Importance of Network Visibility

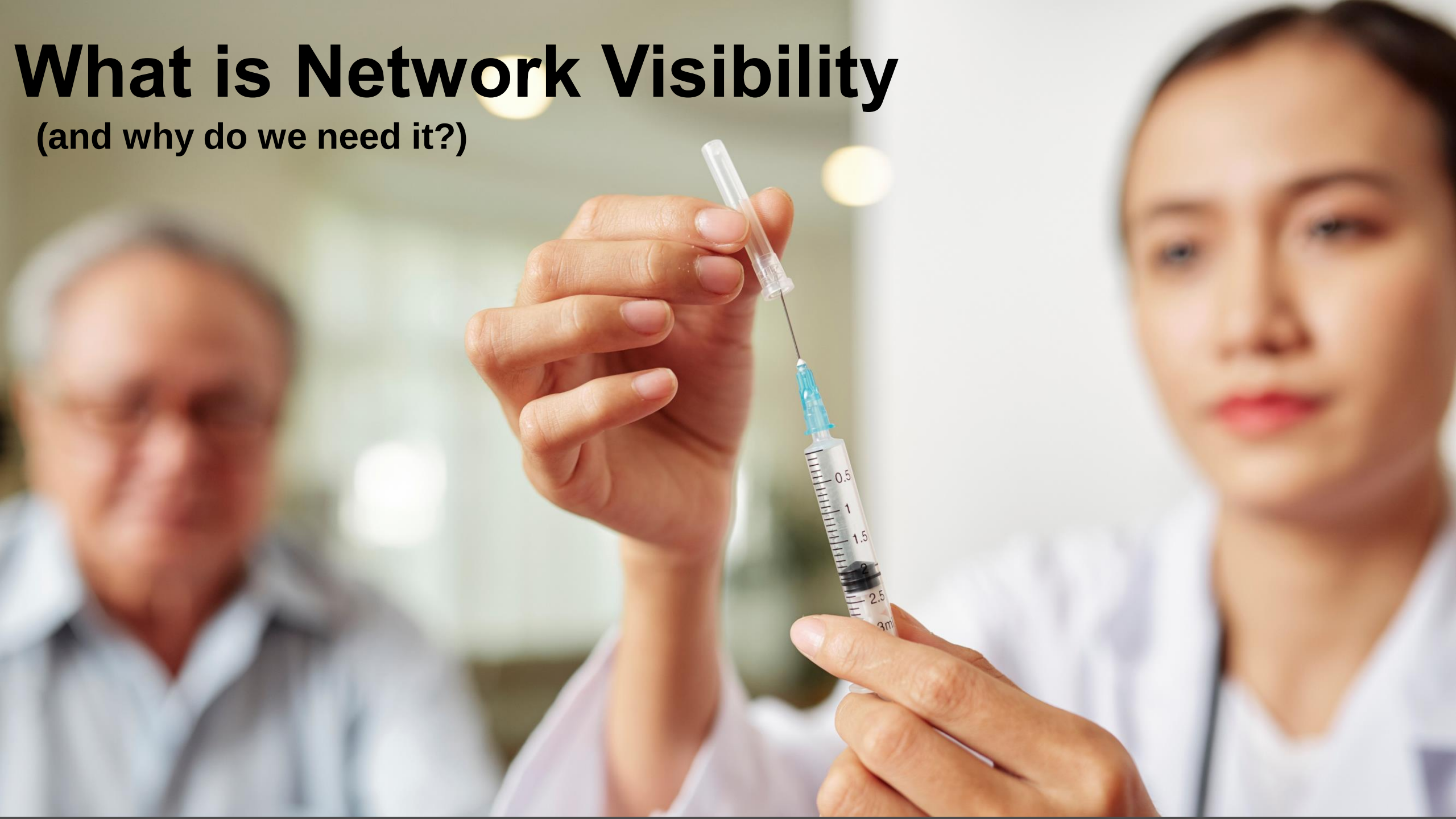
Patrick McCabe

Principal Architect, Keysight Technologies

KEYSIGHT

What is Network Visibility

(and why do we need it?)



Network Blind Spots exist

Lots of Organizations Involved		
Network Ops	Application Ops	Security Admin
Server Admin	Forensics	Privacy & Audit

Vast Array of Tools in Use		
NPMD	APM	Customer Experience
Forensics	IDS, SIEM	Firewall, IPS

Increasingly Complex Environment to Manage

Endpoints

Network

Data Center

Cloud

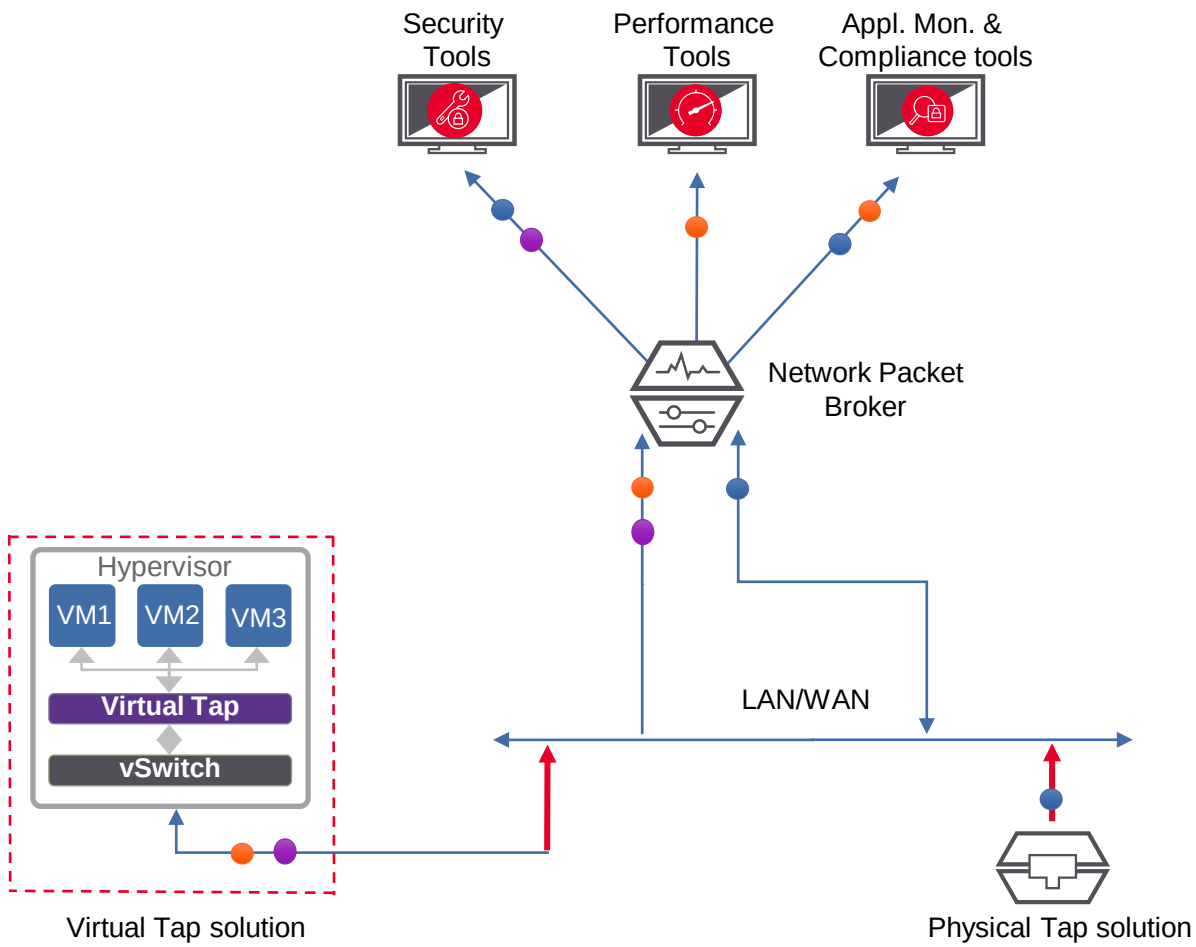
Applications

Basic Visibility Architecture Data Flow

Monitoring Layer
tools provide analytics and perf. metrics

Control Layer
NPBs for filtering, load balance, aggregation, regeneration

Access Layer
Virtual Taps
Physical Taps
Bypass Switch
SPAN Ports



Intelligent Visibility

NETWORK PACKET BROKER

TAP/SPAN

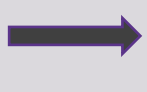
Intelligent Visibility

App & Geo Filtering
NetFlow / Contextual Metadata

Much more intelligent tools

Advanced Visibility

Deduplication, Trimming,
Burst Protection, etc.



Much greater tool efficiency

Basic Features

L2-4 Filters,
Load Balancing

More efficient tool usage

More scalable

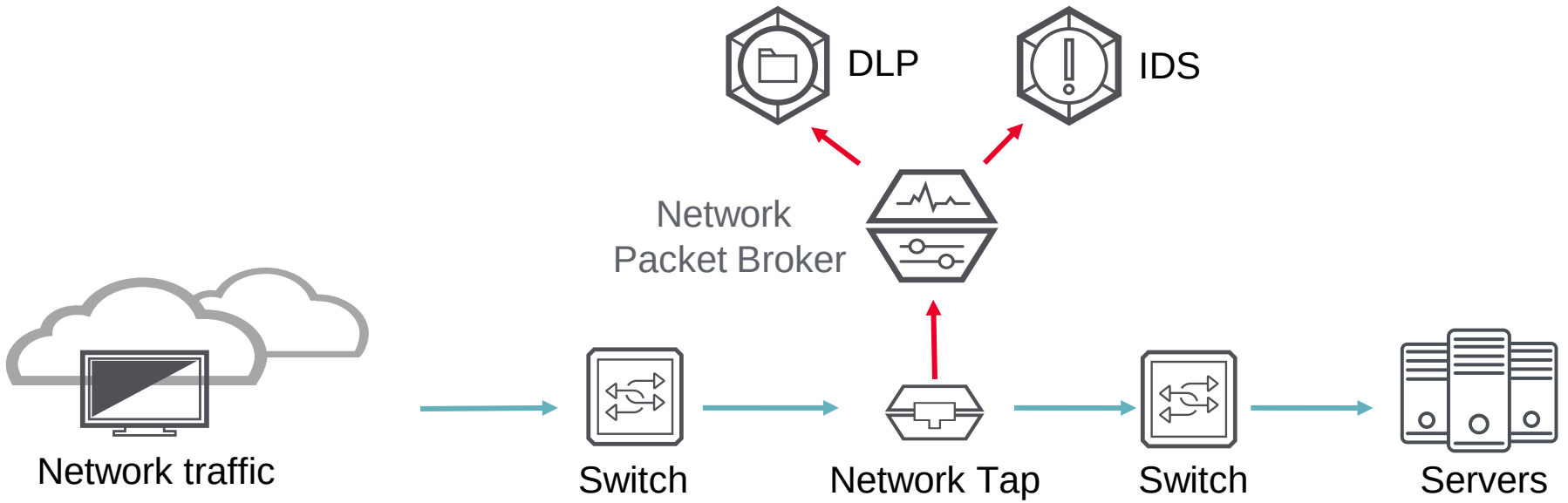
Network TAP/SPAN

Mirrored, Raw Data

Quickly overwhelms tools

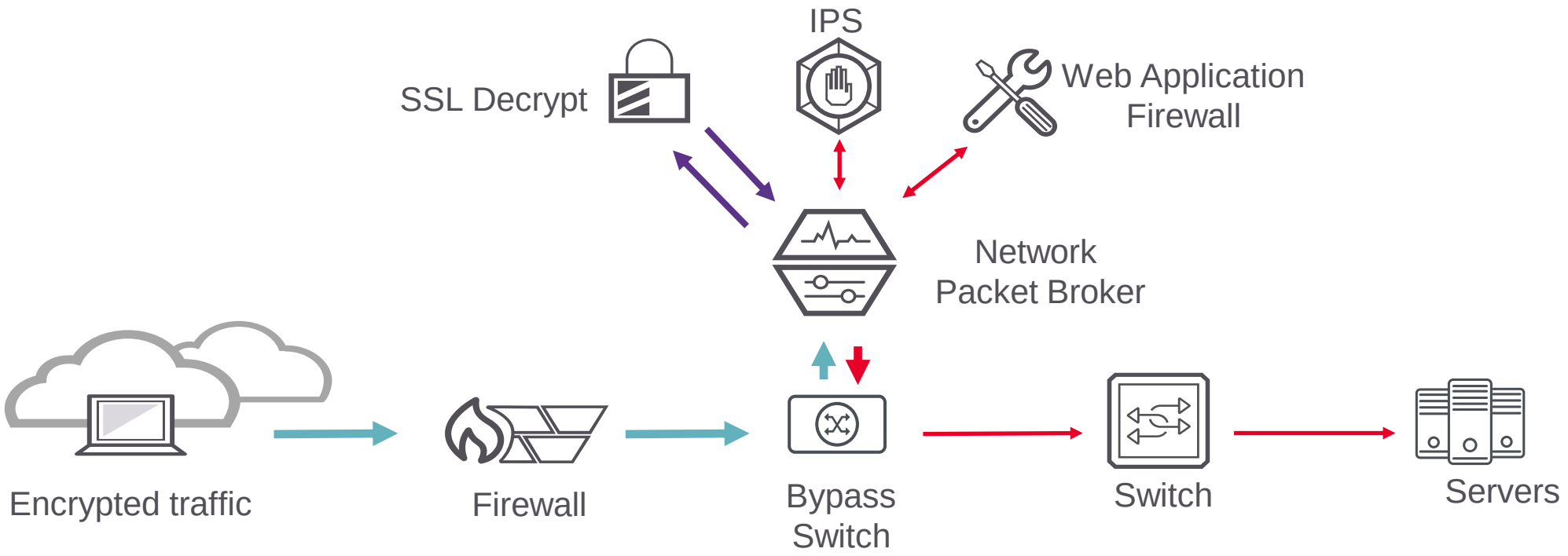
Limited tool ingress ports

Rapid Forensic Investigation Limits Breach Damage



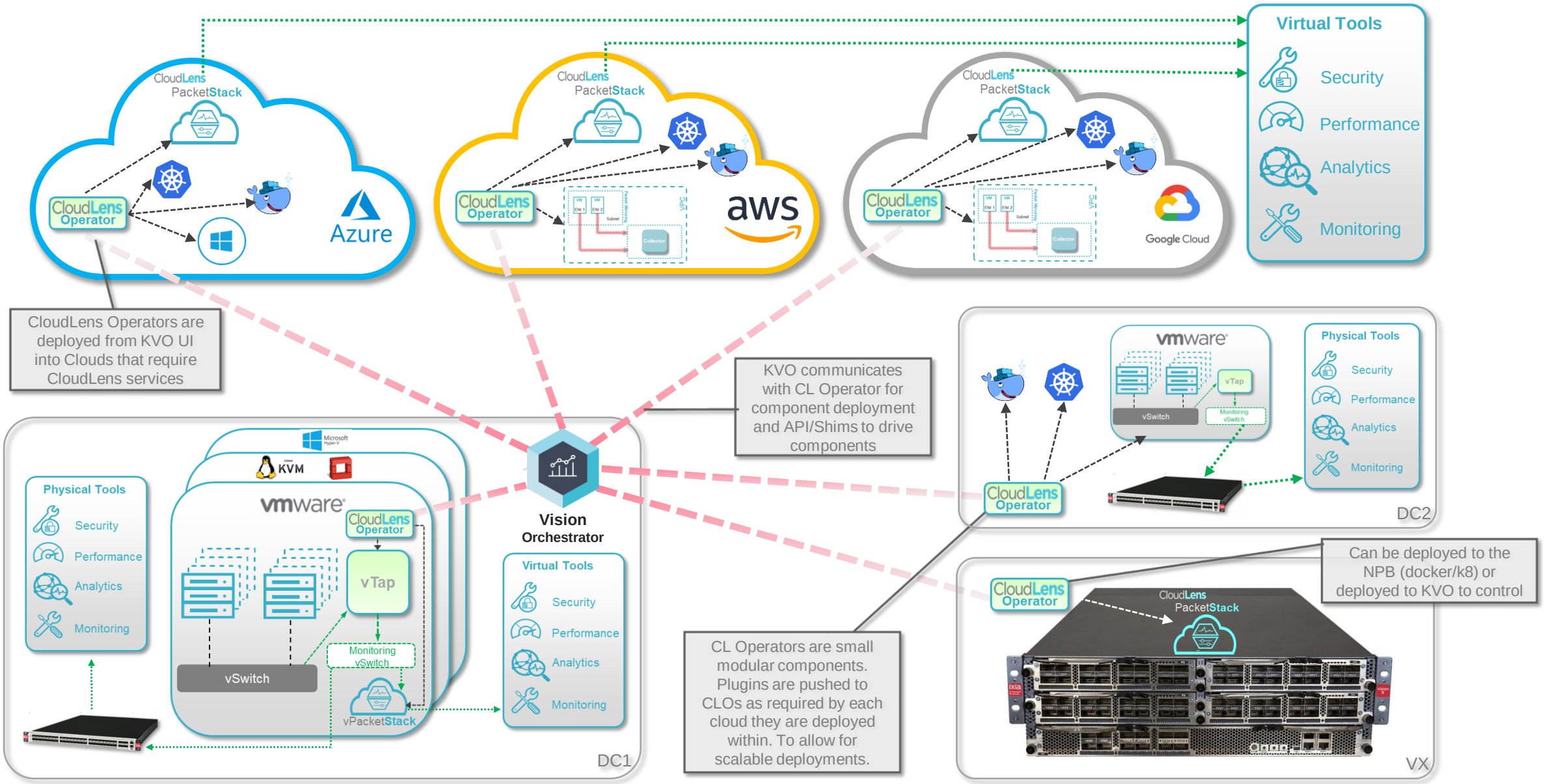
- In 2016, only 43% of breaches were self-detected
- Create NPB filters to collect L2 – L4 data and send it to DLP, IDS, log file tools, and other security tools for analysis
- Perform forensic analysis to see data exfiltration attempts and limit data loss

Appliance-based TLS Decryption With an NPB



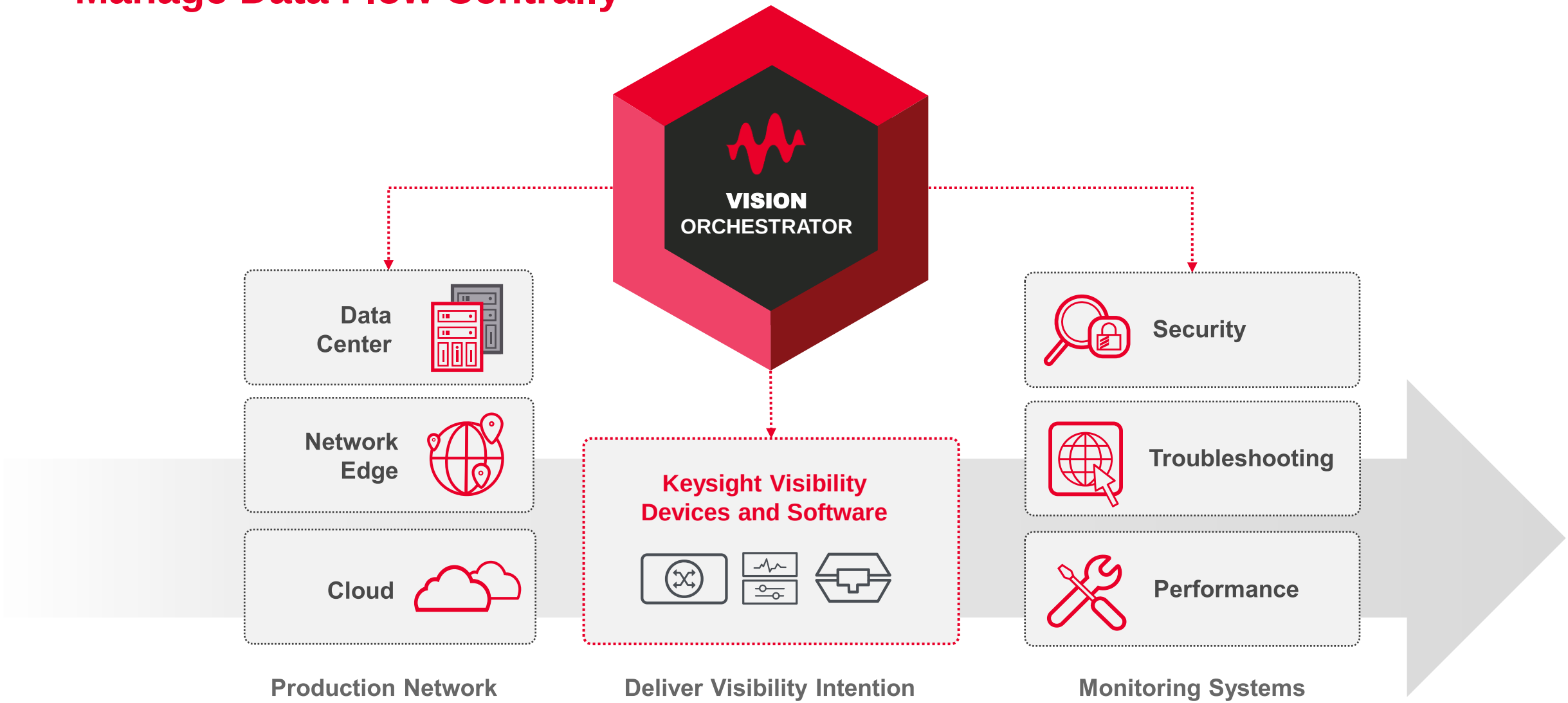
- Up to 50% of all network security attacks in 2017 will use encrypted traffic to bypass security controls
- Expose hidden threats with active decryption technology like A10 and Bluecoat
- NPBs allow for distribution of encrypted data to decryption devices and then the distribution of the now unencrypted data to various tools (NGFW, IPS, DLP, etc.)

CloudLens Deployment Model – High Level Architecture



Note: Some items include future features

Manage Data Flow Centrally



Visibility Architecture Summary

Maximize Network Visibility and Get Real Results

Use cases based upon a visibility architecture will allow you to do the following:

- Self detect breaches and cyber intrusions
- Eliminate blind spots where threat actors thrive
- Secure your network inside the perimeter
- Meet regulatory compliance for your environment
- Reduce cost of security tools
- Reduce the cost of a breach by connecting tools to the network faster and decreasing the associated mean time to repair

KEYSIGHT

Thank you