



# Where's Waldo: Security Awareness Through Network Detection and Response (NDR)

---

Frank Yue, Principal Application Experience Architect





# What is Network Detection & Response?

## Network Detection and Response (NDR)

enables organizations to monitor **network** traffic for malicious actors and suspicious behaviour and react and **respond** to the **detection** of cyber threats to the **network**.

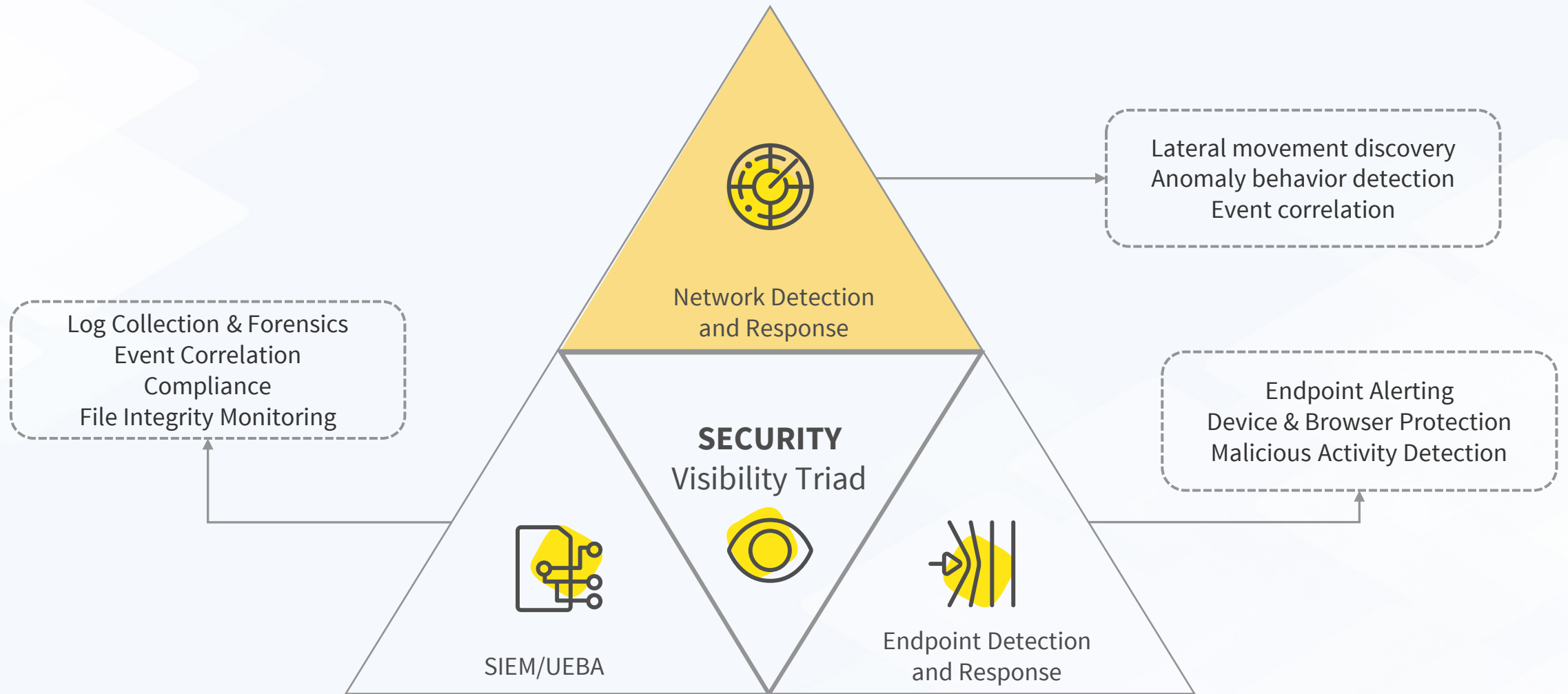




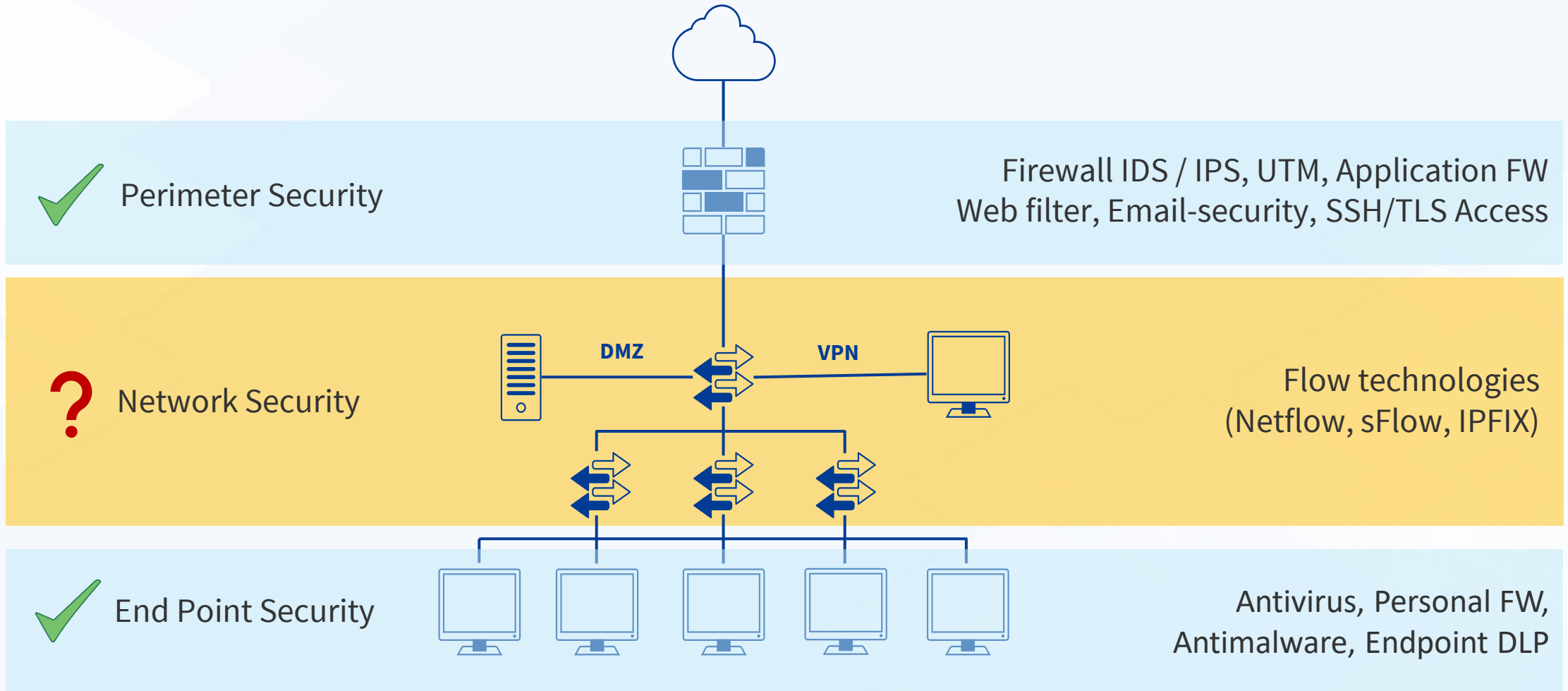
***“Detection and response are more important than blocking and prevention”***

Neil MacDonald, VP Distinguished Analyst, Gartner Security & Risk Management Summit

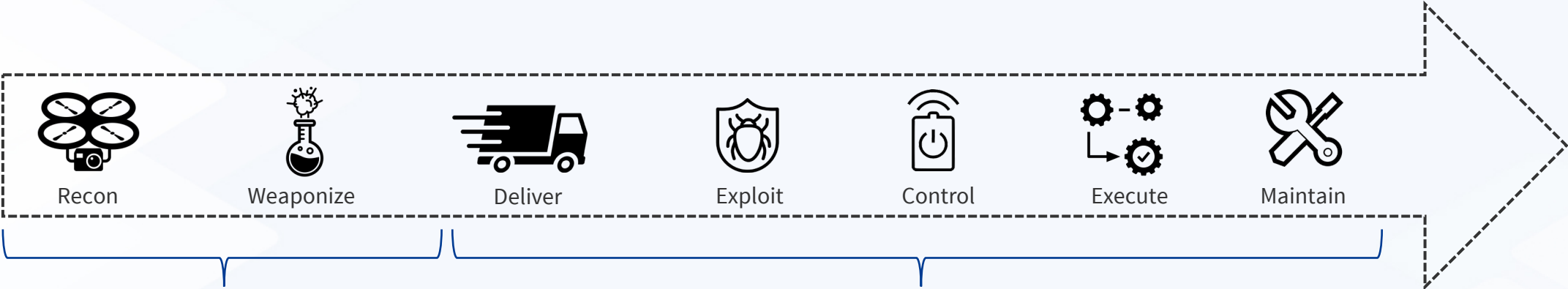
# Security Visibility Triad



# Network Security



# MITRE ATT&CK Framework



### PRE-ATT&CK

- Priority Definition
- Target Selection
- Information Gathering
- Weakness Identification
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

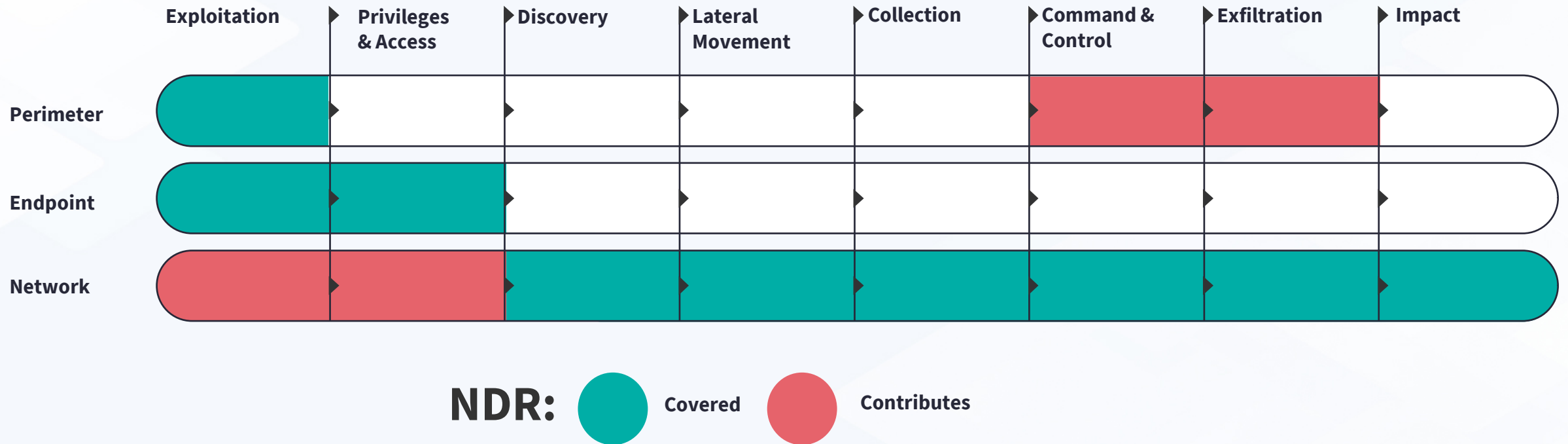
### ATT&CK for Enterprise

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

Combination of endpoint, network and perimeter security required for successful mitigation

# Multi-Layered Security through MITRE ATT&CK Framework

Multiple detection and prevention points are necessary to properly identify ransomware attacks





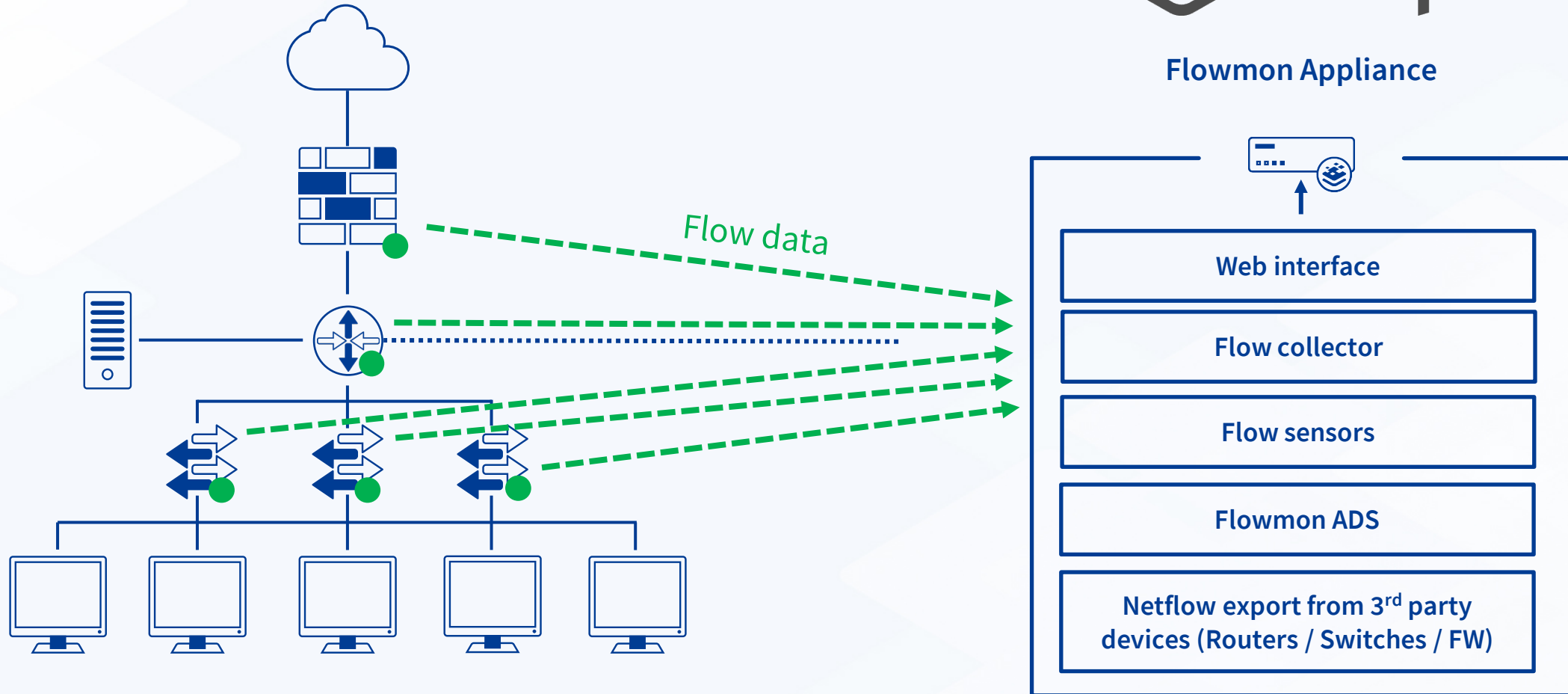
**Let's look at NDR technology...**



# NDR Basic Deployment



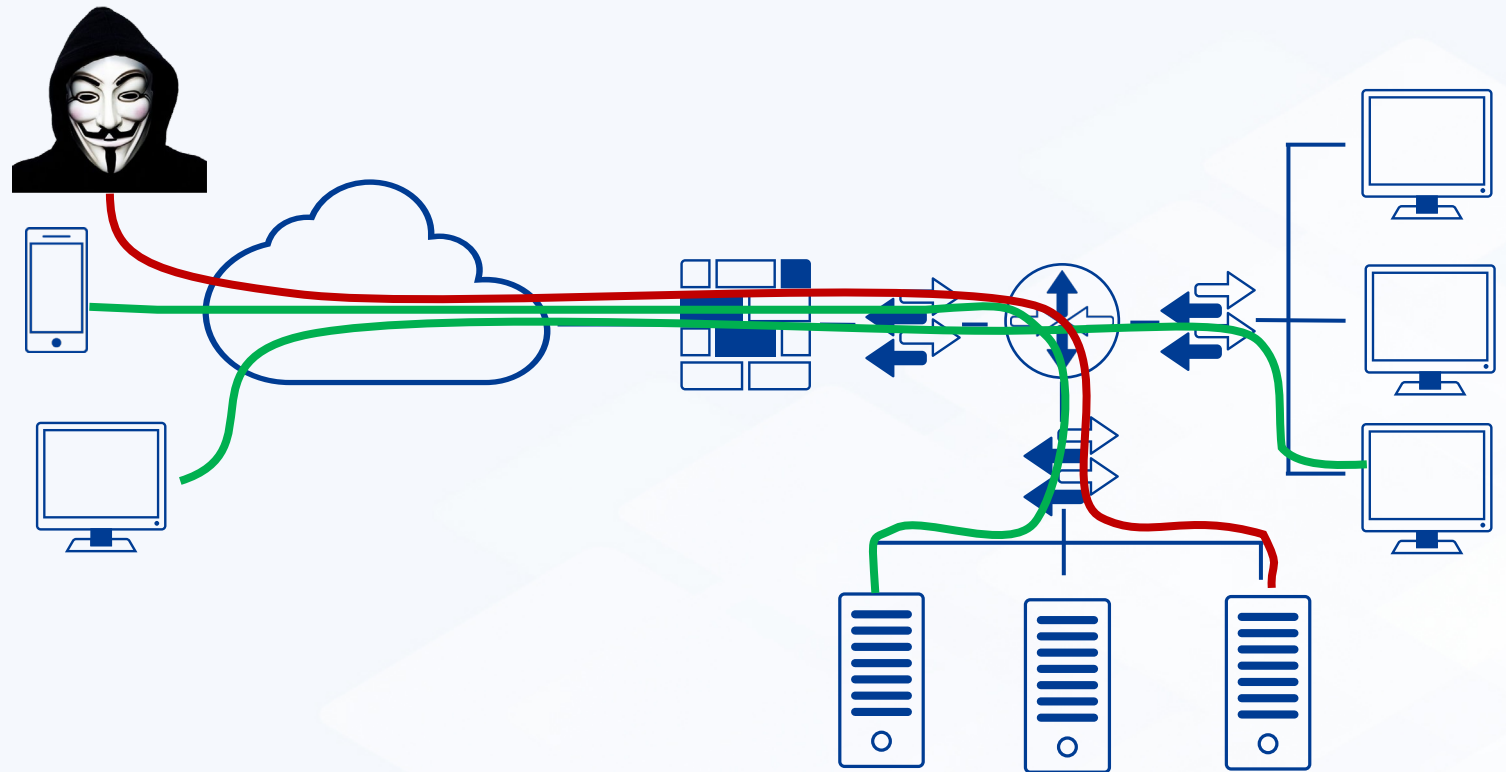
Flowmon Appliance



# Needle In a Haystack

## There is a lot of network traffic

- **Problem:** Separating the good from the bad
- **Solution:** NDR intelligently flags suspicious traffic



# NDR Detection Capabilities

Event #207160 COPY EVENT ID DOCK WINDOW ⋮ ✕

**Type** Data upload anomaly (UPLOAD)  
**Subtype** General  
Reports devices that excessively upload data outside of the allowed network segment. This may indicate the use of services outside of the allowed network segment or even malicious activity (e.g. data exfiltration).

**Detail** Uploaded: 22.82 MiB, downloaded: 0 B, port(s): 2048.

**MITRE ATT&CK** Tactic Exfiltration >> Technique Automated Exfiltration

<b>Detection time</b>	2021-07-26 14:12:03	<b>Event source</b>	192.168.1.50 (unknown) ▾	<b>Probability</b>	100 %
<b>Last update</b>	2021-07-26 14:22:04	<b>Captured source hostname</b>	N/A	<b>False positive</b>	No
<b>First flow</b>	2021-07-26 14:05:43	<b>MAC address</b>	08:00:27:13:b3:a1 ▾	<b>Detected by instance</b>	Default
		<b>User identity</b>	Adam Ondra	<b>Data feed</b>	Default

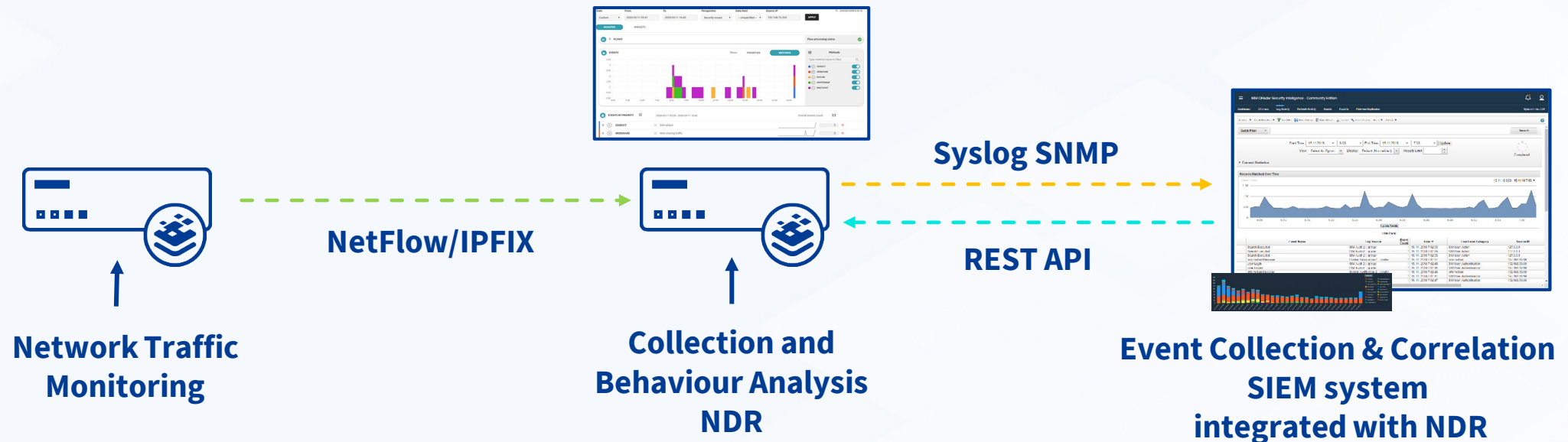
**TARGETS (1)** COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (2)

**ALL IP ADDRESSES** BY COUNTRY BY IP

🇺🇸 1.0.132.227 (node-yr.pool-...otinternet.net) ▾

# SIEM and Security Analytics Integration

- Syslog feed of events are provided to log management, SIEM, big-data platforms, incident handling and SOAR tools
- Response tools are only as useful as their event sources



# You Cannot Manage and Protect What You Cannot See



Detect threats immediately without placing the burden of interpretation on the user



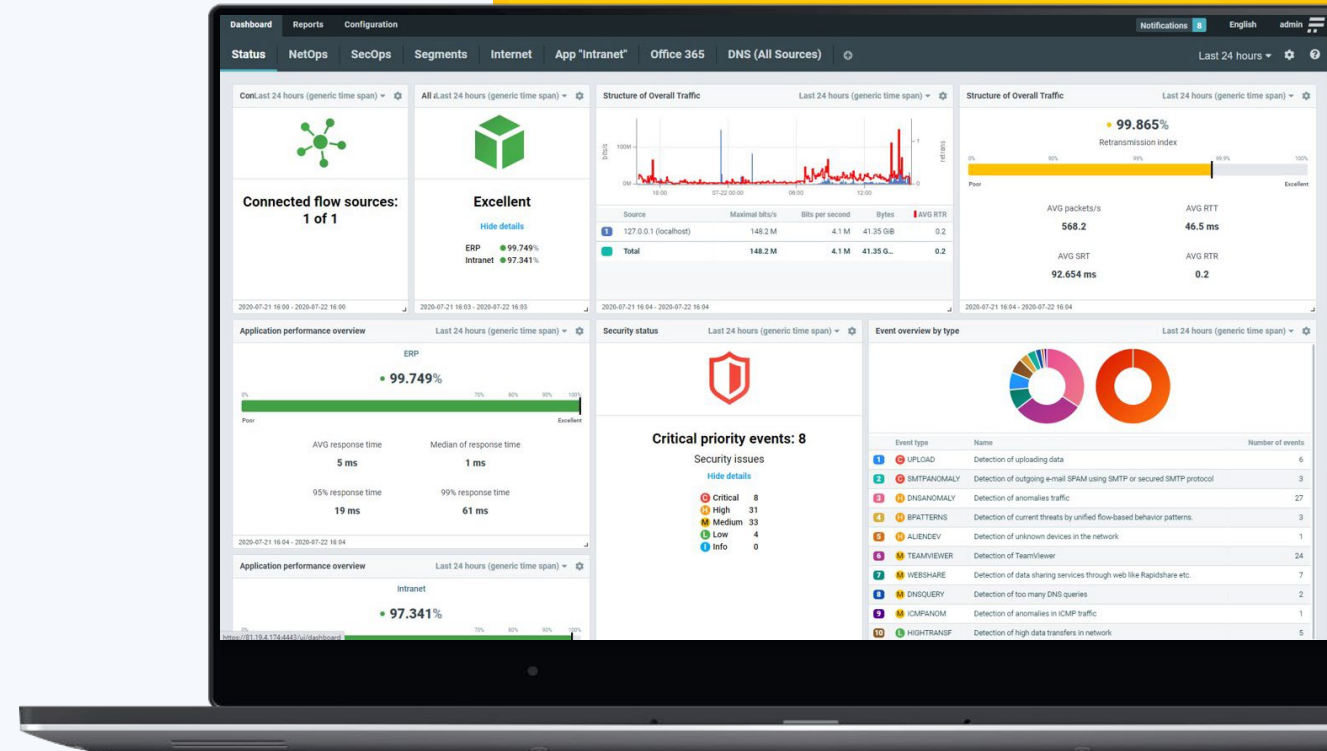
Insight using sophisticated algorithms, machine learning, heuristics, and artificial intelligence



Behaviour pattern recognition, detecting anomalies in their infancy before they become impactful threats



Near real-time detection, providing context including information for remediation





# Customer Story

## Advanced Malware

“Thanks to Flowmon solution, we have detected a seriously infected device within our network. It has been a standard laptop which was redirecting the communication of large amounts of devices into the internet on itself. It was acting as a gate and malware could thus tap this communication, gain the passwords, possibly even redirect the user to fraudulent websites. **We have solved the incident within one hour thanks to the automatic detection through Flowmon ADS.**”

1. User complain to IT about slow network
2. IT admin checks Flowmon ADS – Detected DNS anomalies

#	Detail	Timestamp	NetFlow source	Source
1	Use of unexpected DNS server (with response, connections: 1, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:06:26	mirror_core	192.168.0.14
2	Use of unexpected DNS server (with response, connections: 5, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:06:17	mirror_core	192.168.0.23
3	Use of unexpected DNS server (with response, connections: 5, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:06:04	mirror_core	192.168.0.22
4	Use of unexpected DNS server (with response, connections: 6, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:44	mirror_core	192.168.0.24
5	Use of unexpected DNS server (with response, connections: 3, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:42	mirror_core	192.168.0.35
6	Use of unexpected DNS server (with response, connections: 6, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:23	mirror_core	192.168.0.20
7	Use of unexpected DNS server (with response, connections: 5, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:23	mirror_core	192.168.0.49
8	Use of unexpected DNS server (with response, connections: 9, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:18	mirror_core	192.168.0.27

192.168.0.53

Use of unexpected DNS server 192.168.0.53

192.168.14  
192.168.23  
192.168.22  
192.168.24  
...

3. Malware infected device trying to redirect and bridge traffic probably to get sensitive data



# See what you've been missing

## Free Network Assessment and 30-day Trial

### Discover what is hiding inside your network!

- Network Detection and Response
- Unknown threat detection
- Encrypted traffic analysis
- + Network monitoring and visibility included
  
- Easy to deploy (VMware, KVM, Hyper-V or your public cloud instance).
- Quick time to value - 30 minutes from deployment to dashboard insights
- For more visit <https://kemp.ax/>





**Thank You**  
kemp.ax