the Real Threats Before They Find You

Securing the enterprise gets harder every day with threats lurking within hybrid networks, public cloud services, hosted applications, and an unsuspecting mobile workforce. Eastwind Powered by Ixia CloudLens delivers better, faster security intelligence to help your experts isolate the real threats from today's relentless barrage of false positives.

What needs attention and what does not? Which users are involved? Is their behavior strange? What action should be taken right now?

Better, faster decisions start with better, faster visibility. Eastwind Networks has integrated CloudLens from Ixia into its Infrastructure as a Service (IaaS) sensor as part of a complete visibility solution that works across multiple cloud and on-premise platforms. Eastwind Powered by Ixia CloudLens:

- Delivers 100-percent, "any cloud" visibility and cloud-native elasticity
- Provides access to deep packet-level data for enriched security analytics to identify breaches that would go undetected
- Adds continuous real-time and historical monitoring
- Speeds queries and response times and reduces "alert fatigue"

The joint solution takes visibility to the next level with deeper intelligence, automation, and better speed and scale.

EASTWIND

ixia
A Keysight Business

915-8264-01-4081 Rev A

Eastwind for AWS Networks: Breach analytics at scale and speed

Eastwind delivers deeper intelligence from more sources, with richer context. "Automated hunters" work to identify malicious activity that evades other security solutions. Eastwind leverages data from multiple sources including basic log data from cloud providers, vital packet-level data delivered by Ixia CloudLens, and additional context from Amazon Web Services (AWS) metrics reported by Amazon CloudWatch.

Eastwind Cloud Sensors fuse data from machine learning, signatures, and anomaly detection with a fast, powerful query engine allowing users to interpret months' or even years' worth of data. This comprehensive array of sensors and applications gathers telemetry that is then enriched and analyzed by the Eastwind Breach Analytics Cloud to deliver richer security intelligence.

Insight coupled with hindsight: Eastwind delivers a comprehensive array of sensors and applications that gather telemetry which is enriched and analyzed by the Eastwind Breach Analytics Cloud. Automated hunters provide hindsight to identify malicious activity that has evaded other security solutions to help analysts speed the right responses.

A powerful force multiplier, the solution goes beyond simply flagging events that look suspicious by detecting patterns and anomalies that evade other solutions and applying deeper analytics.

Ixia CloudLens: Packet-level data from the public cloud

In reporting performance, public cloud providers share log and flow data that covers the basic "who, where, and when" of a conversation, but offers little to no insight into actual content. CloudLens from Ixia captures the packet-level data your security analysts and tools are accustomed to receiving in traditional data centers. By providing uncensored access to network traffic, CloudLens enables you to build a security architecture that is future proof, for any cloud, anywhere.

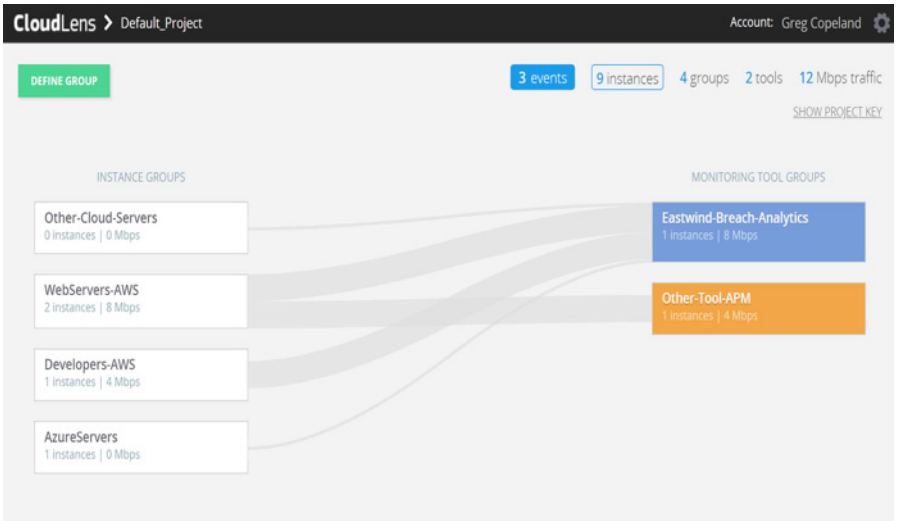
This added depth of insight helps experts identify breaches that can easily go undetected when relying on traditional sources of data. Packet data from CloudLens can be correlated with other Eastwind sources (DNS, SaaS, logs, credentials) for complete context and a single source of truth across hybrid environments.

EASTWIND POWERED BY CLOUDLENS: BUILT FOR SPEED, SCALE, AUTOMATION

Built for the public cloud, the Eastwind Powered by CloudLens solution scales elastically and cost-effectively in tandem with demand. CloudLens sensors gather, filter and groom traffic at the source for efficient delivery to analytics tools both in the cloud and on-premises. Users pay only for what they need without having to backhaul redundant or unneeded packets to the data center.

Integration of the joint solution takes minutes—versus days—as deploying security and network visibility go hand in hand with seamless onboarding of new workloads. Queries are completed quickly so analysts instantly see results and gain insight. Eastwind's Breach Analytics Cloud also converts input to metadata to reduce storage requirements and keep data available for historical trending and monitoring that helps identify threat factors, scope incidents, and reduce "dwell time."

Eastwind Powered by CloudLens adds time-saving automation throughout the process of identifying and remediating threats. New instances are automatically added to the right source and tool groups according to user-defined rules.



Visibility made simple: Ixia's highly intuitive CloudLens GUI makes it easy for users to automate the filtering of data from sources in the cloud to security and performance analysis tools in the cloud as well as traditional data centers.

THE SOLUTION IN ACTION – A REAL-WORLD EXAMPLE

An AWS virtual private cloud (VPC) flow log indicated an unusual level of traffic flowing between two cloud hosts—but did this indicate a security breach, legitimate activity, or a harmless anomaly? Without CloudLens adding context from deep inspection of packet data, it would have been impossible to tell.

Downloading a well-known "test virus" to an EC2 instance with VPC flow logs enabled produces a log line that looks similar to:

```
2018-02-14T20:24:38.000Z 2 369713061426 eni-2443f1ee 172.31.1.254
213.211.198.62 45510 80 6 5 397 1518639878 1518639937 ACCEPT OK
```

Little context is provided in the flow log, and there is no clear way for a security monitoring tool to alert analysts that something of "interest" has just happened and needs to be investigated.

Using CloudLens from Ixia to instrument the same EC2 instance and intelligently mirror packets, rich context was derived from the same network traffic:

Threat Information	
Title	Malicious File
Category	Threat
Priority	High
Message	172.31.1.254 accessed a malicious file from www.eicar.org.
Action	Scan 172.31.1.254 for malware, spyware, or adware.
Application Information	
Application	eicar
Application Hierarchy	tcp > http
URL	www.eicar.org/download/eicar.com
HTTP Code	200
HTTP Method	GET
Category	computing & internet
File Info	
MD5	AA991D6E29BF8EB4C1B56C599DFFCE0A
File Type	data
Size	353.0 B
Requesting Machine	
IP	172.31.1.254
MAC	12:FB:13:AE:28:E9
Port	45510
Bytes Sent	195.0B
Operating System	Linux
Browser	wget
User Agent	Wget/1.15 (linux-gnu)

Responding Machine	
IP	213.211.198.62
IP Owner	IT-Consulting Marc Schneider
Location	Magdeburg, 14, Germany
MAC	12:C0:18:A1:EA:1F
Port	80
Bytes Received	419.0B

Drilling into the packet data gathered by Ixia CloudLens, the Eastwind for AWS Networks solution immediately pivoted to show that the traffic in question was in fact a source of malicious spyware. Automated alerts were triggered prompting proactive action to scan and remove the malware from all the organization's hosted cloud platforms. ***All this took place within moments.***

TRY IT TODAY

Visit https://www.eastwindnetworks.com/cloudlens/ to learn more and request a free 45-day trial of Eastwind Powered by Ixia CloudLens.

ABOUT EASTWIND

Eastwind offers the only breach analytics cloud that provides complete visibility of your key cyber terrain as you undergo digital transformation. We analyze data flowing across hybrid networks and telemetry from cloud providers, hosted applications and mobile workforces—with speed and precision to identify malicious activity, anomalous behavior, insider threats and data leakage. Eastwind enables organizations to embrace emerging technologies such as SaaS and IaaS allowing them to grow with a security first approach.

For more information, visit https://www.eastwindnetworks.com/cloudlens/

ABOUT IXIA VISIBILITY SOLUTIONS

Ixia's Visibility Architecture provides complete visibility into physical and virtual networks, improves security, and optimizes performance monitoring. Each monitoring tool gets exactly the right data needed for analysis to improves the way IT manages data centers and maximize return on investment. Ixia customers include large enterprises, service providers, educational institutions, and government agencies worldwide.

IXIA WORLDWIDE

26601 W. Agoura Road
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

IXIA EUROPE

Harthom Park
Corsham
Wiltshire SN13 ORP
United Kingdom

Sales +44(0)7595.551.047
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127