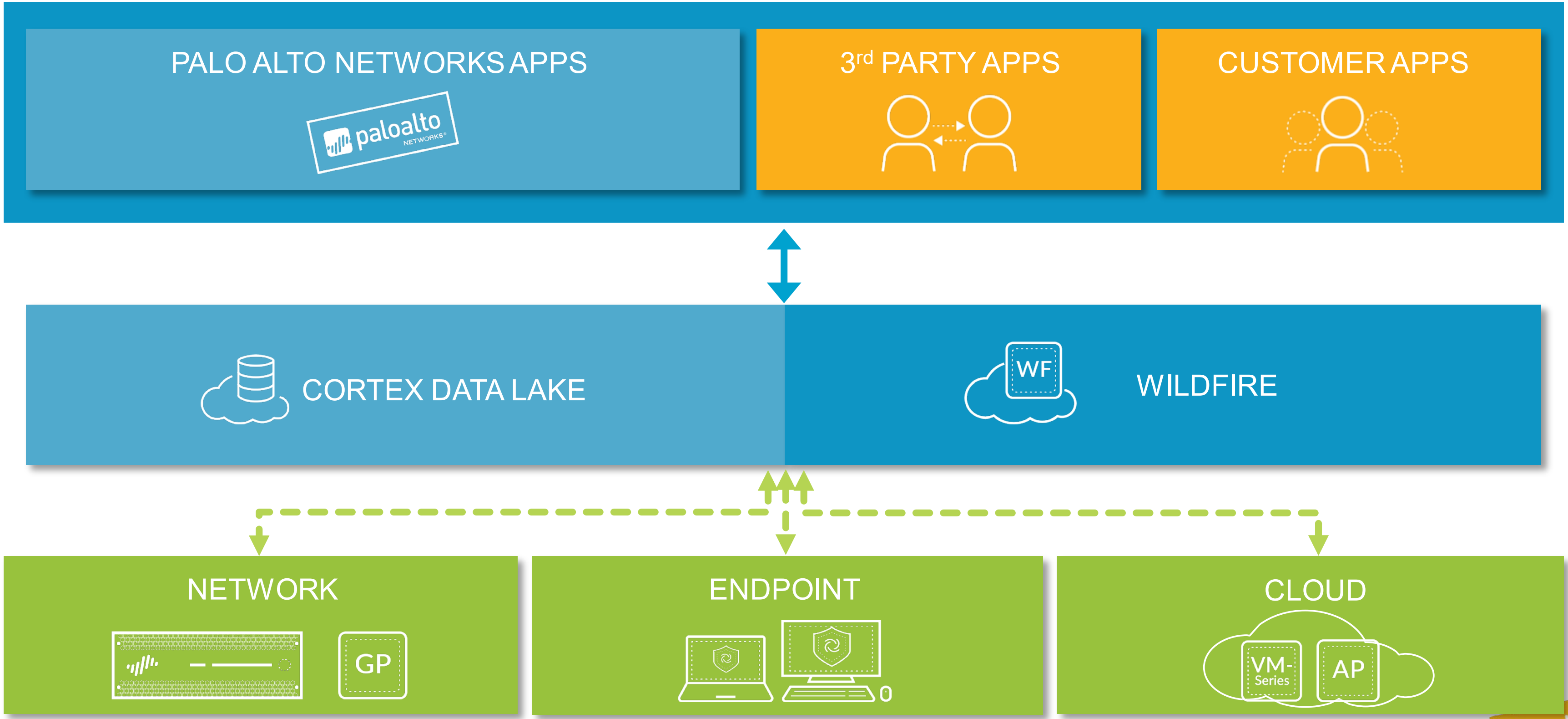
CORTEX XDR

Кирилл Ильганаев

CORTEX™
BY PALO ALTO NETWORKS



PALO ALTO NETWORKS APPS

3rd PARTY APPS

CUSTOMER APPS

CORTEX DATA LAKE

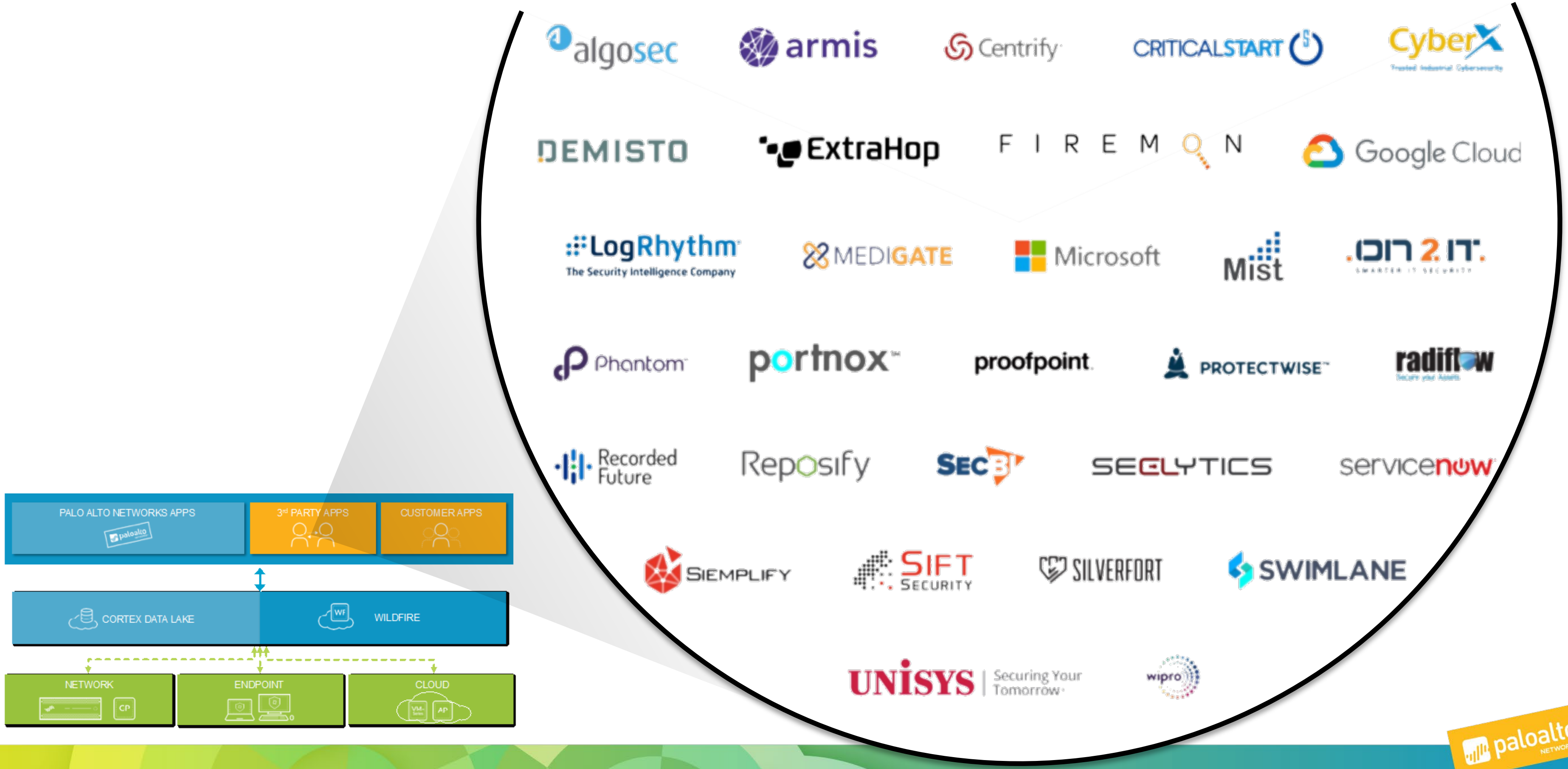
WILDFIRE

NETWORK

ENDPOINT

CLOUD

CORTEX APPS



PALO ALTO NETWORKS APPS

3rd PARTY APPS

CUSTOMER APPS

CORTEX DATA LAKE

WILDFIRE

NETWORK

ENDPOINT

CLOUD

algosec

armis

Centrify

CRITICALSTART

CyberX

DEMISTO

ExtraHop

FIREMON

Google Cloud

LogRhythm

The Security Intelligence Company

MEDIGATE

Microsoft

Mist

ON2IT

Phantom

portnox

proofpoint

PROTECTWISE

radiflow

Recorded Future

Reposify

SECBI

SECLYTICS

servicenow

SIEMPLIFY

SIFT SECURITY

SILVERFORT

SWIMLANE

UNISYS | Securing Your Tomorrow

wipro

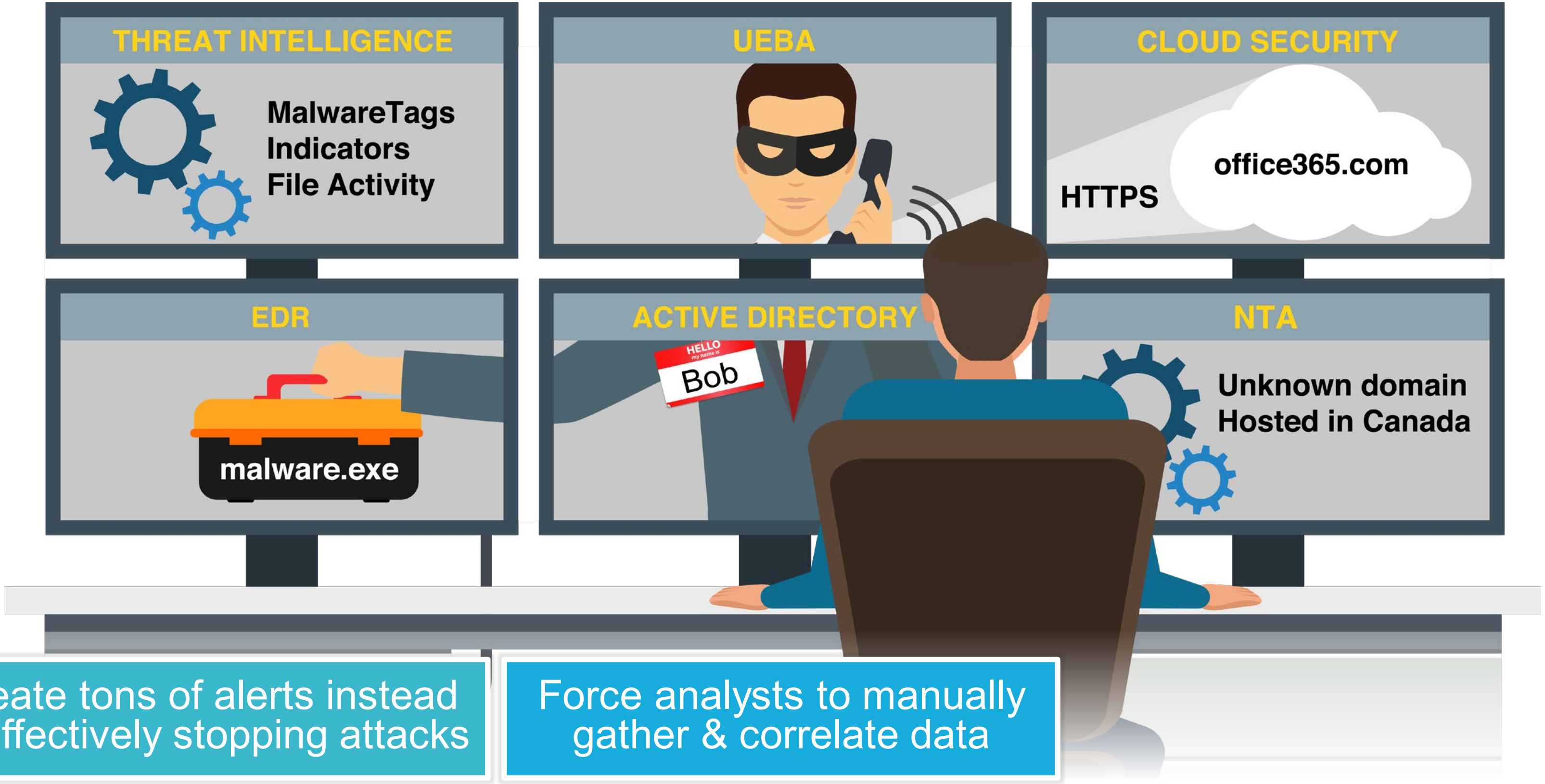
What is CORTEX XDR™ ?

SILOED TOOLS SLOW DOWN INVESTIGATION & RESPONSE

THREAT INTELLIGENCE
UEBA
CLOUD SECURITY
EDR
ACTIVE DIRECTORY
NTA

Create tons of alerts instead of effectively stopping attacks

SILOED TOOLS SLOW DOWN INVESTIGATION & RESPONSE

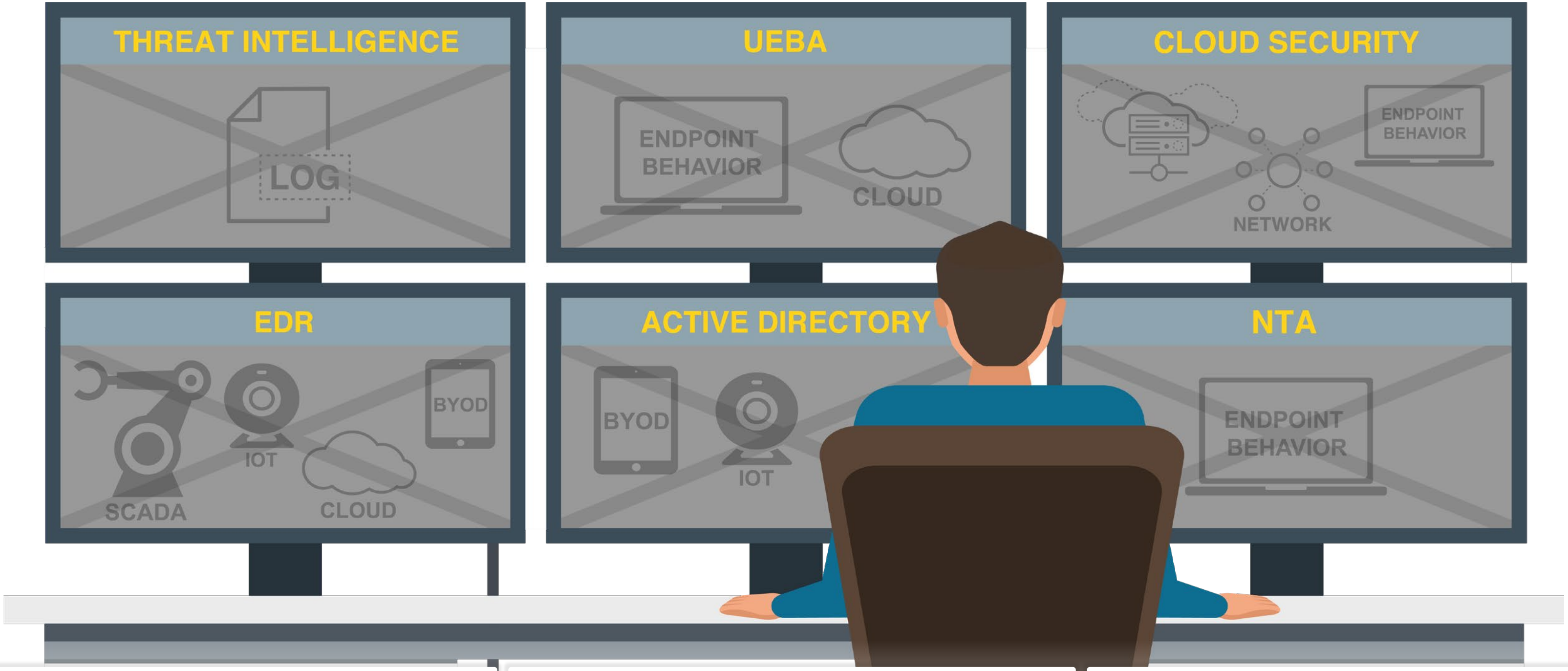


Create tons of alerts instead of effectively stopping attacks

Force analysts to manually gather & correlate data

|

SILOED TOOLS SLOW DOWN INVESTIGATION & RESPONSE

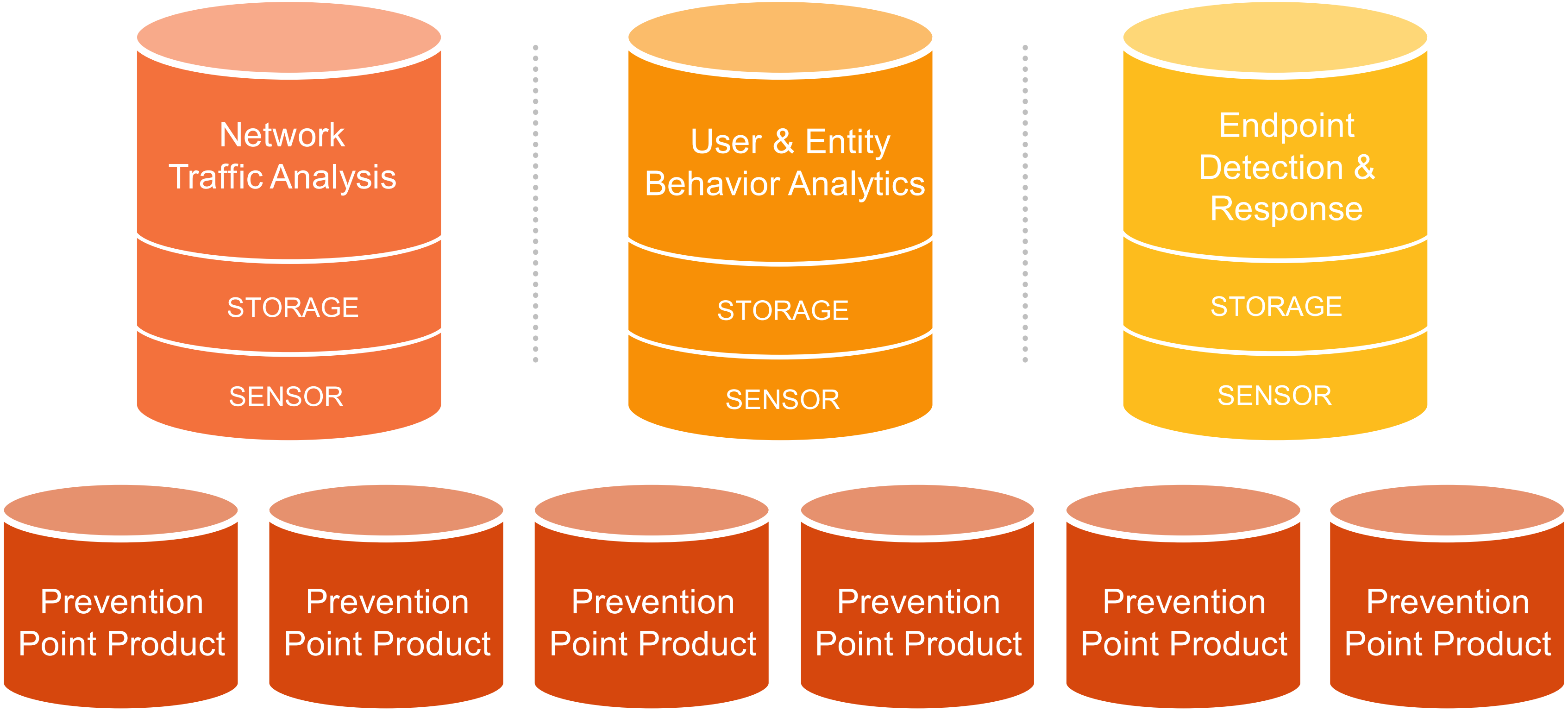


Create tons of alerts instead of effectively stopping attacks

Force analysts to manually gather & correlate data

Rarely collect all the data needed, creating blind spots

BREAKING SECURITY SILOS



Network Traffic Analysis

STORAGE

SENSOR

User & Entity Behavior Analytics

STORAGE

SENSOR

Endpoint Detection & Response

STORAGE

SENSOR

Prevention Point Product

Prevention Point Product

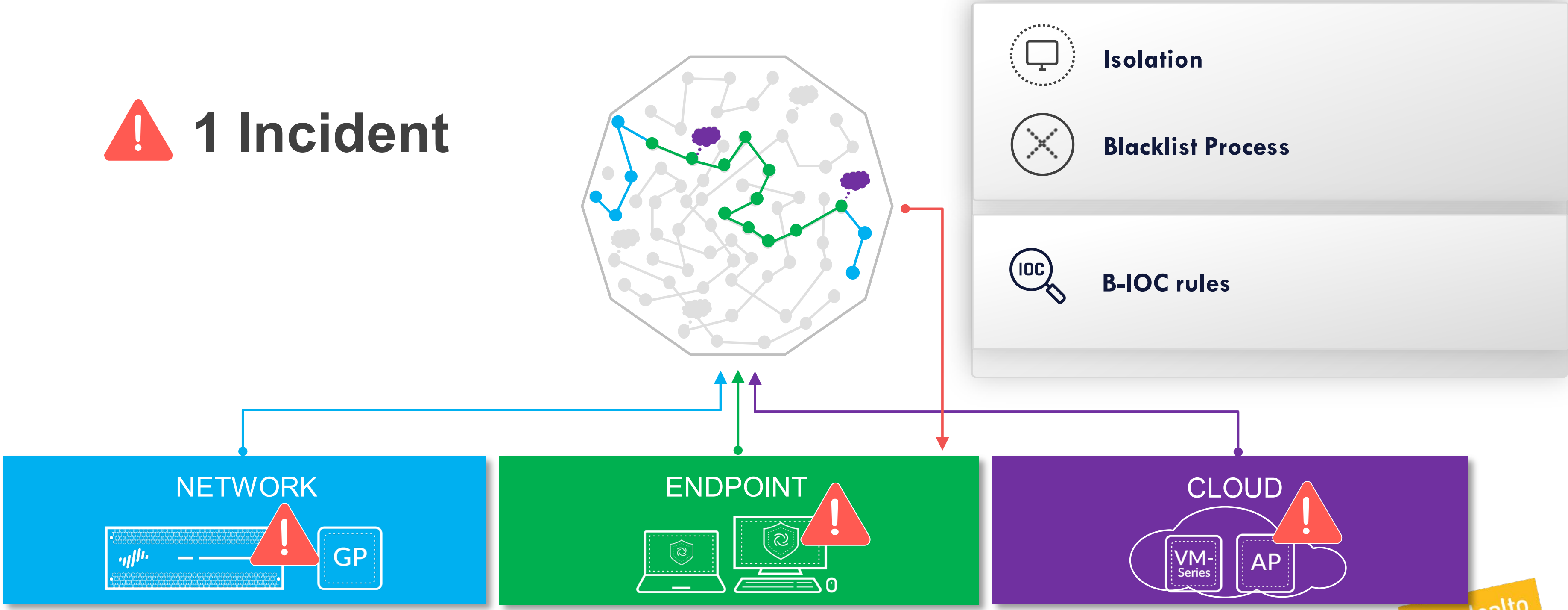
Prevention Point Product

Prevention Point Product

Prevention Point Product

Prevention Point Product

DETECT, INVESTIGATE, RESPOND & ADAPT



1 Incident

Isolation

Blacklist Process

B-IOC rules

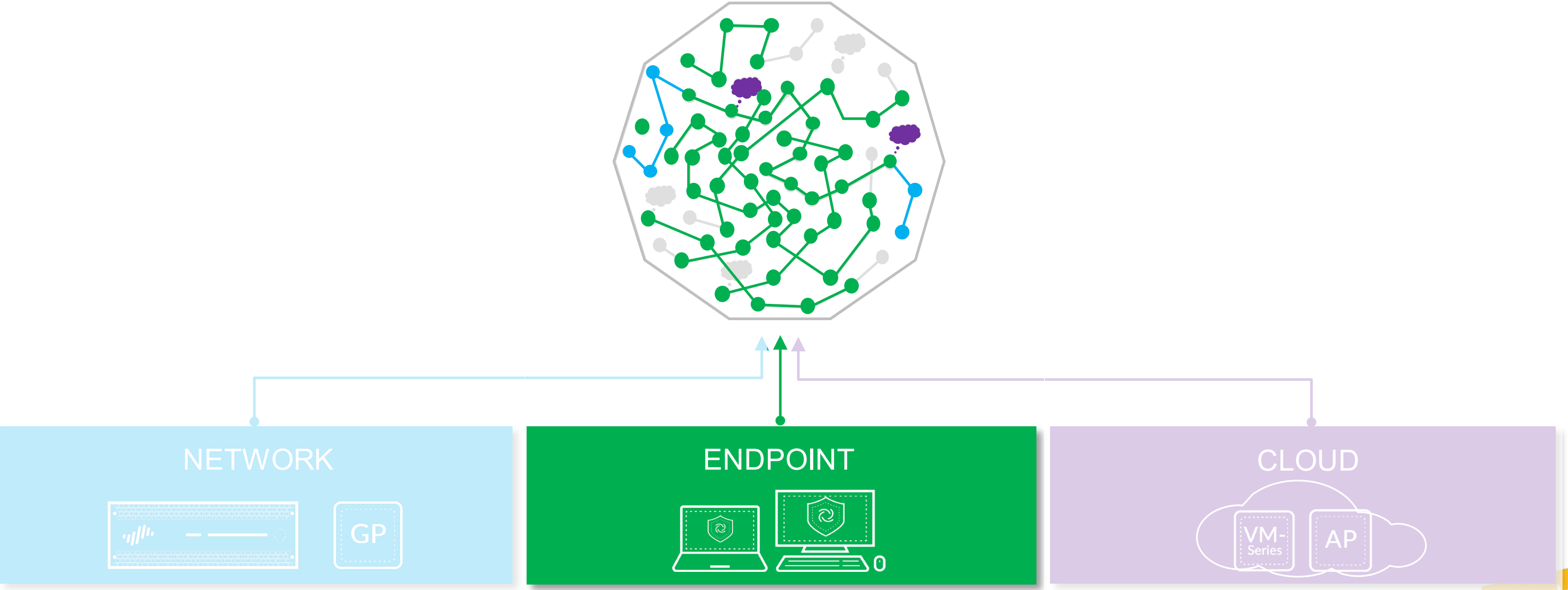
NETWORK

ENDPOINT

CLOUD

OLD VS NEW

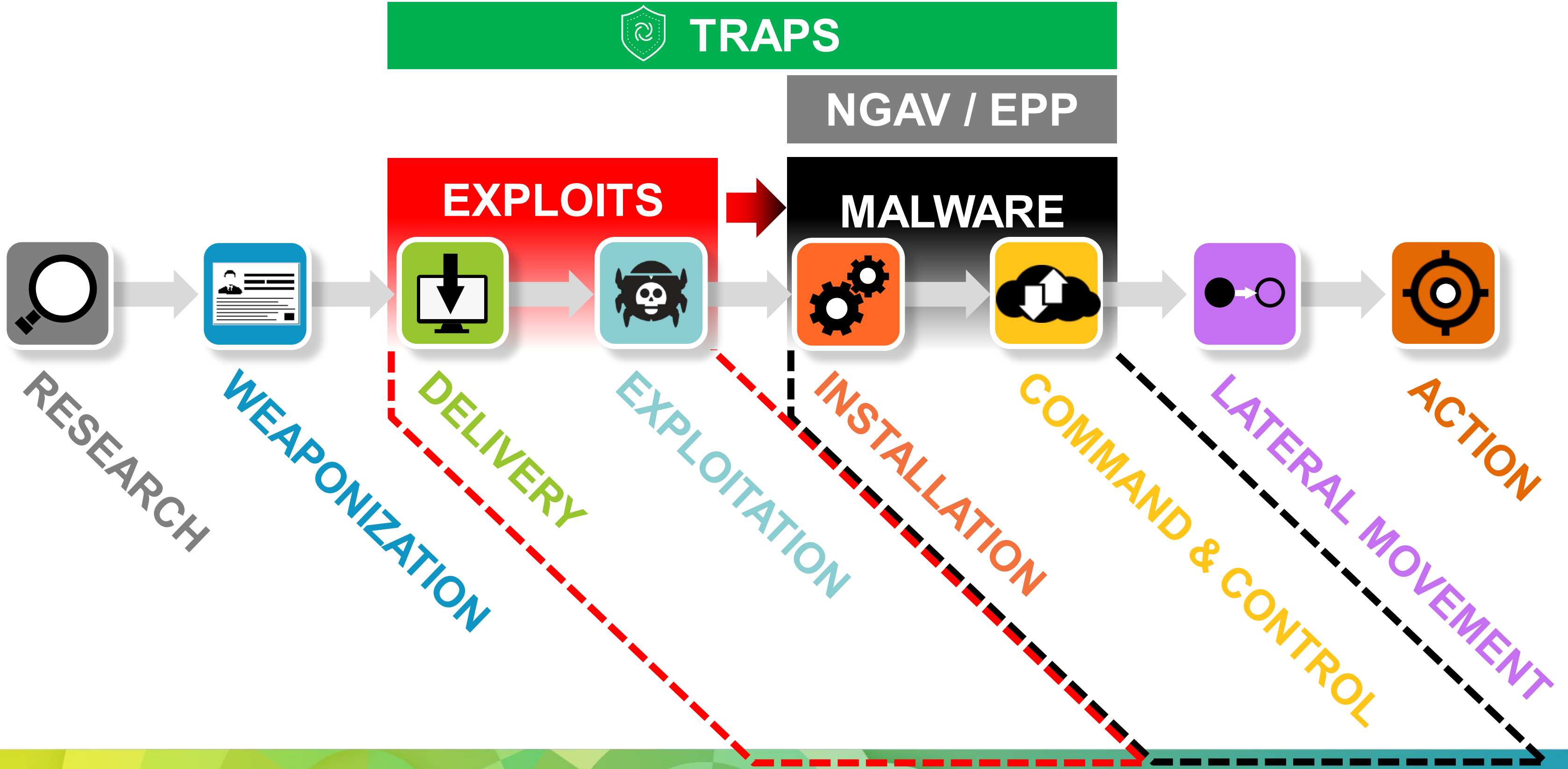
CORTEX XDR – TRAPS' Contribution



TRAPS

ADVANCED ENDPOINT PROTECTION

TRAPS in the Cyber Attack Lifecycle

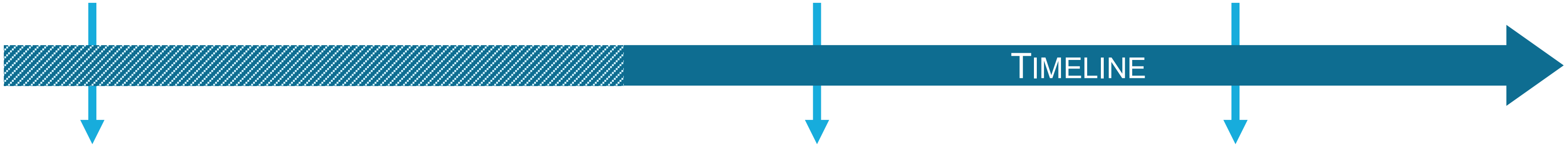


Value of Technique-based Exploit Prevention

SEPT 2017

Apr 2018

Oct 2018



Traps Version 4.1 Released

Vulnerability Discovered in Adobe Flash Player
(CVE-2018-0359)

Attackers Attempted to Exploit Vulnerability.

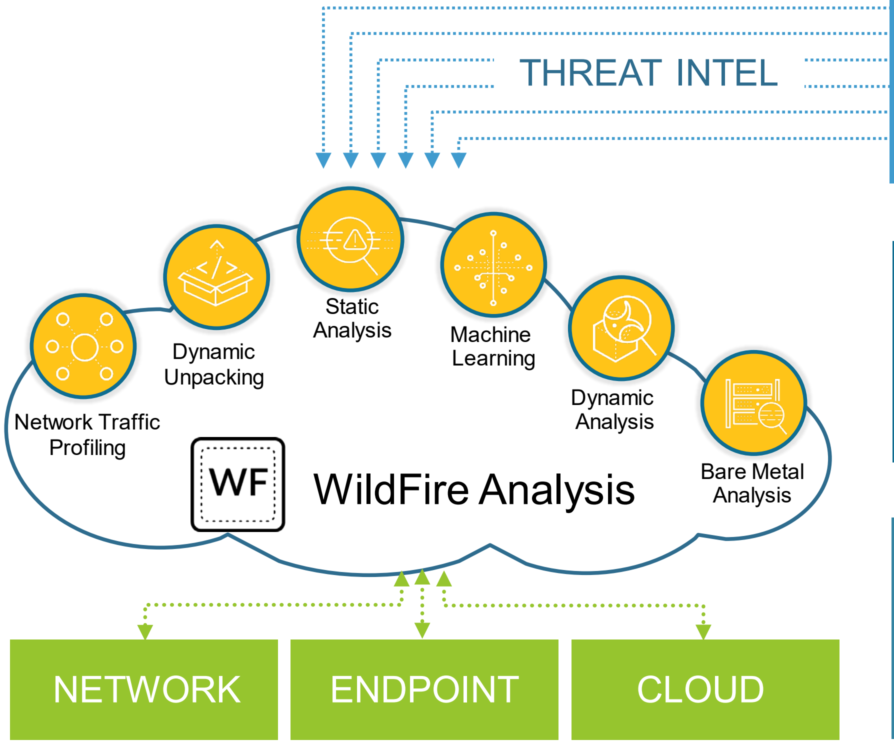
Traps Blocked the Attempt.

Traps v4.1

No Updates or Patches Since Installation

Traps <u>Prevents Zero-day</u> and Unknown Exploits That Have <u>Yet to be Discovered</u>

TRAPS - Malware Protection with WildFire

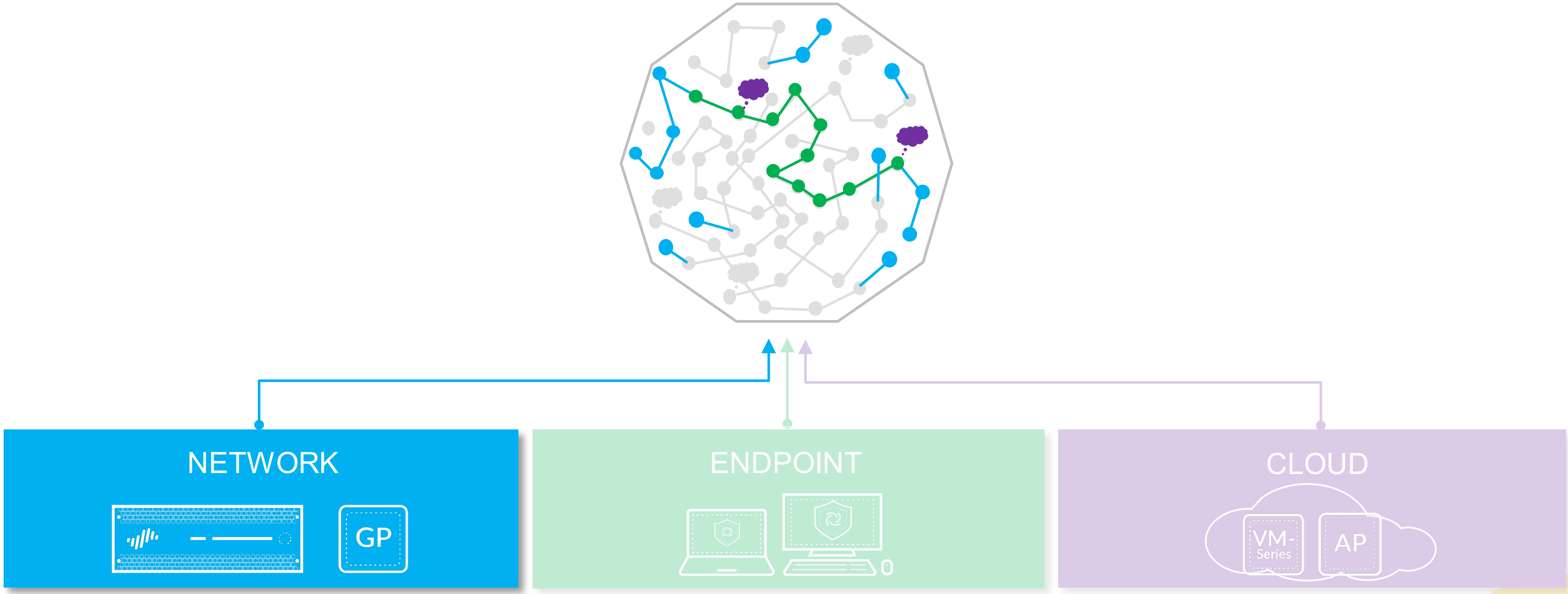


+150 sources of threat intelligence: 60,000 customers, Cyber Threat Alliance, VT…etc.

1000s of thin-PCs conducting **Bare-Metal Analysis**

300M new malware samples detected by WildFire **EVERY MONTH**

CORTEX XDR – NETWORK Contribution



NETWORK

GP

ENDPOINT

CLOUD

VM-Series

AP

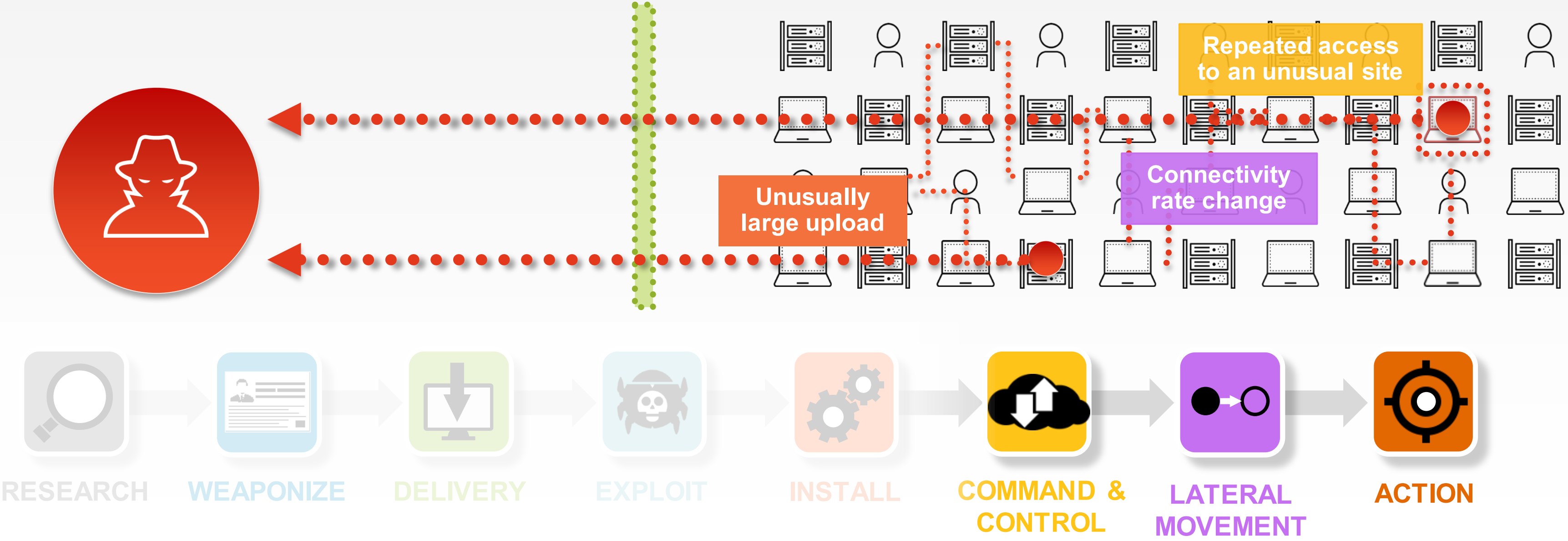
NG-FW

GP

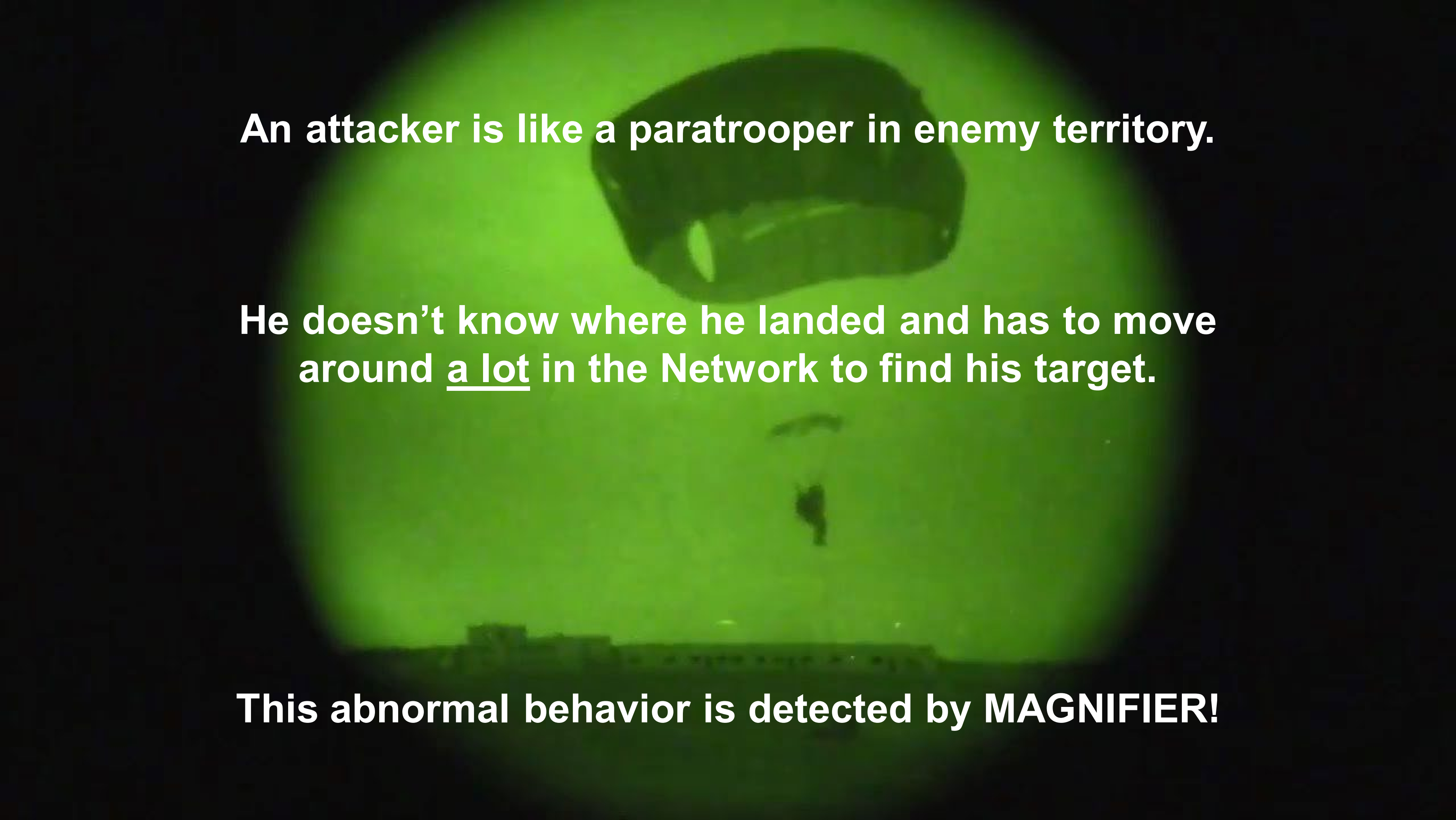
NEXT-GENERATION FIREWALL

CORTEX XDR ANALYTICS

- Attackers must perform thousands of actions to achieve their objective
- Profiles behavior to find anomalies indicative of attack



Detects the behavioral changes that attackers cannot conceal



An attacker is like a paratrooper in enemy territory.

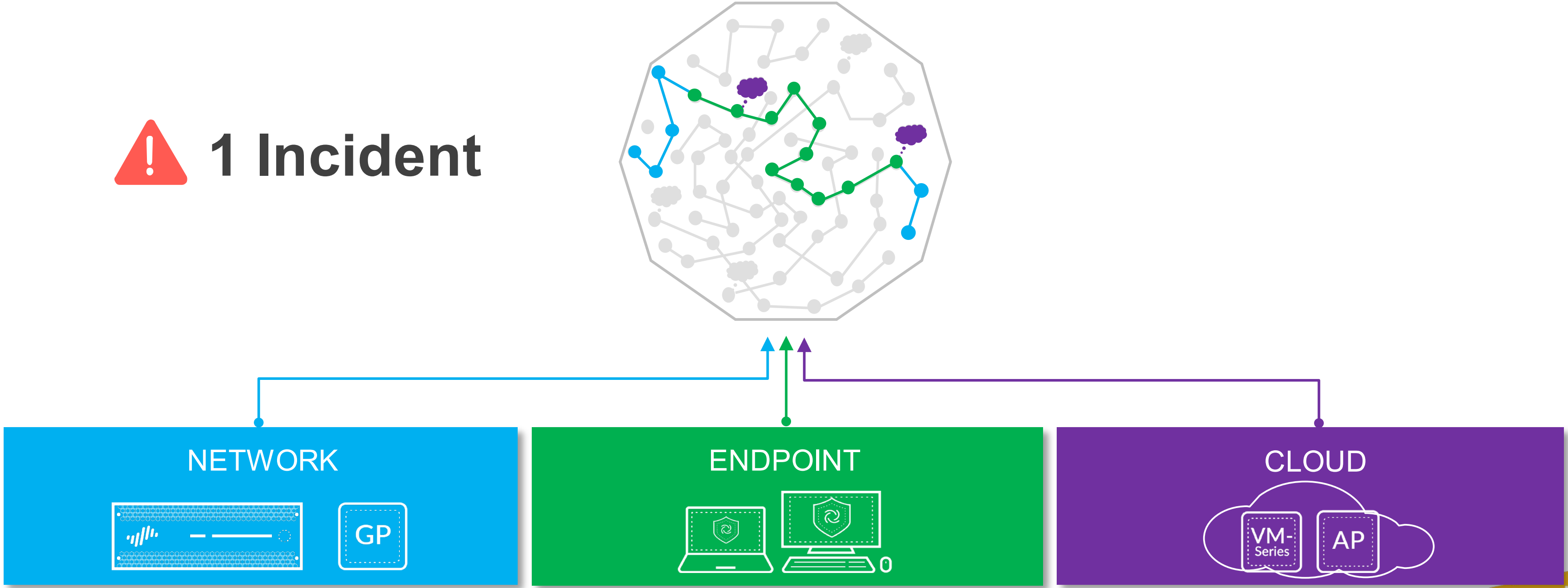
He doesn’t know where he landed and has to move around a lot in the Network to find his target.

This abnormal behavior is detected by MAGNIFIER!

CORTEX XDR™

DETECT, INVESTIGATE, RESPOND & ADAPT

⚠ 1 Incident



NETWORK

GP

ENDPOINT

CLOUD

VM-Series

AP

Спасибо!

Кирилл Ильганаев

kilganaev@paloaltonetworks.com