Progress®

# Hybrid infrastructure & network traffic monitoring in public cloud

**Pavel Minarik**

VP, Technology

# You Cannot Manage & Secure What You Cannot See

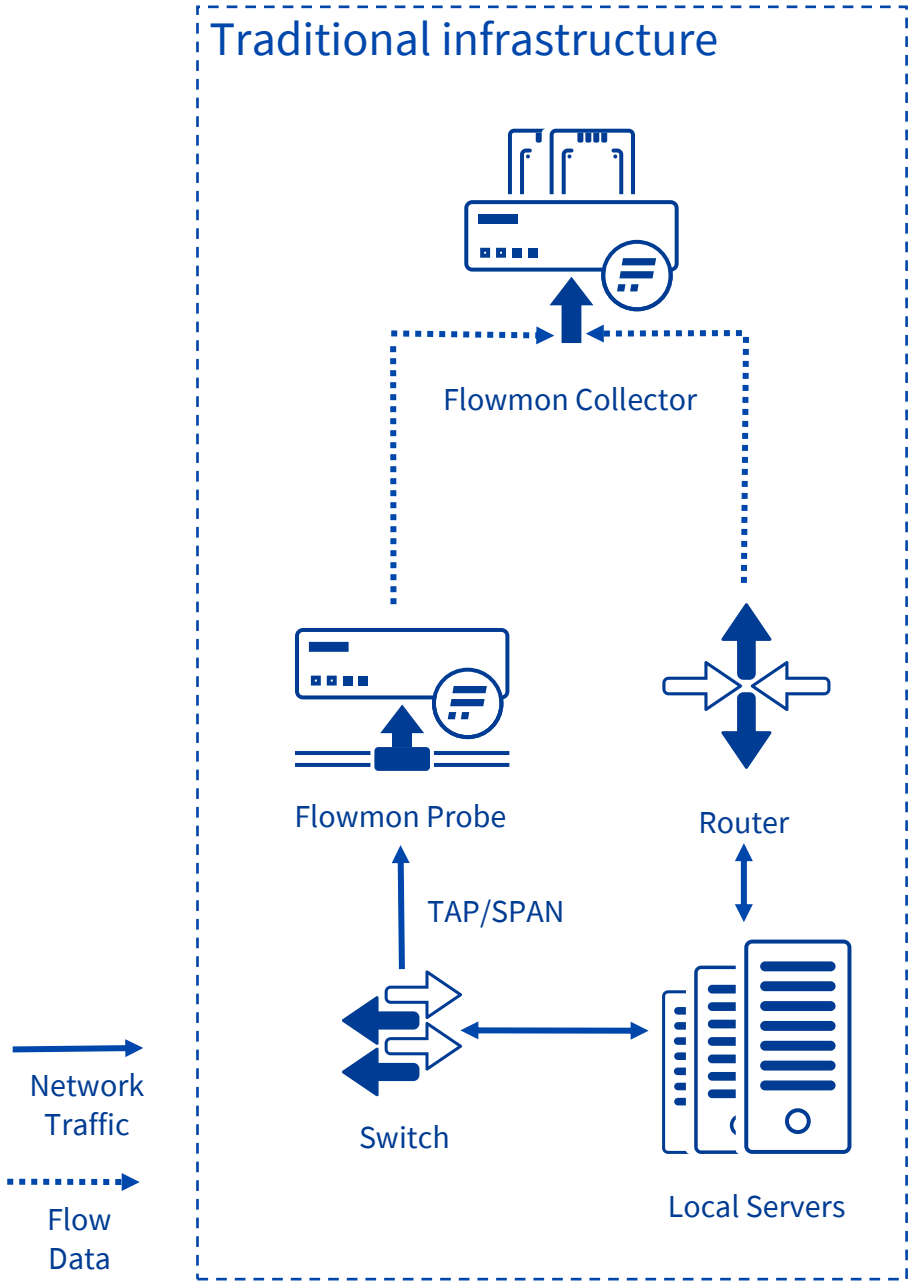
- Single source of visibility across the entire environment.
- Understand network and application performance metrics.
- Detect threats and indicators of compromise in real time.
- Automate analysis, find root cause and respond quickly.

# On-premise network monitoring & analysis

Traditional concept of network traffic monitoring using a combination of network telemetry from existing devices and dedicated sensors providing different levels of traffic inspection.

Flowmon Probes for enriched network telemetry (IPFIX) export and IDS inspection.

Flowmon Collector with Anomaly Detection System for NPMD/NDR functionality.



Progress®

# How do you apply traffic monitoring concept in public cloud?

# Reality of traffic monitoring in the cloud

- Distributed network environment
  - SDN, NFV
- No access to lower stack layers
  - No access to L2 for port mirroring
  - No physical media for tapping
- Provider- or platform-specific implementations
- Built-in tools for traffic/log analysis
- Complex pricing

Progress®

# I don’t want to query 3 different network monitoring tools and manually correlate the results when solving an incident.”

**John**

Security analyst

# Traffic monitoring options in the public cloud

## Native mirroring

- Functionality of the cloud platform to copy packets from virtual interfaces to monitoring appliances deployed in the cloud

## Flow logs

- Traffic statistics generated in form of logs by the cloud platform as such
- Contain information similar to NetFlow v5

## 3rd party agents

- Software components installed on virtual machines to provide a copy of the traffic through tunnel
- Additional complexity, no longer passive

# Pros & cons of different approaches

## Traffic Mirroring

+ Full visibility (including L7)

- Complex configuration

- Likely to be expensive (# of sources + traffic volume = $$$)

***Use cases:***

- Mission critical services
- Cloud data ingestion points

## Flow logs

+ Easy to configure and manage

+ Relatively cheap to operate

- Low data quality and information content

- Processing delays from traffic to logs

***Use cases:***

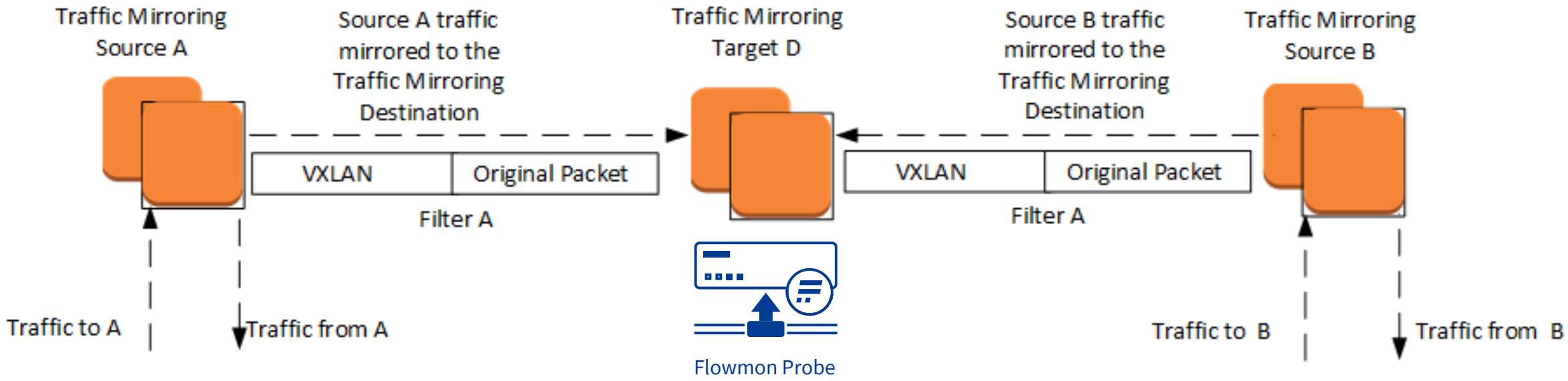
- Large-scale network monitoring
- Multi-region monitoring on single appliance

# Traffic mirroring in the cloud may require special capabilities from monitoring tools

**AWS** delivers copy of the traffic encapsulated in **VXLAN** tunnel

**3rd party tools** leverage different transport mechanisms, e.g. **GRE**

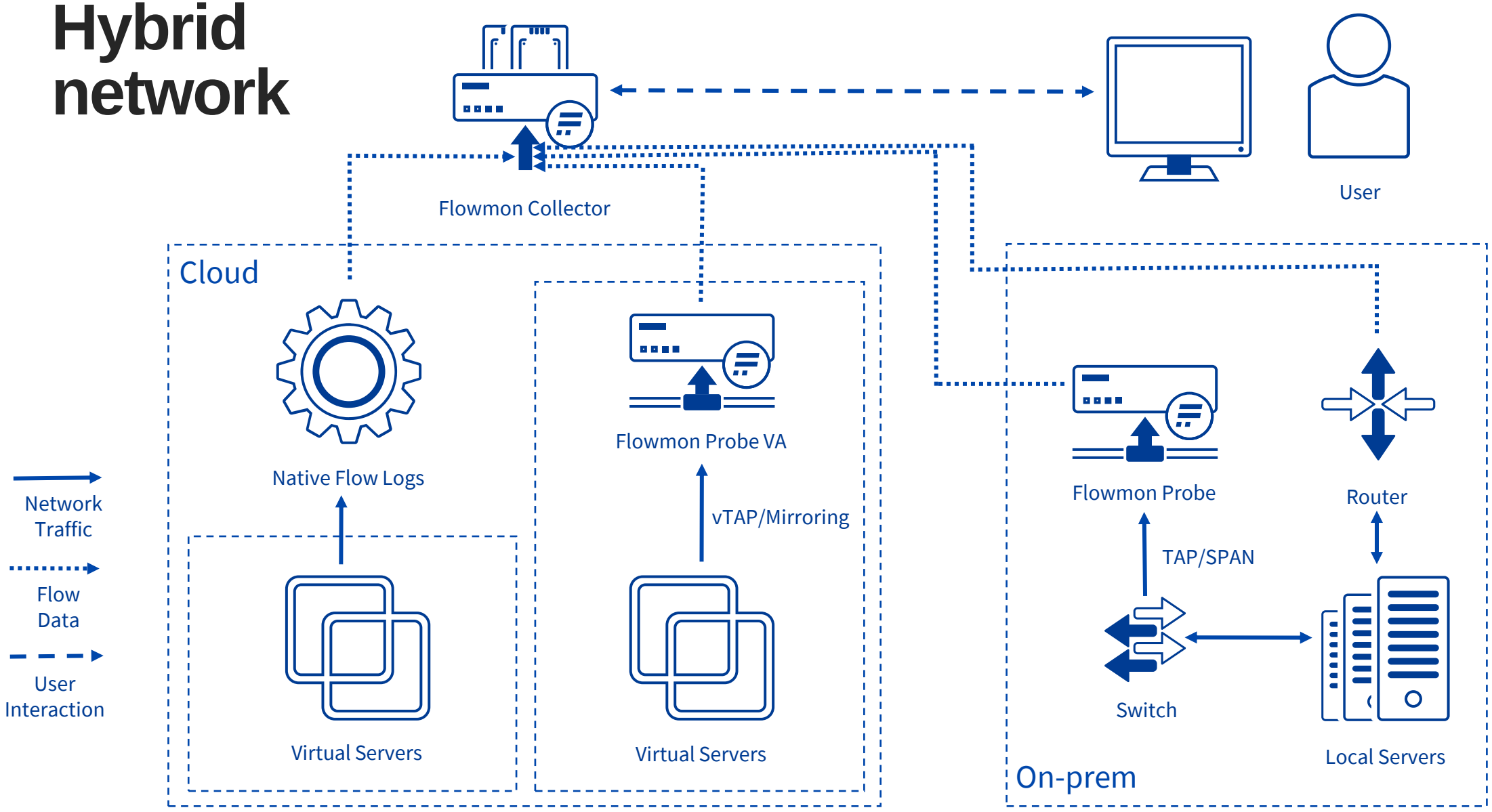
**Sensors** need to **support tunnel decapsulation** to measure the traffic!



Progress®

# Consolidated traffic monitoring in hybrid infrastructure

# Hybrid network

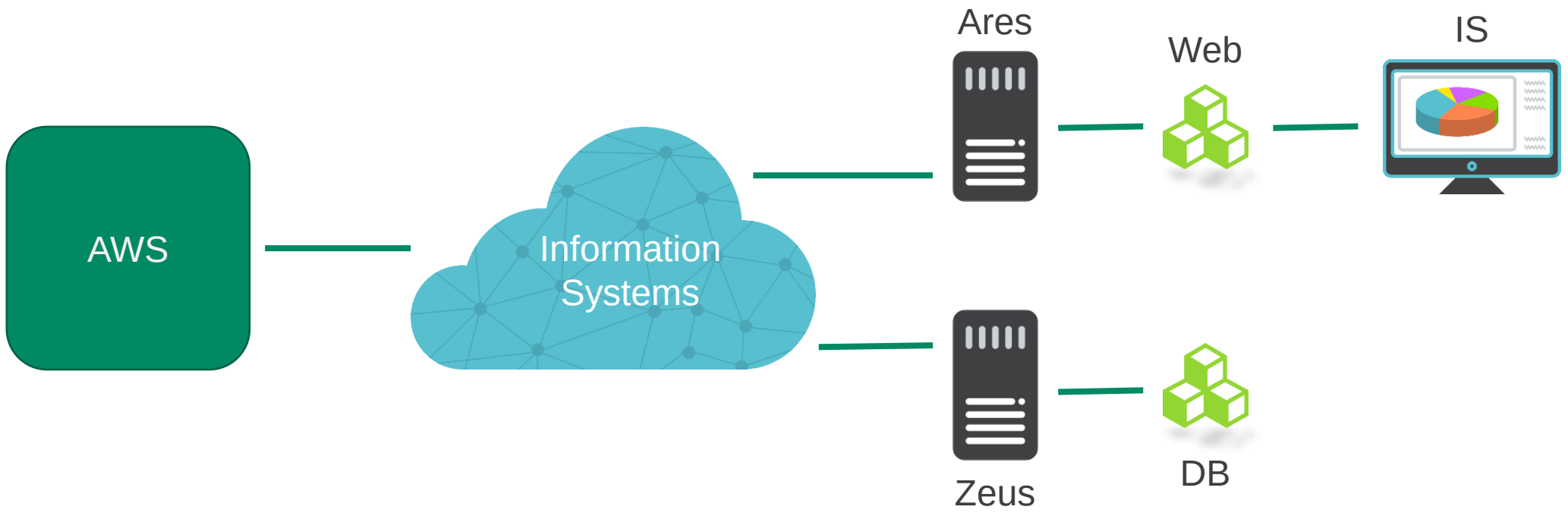


Progress®

# Deep dive into cloud monitoring scenario

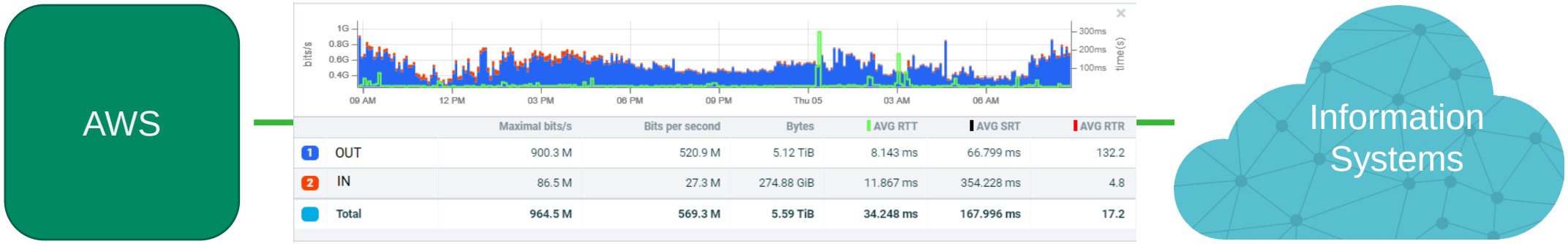
# Cloud monitoring scenario introduction

I need to monitor my VPC in AWS that hosts my Information System, a critical application for users. I'm going to leverage VPC Traffic Mirroring.



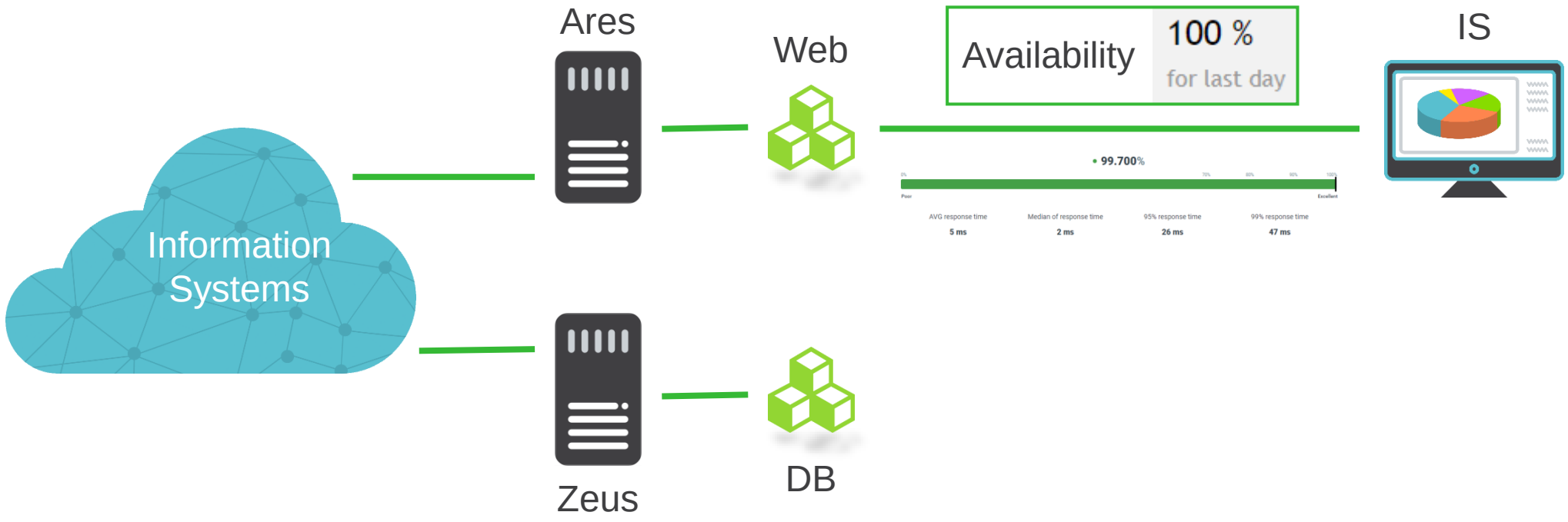
# Bandwidth and performance monitoring

Flow data provide me an understanding of bandwidth utilization and performance metrics across the VPC. Alerts on key metrics are triggered when deviations from baselines are recognized.



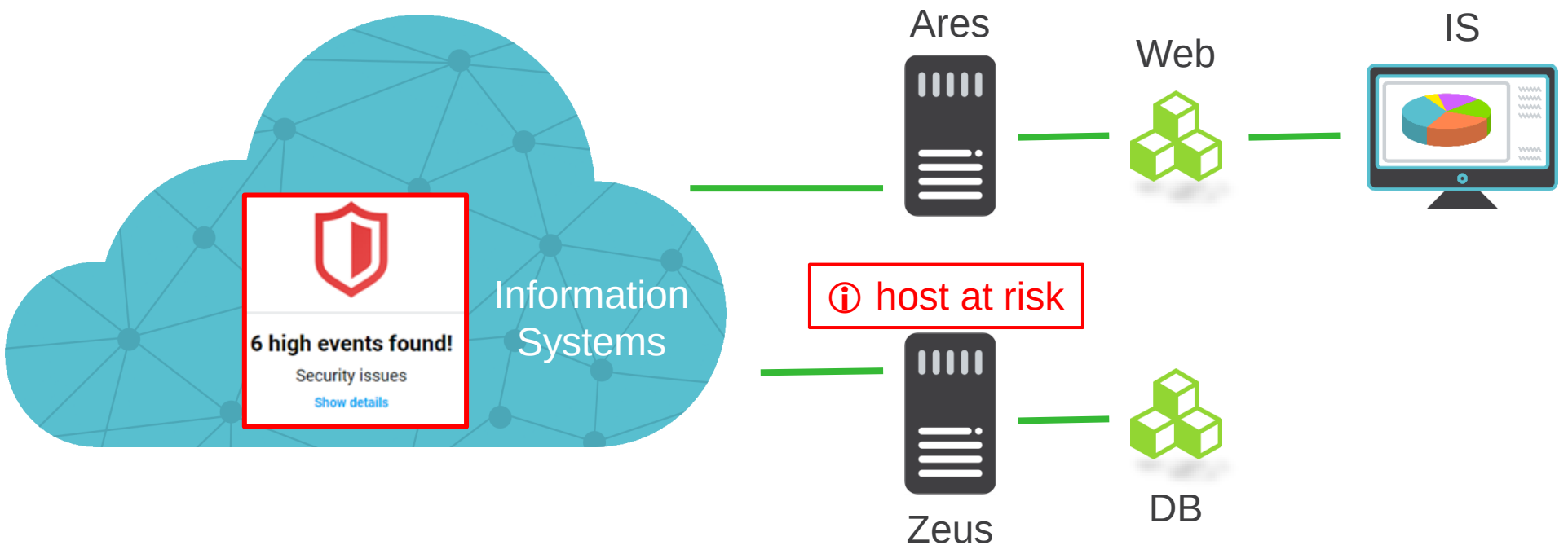
# User experience monitoring

With application layer data I’m able to track individual user transactions in real time and report on real user experience.



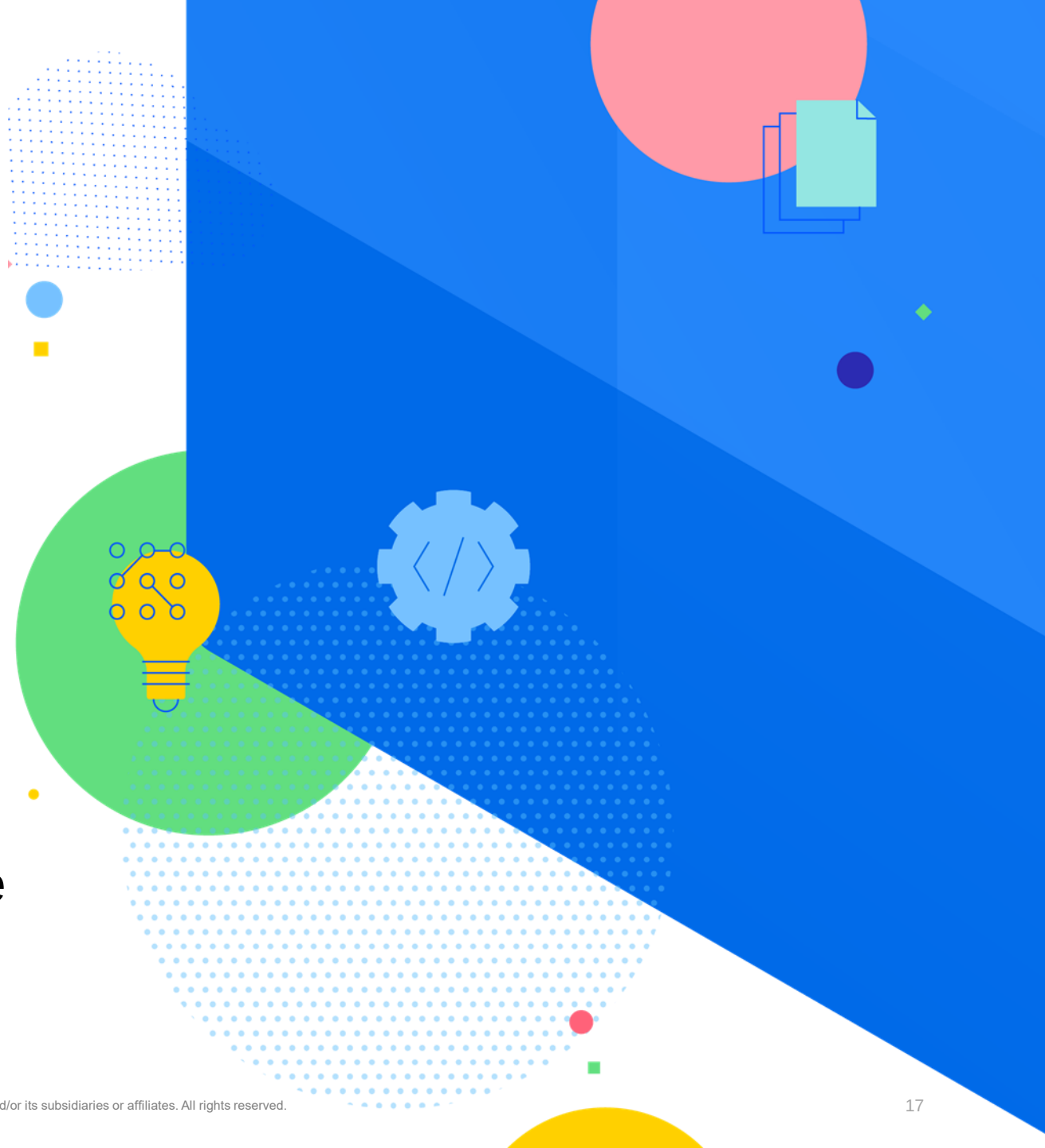
# Security operations built-in

Anomaly detection is using same primary data as network operations.
Reported incidents are tight specifically to my critical infrastructure.



# Behind the scene

- EC2
  - Launch Flowmon Collector instance
- VPC
  - Create Traffic Mirroring Target
  - Create Traffic Mirroring Filter(s)
  - Create Traffic Mirroring Session(s) → per source interface!
- Flowmon Collector with built-in Probe
  - Configure monitoring port for VXLAN decapsulation



# Further resources and reading

- Bridging Visibility Gaps in Hybrid Cloud Monitoring
- Cloud Application Performance Monitoring
- How to Optimize Cloud Monitoring Costs Using Flow Logs in Progress Flowmon
- Flowmon on AWS market place
- Flowmon on Azure market place
- Flowmon on Google Cloud market place


Progress®