WHY VISIBILITY IS KEY TO CLOUD SECURITY

Andreas Hünten
Sr. System Engineer, Ixia (a Keysight business)

September 2019

itsa 2019
Die IT-Security Messe und Kongress

SECURITY AND VISIBILITY

ixia

WHY IP PACKETS ARE IMPORTANT FOR SECURITY TOOLS?

You can't protect what you can't see.

ixia

WHY IP PACKETS ARE IMPORTANT FOR SECURITY TOOLS?

Analysis on Log/Metadata info + no IP packets

IP1 TCP:9650 talks to IP2 TCP:80 for 30 seconds

FW/IP reputation. OK. IP1 and IP2 are not blacklisted

WAF. OK. (Let it go thru, I can't see anything else)

SIEM. OK. I don't see any deviation from baseline

Analysis on Log/Metadata info + IP packets

IP1 TCP:9650 talks to IP2 TCP:80 for 30 seconds
+ actual conversation (the IP packets/pcap)

FW/IP reputation. OK. IP1 and IP2 are not blacklisted

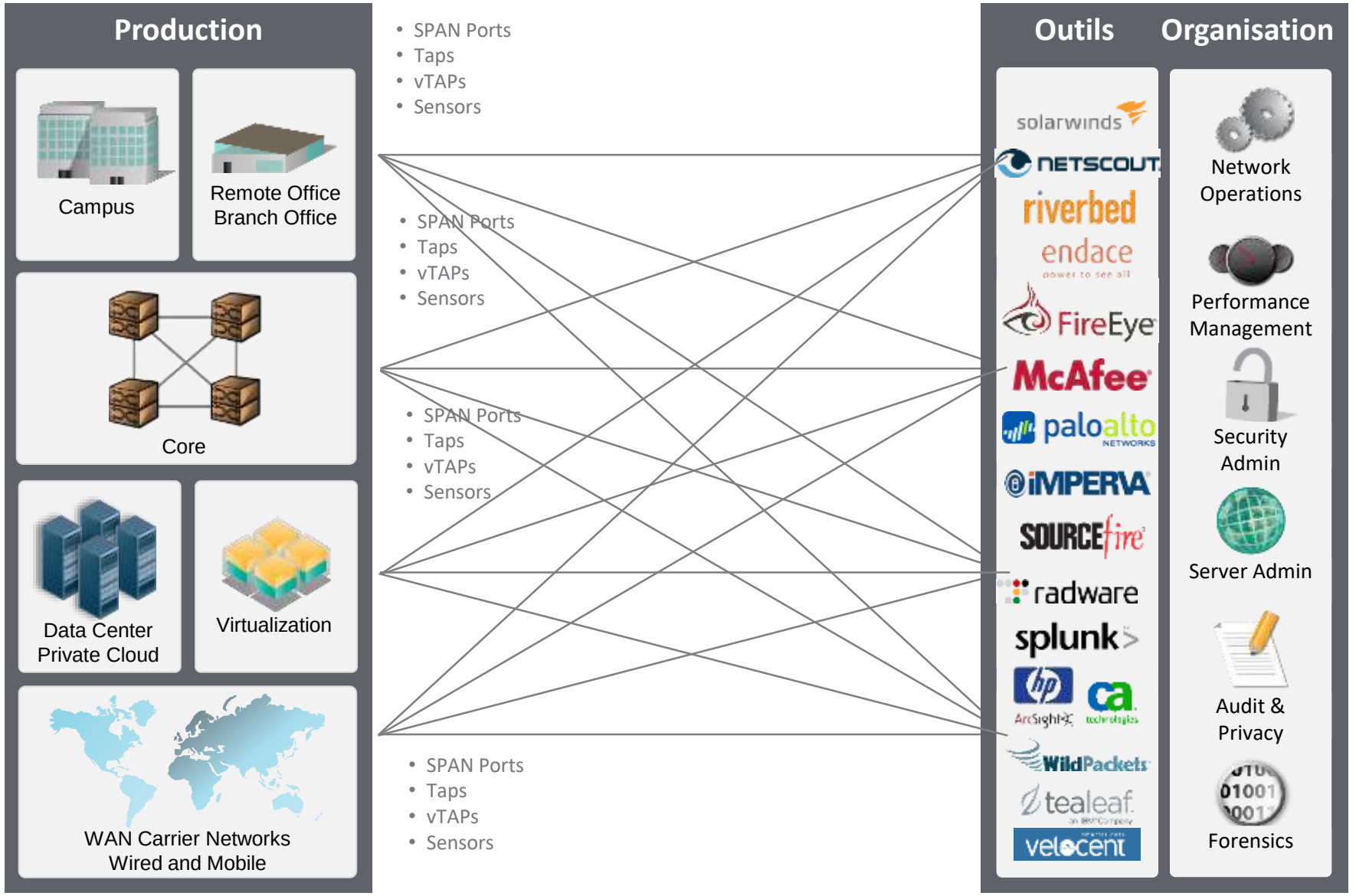
```
SELECT *
FROM customers
WHERE customer_id = '1234567';
DELETE *
FROM customers
WHERE 'x' = 'x'
```

WAF. Hey this looks like a SQLi tautology attack.
Block it !!

Malicious content identified

ixia

HOW TO DELIVER A COPY OF THE RIGHT TRAFFIC TO THE TOOLS



Simple to use

Multiple tools

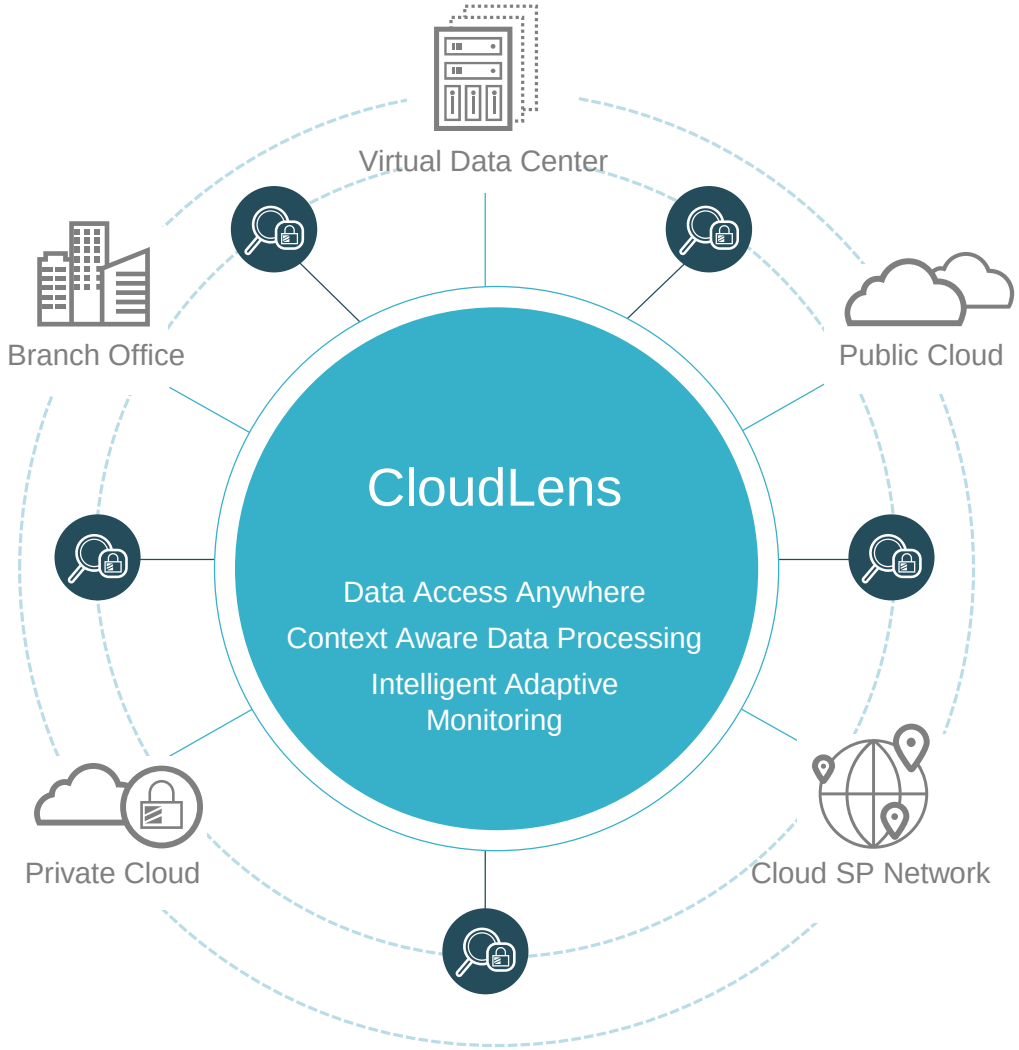
Safe for simultaneous users & tools accessing same source data

ixia

IXIA PROVIDES END-TO-END INSIGHT

- Monitor virtual traffic at the branch office, data center or cloud
- Capture and send packets and flows of interest to monitoring tools
- Support both physical, virtual and cloud environments
- Limit amount, type of data sent to monitoring tools, adjust dynamically

You can't protect what you can't see.

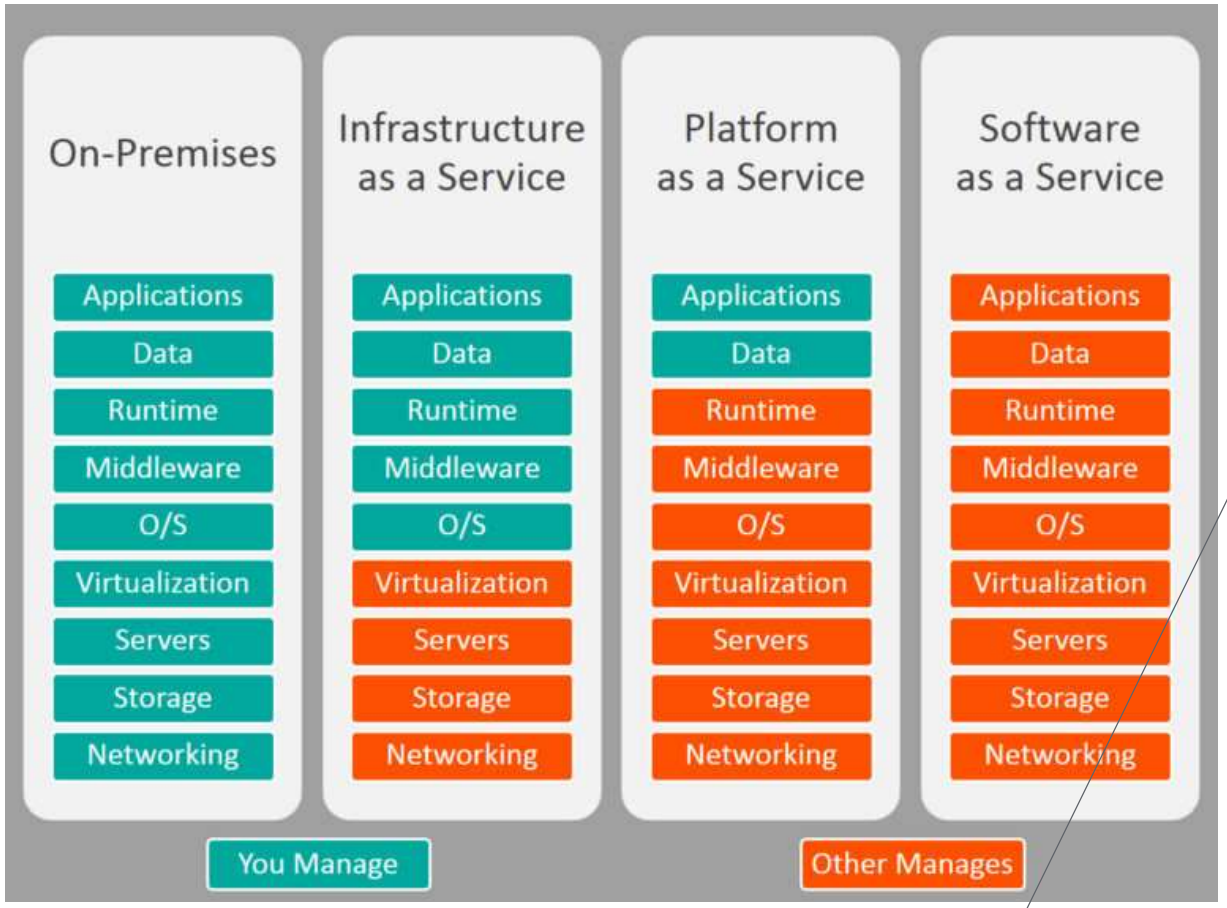


ixia

CLOUDLENS IS BUILT TO HANDLE CLOUD ELASTICITY

ixia

HOW IXIA GIVES YOU VISIBILITY ON EACH CLOUD



Physical Tapping

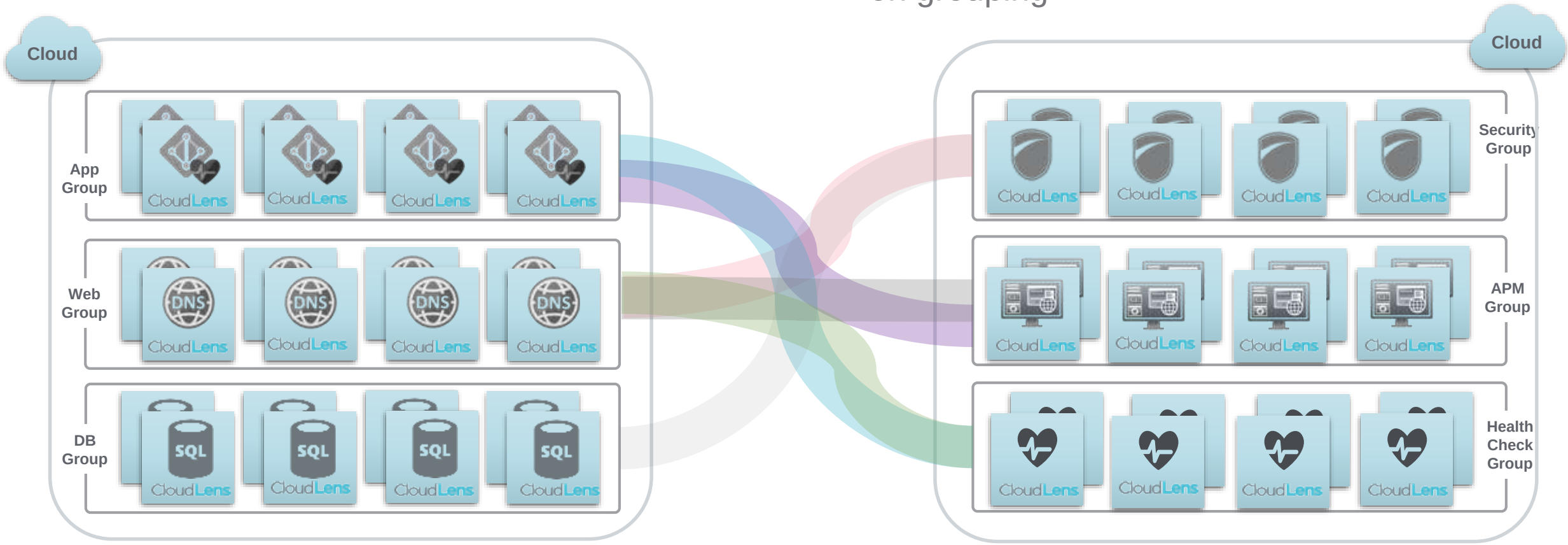
CloudLens sensor

HawkEye Real Services
Office365

ixia

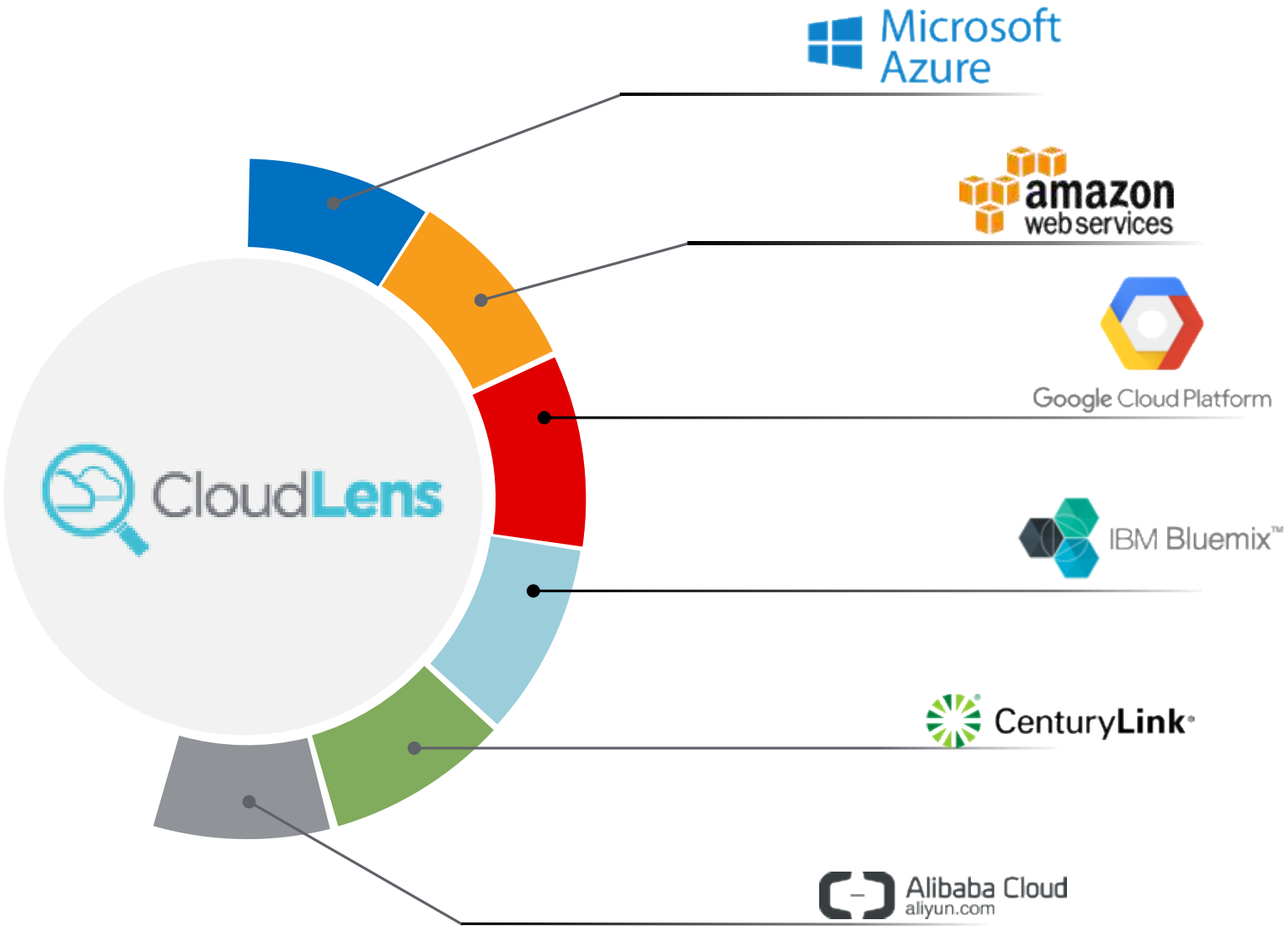
CLOUDLENS IS BUILT TO HANDLE CLOUD ELASTICITY

- New instances are automatically categorized
- Filtering rules are automatically applied based on grouping

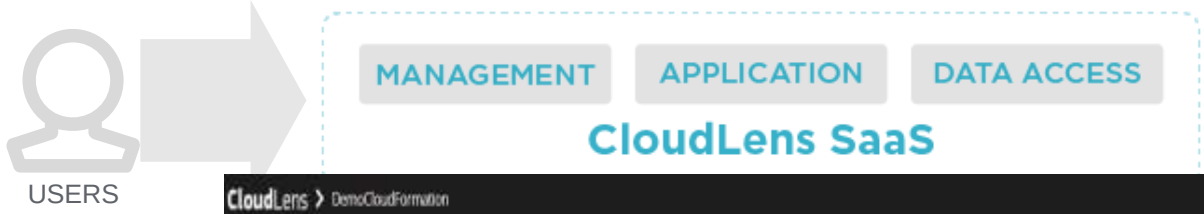


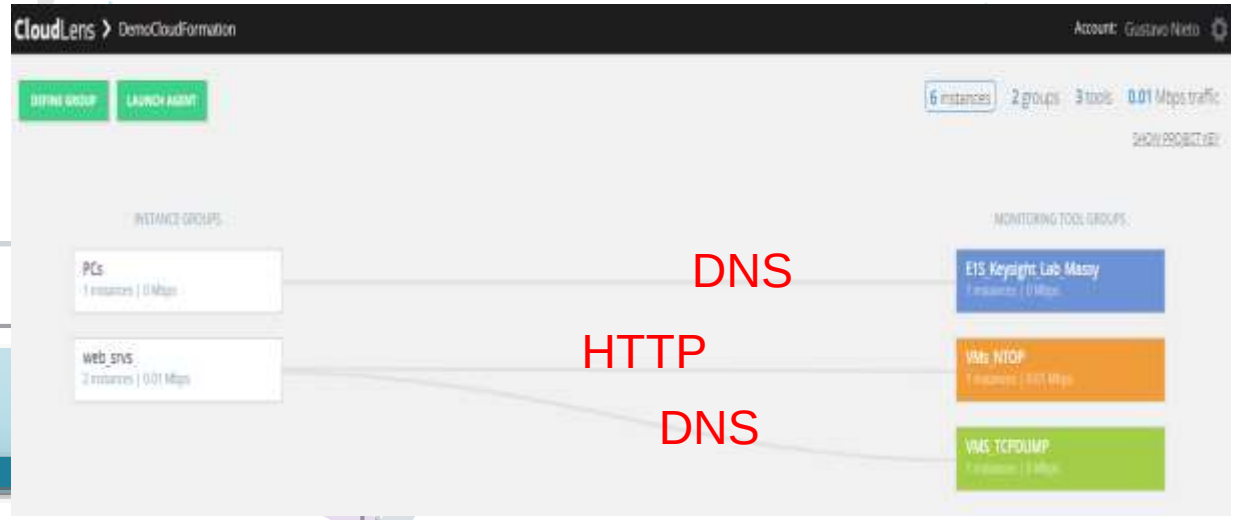
ixia

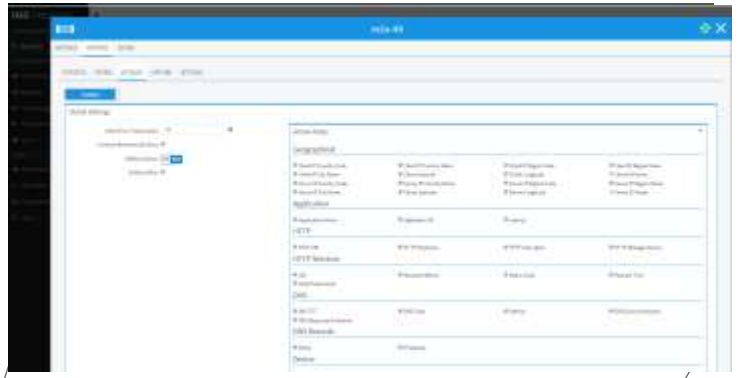
CLOUDLENS MULTI-CLOUD SUPPORT



CLOUDLENS FOR THE HYBRID CLOUD





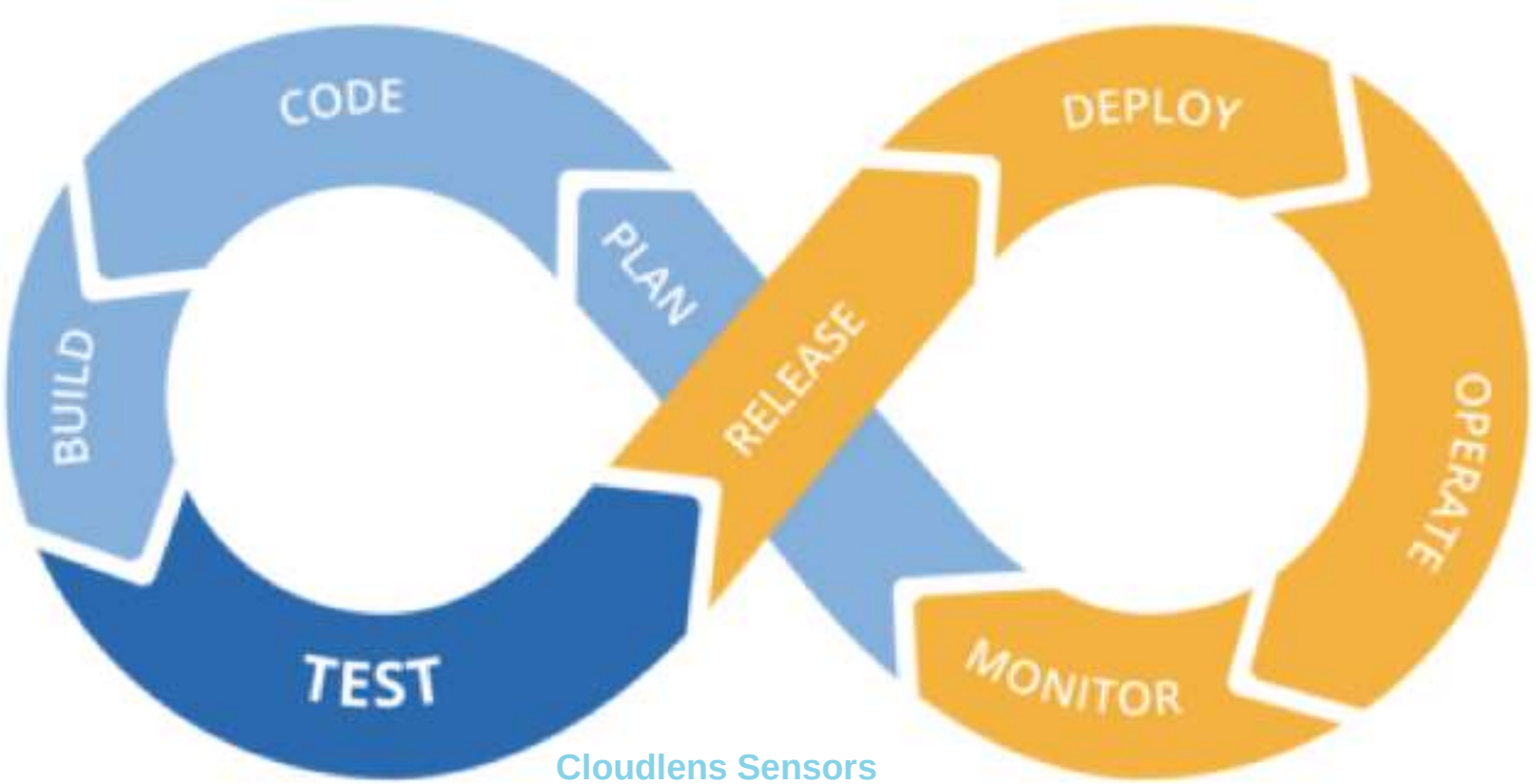


ixia

CLOUDLENS FOR ISOLATED ENVIRONMENTS

ixia

ENHANCING VISIBILITY IN DEVOPS



Cloudlens Sensors

ixia

ACHIEVING VISIBILITY & SECURITY IN THE CLOUD

THE BENEFITS OF CLOUDLENS SAAS

ELASTIC SCALE ON DEMAND

- ✓ CLOUD-NATIVE
- ✓ Scales with the source and tool
- ✓ Automatically load balances

EASY TO USE

- ✓ Drag & Drop Interface (GUI)
- ✓ Dynamic – no dependency on physical location
- ✓ Quick setup process - Installs as Docker container

REDUCE ERRORS

- ✓ Minimal management and configuration
- ✓ Saves time and money
- ✓ Enhanced, intelligent filtering based on instance metadata

ENHANCED SECURITY

- ✓ Visibility into how data is handled and used.
- ✓ Data is stored and managed in compliance with applicable laws, regulations and standards.

All within Ixia's visibility ecosystem –
So customers can achieve their security and compliance objectives in the cloud

ixia

THANK YOU

IN CASE OF QUESTION OR COMMENTS

FEEL FREE TO REACH OUT!

Halle 9, Stand 536

Andreas Hünten
Senior System Engineer, Ixia Solutions Group
Keysight Technologies

e: andreas.huenten@keysight.com
m: +49 (0) 171 845 0465