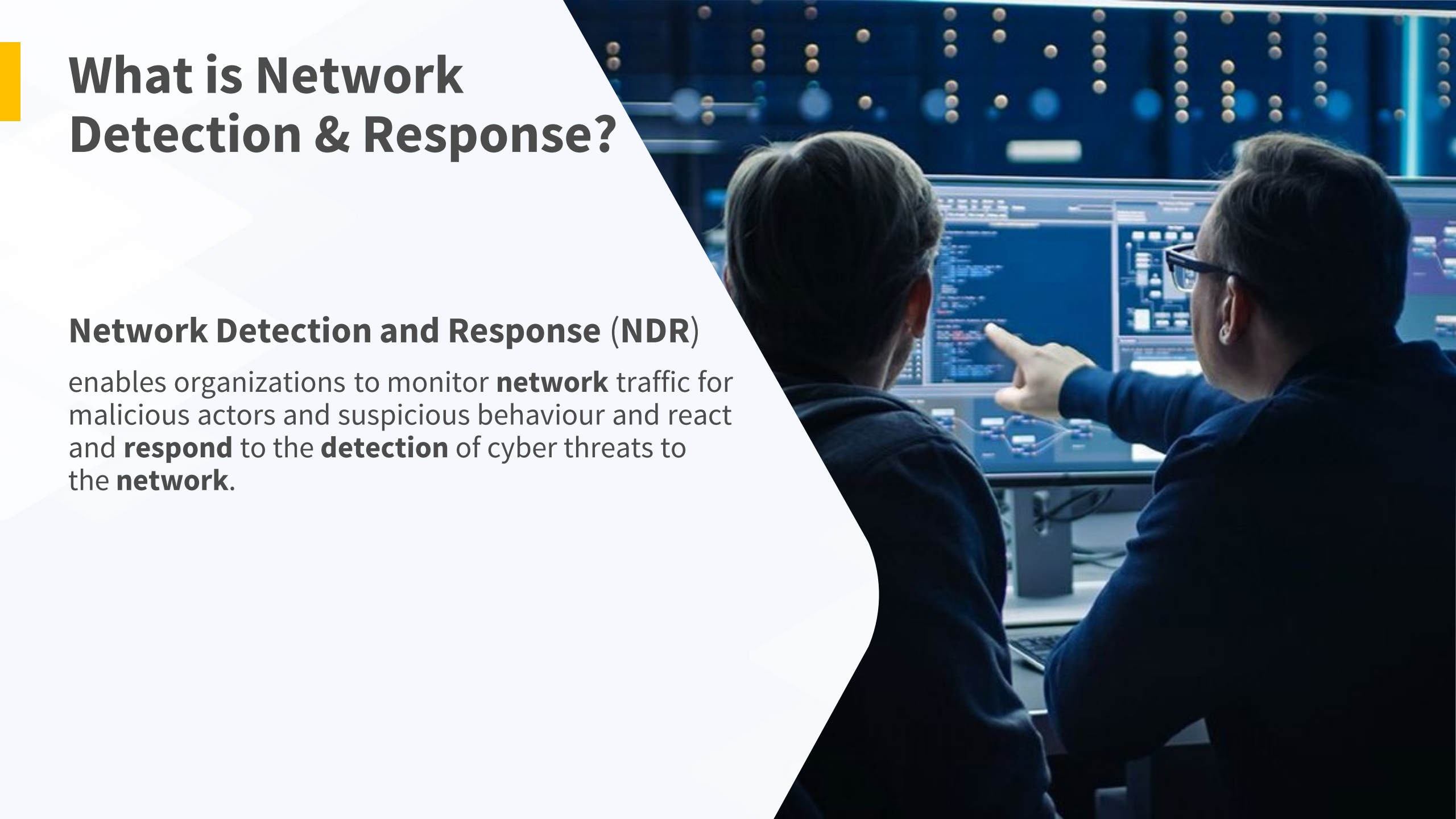
kemp

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**.

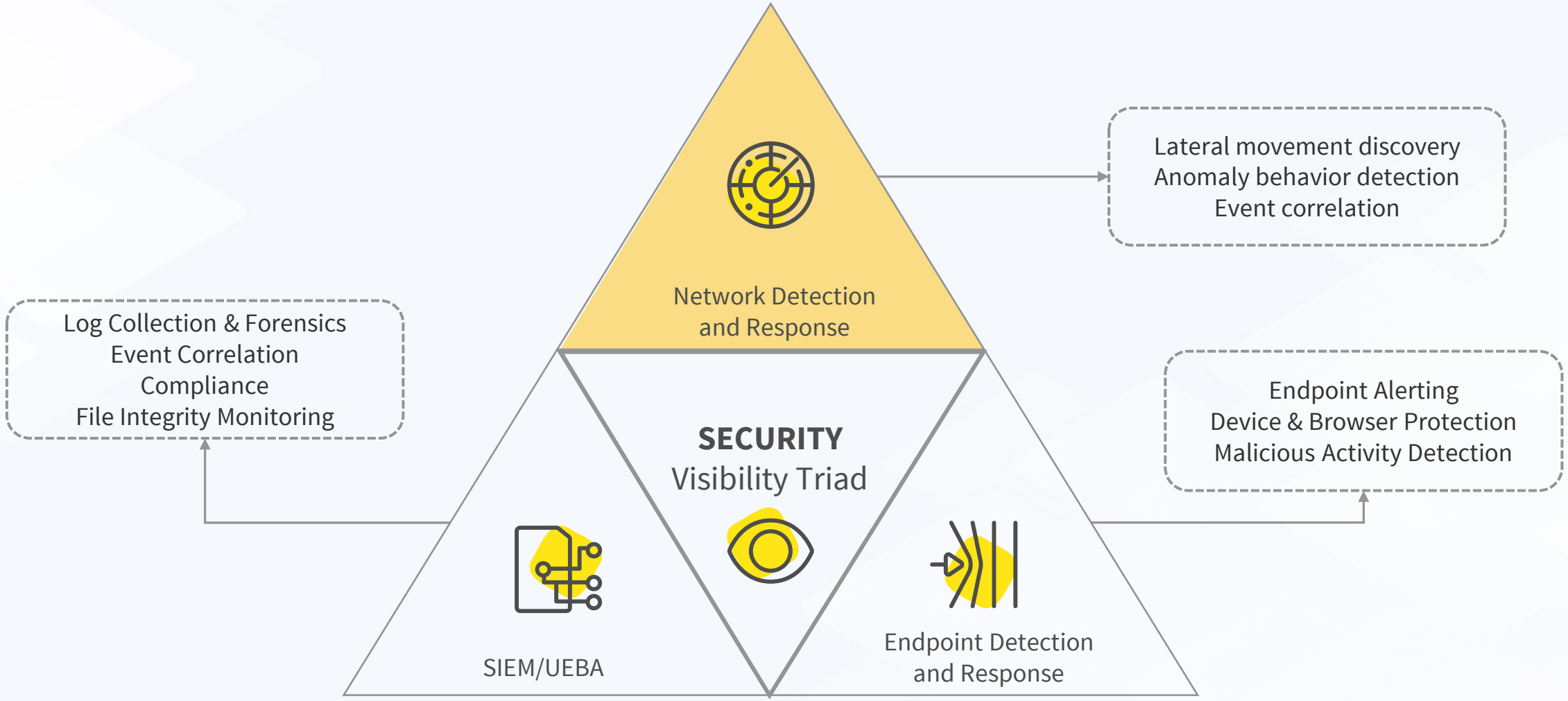
Gartner®

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

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

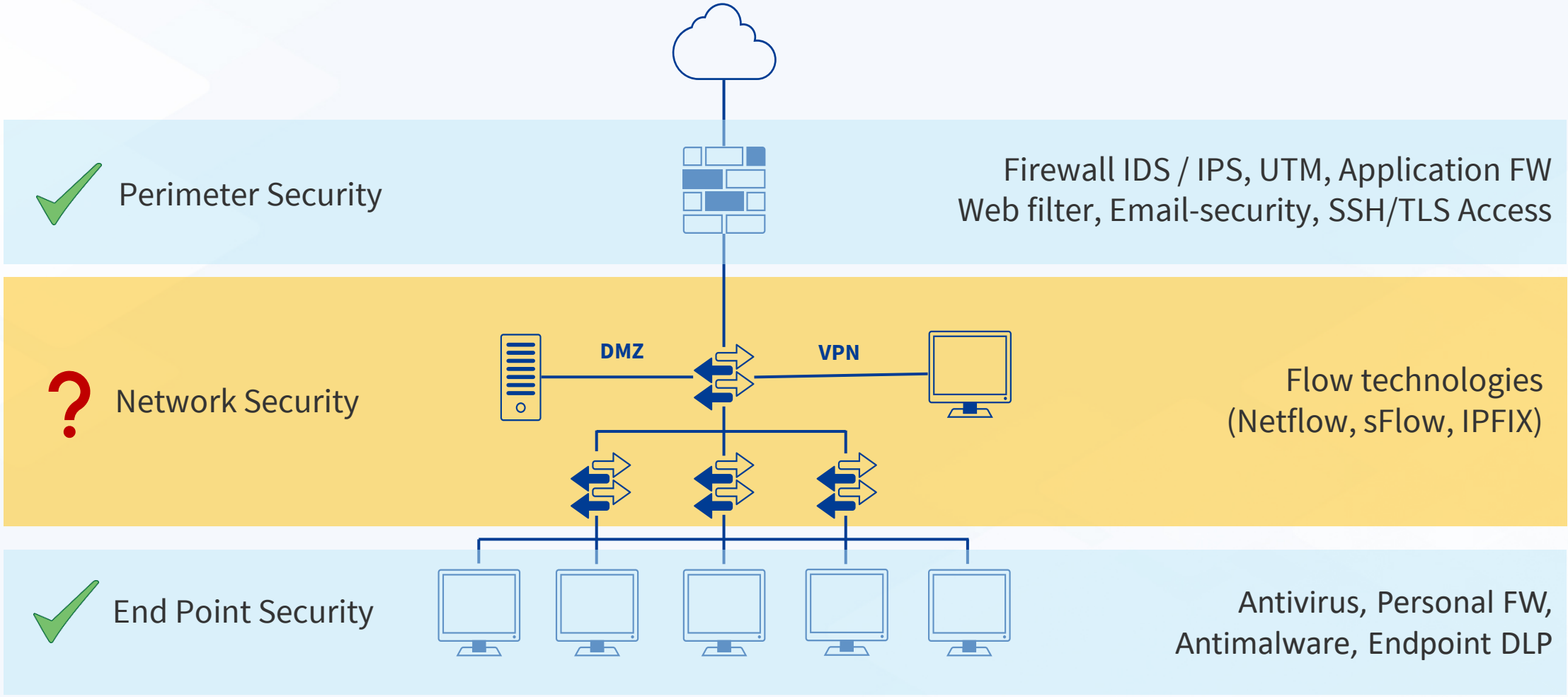
kemp

Security Visibility Triad



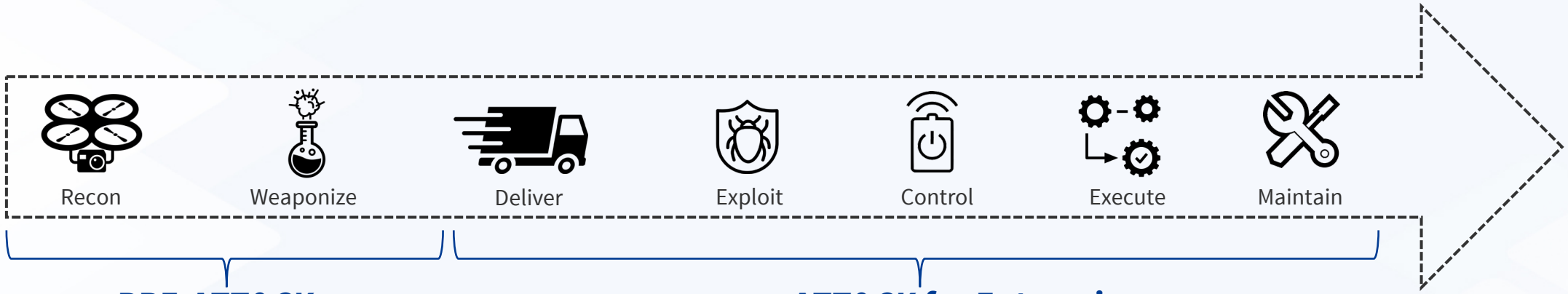
kemp

Network Security



kemp

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

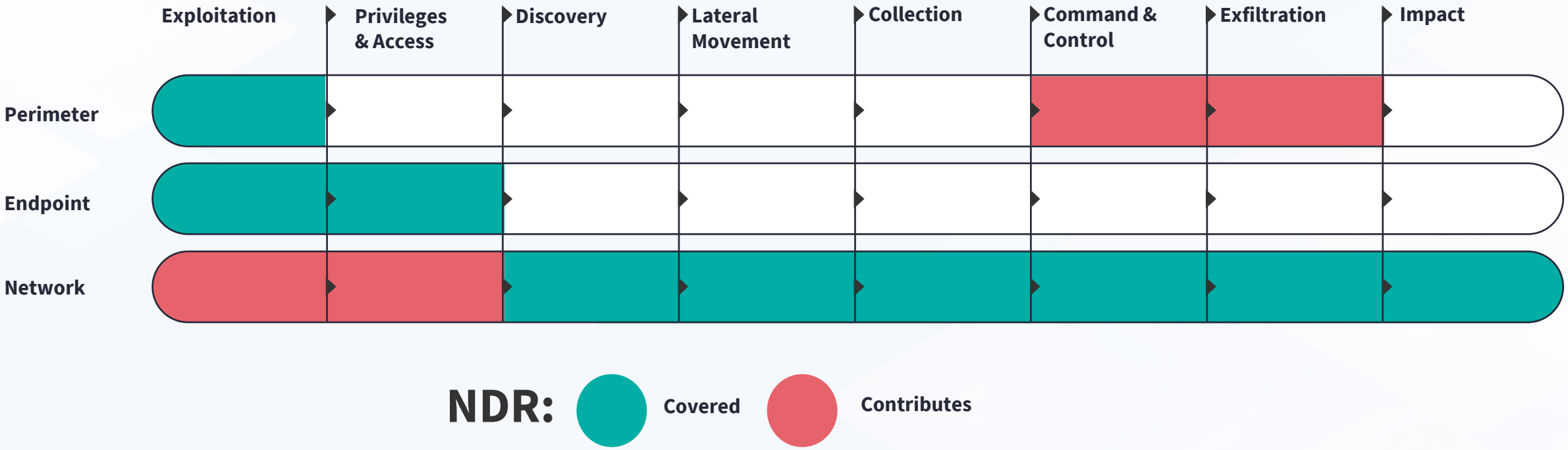
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact

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

kemp

Multi-Layered Security through MITRE ATT&CK Framework

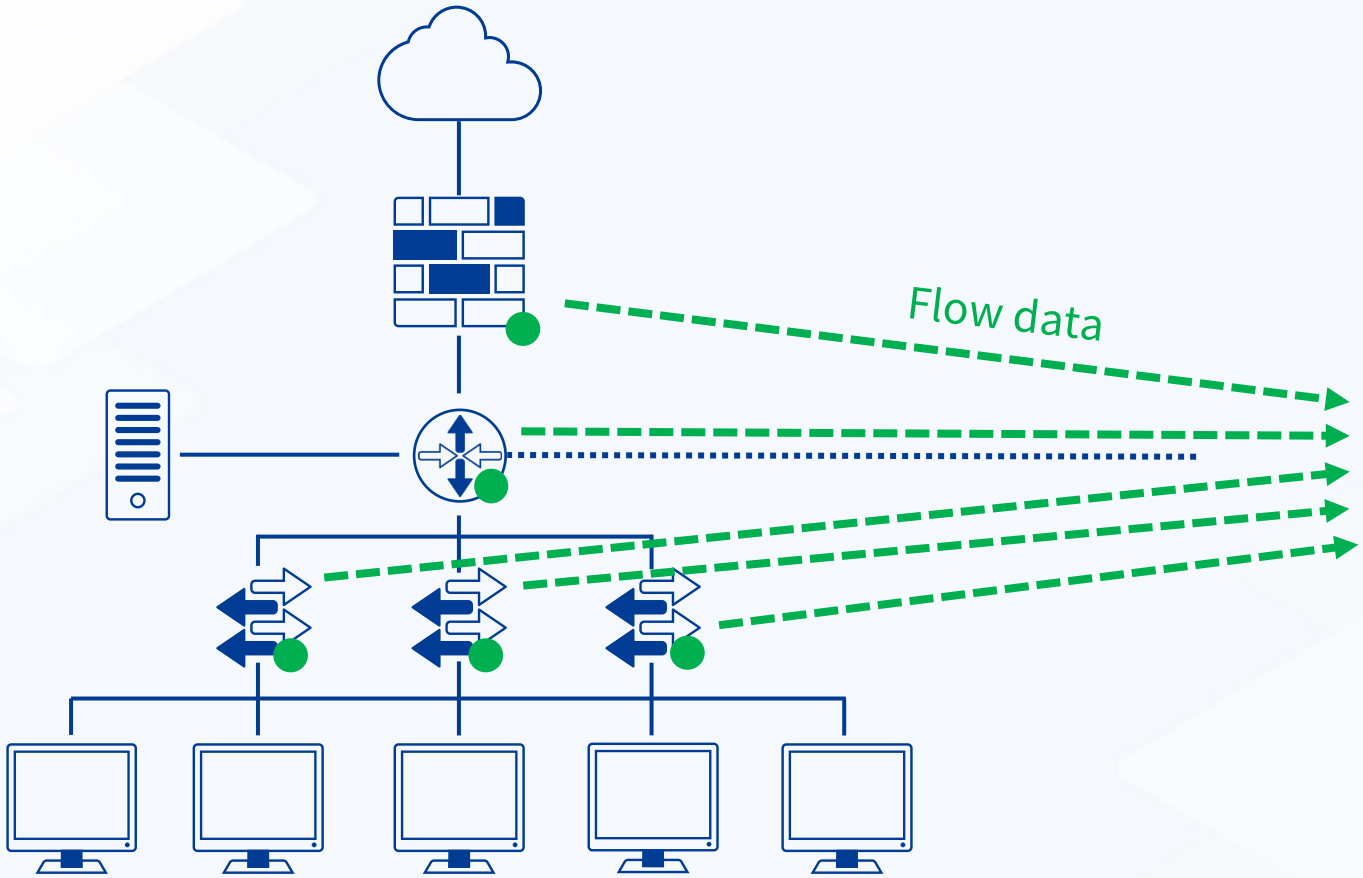
Multiple detection and prevention points are necessary to properly identify ransomware attacks



kemp

Let’s look at NDR technology…

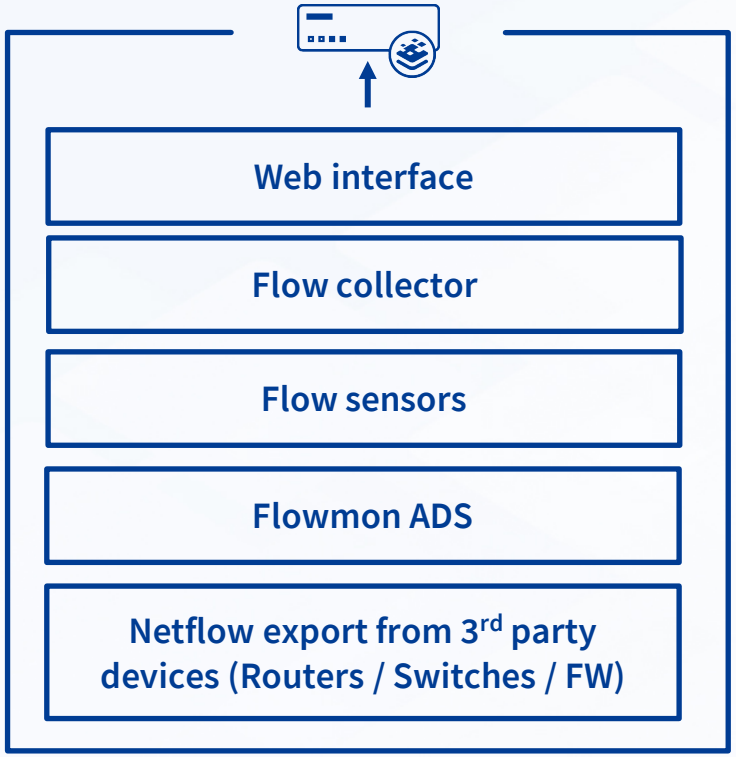
NDR Basic Deployment



Flow data

kemp

Flowmon Appliance

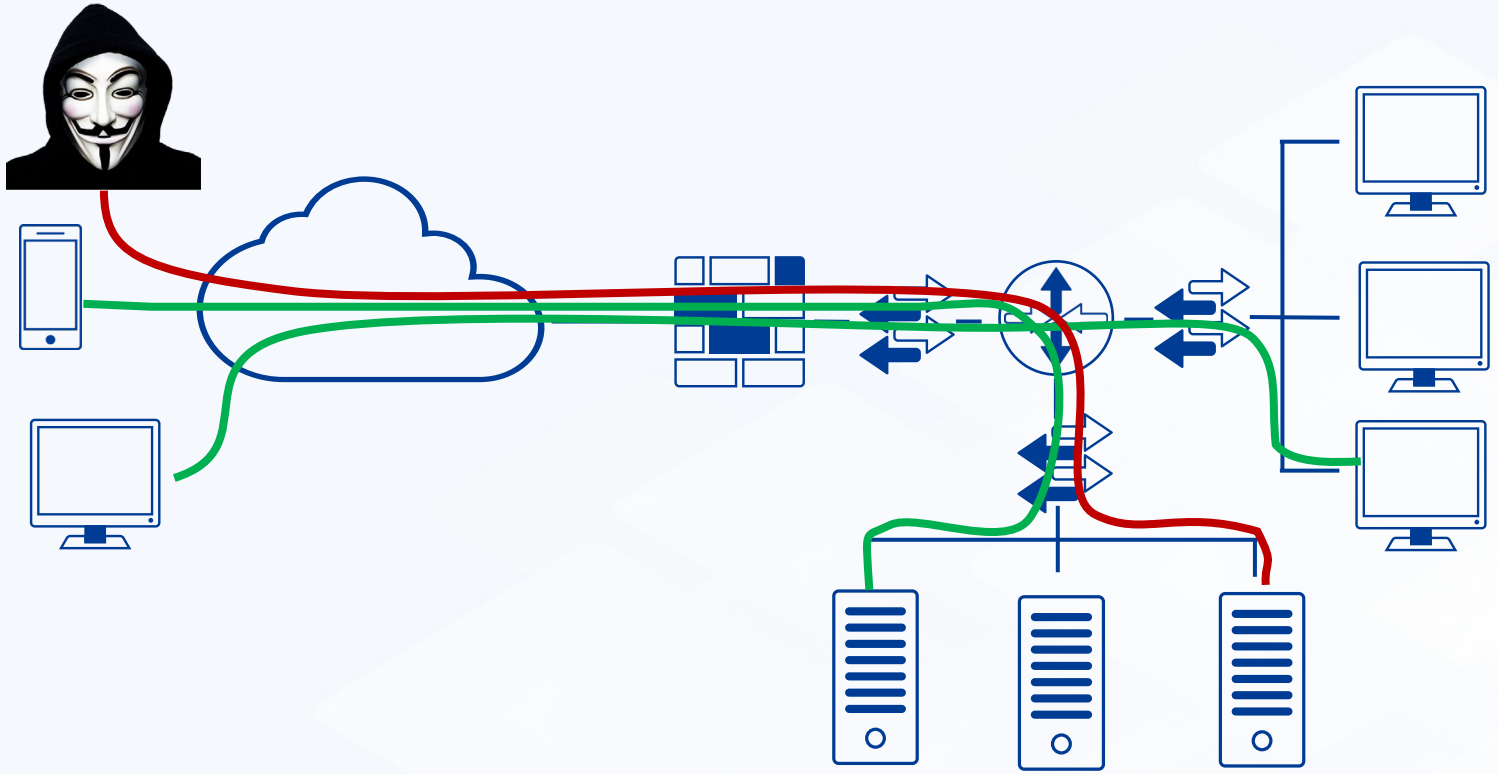


kemp

Needle In a Haystack

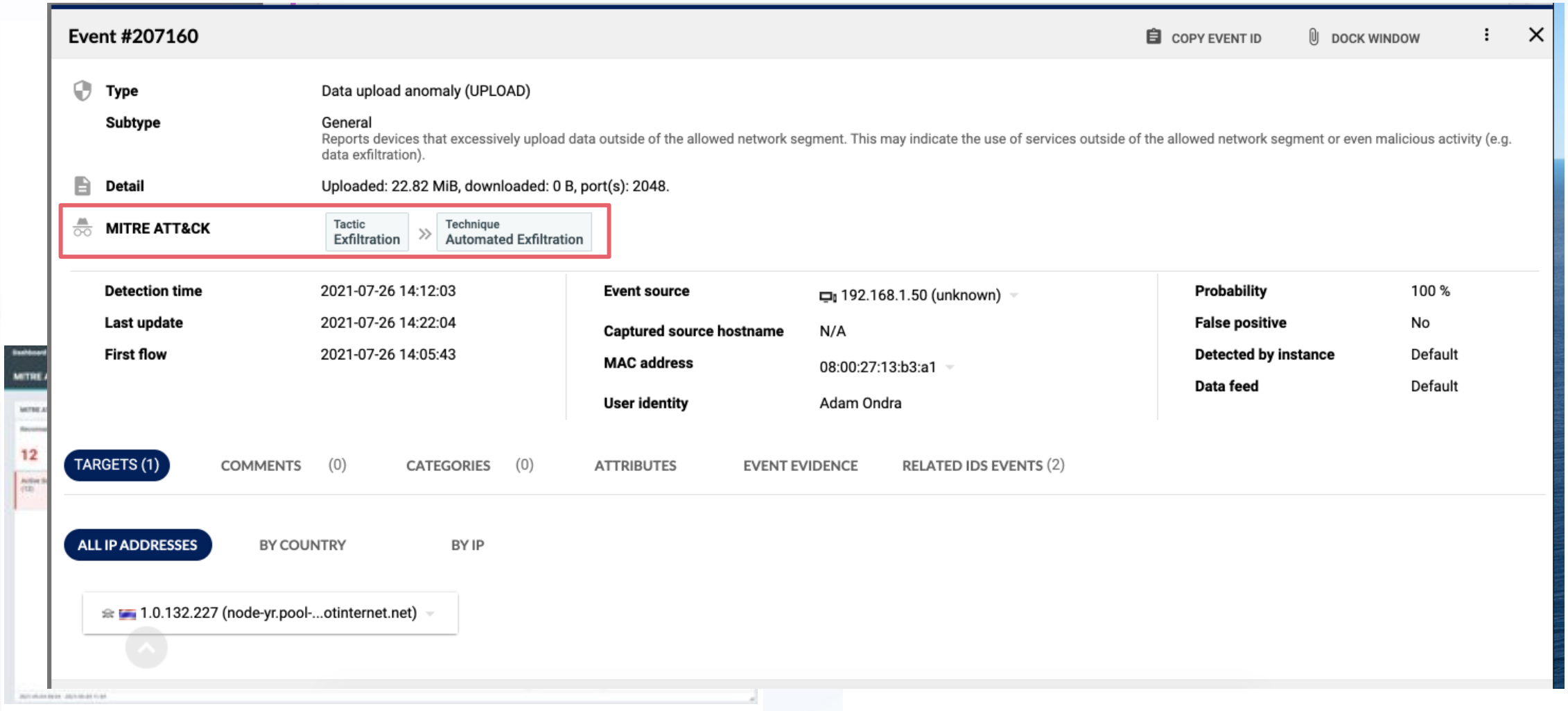
There is a lot of network traffic

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



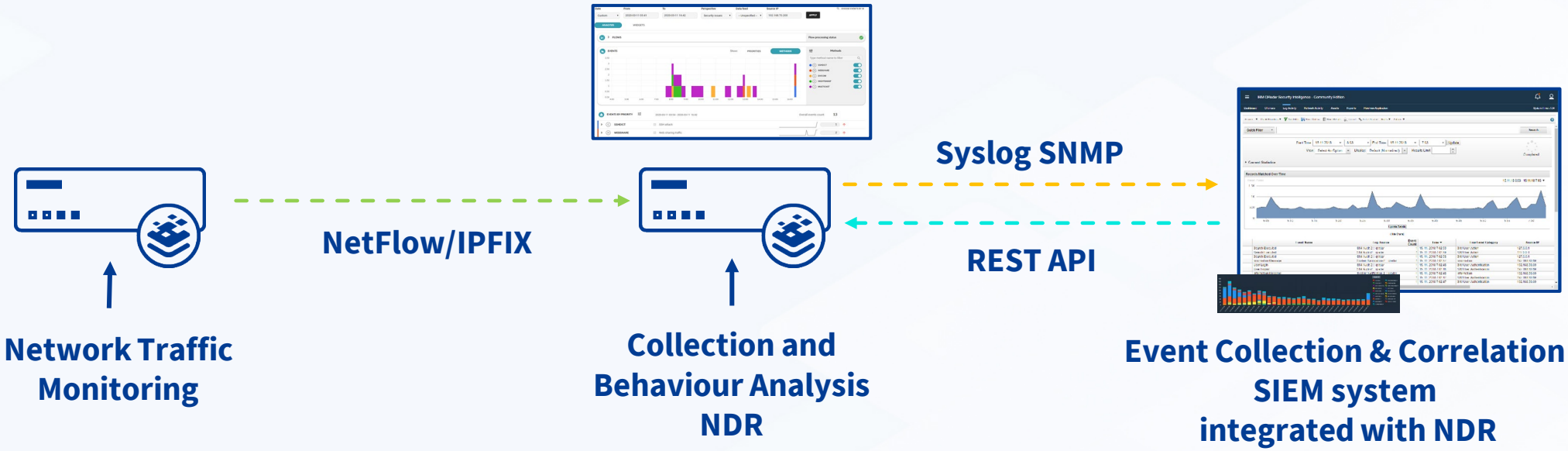
kemp

NDR Detection Capabilities



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



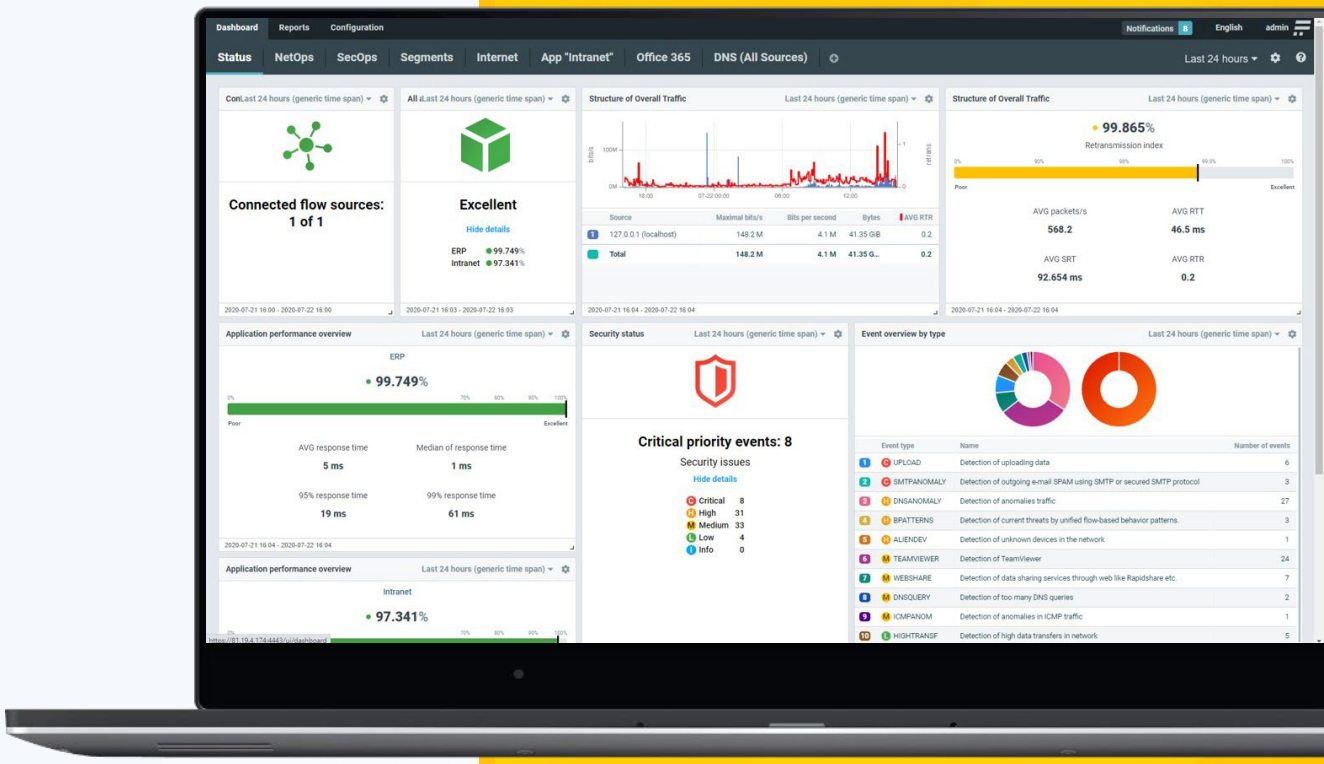
You Cannot Manage and Protect What You Cannot See

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



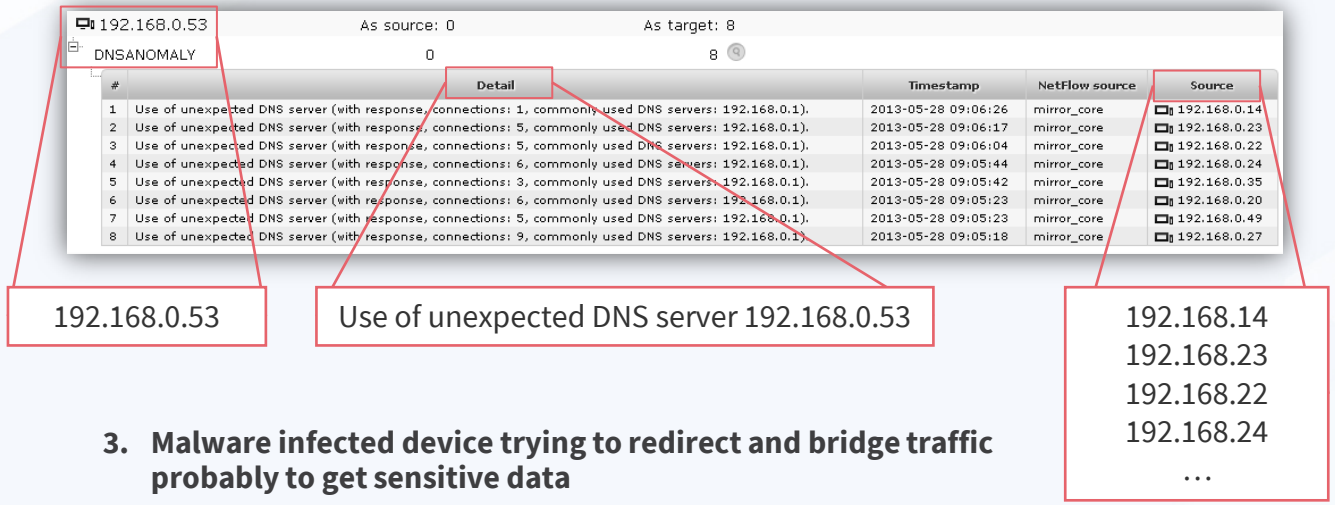
kemp

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



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