

WHY **VISIBILITY** IS KEY TO **CLOUD SECURITY**

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

September 2019



SECURITY AND VISIBILITY



Deploying a Layered Visibility and Cybersecurity Architecture

WHITE PAPER

FUNDAMENTAL SHIFT IN GOVERNMENT CYBERSECURITY OCCURRING

It should be no surprise to anyone that government data networks are under a constant threat of attack. According to a Wired Magazine article (Inside The Cyberattack That Shocked The US Government by Brendan I. Koerner), the United States Office of Personnel Management (OPM) website alone is attacked approximately 10 million times per month. However, the discovery of the April 2015 OPM security breach that compromised the personnel records of 80 million Americans was a wake-up call that something needs to be done.

President Trump's Presidential Executive Order 13800 mandates all government agencies to adopt the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Part of the new executive order mandates government networks to operate within a context that supports an Identify, Protect, Detect, Respond, and Recover approach. This includes all of the network, not just security-focused appliances and solutions.

As part of this initiative, there are three actions to consider for strengthening network security and eliminating component obsolescence of critical infrastructure components:

- Understand why your security and visibility architectures should be integrated
- Understand the concept of security resilience and how it helps cybersecurity
- Deploy a visibility architecture to support the NIST cybersecurity initiative

President Trump's Presidential Executive Order 13800 mandates all government agencies to adopt the NIST Framework for Improving Critical Infrastructure Cybersecurity.



ten verhindern lassen.

nfalls eine



SOLUTION BRIEF

Offload SSL Decryption to Improve Security Tool Performance

DEPLOYMENT SCENARIO: INLINE NETWORK VISIBILITY

Most enterprise applications are now encrypted using either the secure sockets layer (SSL) standard or its updated version called transport layer security (TLS). While many security tools include the ability to decrypt traffic so that the incoming data can be analyzed for security purposes, this comes at the expense of CPU performance and can dramatically slow (up to 80%) a security way to maximize your return

extend their lives with a visi

SOLUTION COMPONENT

- Ixia's Network Packet Brokers
- SSL Decryption tool



A STEP-BY-STEP GUIDE TO Securing the Enterprise

With each new device inserted into your network, each new location where you do business, each new service deployed within a cloud, your company's attack surface grows. Securing your business is too vital to your brand reputation to risk going it alone, or relying on piecemeal solutions.

Ixia's 360° approach to securing the enterprise delivers intelligence—and powerful advantages—every step of the way. With hackers becoming ever more industrious, and information technology (IT) more complex,

WHY IP PACKETS ARE IMPORTANT FOR SECURITY TOOLS?

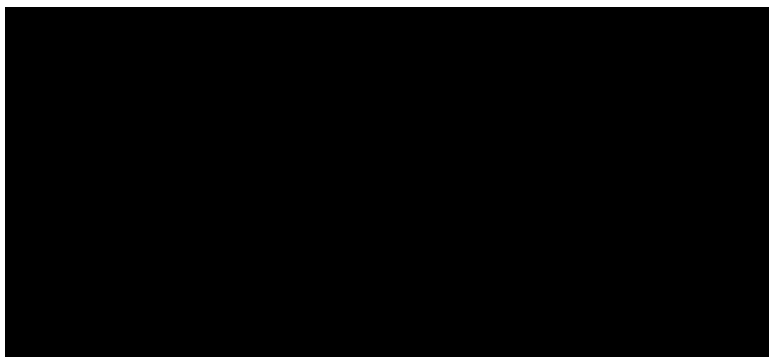
You can't protect what you can't see.

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'
```

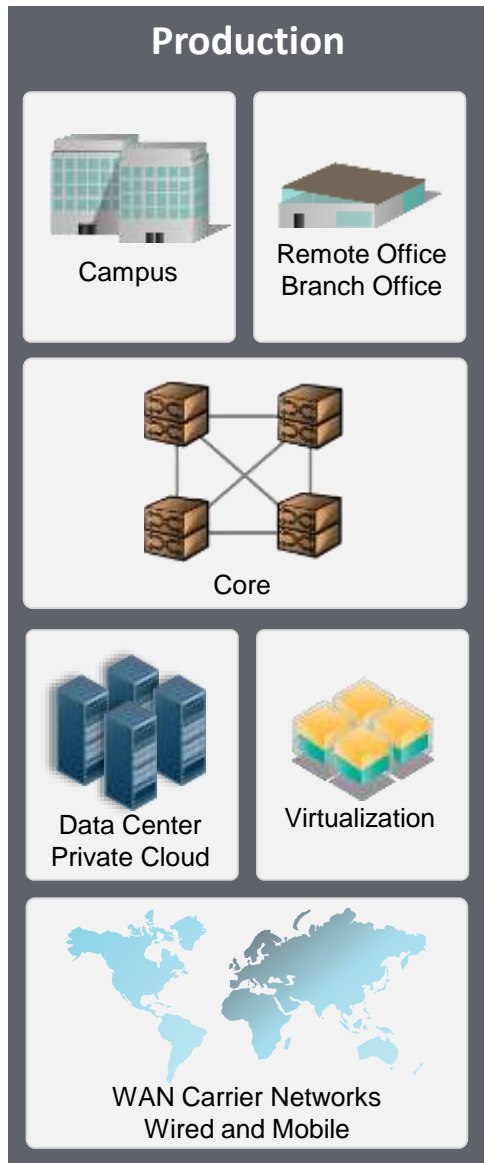


WAF. Hey this looks like a SQLi tautology attack.
Block it !!



Malicious content
identified

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



- SPAN Ports
- Taps
- vTAPs
- Sensors

- SPAN Ports
- Taps
- vTAPs
- Sensors

- SPAN Ports
- Taps
- vTAPs
- Sensors

- SPAN Ports
- Taps
- vTAPs
- Sensors



Simple to use

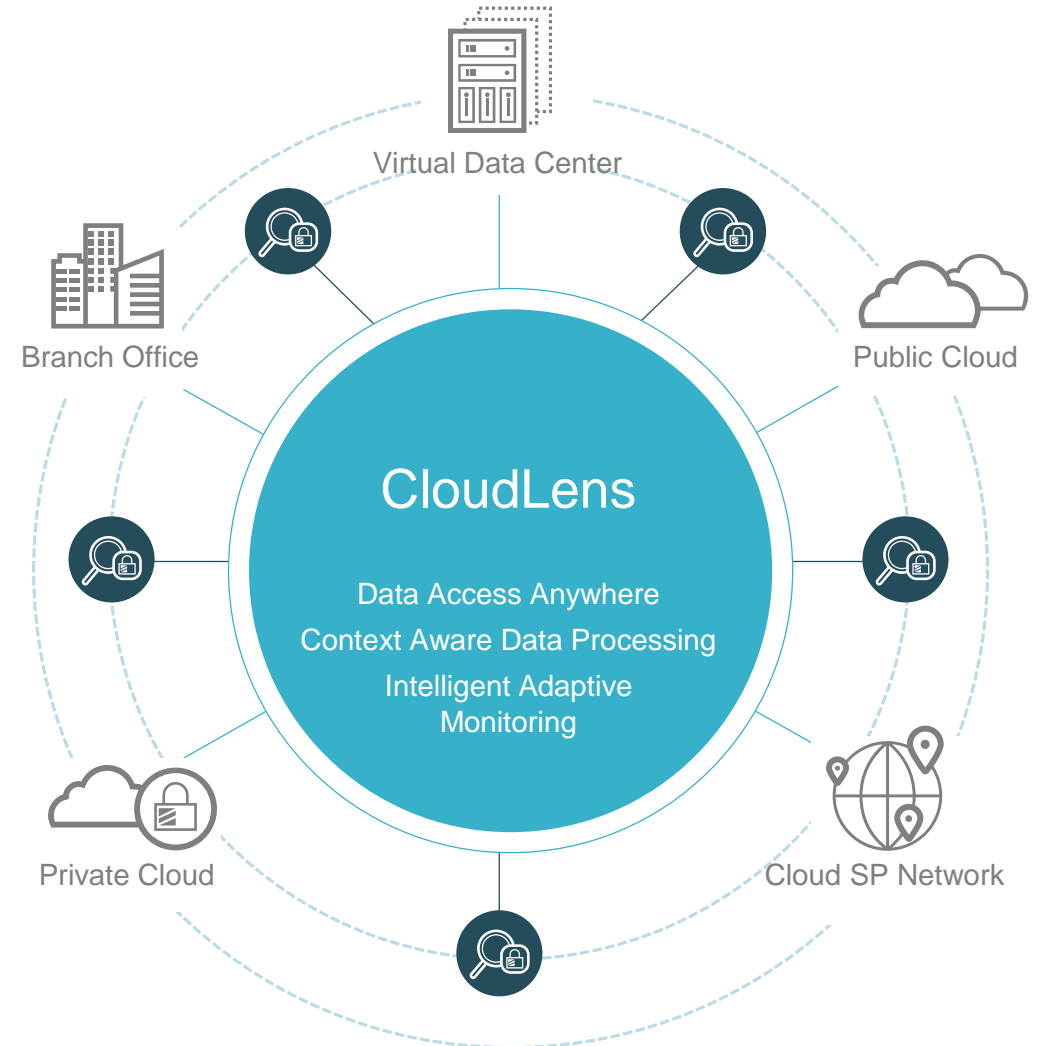
Multiple tools

Safe for simultaneous users & tools accessing same source data

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

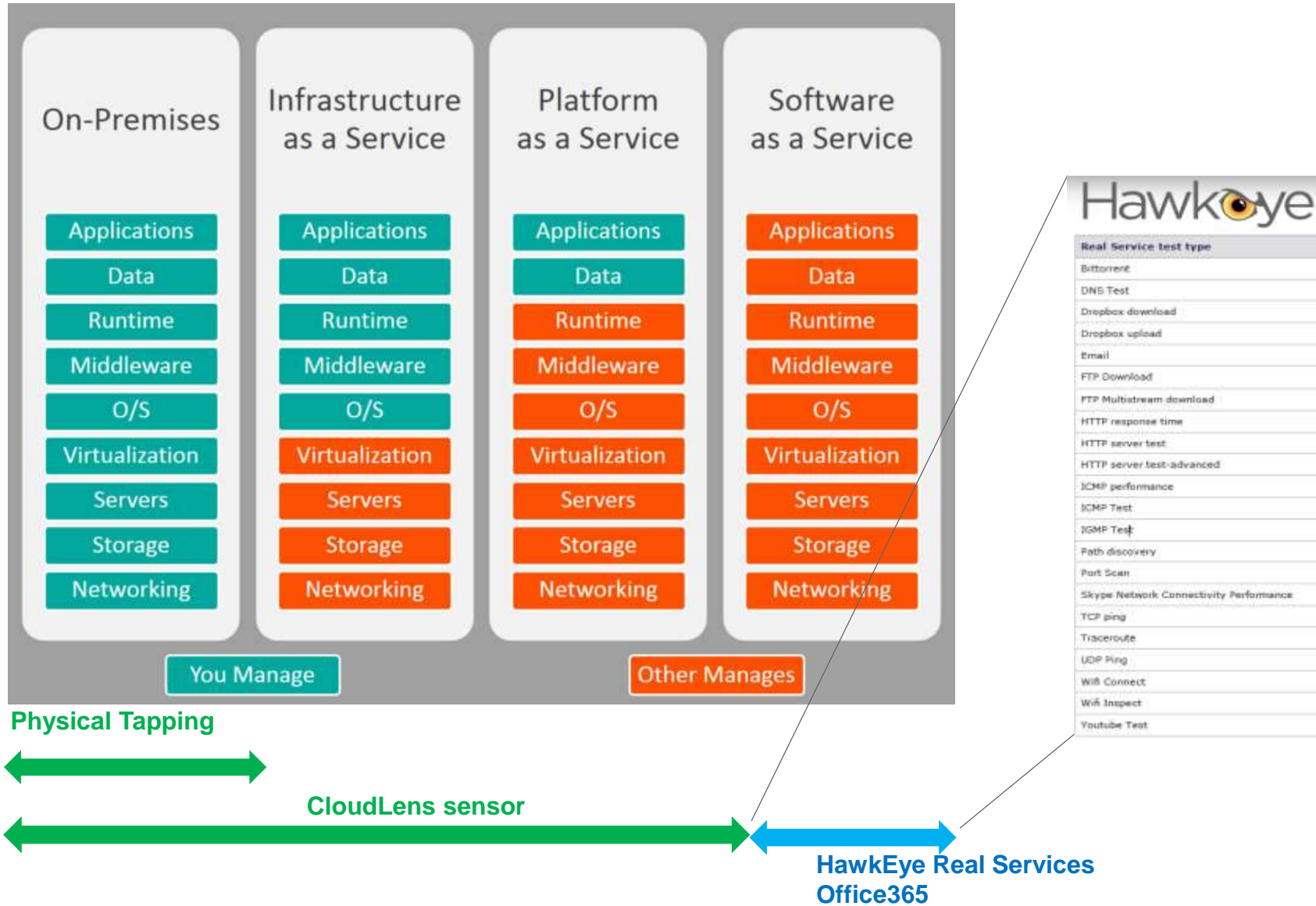
You can't protect what you can't see.



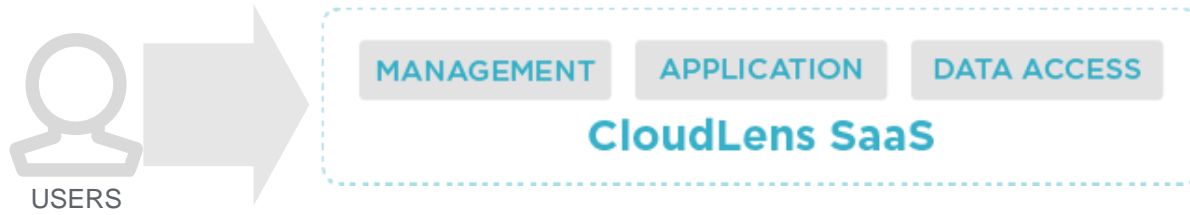
CLOUDLENS IS BUILT TO HANDLE CLOUD ELASTICITY



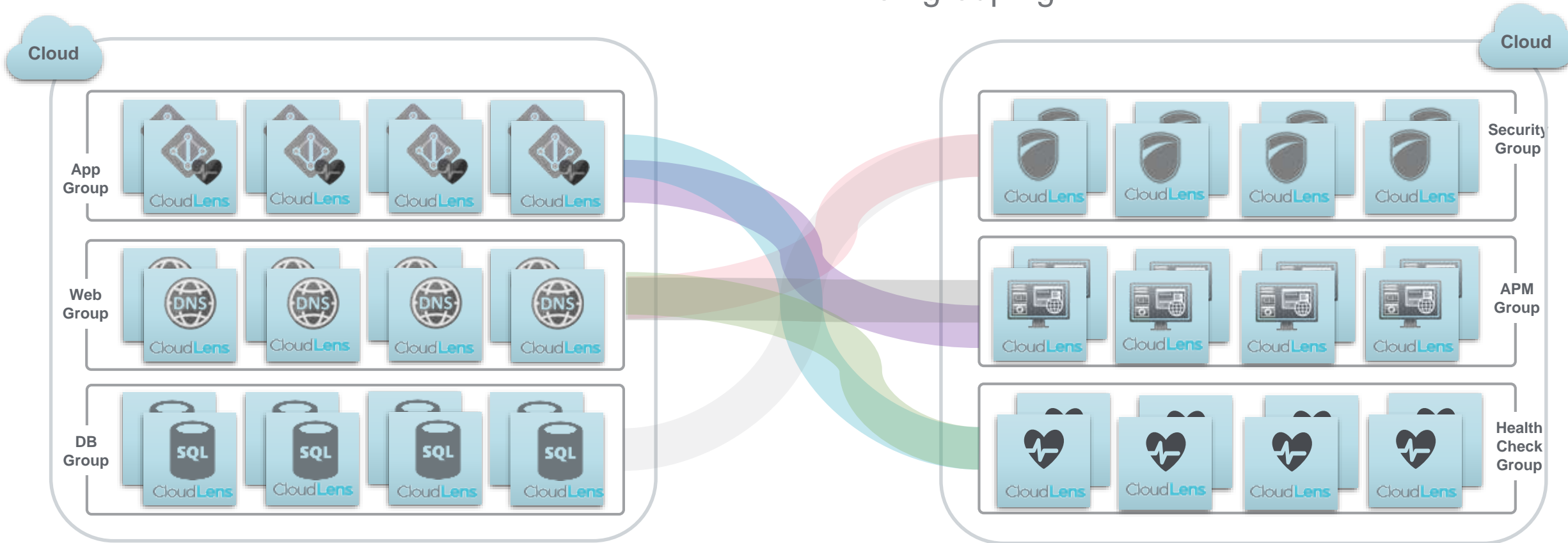
HOW IXIA GIVES YOU VISIBILITY ON EACH CLOUD



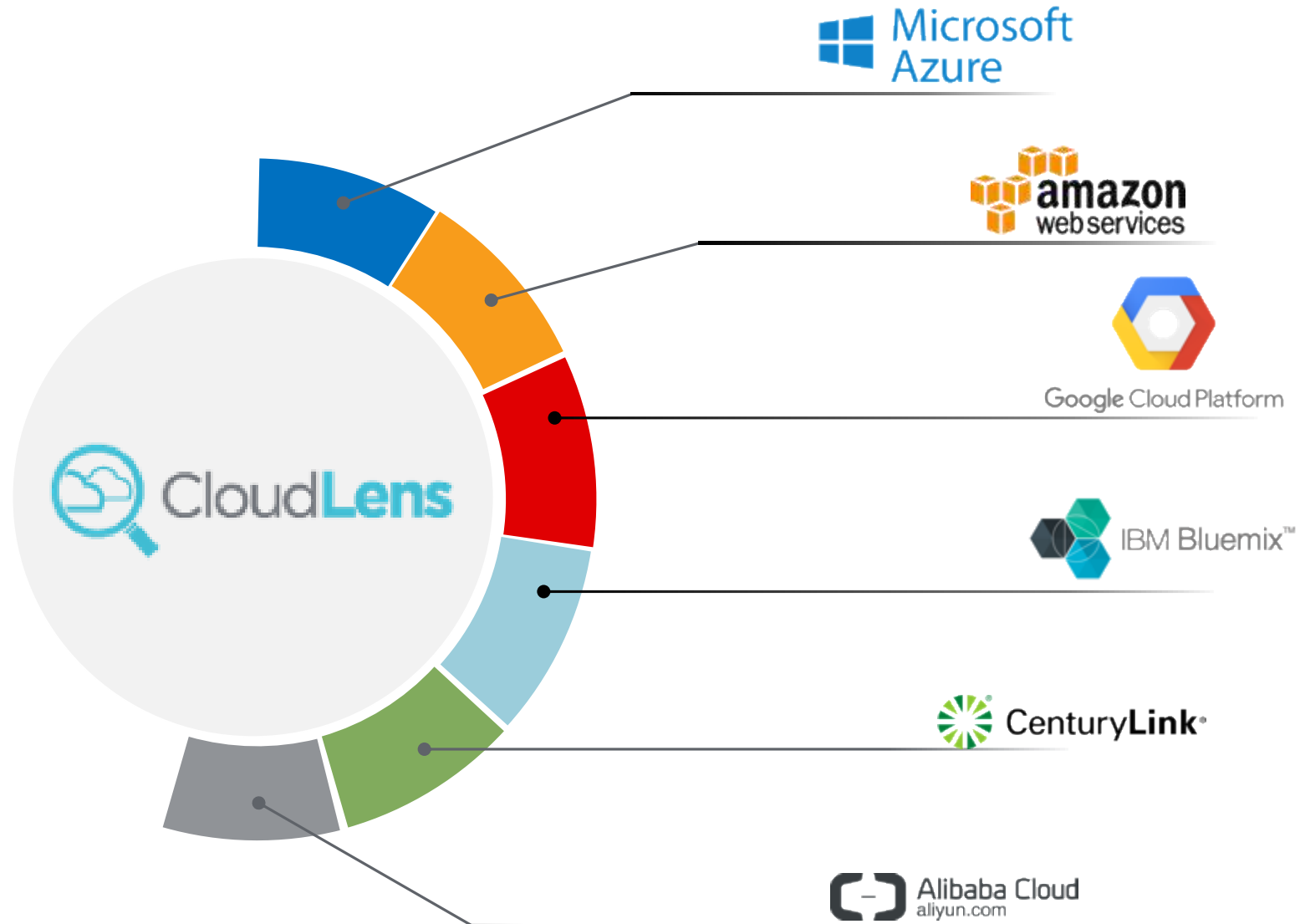
CLOUDLENS IS BUILT TO HANDLE CLOUD ELASTICITY



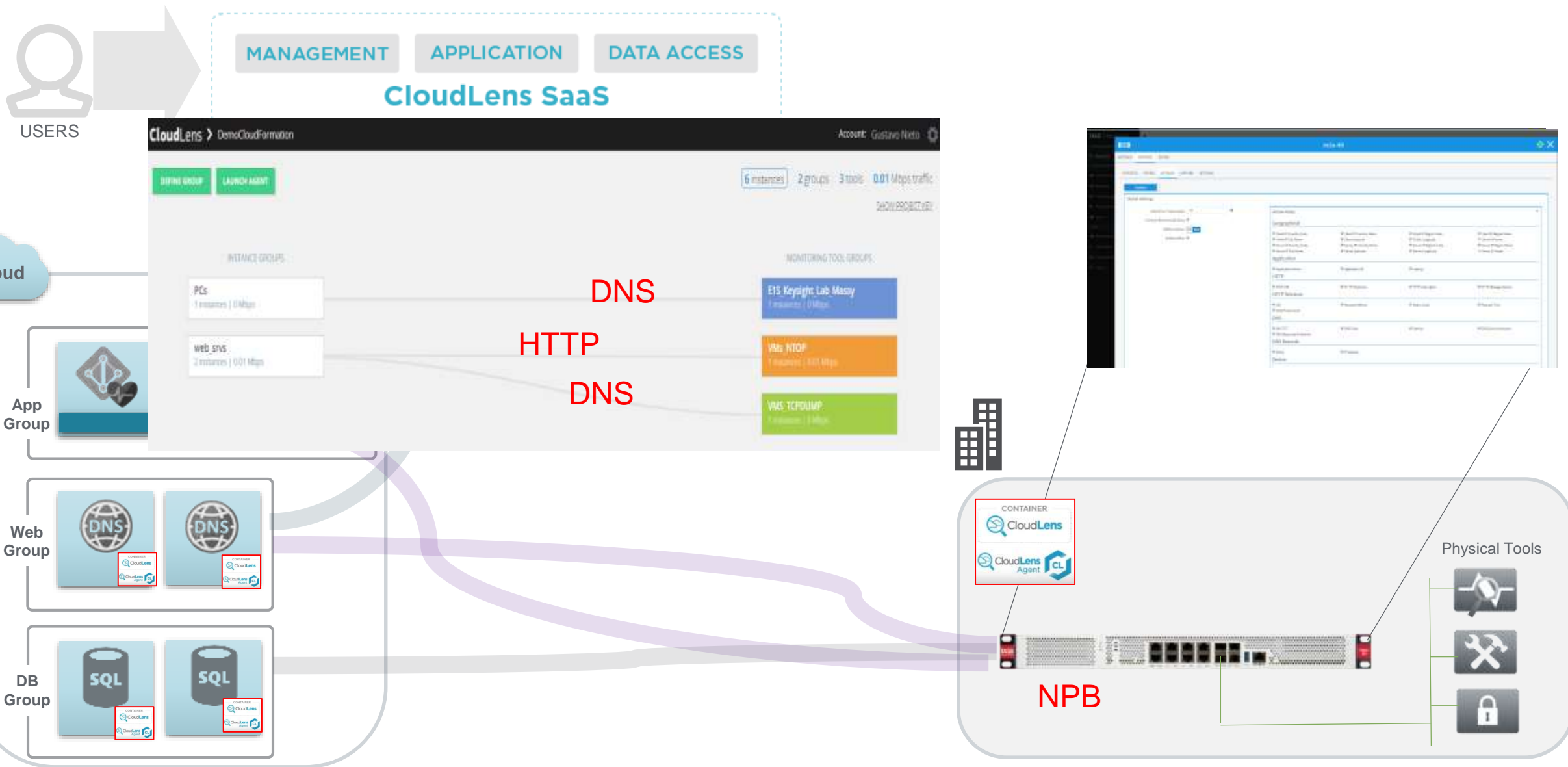
- New instances are automatically categorized
- Filtering rules are automatically applied based on grouping



CLOUDLENS MULTI-CLOUD SUPPORT



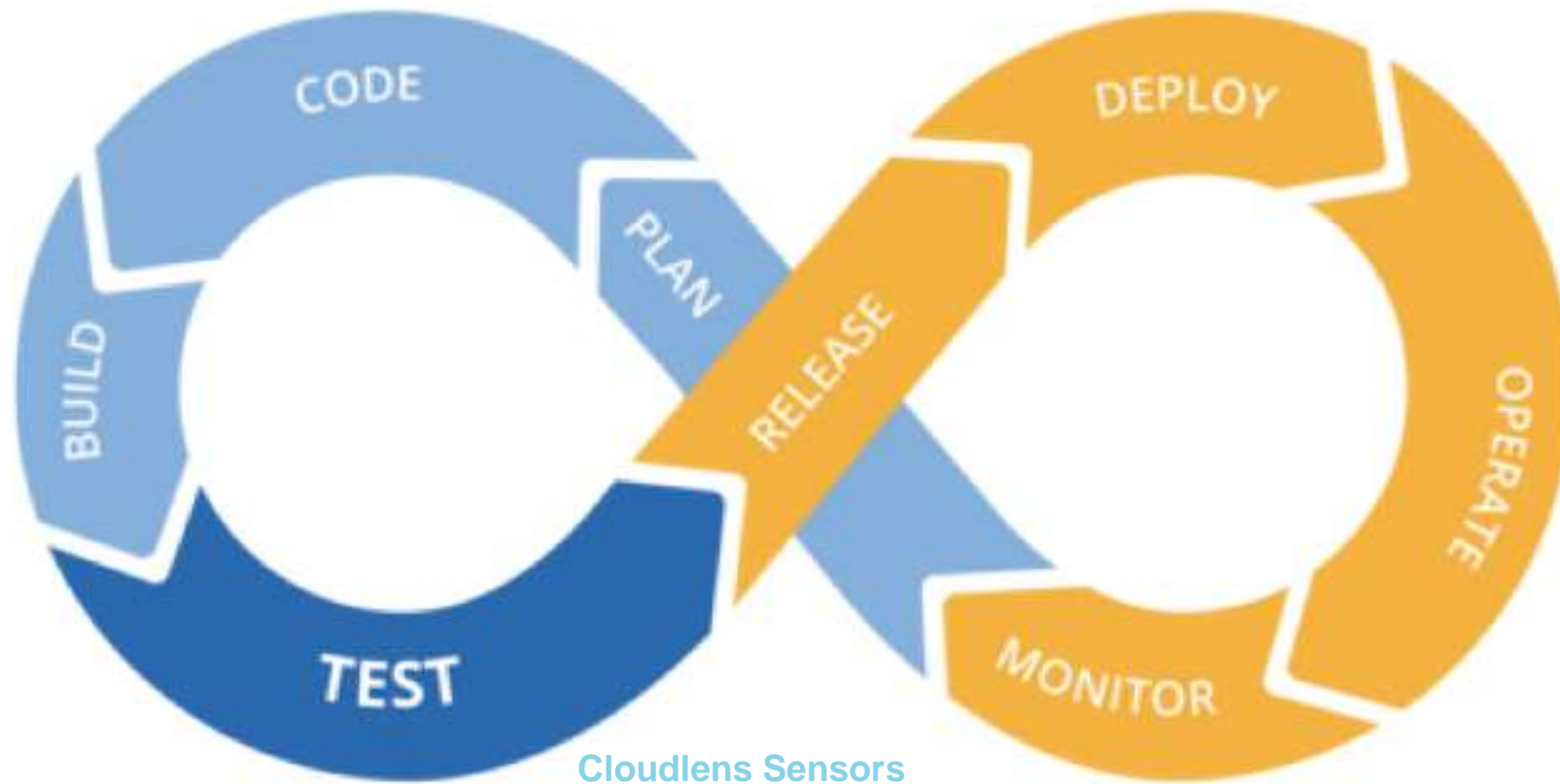
CLOUDLENS FOR THE HYBRID CLOUD



CLOUDLENS FOR ISOLATED ENVIRONMENTS



ENHANCING VISIBILITY IN DEVOPS



Cloudlens Sensors



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

THANK YOU

IN CASE OF QUESTION OR COMMENTS

FEEL FREE TO REACH OUT!

Halle 9, Stand 536

Andreas Hüntten

Senior System Engineer, Ixia Solutions Group
Keysight Technologies



e: andreas.huenten@keysight.com

m: +49 (0) 171 845 0465