Trellix

3-6 November 2025

EMEA & LTAM Tech Summit

Madrid, Spain

Trellix

Network Detection & Response (NDR)

Defend, Prevent, Investigate, Contain, Respond, Hunt, & Forensics from Network

Today's Presenters

Ravi Adireddy

Director, Product Management

Hemant Pandya

Sr. Solutions Engineer

Mohammed Hasanain

Solutions Engineer

Trellix

Content being Presented Today

Trellix NDR Solution Capabilities	30 Minutes
NDR Key Use-cases	20 Minutes
NDR Architecture, Design, Integrations	20 Minutes
NDR Roadmap	20 Minutes
Break	30 Minutes
NDR Demonstration	40 Minutes
NDR Licensing	10 Minutes
Trellix NDR Differentiators	20 Minutes
Q & A	20 Minutes

Trellix

Trellix

Trellix NDR Solution Capabilities

Duration - 30 Minutes

Trellix

Challenges

An Organization’s evolving Challenges

Are you only seeing half the picture?

69%
[2]Unknown, poorly managed assets

35%
[3]Ignored alerts

16 days
[1]Global median dwell time

133%
[4]Increase in number of assets to protect

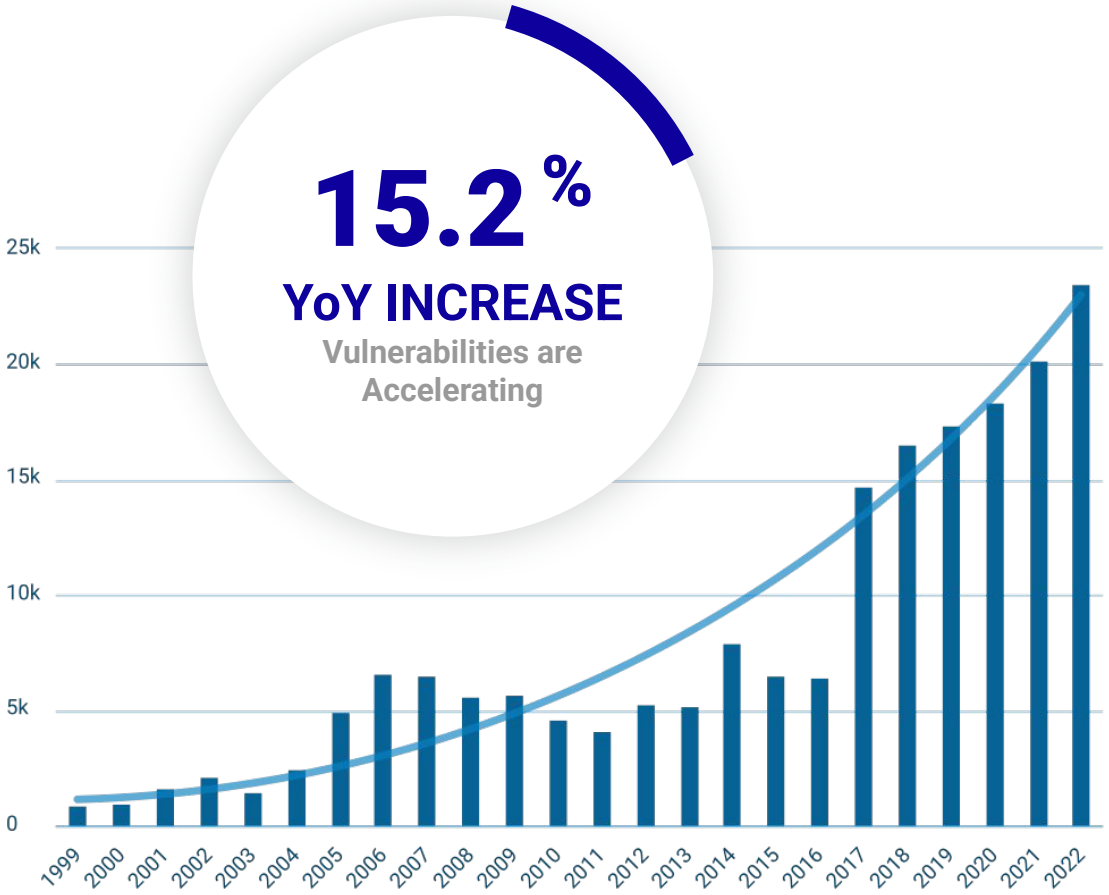
[1]Mandiant. 2023. M-Trends 2023 Mandiant Special Report

[2]ESG 2023 (https://www.esg-global.com/research/esg-research-report-security-hygiene-and-posture-management)

[3]FireEye 2021 (IDC InfoBrief "The Voice of the Analysts: Improving Security Operations Center Processes Through Adapted Technologies")

[4]JupiterOne 2023 (The 2023 State of Cyber Assets Report)

Vulnerability Sprawl



- Over 2000 vulnerabilities (CVEs) **every month** and growing; 300-500 applicable to every organization regardless of size
- Vulnerability scanners do a poor job of prioritizing – one-size-fits-all metrics that leave huge backlogs and **fail to capture how breaches/ransomware happen**
- Three options – manual analysis, roll your own prioritization system, or try to patch everything
- New assets (transient/ephemeral/unmanaged) pop-up without following due process - who is aware?

Trellix

Today’s Network Challenges

Network Security Manager

“We can’t keep up with monitoring our complex network and the amount of alerts generated by the tools we do have.”

Network Security Architect

“Honestly, we’re struggling to maintain visibility and control in a complex, distributed network while managing alert volumes and balancing security with performance."

Security Operations Center (SOC) Director / Sr. SOC Analyst

“I need a system to be better and faster at detecting, prioritizing, and remediating breaches. It is too much effort to maintain the networks.”

Trellix

Today’s Network Challenges

Security Blind Spots

Growing Assets:

133%

Increase in number of assets to protect

Trellix

Today’s Network Challenges

Security Blind Spots

Growing Assets:

133%

Increase in number of assets to protect

69% of organizations reported unknown, poorly managed assets on the network

Trellix

Today's Network Challenges

Security Blind Spots

Growing Assets:

133%

Increase in number of assets to protect

Persistent Attackers

Recurring Attacks

43%

Organizations hit by ransomware were hit more than once[4]

69% of organizations reported unknown, poorly managed assets on the network

Trellix

Today's Network Challenges

Security Blind Spots

Growing Assets:

133%

Increase in number of assets to protect

Persistent Attackers

Recurring Attacks

43%

Organizations hit by ransomware were hit more than once[4]

Complex Investigations

Ignored Alerts:

35%

Security analysts who say alerts are ignored when the queue is full[3]

69% of organizations reported unknown, poorly managed assets on the network

Trellix

Remain with the Status Quo or Not?

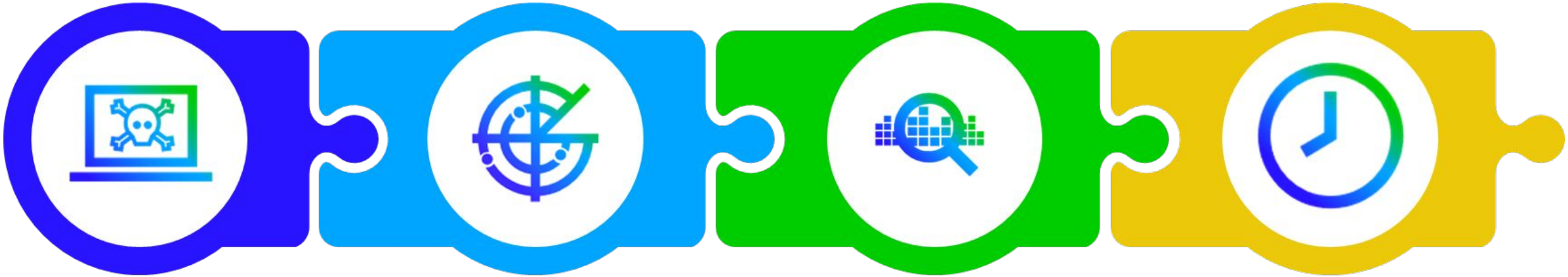
Increased security blind spots

Increased breaches / cyber attacks

Lack of information for investigation

Trellix

More is needed for Advanced Threat Protection



Keep known threats out

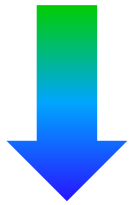
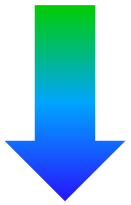
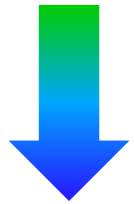
Detect unknown, emerging threats

Investigate the breach

Respond Quickly

Trellix

Required Capabilities to Solve Challenges

Security Blind Spots	Persistent Attackers	Complex Investigations
		
Eliminate blind spots	Disrupt attackers at each stage	Speed investigation and response

Trellix

NDR Aligns with Security Priorities

Strategic Decision

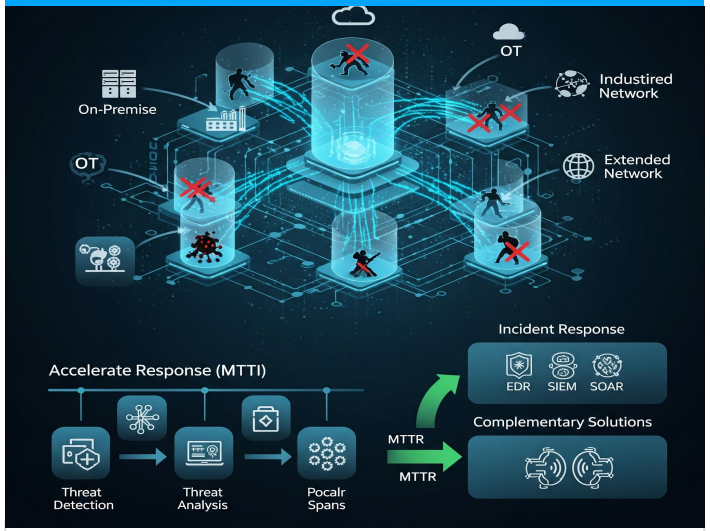
Align on Strategic Security Objectives

Supports: Defense in Depth for your investments in broader security initiatives (Compliance, AI, Zero Trust, Cloud)

Protects: Living off the Land (LOTL), Advanced Persistent Threats, and Insider Threats

Improves: Visibility and your Incident Response by complementing Endpoint Detection and Response (EDR), SDR, Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR)

Technical Decision



Accelerate Investigation and Response

Empowers: Acceleration in response and improved Mean Time to Investigate (MTTI) and Mean Time to Resolve (MTTR)

Monitors: On-premises, Cloud, OT, and extended network infrastructures

Disrupts: Attackers at every stage of the cyber kill chain

Operational Decision

Integrate Seamlessly with SOC Process

Integrates: With the existing Security Operations Center (SOC) tools and workflows

Enables: Tier 1 and Tier 2 analysts to advance their skills during alert triage

Minimizes: Noise with better threat efficacy

Trellix

Why Trellix?

35

Our security products are backed by years of **experience**.

3600

Trellix employees in 185 countries provide **24/7/365 service**

53,000+

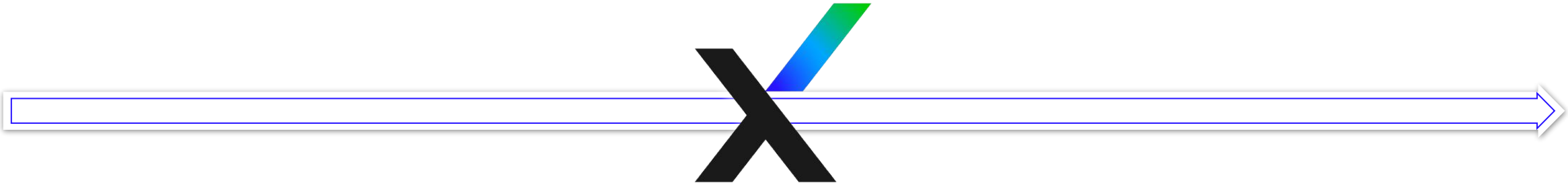
Customers supported **globally**

250+

Global Advanced **Threat Intelligence** Researchers

80

Customers in the **Fortune 100**



QKS Group

SPARK Matrix Named Trellix as Leader in Network Detection and Response. 2024

FORRESTER®

Large Vendor in the Forrester Now Tech: Network Analysis And Visibility Q1-2023

IDC

Ranked 5th in IDC's 2023 Worldwide Trusted Access and Network Security Market Share.

Gartner®

Named a **Representative Vendor** in the Gartner Market Guide for Network Detection and Response (NDR), 2024

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

Network Detection and Response: Publisher's Choice Award

Trellix

Trellix

Trellix NDR Solution

Approach & Capabilities

Strategy and Vision

Formulate and implement a defense-in-depth strategy to minimize the attack surface and response times

Visibility

Deliver enhanced visibility across complex on-premises, cloud and hybrid networks. Going beyond just endpoints, to provide complete asset discovery for both IT and IoT/OT environments.

Detection and Analytics

Offer superior efficacy by encompassing a multi-layered, ML-based detection approach with high-fidelity detections for known, unknown and emerging threats.

Analyst Experience

Enable defenders to proactively reduce breach risk. Rapidly respond to threats throughout the entire cyber-kill chain leveraging Agentic A.I-guided investigations; reduce alert fatigue.

Integration

Provide deeper, actionable detections through a centralized console. Aggregate and correlate network telemetry from multiple sources. Enable Hyperautomation.

Trellix

The best of both worlds

Legacy & Evolution from SecOps

Built for:

- SOC, MDR & IR Operations
- Enterprise scale
- Threat-model based

Battle-tested & Proven Products Capabilities

Extended with:

- NTBA
- Endpoint visibility

Trellix Security Platform

Integrated with:

- Trellix Threat Intelligence
- XDR Platform
- Trellix WISE

Trellix

The Trellix® Approach

Eliminate blind spots

- Not just perimeter - N/S and E/W
- On-premises, cloud, or hybrid environment visibility
- Asset discovery and monitoring

Disrupt attackers at every stage

- Not just initial compromise
- Multi-layered (ML) based approach
- Detection of known, unknown, and emerging threats

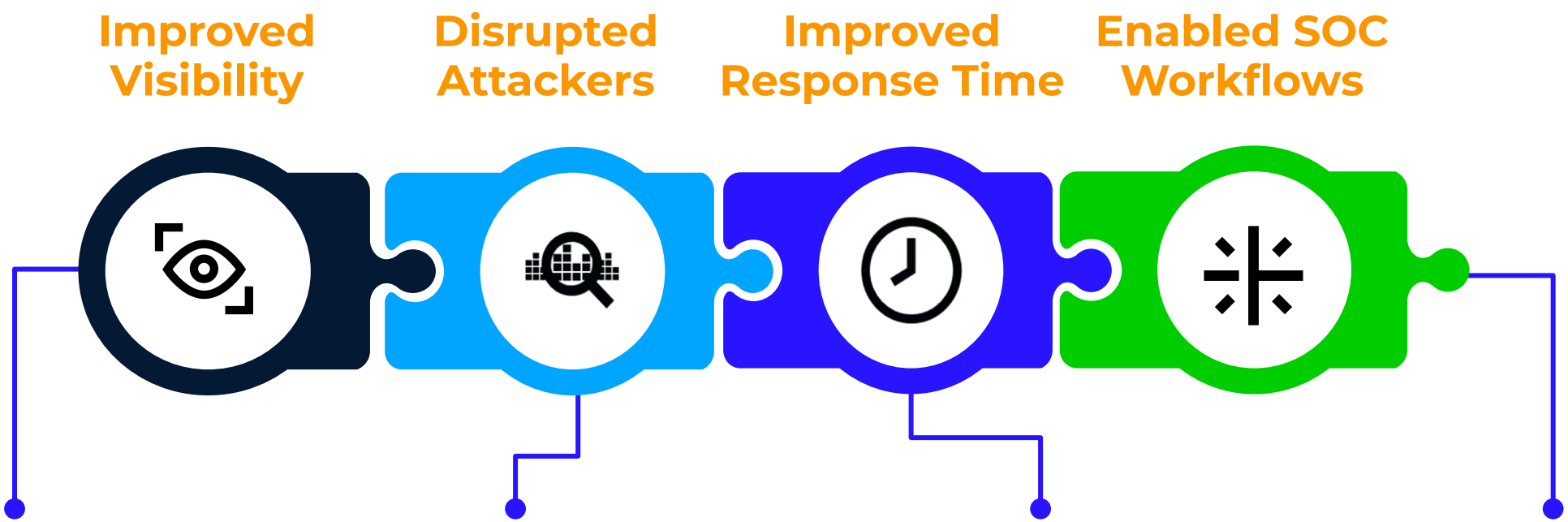
Speed investigation and response

- Alert prioritization and enrichment
- Attack impact scoping
- Guided investigation and workflow
- Network based response

Built on a heritage of innovation in network threat detection and threat intelligence research

Trellix

Continued..



Eliminates Blind spots

AttackPath and assets discovery, continuous alerts, L7 metadata analysis, and netflow, across complex networks and endpoints for comprehensive threat detection

Reveals and Blocks Hidden Threats

Multi-layered detection at each MITRE framework stage, for E-W and N-S traffic

Accelerates Investigations

Trellix Wise™ GenAI-driven enrichment and guided workflows with risk-based prioritization of threats and vulnerabilities

Reduces the Breach Risks and Future Compromise

High-fidelity, low-noise alerts and actionable intelligence with hyper-response automation

Trellix

Disrupt Attackers at Every Stage

Traditional Network Perimeter Security

Trellix® Network Detection and Response

- Reconnaissance attack detection

- Multi-flow, multi-vector execution
- Signature-based intrusion prevention
- Domain and URL blocking
- Full protocol analysis
- Phishing detection

- Behavioral malware detection
- Zero-day attacks
- Malware emulation
- Riskware
- Outbound file scanning
- Remote code execution detection

- “Pass the hash” detection
- Detect tools used for credential and password dumping
- Fileless malware for extracting credentials

- Network mapping
- Host and service enumeration
- User hunting to identify high value admin rights

- Beaconing detection
- Malware callbacks
- Web shell detection
- Traffic anomaly detection
- TLS fingerprint anomalies
- IoT callback detection

- ML exfil module detects unusual file transfers
- Signature-based exfil detection

Leveraging multiple detection and AI approaches

Trellix

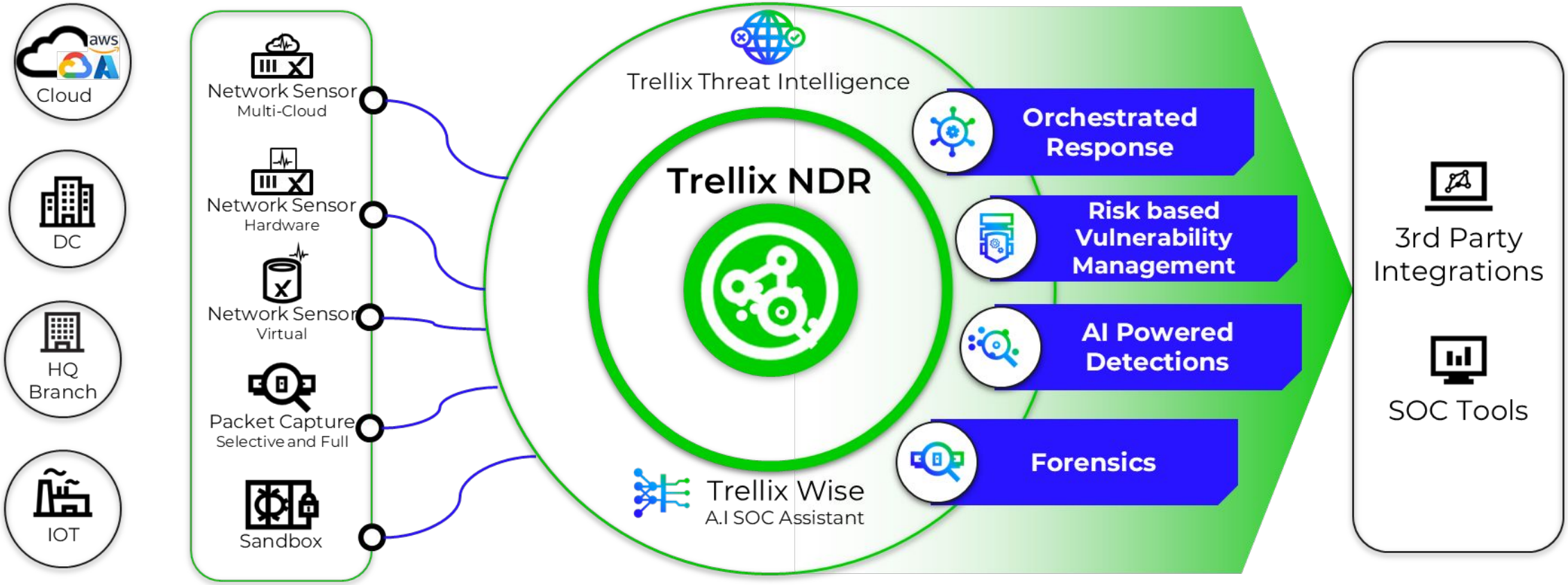
Accelerate Investigation and Response

Advanced Threat Detection	Hunting	Investigation	Scoping	Containment and Remediation
Advanced signatures, ML / AI, and behavioral analysis detect emerging threats	Full PCAP, L7 metadata, and flow data visibility for advanced hunting	Automated enrichment with threat intel, MITRE techniques, and analytics speeds investigations	Multi-sensor correlation and integrations deep visibility for forensics and root cause analysis	Enables informed responses with XDR, SOAR and ticketing system

Provides visibility and alert priority to respond quickly

Trellix

Trellix Network Detection and Response (NDR) Platform



Trellix

Trellix NDR Platform Components

Trellix® Network Investigator - NDR Console

AI/ML and Correlation Detection – Risk Based Scoring

- Threat Intelligence
- Hyper-Automation
- Trellix WISE
- Attack Path Discovery
- Asset Discovery

Network Security

Block Advanced Threats and Callbacks, evasive Malware, and detect lateral movement and data-exfiltration using ML powered security engines

Network IPS

Protect your Enterprise Network with high performing Intrusion Prevention Systems

Network Forensics

Add full packet capture and advanced network investigation features to quickly rebuild and analyze large segments of traffic

Dynamic File Analysis

Detect unknown and zero-day malware with dynamic analysis, built-in countermeasures, 2000+ simultaneous executions, and 200+ configurations

Trellix NDR Sensors

Trellix

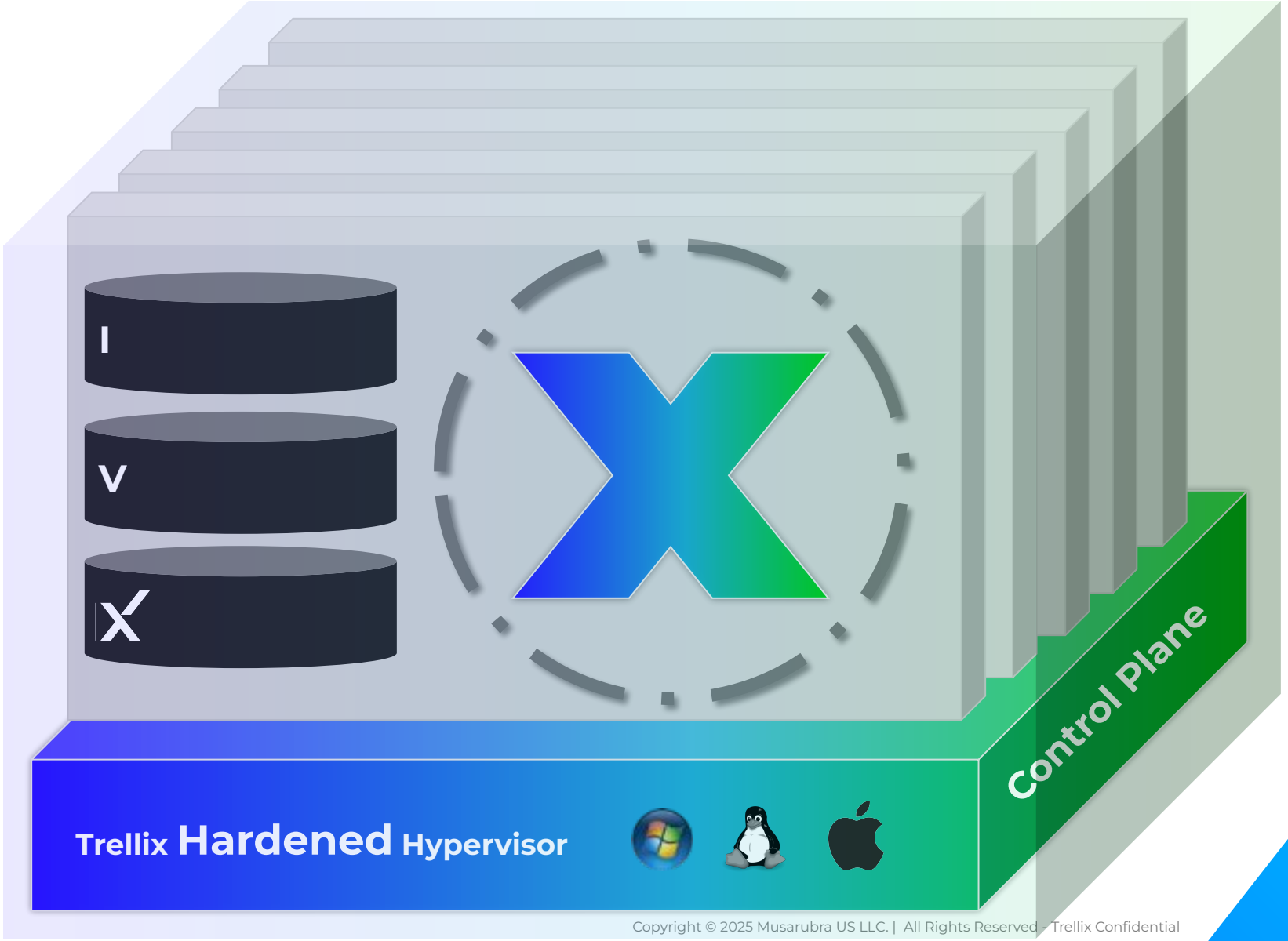
Trellix NDR Key Capabilities

Threat Detection	Visibility	Investigation & Forensics	Hunting	Response & Remediation
ML/AI, Behavioral detection	Automated Asset Discovery	Trellix WISE (Gen AI) guided investigation	Event Based, Complete and Selective Packet Capture.	Hyper Automation Response capability and ticketing system
Lateral Movement	User Entity and Flow Risk Aggregate Scoring	Automated Alert enrichment with threat intelligence	Store 30/60/90/ days worth of logs.	Native Active Inline Blocking
Phishing on Network	Attack Path Discovery	Attack MITRE map and analytics		
Living of the Land Detection	OT and IT network Visibility			
Sandbox (IVX)	Unified security through integration			
OT Threat Detection				
Correlated Exploit Detection				

Trellix

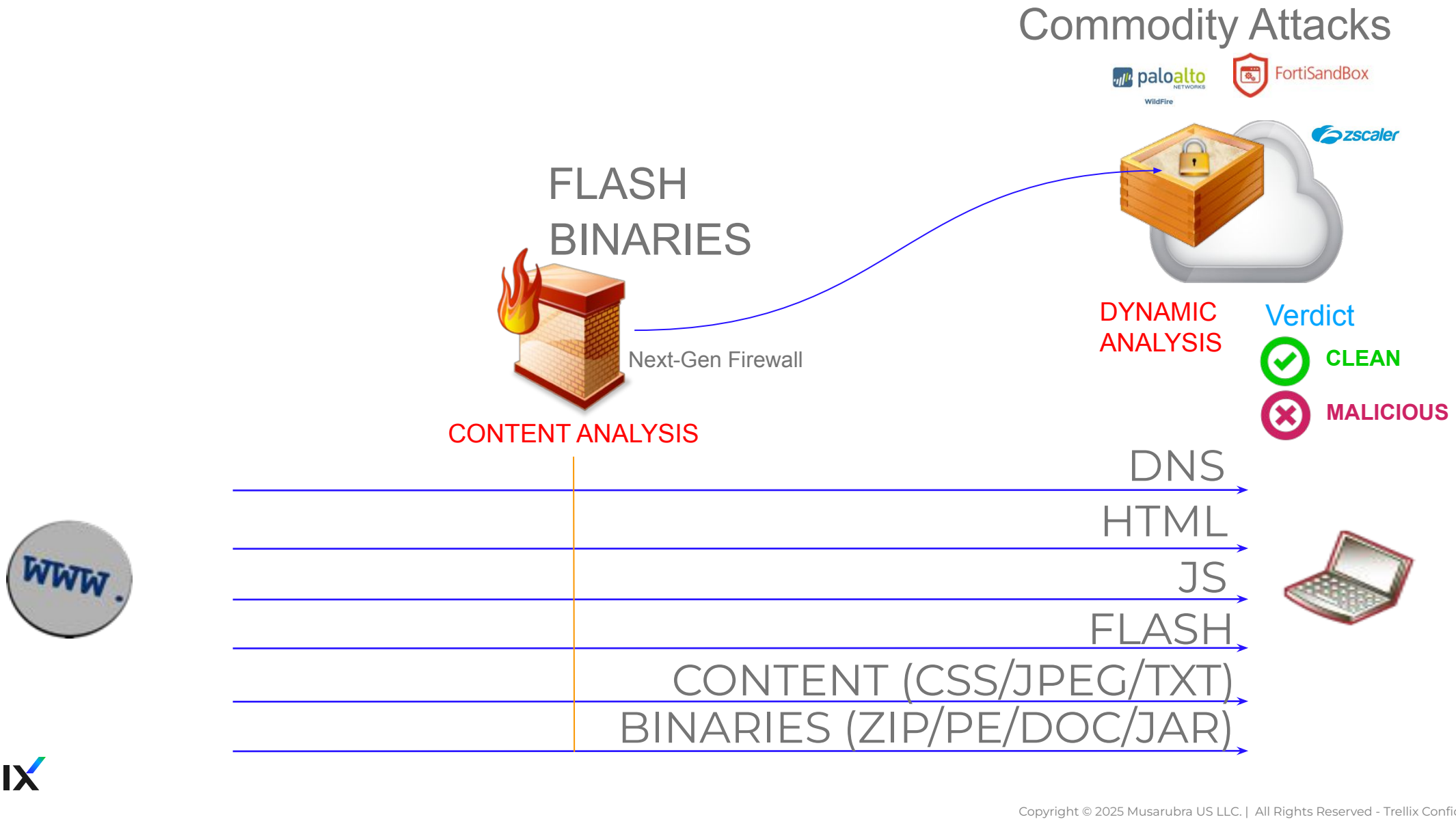
Trellix Intelligent Virtual Execution (IVX)

- Best-of-Breed Dynamic Analysis
- Custom Hardened Hypervisor
  - Designed for Threat Analysis
  - Built-in countermeasures
  - VM Evasion Detection
  - Windows, OSX, and Linux
- 200+ simultaneous executions across *multiple OS, service packs, applications*, and file types.
- Available in on-prem appliance, virtual (ESXi & Nutanix), and cloud (AWS)
- Multi-Vector and Multi-Flow



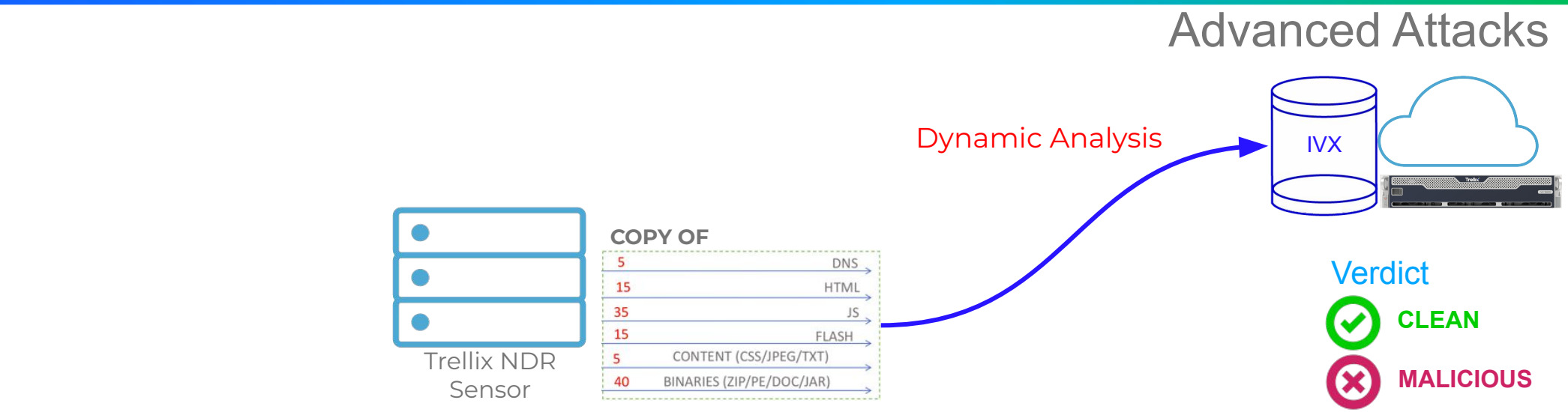
Trellix

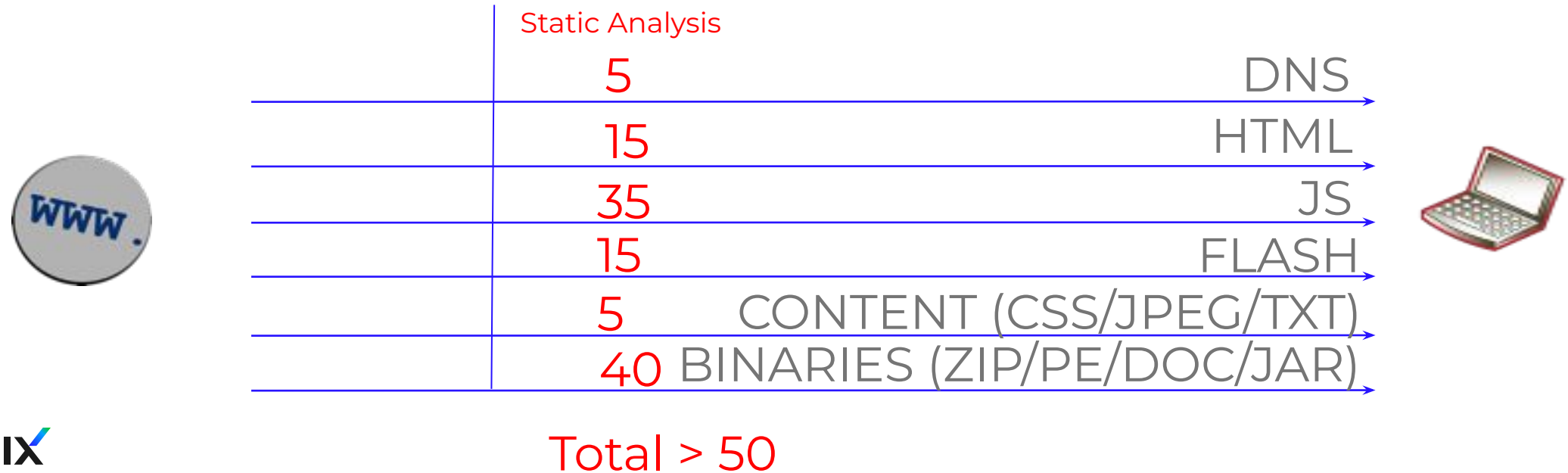
Single-Flow (File based) Analysis



Trellix

Multi-Flow (Session based) Analysis



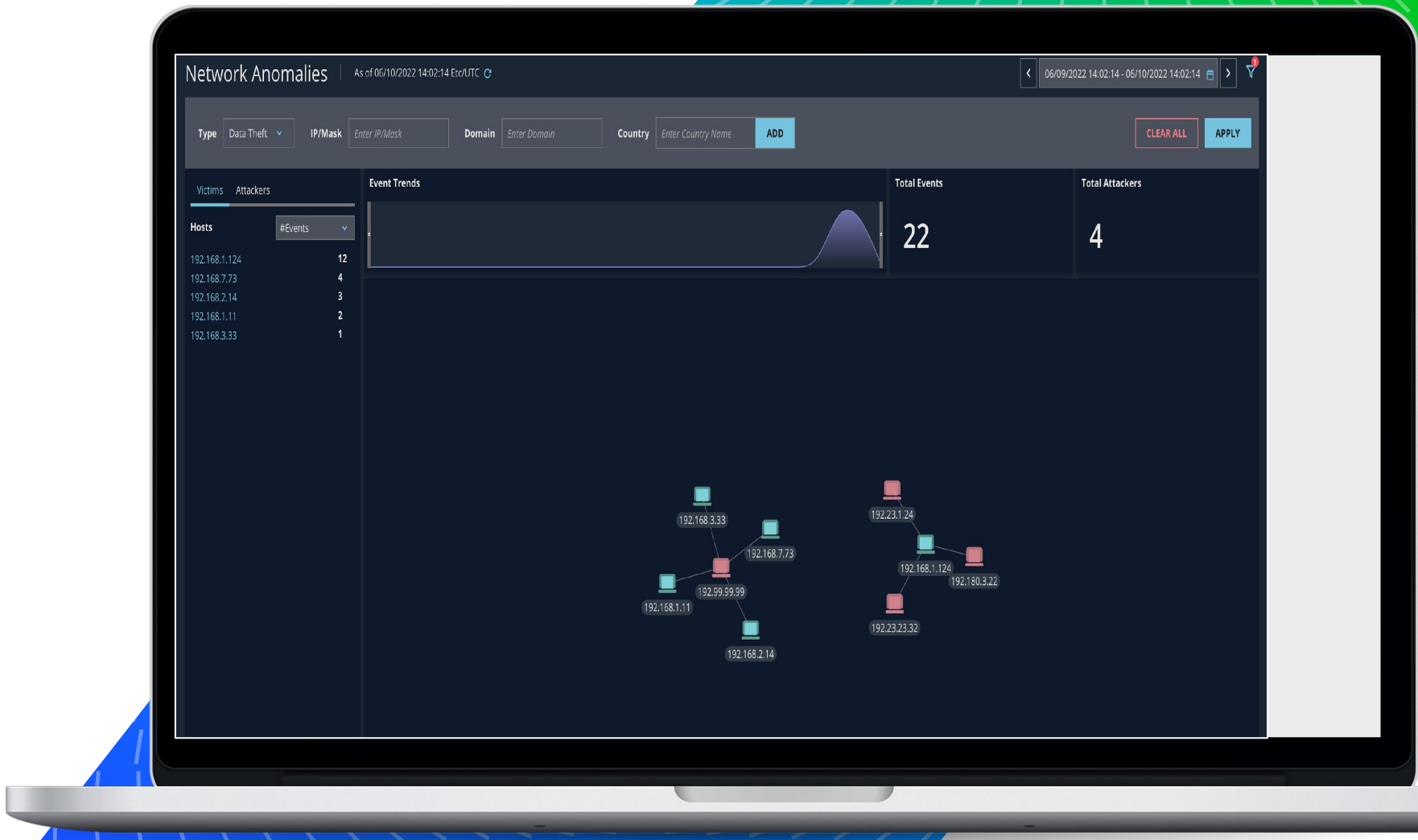


Trellix

Network Anomaly Detections:

Data Exfiltration

- Detects anomalies in network traffic based on data volume and historical behavior
- ML-based volumetric analysis of flow data
- Adjusts to different size networks & traffic patterns to best baseline
- Bi-directional net-flow records from Suricata engine

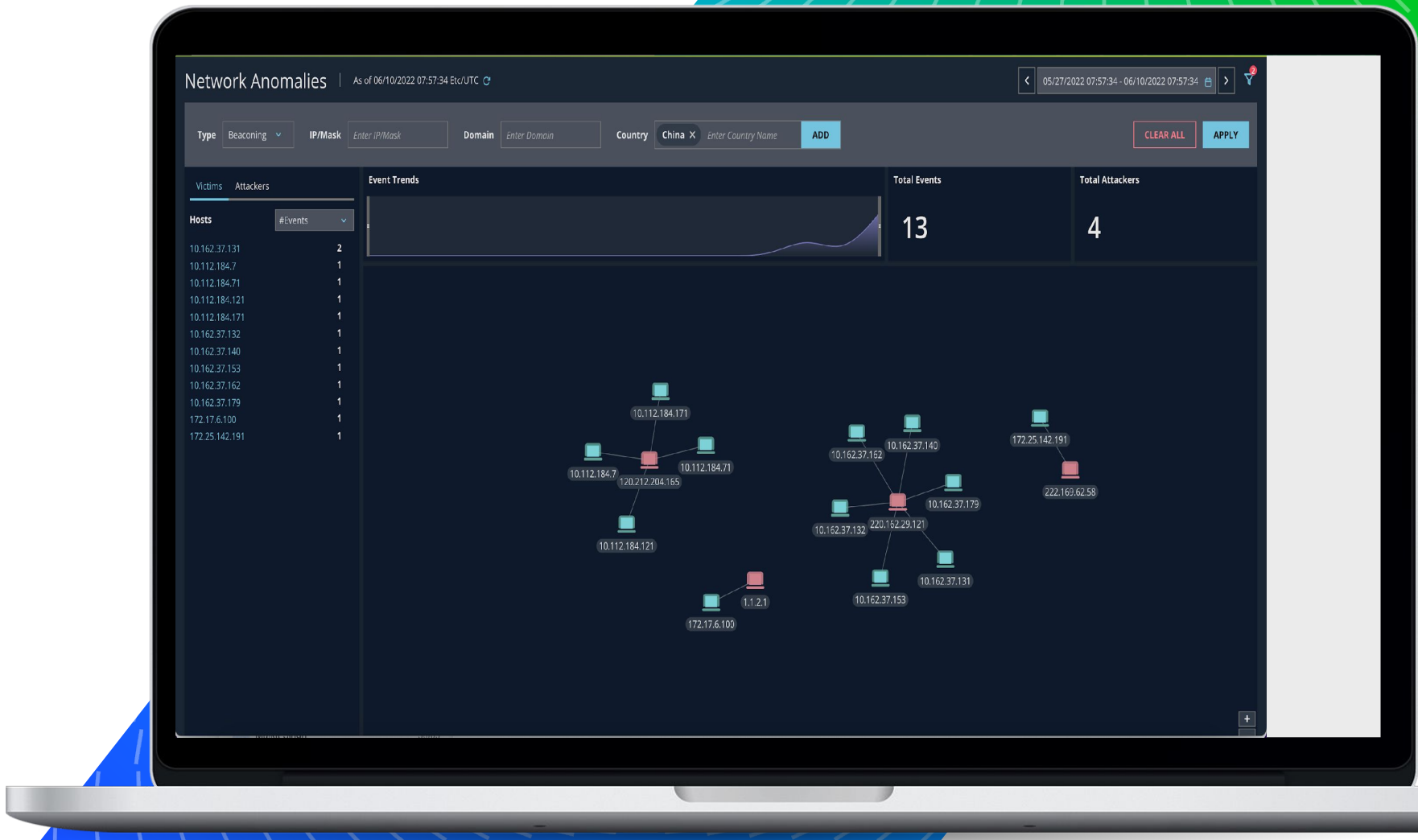


Trellix

Network Anomaly Detections:

Beaconing

- Unsupervised ML-powered detection based on *time-series* data
- Relies on flow and protocol metadata leveraging Suricata engine
- Alerting based on source/destination pairs



Trellix

Smartvision

Detect post-exploitation network activity along the attacker kill chain

- **Advanced correlation engine**
  - Provides detection across the attack lifecycle and expands east-west and data center traffic inspection
  - Uses hundreds of rules to detect signals of malicious activity for post-exploitation
  - Generates high-fidelity alerts by correlating these weak indicators of compromise with other disparate sources (IPS, IVX)
- **Machine-learning data exfiltration module**
- **Detonation using IVX of executables transferred over SMB**
- **Alert Context**
  - Provides 10 minutes of L7 context around every real-time alert. Data is presented in It is provided in a visual format to speed investigations for non-experts.

Trellix

Network Forensics

High-Performance Packet Capture

LOSSLESS PACKET CAPTURE
Vital to effective network forensic investigations

HIGH-PERFORMANCE
Record speeds of up to 20 Gbps

INTELLIGENT CAPTURE
Selective packet filtering for maximum efficiency

High-Fidelity Data Analysis

ULTRAFAST SEARCH
Leverage unique indexing architecture for fast answers

INTEGRATED INTELLIGENCE
Add rich context to IOCs and alerts

EASY DRILL DOWN
Quickly respond to alerts that matter

Grows with Your Network

EXTENSIVE VISIBILITY
Session decoder support for a myriad of protocols and file types

FLEXIBLE PLATFORM
Scales to meet distributed and large enterprise needs

THREAT HUNTING
Perform retrospective threat hunting and analysis

Trellix

Key Trellix Packet Capture Benefits

Centralized Visibility

- Custom Dashboards
  - View Capture Packets
  - Analyze Capture Packets
  - Metadata and activity

Centralized Forensics

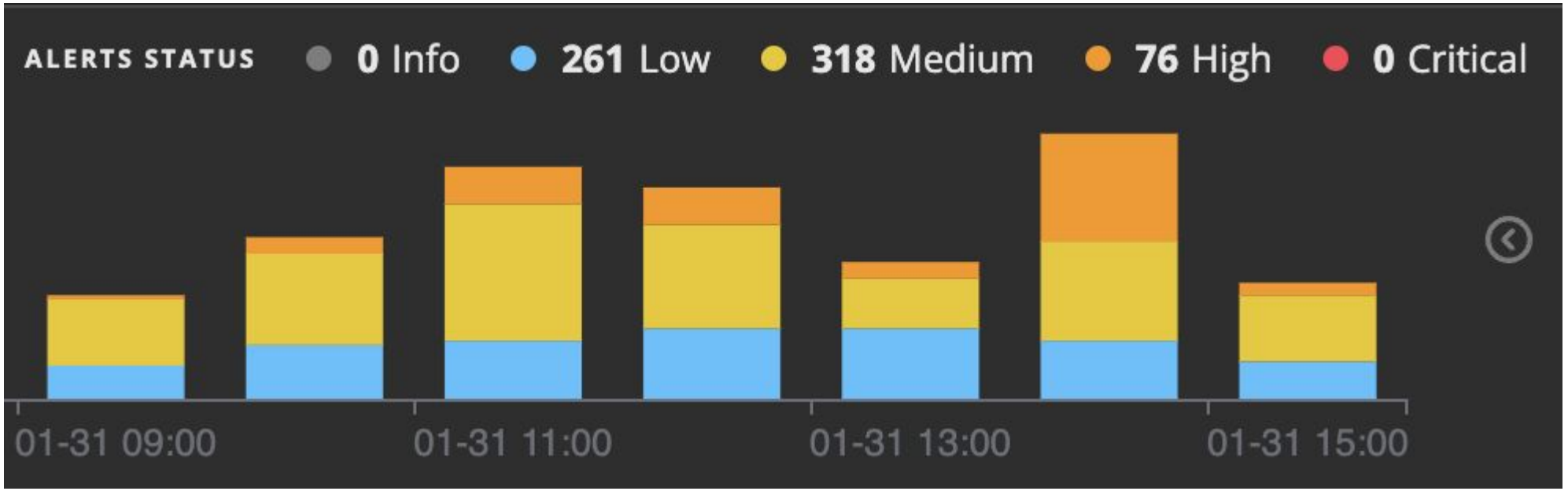
- Full Packet capture for egress/ingress
- Distributed Environments
- Threat hunting using indexed metadata from protocols:
  - HTTP, DNS, TLS, FTP, SSH, etc..

Threat Intelligence

- Threat Intelligence Feed:
  - IOCs
  - Early detection
  - Proactive threat hunting

Trellix

No critical alerts, do I look at the rest?



*Would you look through **all** 76 high alerts? How about 381 medium? 261 low?*

Trellix

Generative AI vs Agent AI

According to DJ Rich ”Why Don't AI Agents Work (Yet)?” video at: https://www.youtube.com/watch?v=kpOWmwA6tJc

4 factors

- **Autonomy**: acts without human intervention or supervision
- **Social Ability**: interacts with other agents
- **Reactivity**: perceives its environment and takes actions in response.
- **Proactivity**: forms goals and peruses them on its own.

“Any agent capable of adapting to a sufficiently large set of distributional shifts must have learned a causal model of the data generating process.”

Google DeepMind - https://arxiv.org/pdf/2402.10877

The Knowledge Engineering Review, Vol. 10:2, 1995, 115–152

Intelligent agents: theory and practice

MICHAEL WOOLDRIDGE[1] and NICHOLAS R. JENNINGS[2]

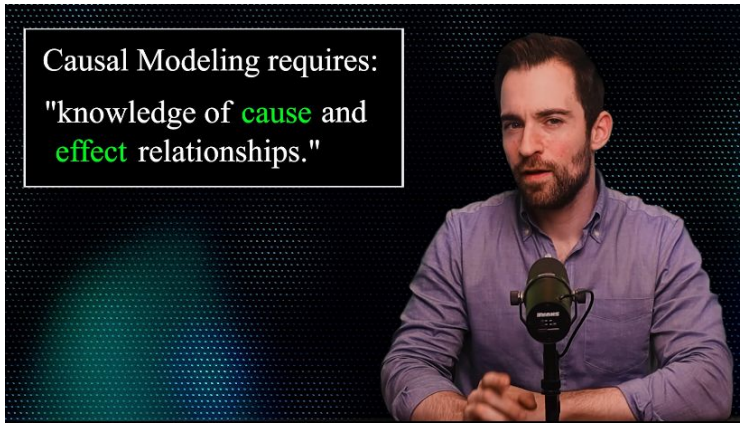
[1]*Department of Computing, Manchester Metropolitan University, Chester Street, Manchester M1 5GD, UK (M.Wooldridge@doc.mmu.ac.uk)*
[2]*Department of Electronic Engineering, Queen Mary & Westfield College, Mile End Road, London E1 4NS, UK (N.R.Jennings@qmw.ac.uk)*

Published as a conference paper at ICLR 2024

ROBUST AGENTS LEARN CAUSAL WORLD MODELS

Jonathan Richens*
Google DeepMind

Tom Everitt
Google DeepMind



Trellix

Counterfactuals

https://web.cs.ucla.edu/~kaoru/3-layer-causal-hierarchy.pdf

Based on Judea Pearl's Causality: Models, Reasoning, and Inference.

Year: 2000

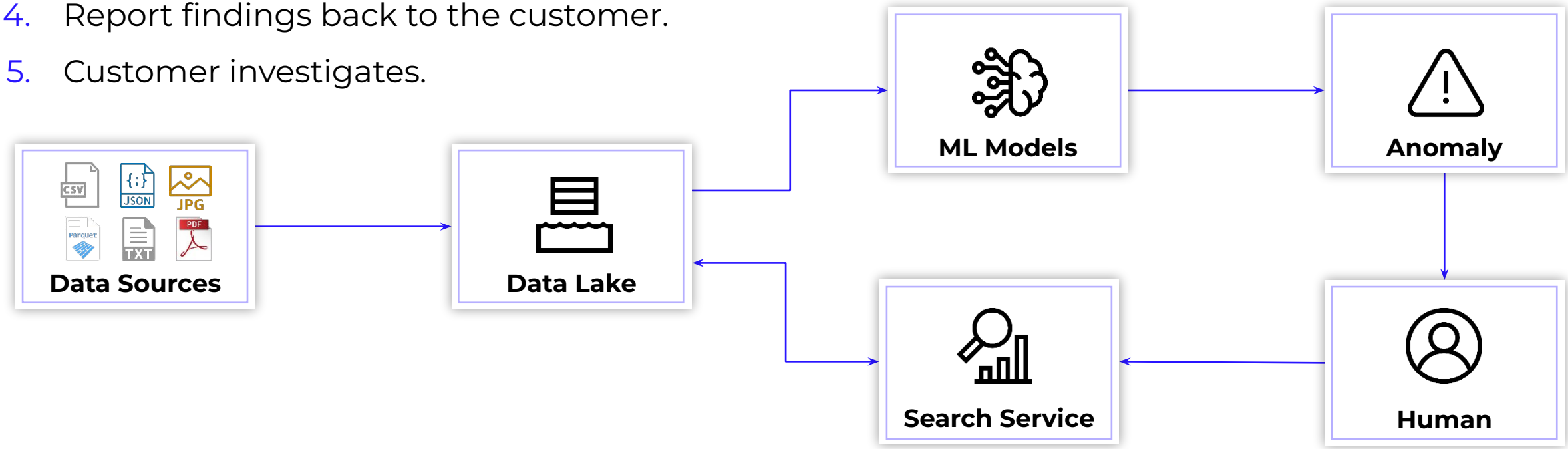
Level (Symbol)	Typical Activity	Typical Questions	Examples
1. Association $P(y\|x)$	Seeing	What is? How would seeing X change my belief in Y?	What does a symptom tell me about a disease? What does a survey tell us about the election results?
2. Intervention $P(y\|do(x), z)$	Doing	What if? What if I do X?	What if I take aspirin, will my headache be cured? What if we ban cigarettes?
3. Counterfactuals $P(y_x\|x', y')$	Imagining, Retrospection	Why? Was it X that caused Y? What if I had acted differently?	Was it the aspirin that stopped my headache? Would Kennedy be alive had Oswald not shot him? What if I had not been smoking the past 2 years?

Figure 1: The ladder of causation

Trellix

Our Pre-AI Approach

1. Create thousands of connectors and parsers to normalize event data from anywhere.
2. Store all of the data on S3 and OpenSearch.
3. Analyze the data for anomalies with Amazon Elastic MapReduce or EMR (Managed big data platform/service) and ML models.
4. Report findings back to the customer.
5. Customer investigates.



Trellix

Effective, but Hard to Scale

What worked

- Ingesting data
- Analyzing and matching
- Searching obscene data volumes

What didn't

- Didn't have time to investigate all findings

Trellix

Trellix WISE AI: Accelerating Investigations

Reduce security teams' workloads and improve confidence in security posture

See Everything that Matters

- Enhanced visibility into events throughout the attack kill chain leading to alerts
- Visualize connections to reveal sophisticated, evasive threats

Maker Better, Faster Decisions

- Get immediate high-level understanding and scope of alerts, with crucial context from detections mapped to MITRE attacker tactics and techniques
- Upskill analysts of all levels with AI-guided, context-enriched investigations and remediation guidance based on the individual threat
- Analysts can interact with Wise using natural language to ask questions for additional information related to alerts

Expedite Workflows and Remediation

- Automatically collect and correlate artifacts related to a threat for faster triage and remediation

Improve security team throughput

Save **8 hours per 100 alerts**

Uplevel every analyst, not just Tier 1

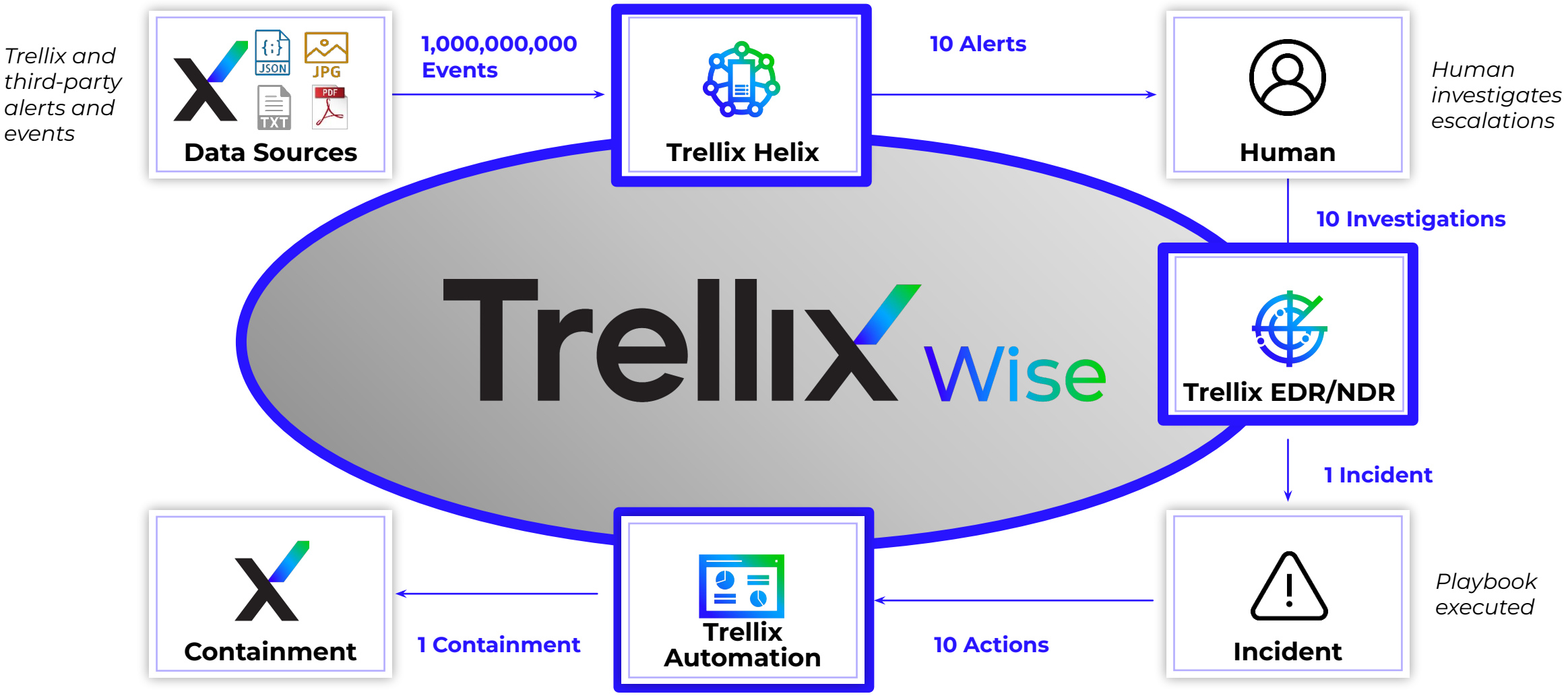
Context enriched investigations from telemetry and other alerts

Accelerate mean time to investigation (MTTI)

10 times faster triage and remediation

Trellix

AI-Powered Platform

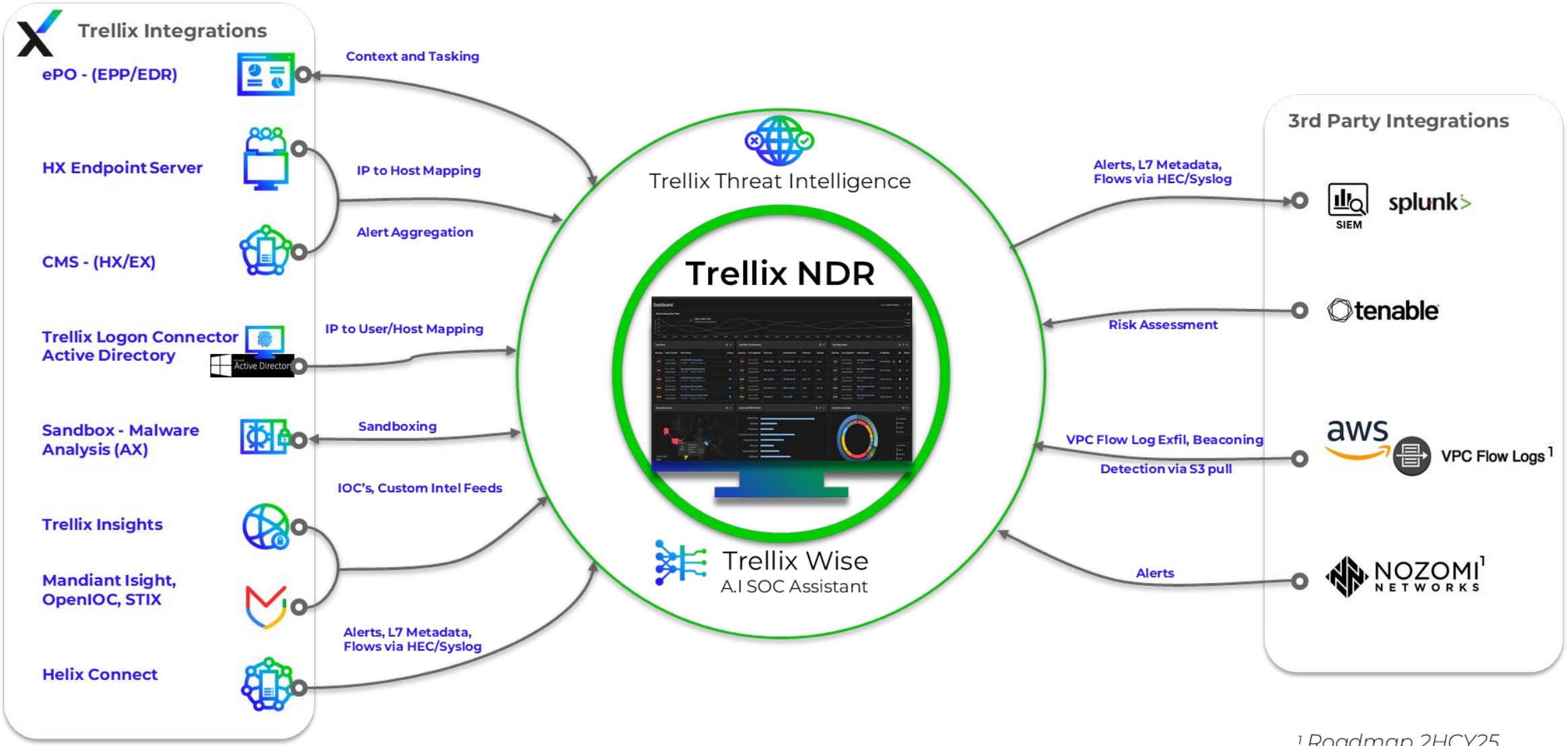


Trellix

The AI Arms Race

Trellix

Trellix NDR Integrations



[1] *Roadmap 2HCY25*
[2] *Roadmap 1HCY26*

What is Hyperautomation?

"Hyperautomation is a business-driven, disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible."

Security Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms, including: artificial intelligence (AI), low-code/no-code tools, packaged software, and other types of decision, process and task automation tools."

Gartner Research

Trellix

SOAR vs. Hyperautomation

Why aren't traditional automation solutions enough?

SOAR

- Coding Expertise Required
- Restricted automation capabilities
- Limited AI
- Challenging to integrate products
- High implementation and maintenance costs

Hyperautomation

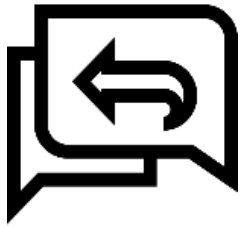
- Low-code, no-code solution
- Automation across tools, environments
- Deeper AI integration capabilities
- broader , simplified integrations
- Faster implementation, low maintenance

Trellix

How do you Make Automation Successful?

UNIFY

Pre-built, app agnostic integrations



SIMPLIFY

Standardized, shareable workflows

AMPLIFY

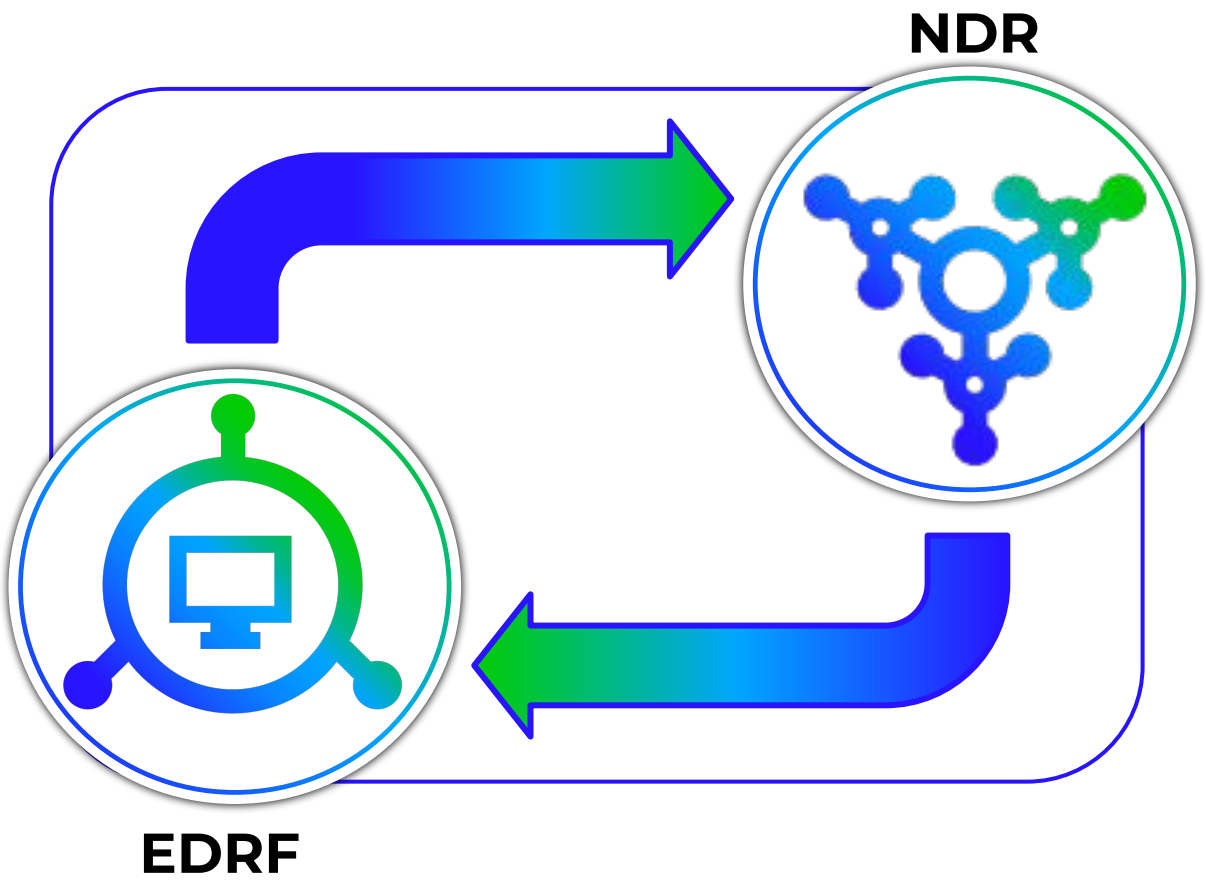
Low-code, team-focused automation

Low cost, low risk architecture

Speed visibility, drive efficiency & shift to “automate-first”

Trellix

A Perfect Complement to Trellix EDRF



- Discover unmanaged endpoints and IOT devices
- Hunt for unusual user behavior
- Identify suspicious file transfer
- Determine potential Command and Control (C&C) traffic and compromised devices
- Rapidly scope an incident
- Identify lateral movement attempts
- Identify potential exfiltration and reconstruct stolen material
- Respond to block ransomware and vulnerability exploitation

NDR enables and accelerates key SOC playbooks!

Trellix

Attack Path Discovery (APD)

Eliminate Blind Spots

Data Sources

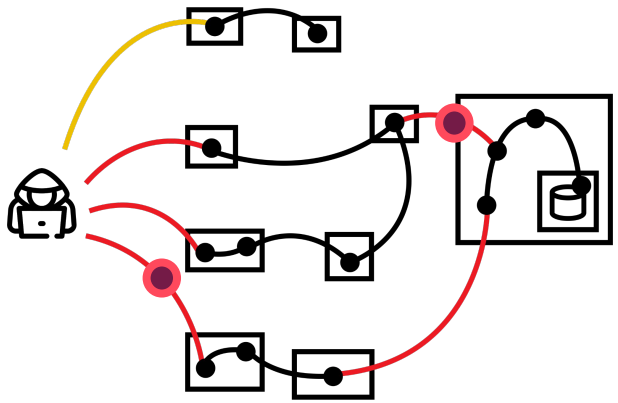
File Permissions
Network Topology
Assets
Access Rights
Application Usage
Active Directory
Cloud Services
User Activity
Asset Criticality

Vulnerabilities

RAPID7
tenable
Qualys.

Trellix NDR - Attack Path Discovery

Automated Blast Radius Modeling



Context Aware Prioritization

Attack Scenarios Database

Not Exploitable
Deprioritized
(25% – 50%)

Results

Prioritize
Vulnerabilities Daily

Track Business Risk
Over Time

Automate Your
Remediation
Workflow

NDR Attack Path Discovery - Risk Scoring

Trellix NDR - Business Value & Outcomes

Centralized, Intelligent Visibility, and Analytics

Centralized Detection, Investigations/IR, and Hunting

- **Prioritize and Triage Alerts using AI**
- **Anomalies** - lateral movement, data exfil, and C2
- Traffic analysis in **distributed environments**

Operational Efficiency and Threat Intelligence

- **Reduce manual analysis (Context, AI)**
- Enrich threat intel across multiple network segments
- **Identify threat trends and risk exposure**

SOC Workflow Integration

- **Enrich Context for Investigations**
- **Forensics** - Detection to PCAP Reconstruction
- Threat Hunting (IOC's, Threat Intel)
- **Integrate with Sandbox/EDR/SIEM/SOAR**

SOC Maturity

- Enable **Tier 1 and 2 analysts for faster triage**
- Reduce the need for packet analysis skills
- Provide rich network data up to L7
- **Contextual alert aggregation across sensors**

Trellix

Trellix

NDR Key Use-Cases

Duration - 20 Minutes

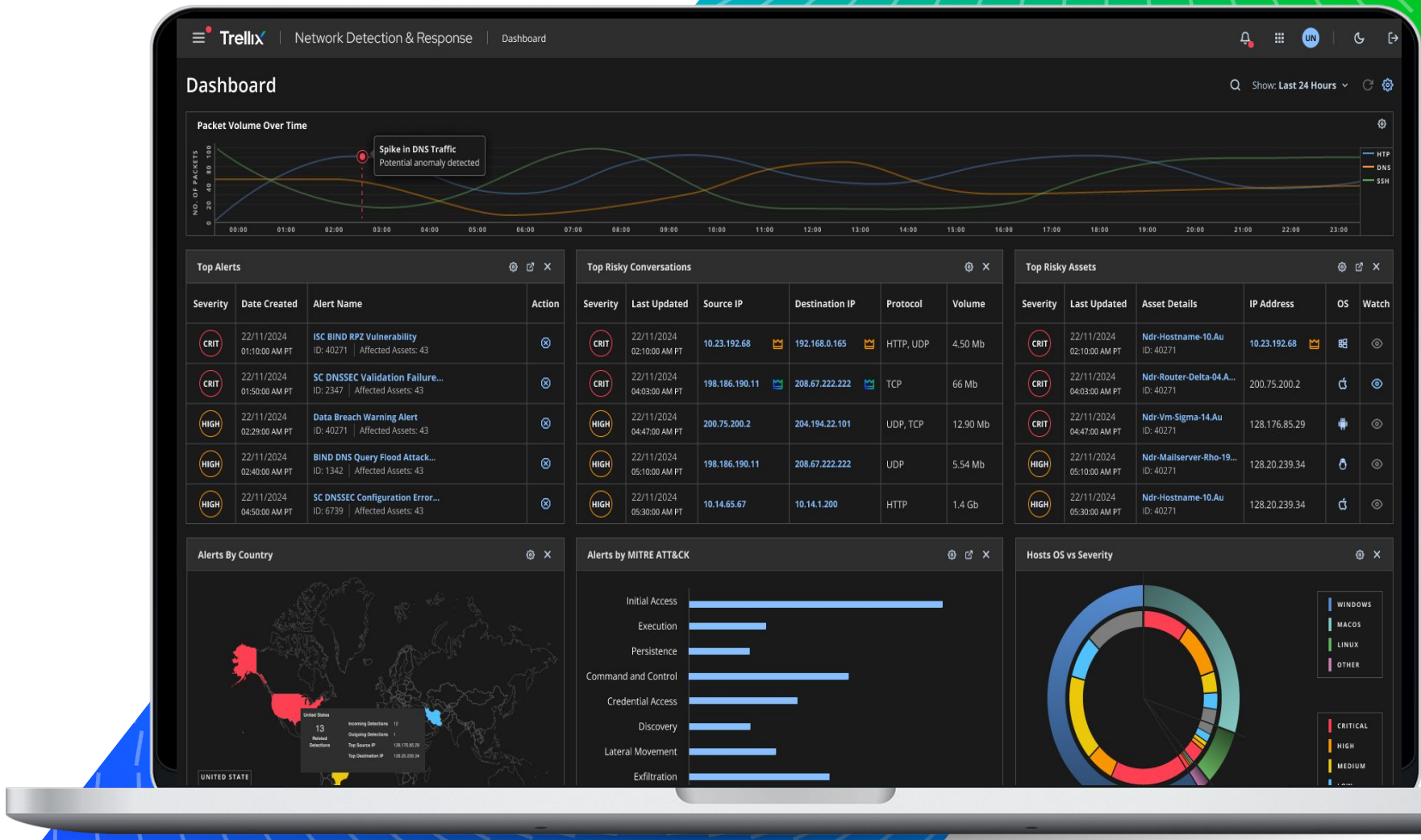
Analyst Workbench

Feature highlights

- A single pane of glass to view **top risky** assets, alerts, conversations, asset
- Displays alerts by Geo Location, Severity and MITRE ATT&CK

Customer Value

- A **unified dashboard** highlights **critical risks**, enabling faster, **prioritized investigations** and **response**.



Trellix

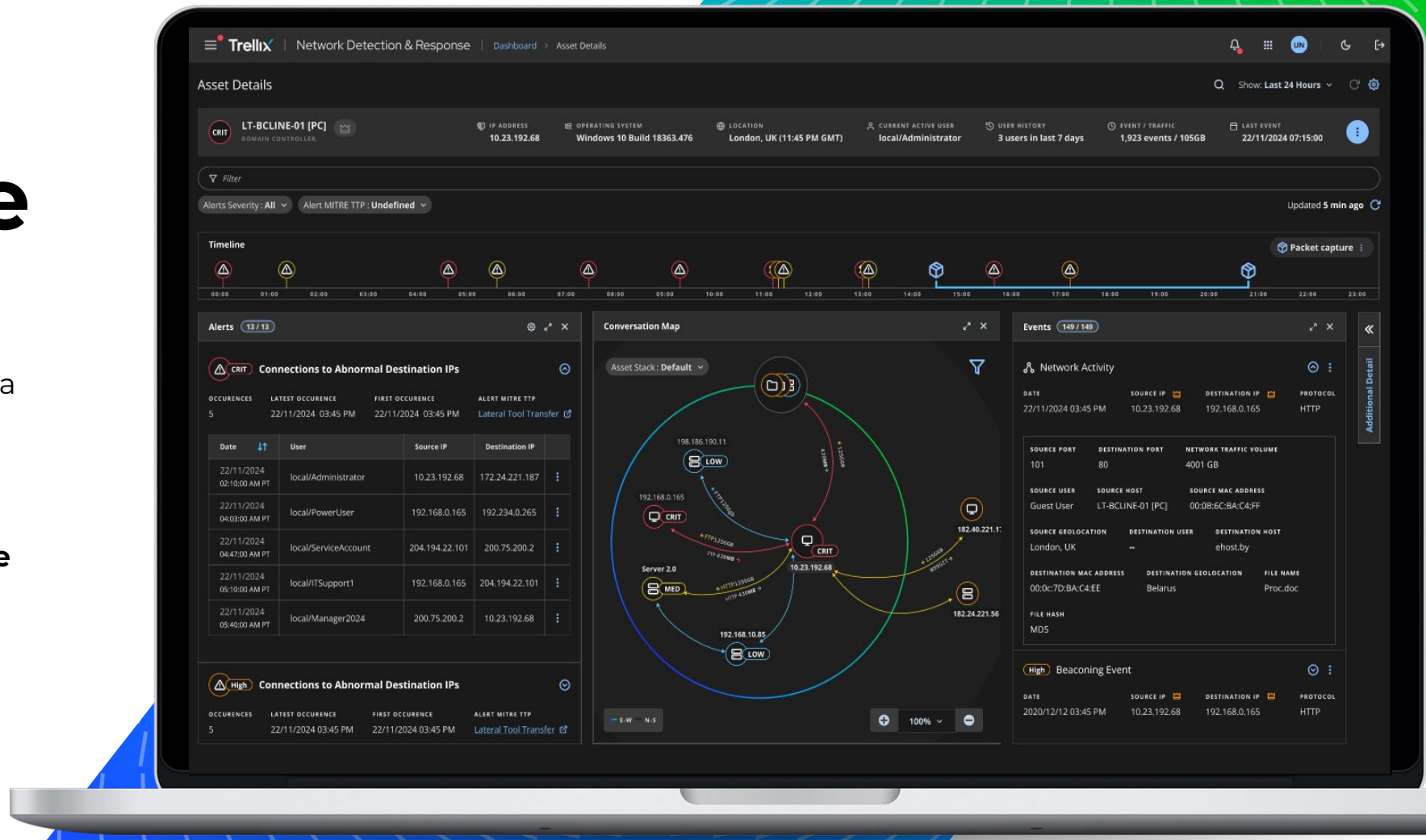
Asset Details Page

Feature highlights

- Provides a **consolidated view of critical asset information** enabling a quick understanding of the asset's status and context.
- A **conversation graph** visualizing primary and secondary interactions for **both EW and NS traffic from the asset**, and an events panel detailing all events, netflow, and anomalies.

Customer Value

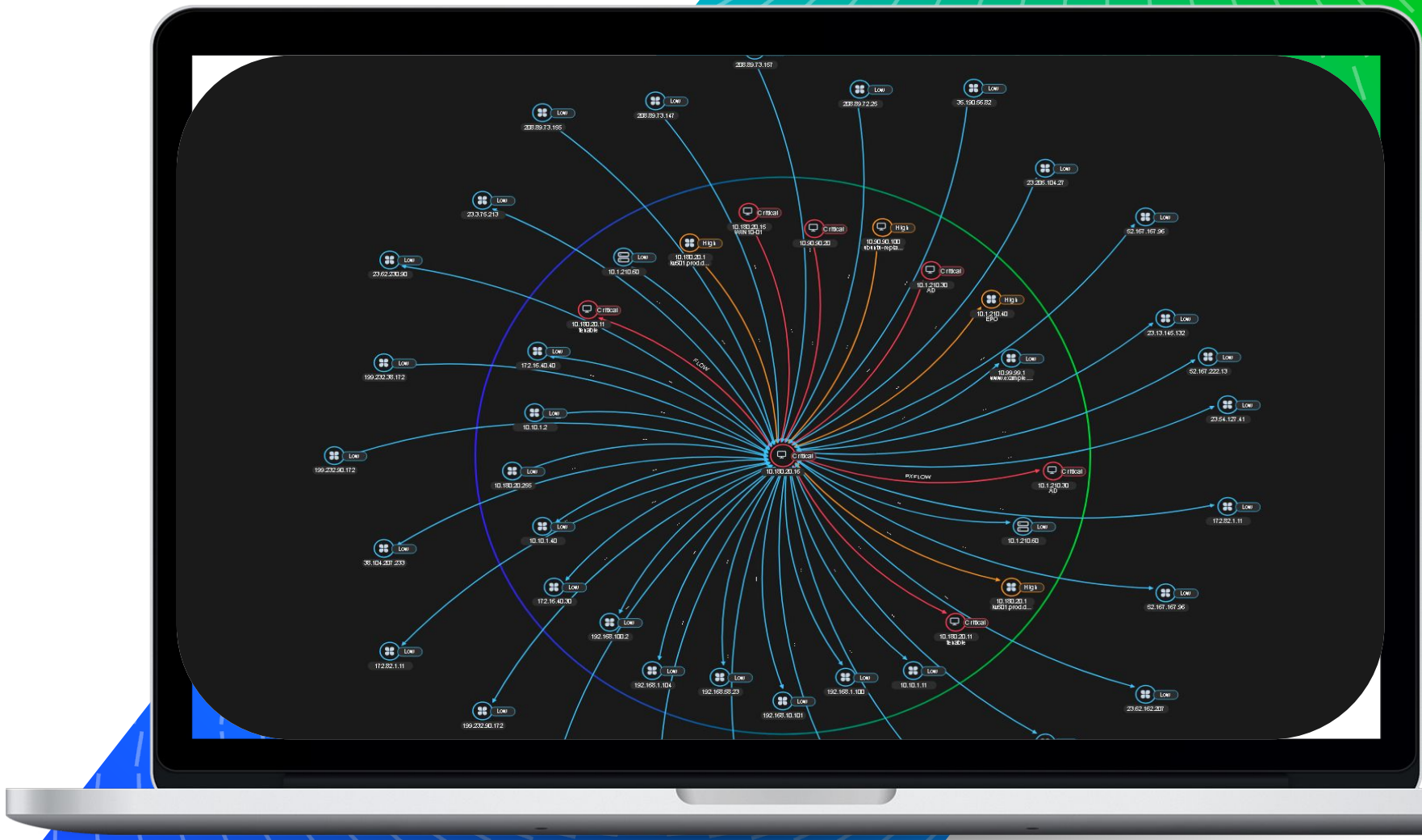
- A unified view of alerts to simplify investigations, reduce fatigues and accelerate SOC response.



Trellix

Eliminate Blind Spots

- **Shadow IT Visibility**
  - On-Premises, Cloud, and hybrid
  - Visualization of traffic patterns across hosts
  - Extend security visibility of existing security investment
- **Threat Coverage**
  - North/South Network Traffic
  - East/West Network Traffic
- **Passive Asset Visibility**
  - Discover
  - Classify
  - Risk Prioritization



Shadow IT Visibility for Distributed Networks and Threat Coverage for all Network Traffic and Type Of Assets

Trellix

Visibility in Complex Networks

Blind spots are often identified during incident post-mortem

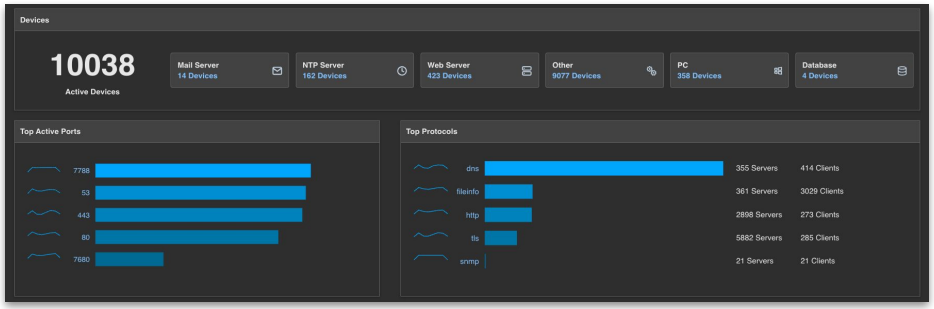
Digital transformation increases complexity and risk to secure network environments

Customers need visibility to secure:

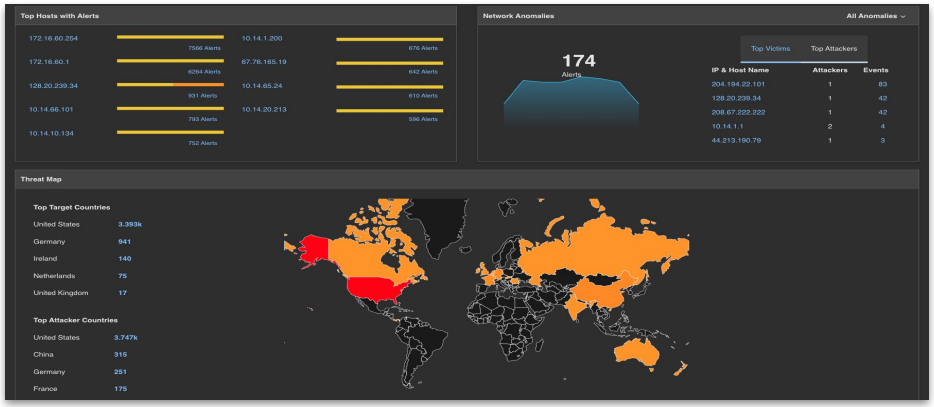
- On-prem, cloud, hybrid, and OT networks
- High-throughput data centers and user workplaces
- Network packet and app-layer visibility

Trellix® NDR leverages existing investments and increases actionable visibility:

1. Asset Discovery



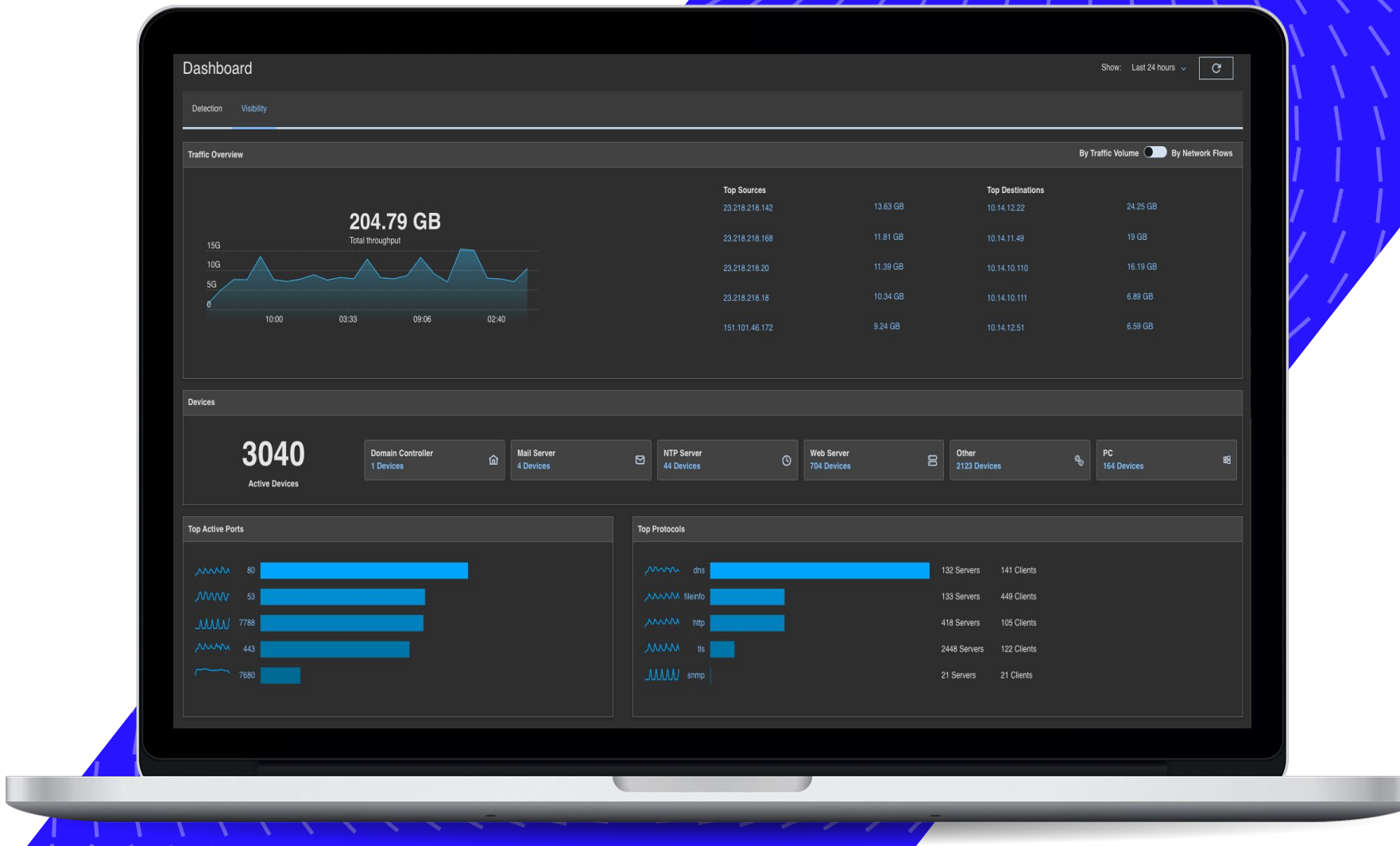
2. Intuitive dashboards for app layer visibility



Trellix

Visibility Dashboard

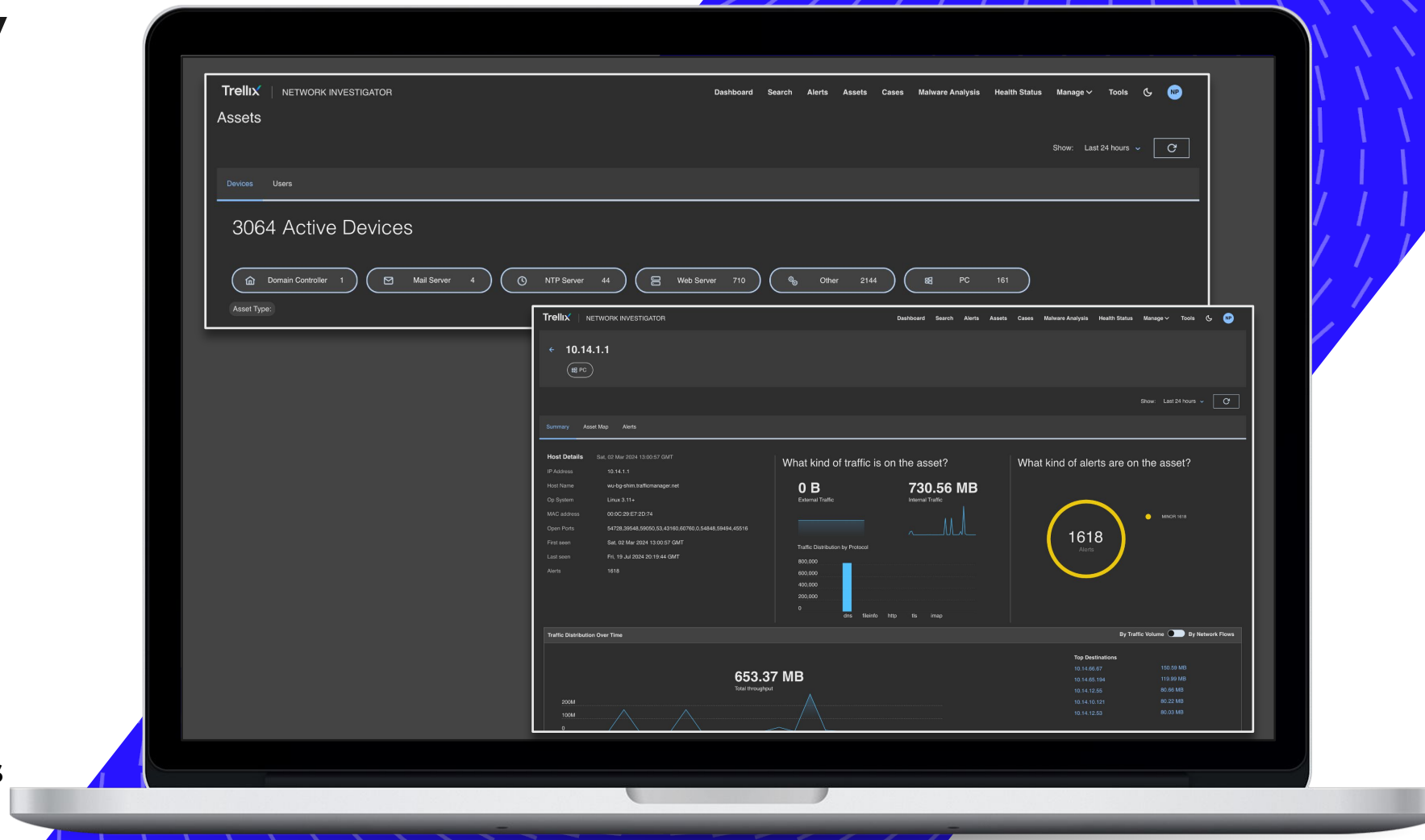
- **Traffic overview**
  - Top talkers
  - Top ports
  - Top protocols
- **Active assets on the network**



Trellix

Asset Discovery

- **Identifies various assets on the network**
- **Utilizes heuristics, HTTP User-agent, DHCP fingerprinting and other techniques for detection**
- **Classifies assets into categories:**
  - Servers (Web, DNS, Database, etc.)
  - Mobile devices, Laptops / PCs
  - IP Cameras, Medical devices, Printers
  - Routers / Gateways, Access points
- **New web UI page displays discovered assets**



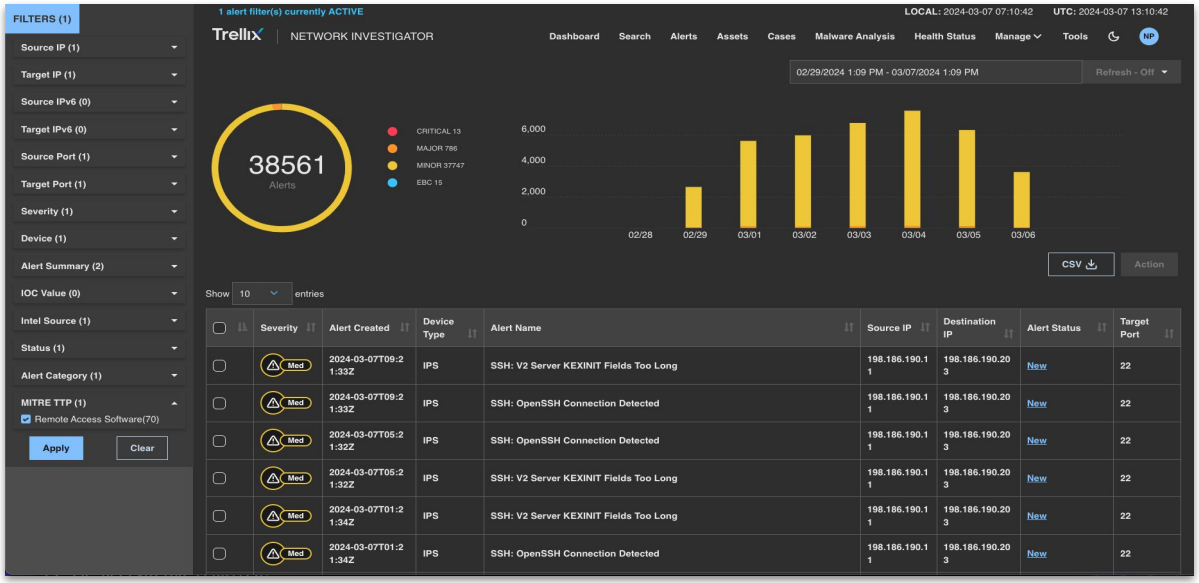
Sophisticated Attacks Evade Detection

Customer needs multi-layered detections to expose sophisticated threats

Sophisticated threats go undetected by existing network security infrastructures.

- Attackers take advantage of ***disconnected network tools***
- Evasive attackers hide their attack activity within the ***complexity of enterprise networks and blind spots***
- Low and slow attacks hide within ***constantly changing "normal" baselines*** that evade anomaly based detection

Trellix® NDR leverages advanced analytics to detect attacker activity like data exfiltration:

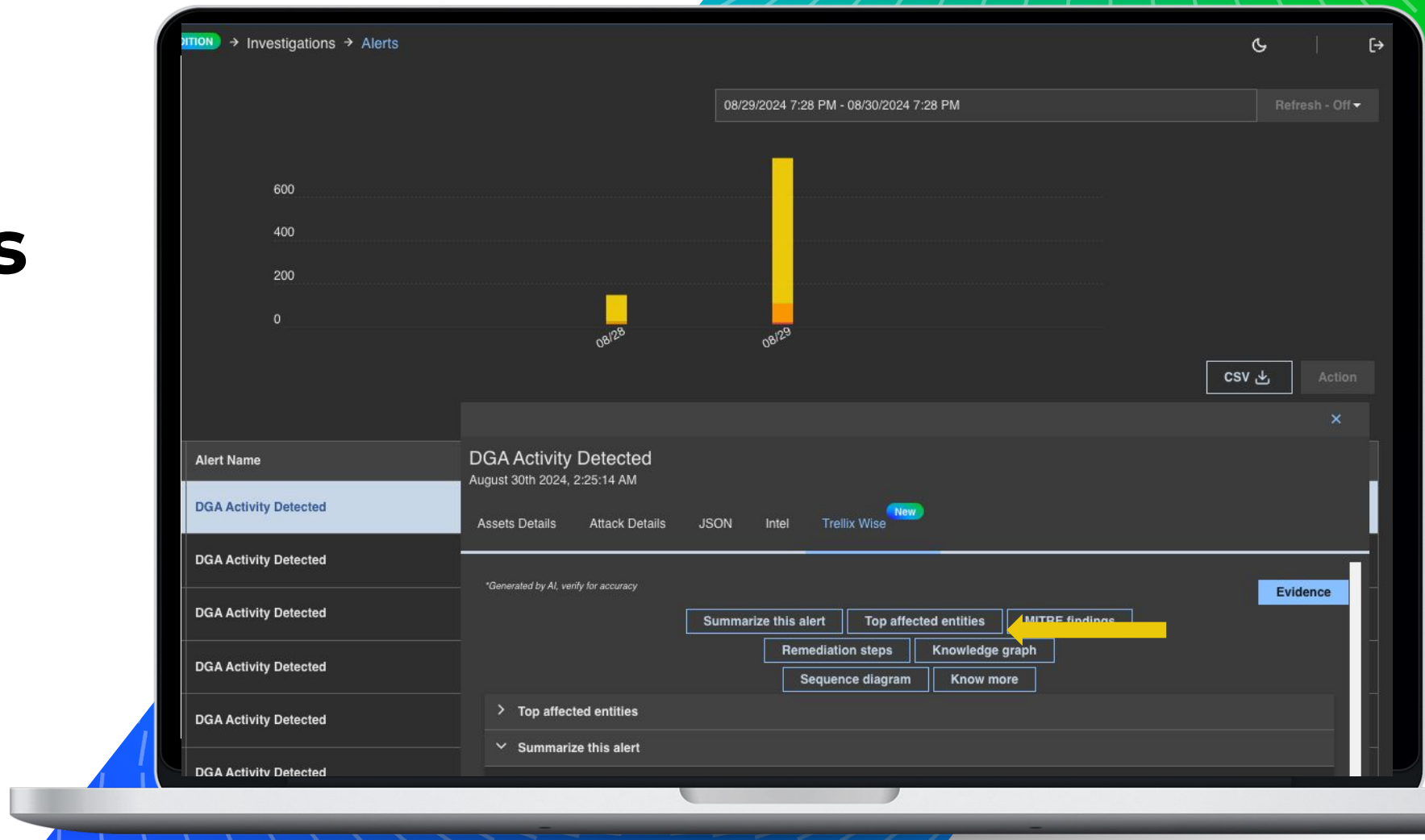


Trellix

AI Performs Deep-Dive Network Investigations with a Click

Similar to EDR for the host, deep-dive on network activity using Trellix Wise for NDR.

- **What happened?**
- **What are the MITRE mappings?**
- **What actions can I take?**
- **Where can I get more information?**



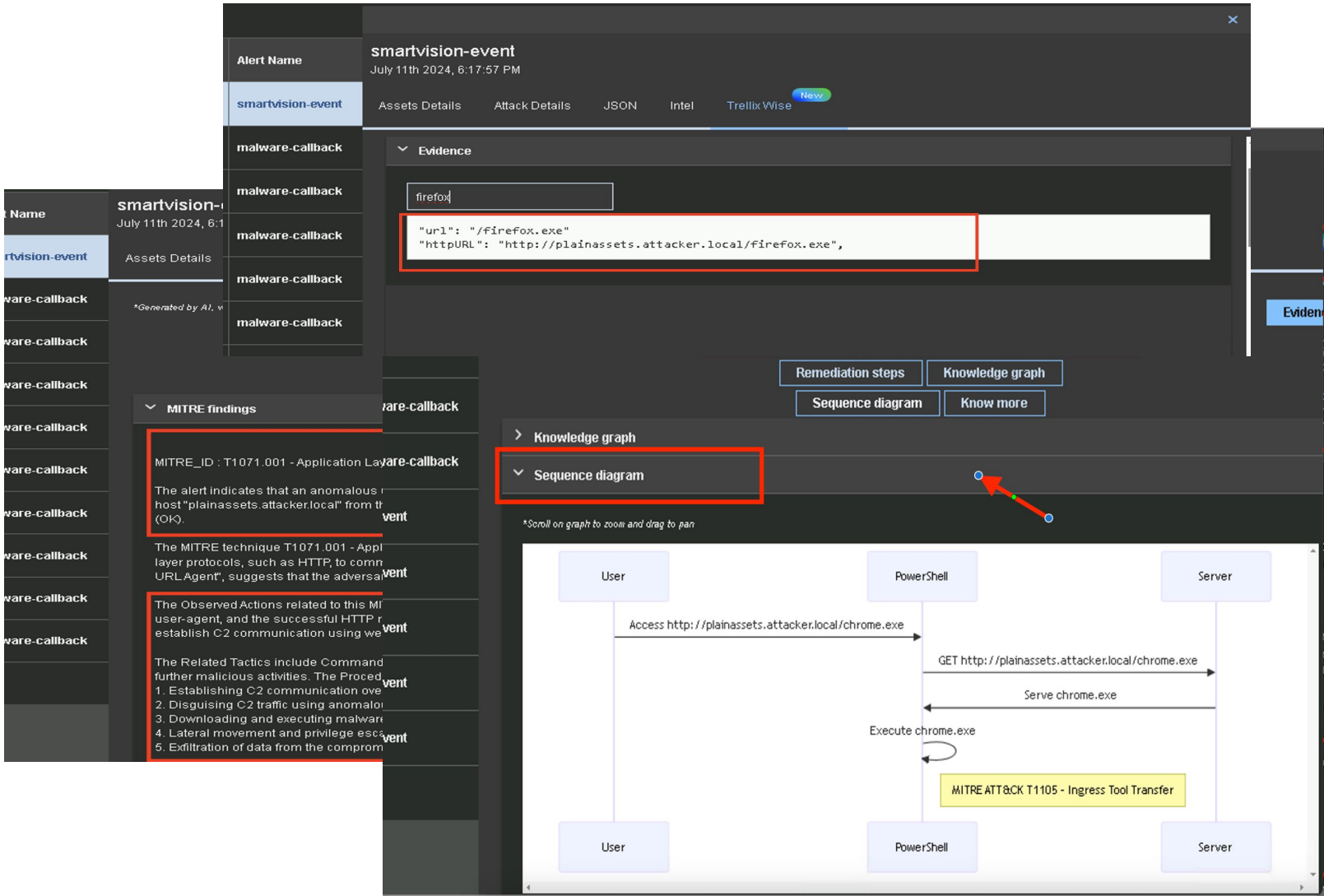
Trellix

How can I hunt using GenAI?

Trellix Wise - relieve alert fatigue, enable analysts

Trellix Wise Details

- Summarize Alert
- Top affected entities
- MITRE Findings
- Remediation steps
- Knowledge graph
- Sequence diagram
- Know more
  - Interact and ask more questions
- Evidence



Trellix

DGA Activity Detected

August 30th 2024, 2:25:14 AM

Assets Details | Attack Details | JSON | Intel | Trellix Wise (New)

Generated by AI, verify for accuracy

Evidence

Summarize this alert | Top affected entities | MITRE findings

Remediation steps | Knowledge graph

Sequence diagram | Know more

Top affected entities

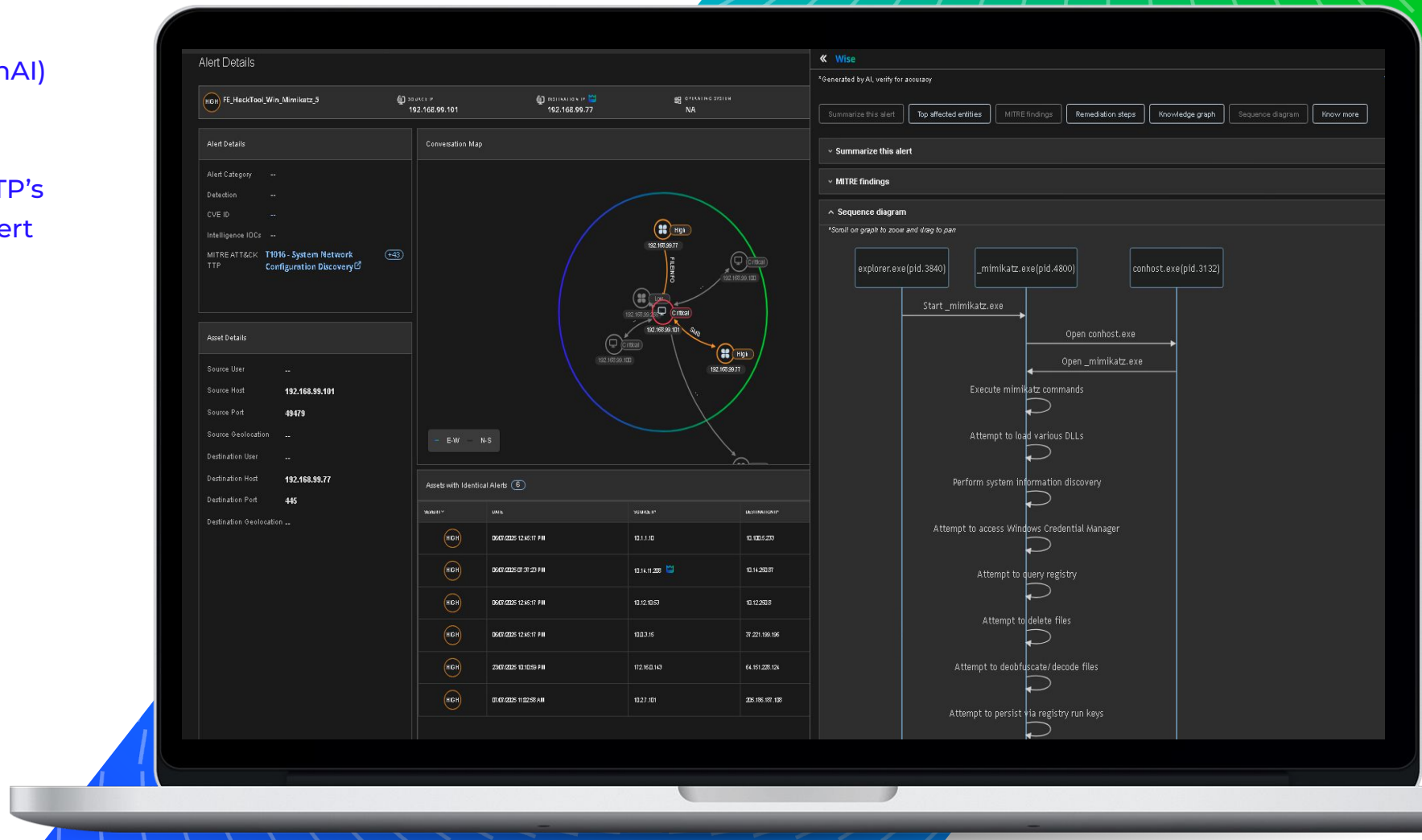
Summarize this alert

Summary:
The alert indicates that DGA (Domain Generation Algorithm) activity was detected, which is a common technique used by malware to establish communication with a command and control (C2) server. The most important event is the connection to the domain "ok1static.oktacdn.com", which is likely a malicious domain generated by the DGA. The investigation should start by analyzing the network traffic and the host that initiated the connection. The suspicious events include the DGA activity and the connection to the potentially malicious domain. The alert was first detected on the host with the IP address 10.14.11.48.

Key Points:
- The DGA activity is the most important event, as it indicates the presence of malware on the network.
- The suspicious processes include any processes that may have initiated the connection to the malicious domain.
- The events are related in that they all contribute to the detection of the DGA activity, which is a common technique used by malware.
- The events may imply that the host with the IP address 10.14.11.48 is infected with malware that is using a DGA to communicate with a C2 server.

Improve Response Time

- **Reduce manual analysis**
  - Triage Alerts using Trellix Wise™ (GenAI)
  - Provide quick summary of alert
  - Quickly scope affected entities
  - Get detailed information on MITRE TTP's
  - Get sequential steps related to the alert
  - Interact with Trellix Wise - Ask more questions
- **Enrich alert context**
  - Sensor flows and metadata
  - Vulnerability management data
  - ePO endpoint data
- **Identify threat trends and risk exposure**
  - Asset details - SOC-driven workflows
    - Alerts
    - Conversations
    - Events
  - Visibility into vulnerability sprawl
    - Attack-radius modeling
    - Context aware exposure
      - User
      - Asset
      - Privilege
      - Overall Risk

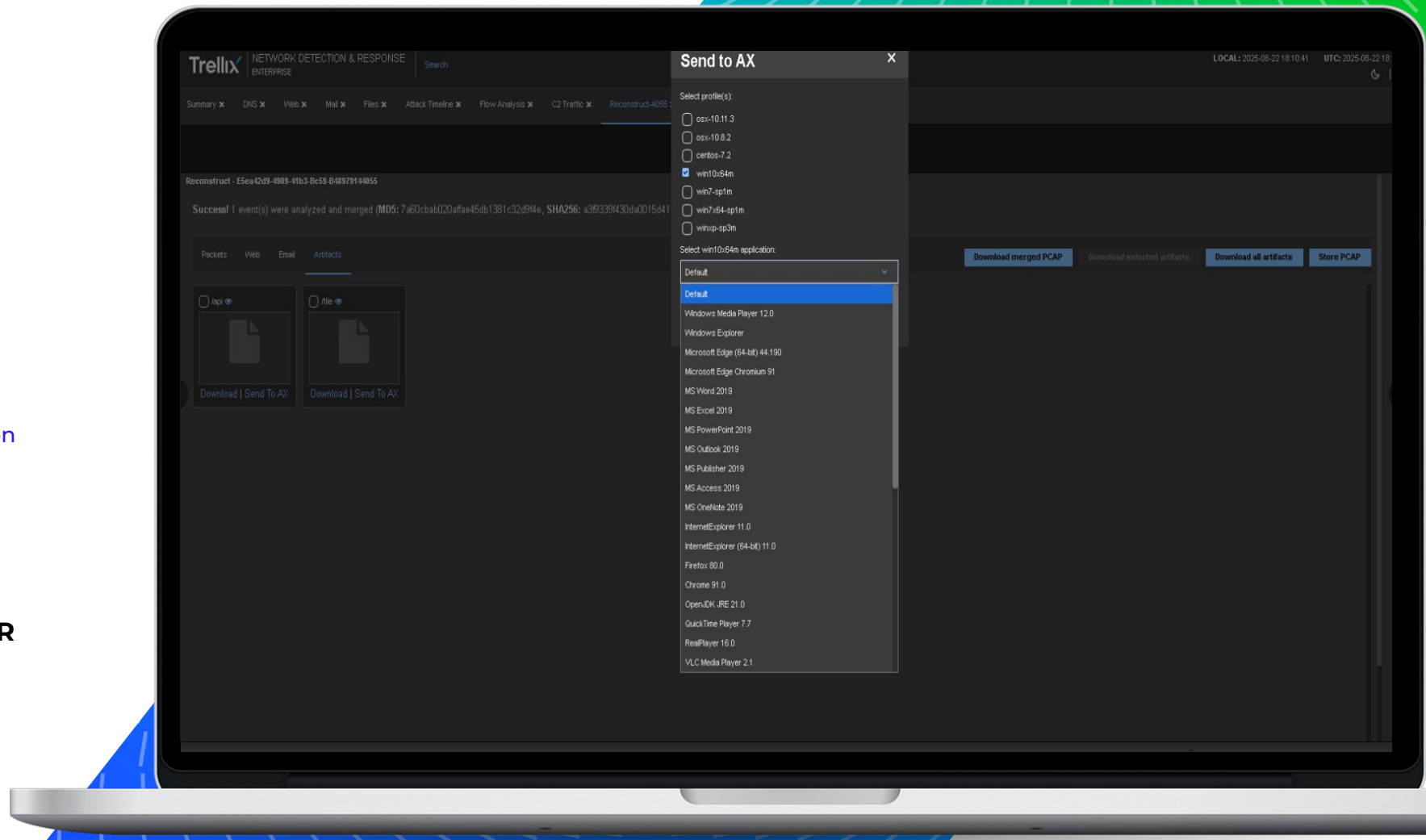


Trellix Wise™ GenAI-driven enrichment and guided workflows accelerate investigations

Trellix

Enable SOC Workflows

- **Quickly Triage Alerts**
  - SOC Analyst Workbench
  - Asset categorization by criticality
    - Risk-based scoring and aggregation framework
    - Top alerts & by geo
    - Risky assets and sessions
    - Asset OS Vs Severity
  - MITRE ATT&CK Dashboard
- **Support Threat Hunting/Forensics**
  - Forensics - Detection to PCAP Reconstruction
  - Threat Hunting
    - IOC/IOA
    - Threat Intelligence
    - Flows/L7 Metadata
- **Integrate with Sandbox, EDR, SIEM, SOAR**

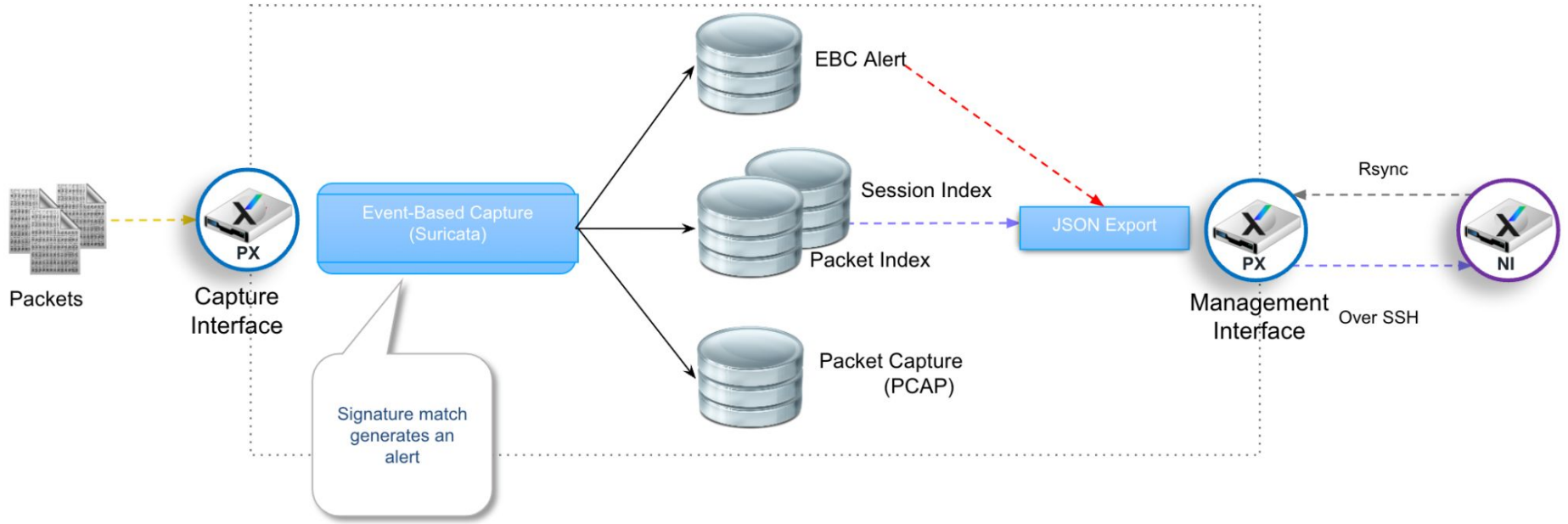


Prioritization enables Tier 1 and 2 analysts for faster triage, answering: “What do I focus on first?”

Trellix

Trellix Packet Capture (PX) – w/Forensics

- **Lossless packet capture** up to 20Gbps provides vital data into effective network forensic investigations
- **Extensive Visibility** session decoder to view and search web, email, FTP, DNS, SSL details and files
- **Ultrafast search** leverages unique indexing architecture for fast answers
- **Easy drill down** allows analysts to quickly respond to alerts that matter
- **Event Based Capture (EBC)** that uses defined and custom Suricata rules to capture data around a specific event in network traffic



Trellix

Trellix Network Forensics

Key Use Cases

Effective Searching

- List
- Saved Searches
- Scheduled Queries
  - Export results to SIEM
- PX Filters
- Build SOC analyst dashboards
- Traffic analysis in distributed environments

Captured Data - Find Anomalies

- Find Anomalies via Search:
  - Malformed HTTP Header
  - Suspicious Domains-random strings, Downloads
  - Rare protocols used for outbound connections
  - Data Exfil - B64 Blobs in POST Body

SOC Workflow Integration

- Enrich EBC Alerts
- Forensics - Detection to PCAP Reconstruction
- Threat Hunting (IOC's, Threat Intel)
- Integrate with Sandbox
- Integrate with SIEM/SOAR

Custom Rule Management

- Central Signature Update Tool engagement
  - Manage Rulesets
  - Deploy / Remove Rulesets

Trellix

Discussion and Demo Use Cases

Key: Use Cases

Effective Searching

- List
- Saved Searches
- Scheduled Queries
  - Export results to SIEM
- PX Filters
- Build SOC analyst dashboards
- Traffic analysis in distributed environments

Captured Data - Find Anomalies

- Find Anomalies via Search:
  - Malformed HTTP Header
  - Suspicious Domains-random strings, Downloads
  - Rare protocols used for outbound connections
  - Data Exfil - B64 Blobs in POST Body

SOC Workflow Integration

- Enrich EBC Alerts
- Forensics - Detection to PCAP Reconstruction
- Threat Hunting (IOC's, Threat Intel)
- Integrate with Sandbox
- Integrate with SIEM/SOAR

Custom Rule Management

- Central Signature Update Tool engagement
  - Manage Rulesets
  - Deploy / Remove Rulesets

“A knife to a gunfight”

Who’s to blame?

What are the possible outcomes?

Trellix

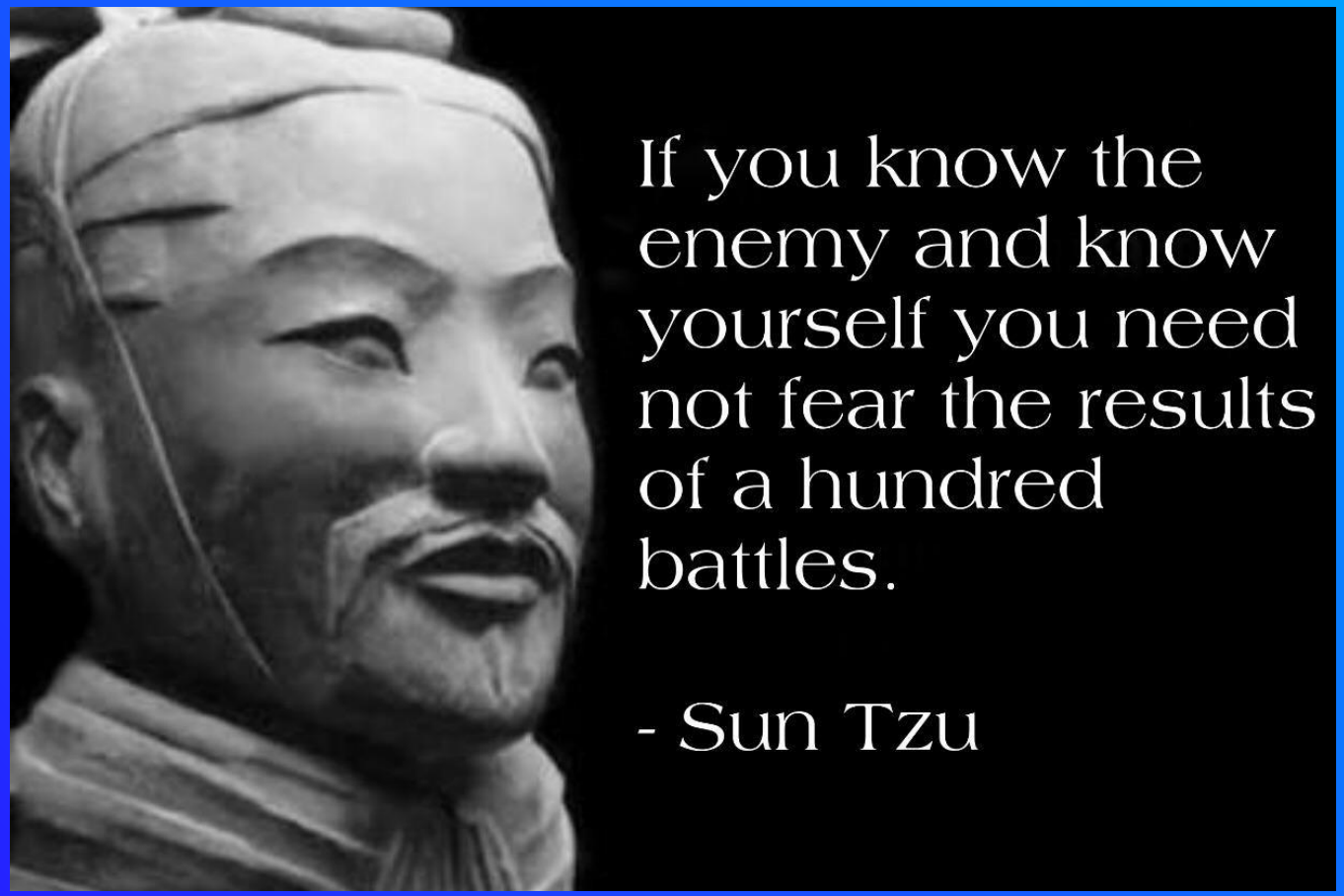
What are the possible outcomes?

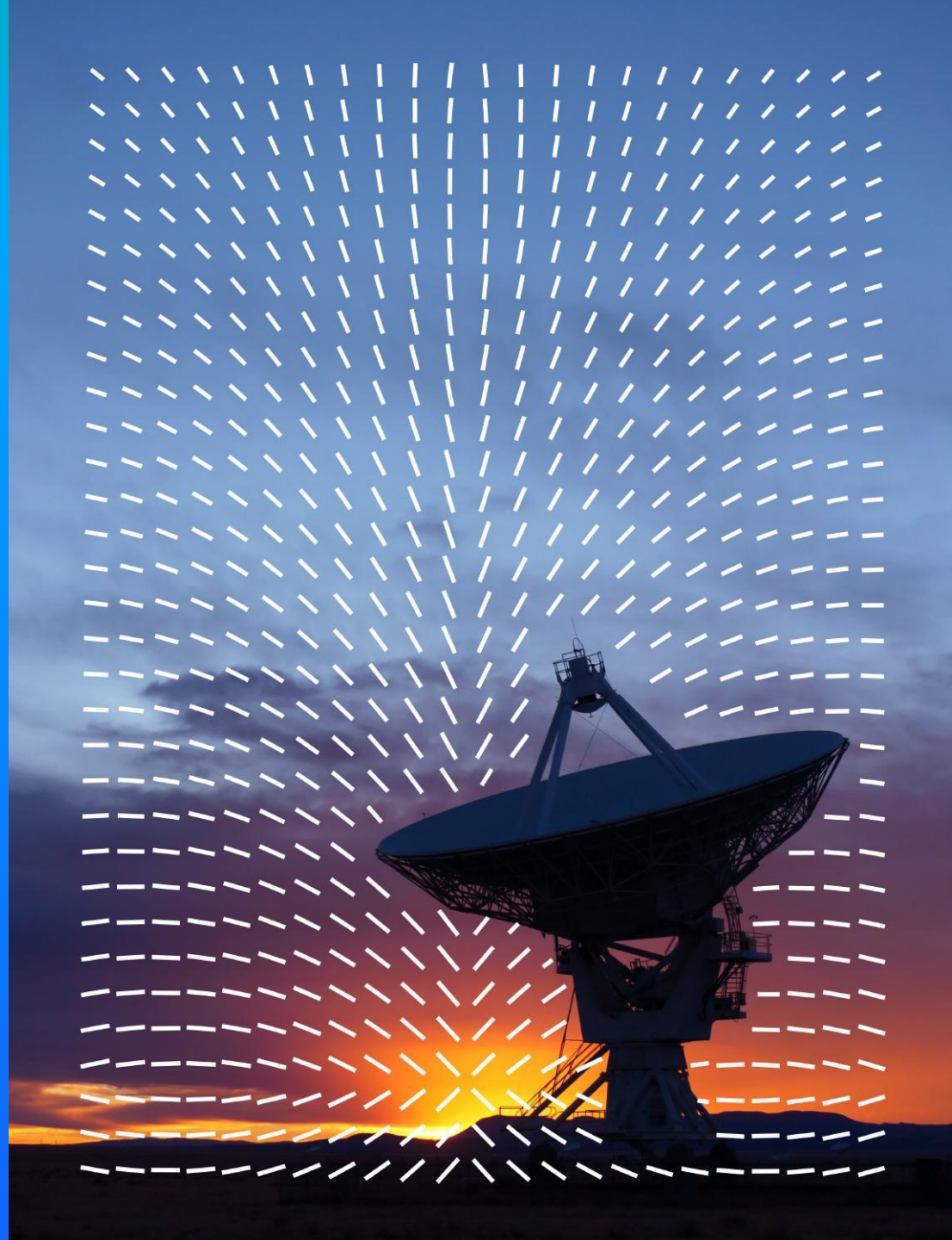
The Battle of Shiroyama, 1877

Belligerents	
Japan	Satsuma Domain
Commanders and leaders	
Yamagata Aritomo	Saigō Takamori †
Strength	
30,000[1]	500
Casualties and losses	
30 killed[2]	500 killed

Trellix

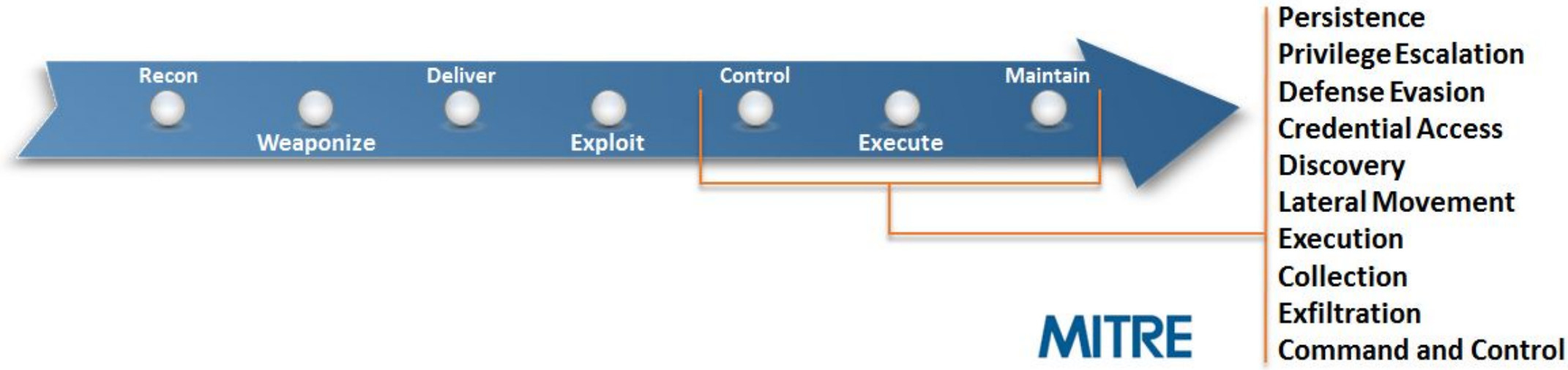
Thriving through the age of Cyberwarfare





MITRE ATT&CK®

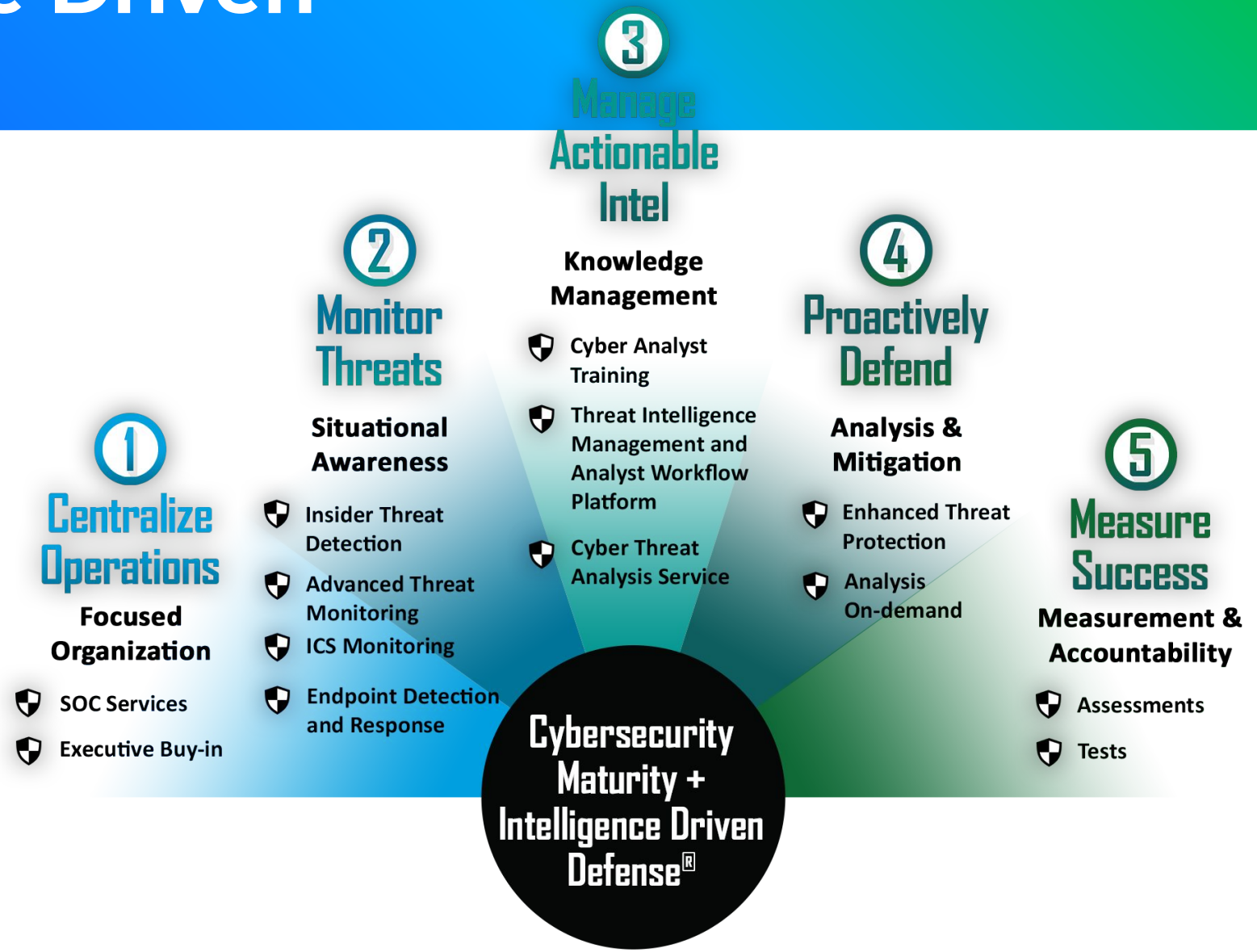
To better understand the enemy



Trellix

Intelligence Driven Defense

Lockheed Martin



Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/intelligence-driven-defense.html

The Threat Intelligence Group
Part of the Advanced Research Center (ARC)

Moto: “Always Vigilant against Evil”

24/7 mission-critical insights on the evolving threat landscape

Valuable Intelligence based on:

- Product integrations
- Custom intelligence collections
- In-depth research

History

- 2015 Support US Intelligence Community (IC)
- Expand service to IC agencies, defense orgs, Homeland Security, Federal law, commercial & financial orgs
- 2022 Trellix (McAfee & FireEye) ARC

Trellix

https://www.trellix.com/en-us/platform/threat-intelligence.h

Operational Threat Intelligence Foundation

1.5 PB	8.75 TB	2B	>100
of data (samples)	data processed per day	email samples per day	malicious file detections per month

Real-time, reliable, information to:

1. Anticipate threats
2. Detect and block threats
3. Accelerate informed responses

Trellix

Data-Driven Threat Intelligence Trellix Insights

Insights has intelligence on:

+4000
campaigns

+250
different threat groups

+2250
different malicious and non-malicious tools

+100
actors and tools with extensive tracking

Advanced Threat Landscape Analysis System(ATLAS):

+/-250
malicious file detections in last 30 days.

13.8
Thousand Unique MD5 campaigns detections

13.8
Thousand Unique MD5 campaigns detections

Trellix

Global Threat Intelligence Group

Moto: “Always Vigilant against Evil”

+200
researchers

- Located in multiple time zones, 24/7 coverage.
- Concentrated hubs in Europe and East Coast US.
- Analysts remote and on-site with customers.
- Native speakers in Russian, Chinese, Vietnamese, French, German, Spanish, Portuguese, Hebrew, Arabic and Dutch.
- Skillset, from analyst to Vuln and Malware research
- Customers ranging from National CERTS, IC agencies, LE Agencies, Defense, and commercial orgs.
- Top Publications
- Data-driven research from intel to products.

Trellix

Partnerships and Relationships

Intelligence-sharing partnerships:

- MISP CIRCL.
- JCDC CISA.
- Mandiant inc. RPP.
- CyberVeilig Nederland.
- Intel471.
- JPCert.
- AIS CISA (under development).

Relationships Public Sector:

- Europol EC3 Advisory Group
- NSTAC
- JCDC
- NSA CCC
- FBI
- NCA
- NHTCU.

Trellix

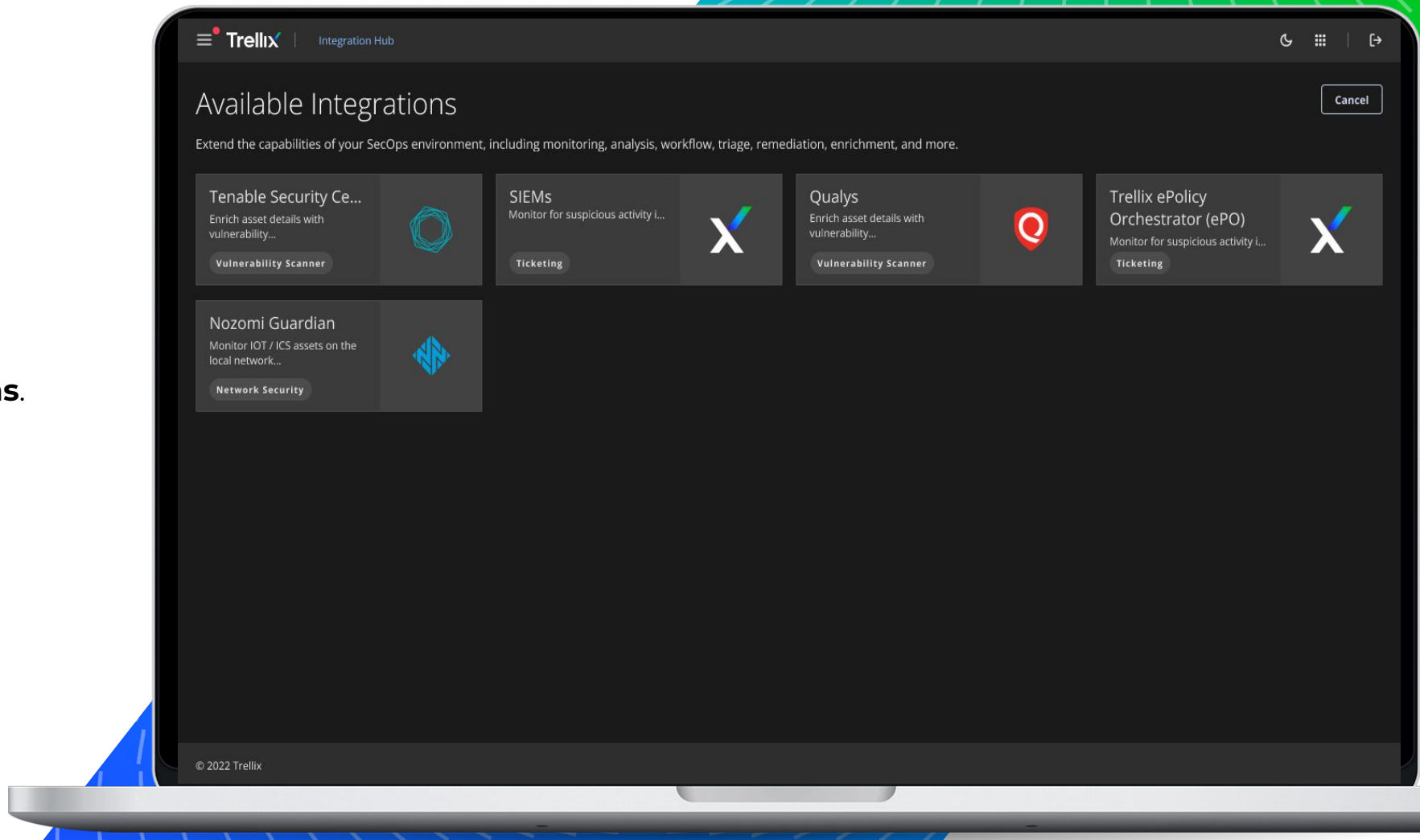
Integration
s Hub

Feature highlights

- Enables broader visibility and context with **3rd party integrations**.
- Supports **ingestion, enrichment**, **notification, and tasking** of data, including **log data, threat intelligence, endpoint data, and 3rd-party security events**.

Benefit

- It reduces the **time needed** for investigations by centralizing disparate data and **providing additional context**.



Trellix

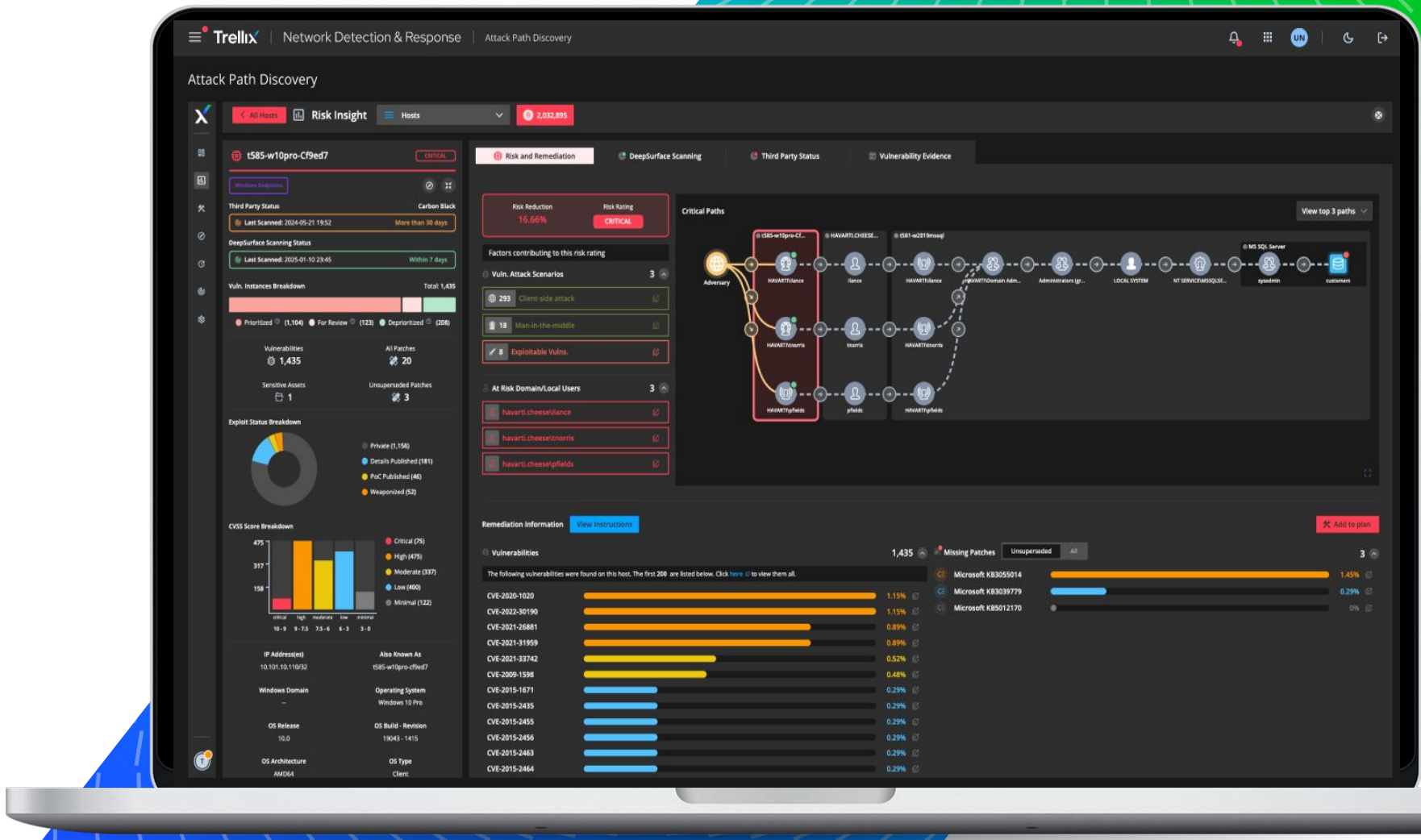
Attack Path Discovery

Feature highlights

- Visualizes **potential attack paths** that threat actors could exploit to **compromise critical assets**, leveraging vulnerability data and network topology to **model potential privilege escalation** and **lateral movement** scenarios.

Benefit

- **Attack Path Discovery** enables security teams to proactively **eliminate high-risk attack vectors** before attackers can exploit them, allowing security teams to **prioritize patching based on actual risk paths** rather than generic severity scores, and focusing limited resources on **vulnerabilities that truly matter.**



Trellix

APD - Context-Aware Prioritization - Scenario 1

User Exposure : NONE **Asset Exposure :** NONE **Privilege Exposure :** NONE **Overall Risk :** NONE

Trellix

APD - Context-Aware Prioritization - Scenario 2

User Exposure : LOW **Asset Exposure :** NONE **Privilege Exposure :** NONE **Overall Risk :** LOW

Trellix

APD - Context-Aware Prioritization - Scenario 3

User Exposure : HIGH **Asset Exposure :** HIGH **Privilege Exposure :** CRIT **Overall Risk :** CRIT

Trellix

Anomaly Detection on ICS network

Is there behaviour of a device similar to that of an infected one?

Is a User logged into a device they doesn't use?

Is an ICS device connected to an unusual host (external/internal)?

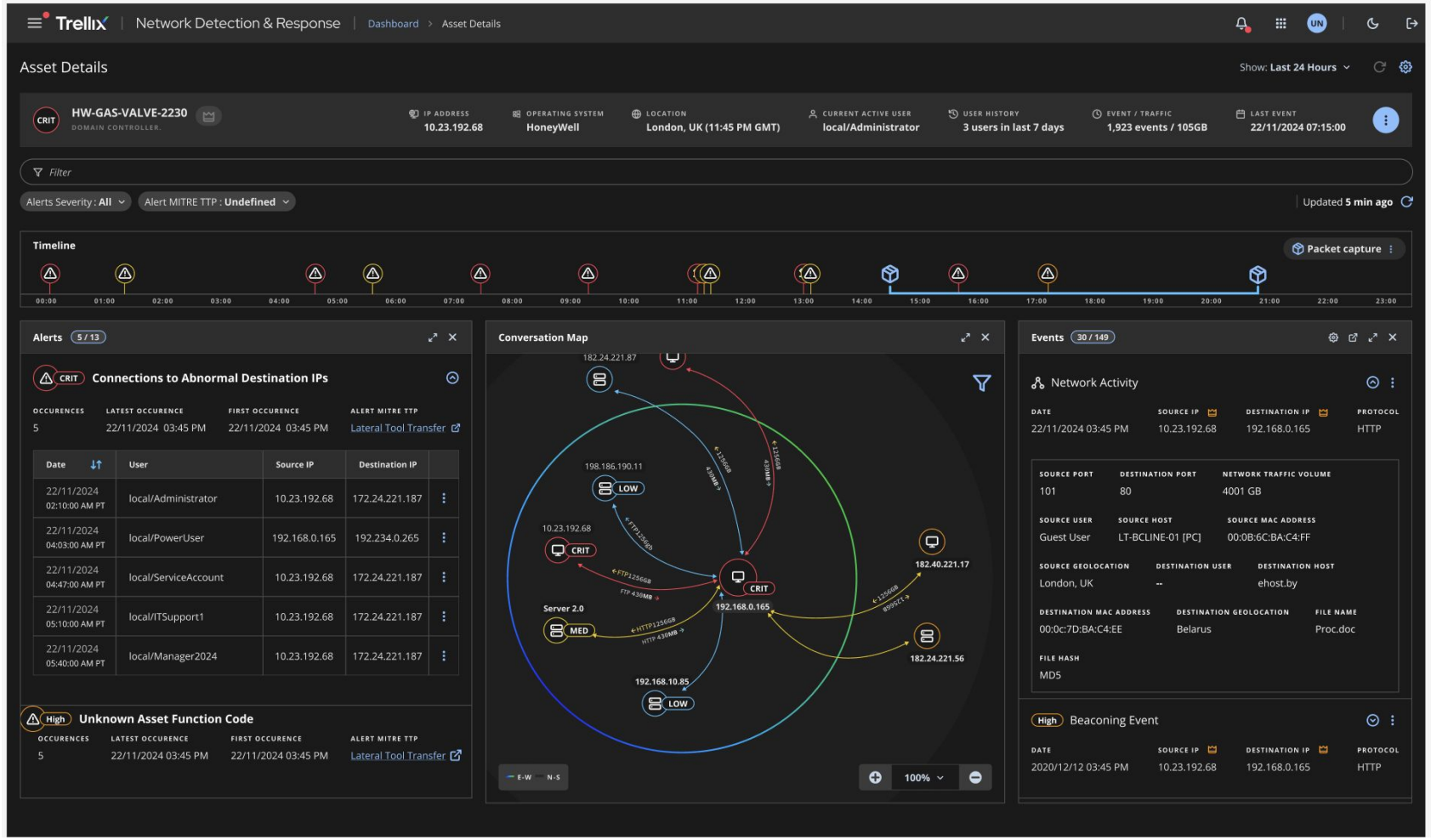
Is someone scanning your IoT/Enterprise network.?

Is there a User who has access to critical infrastructure been compromised?

Was someone successfully able to steal credentials by phishing?

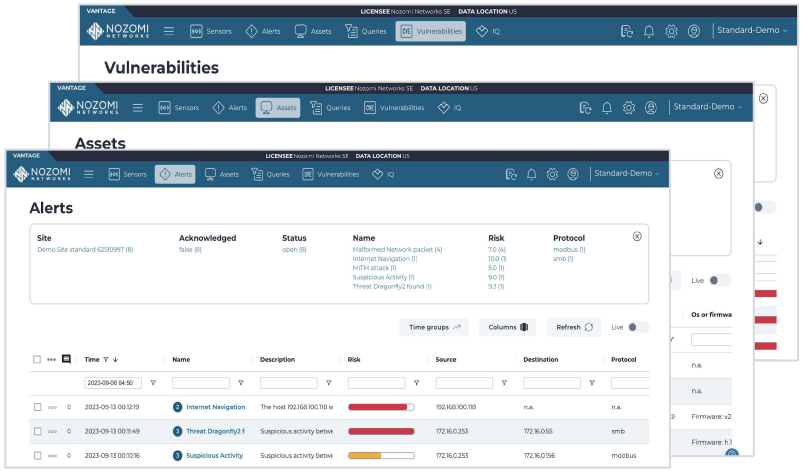
Is someone trying to push a malicious binary from enterprise from Enterprise to ICS?

70+ AI/ML models that will detect different anomalies and malicious activity on ICS networks.

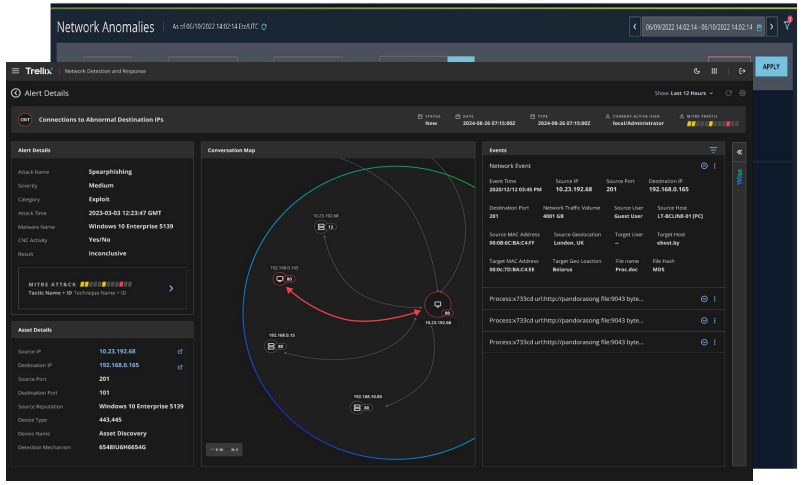


Trellix

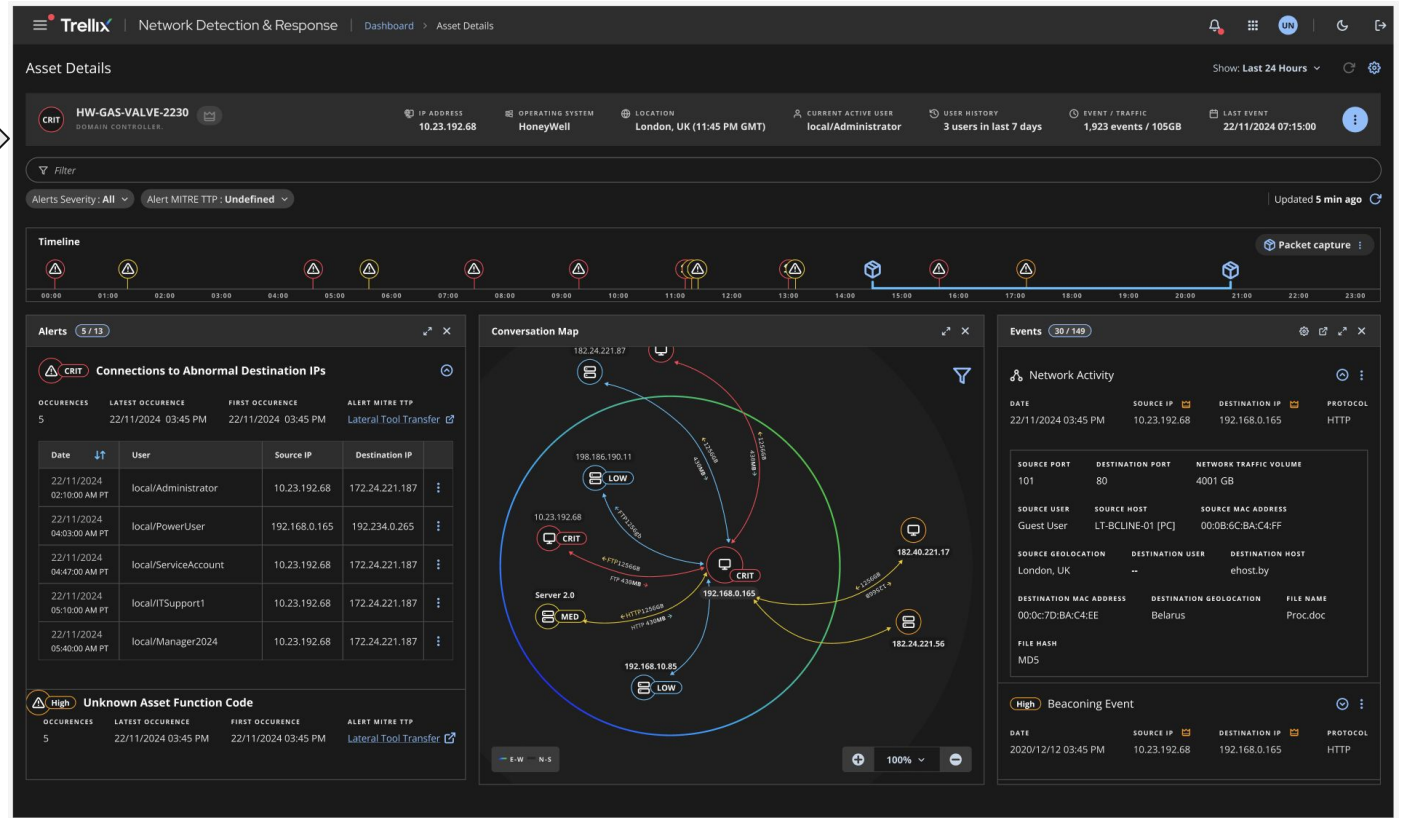
Unified Platform



ICS

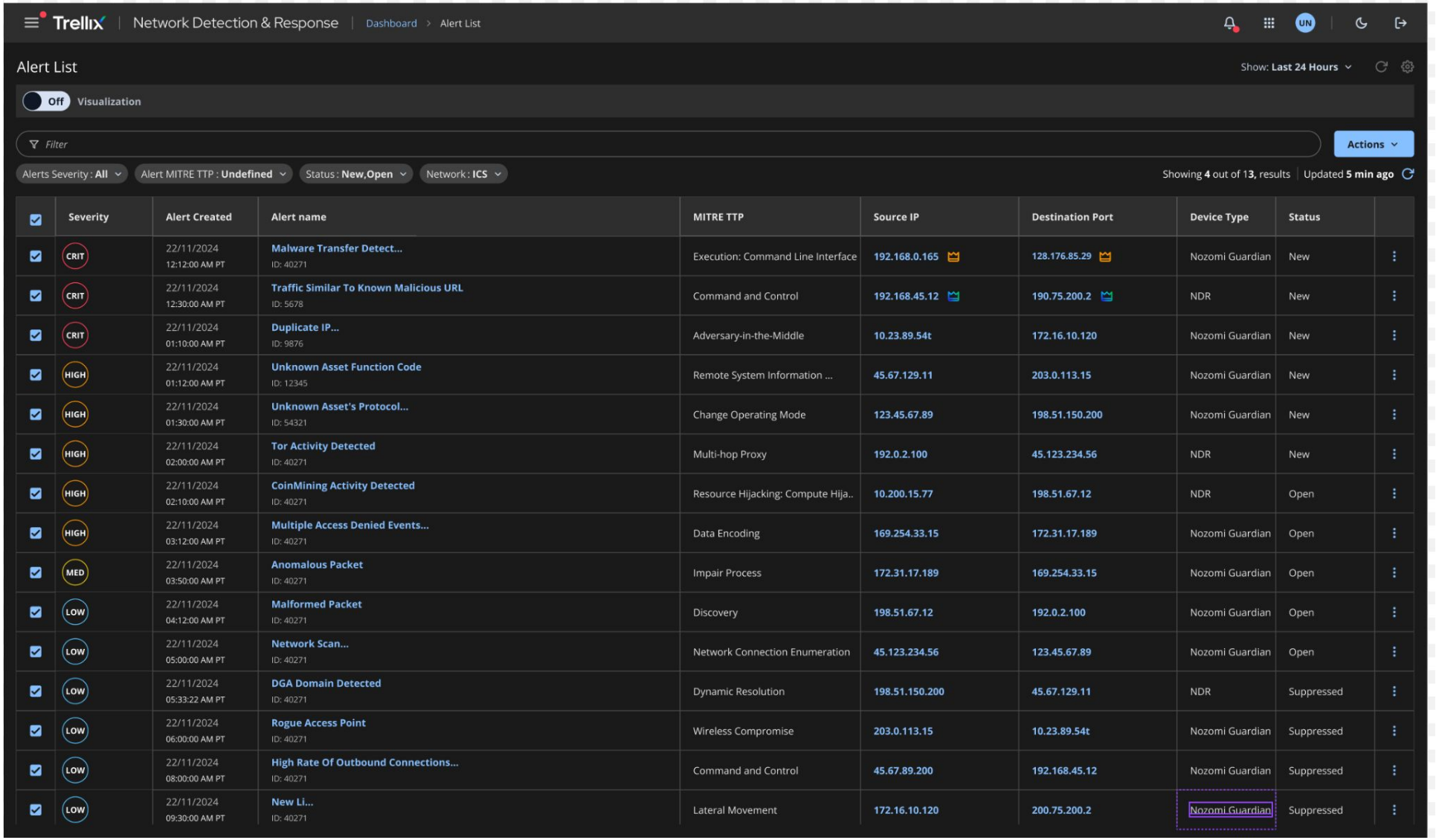


Enterprise



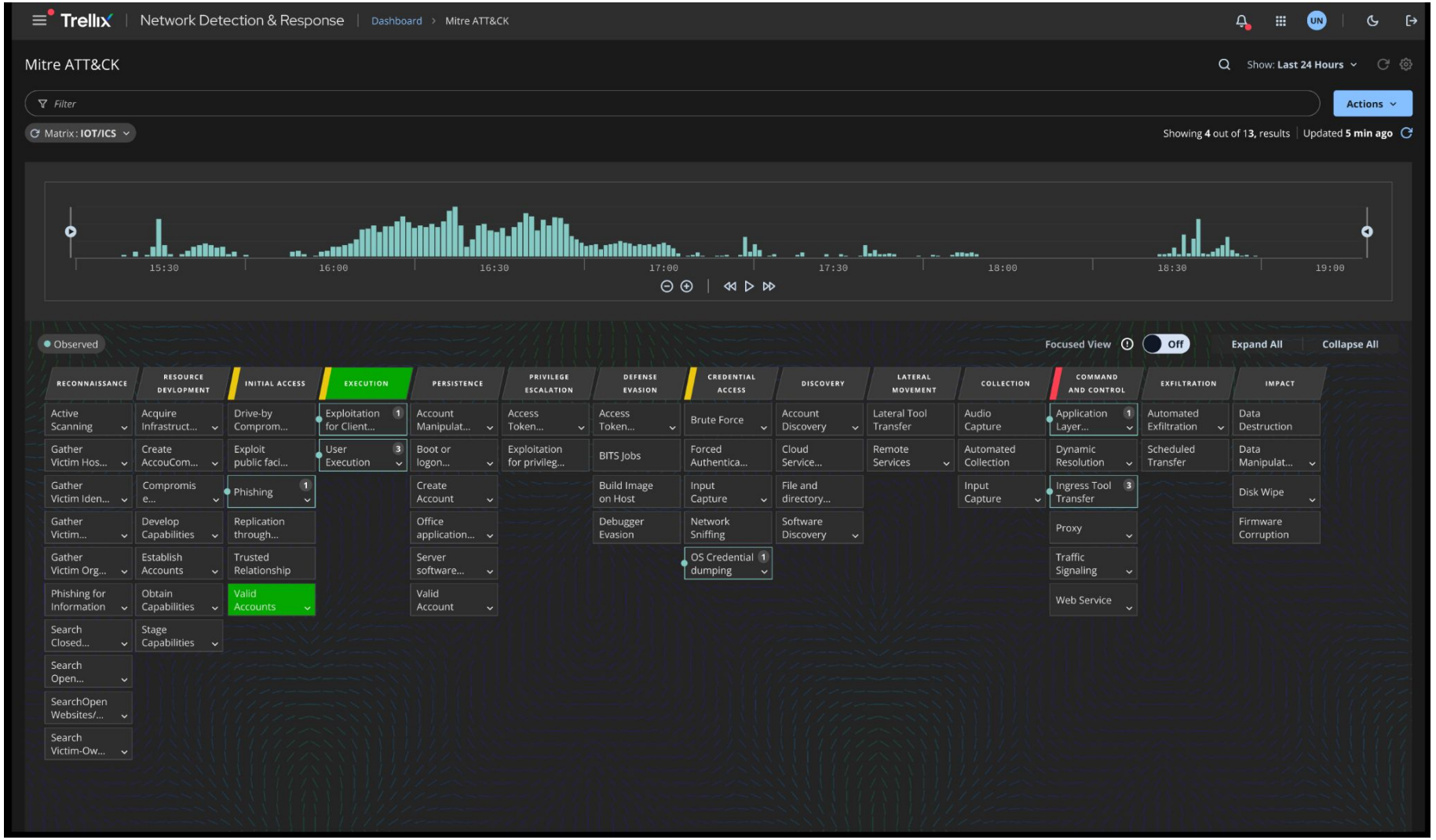
Trellix

Nozomi Alerts in NDR



Trellix

Enterprise & ICS MITRE Mapping



Trellix

Trellix® NDR Use Cases: Values and Outcomes

Centralized, Intelligent Visibility, and Analytics

Detection, Forensics, Incident Response (DFIR), Threat Intelligence and Threat Hunting

- **Prioritize and triage alerts using AI**
- **Anomalies** - lateral movement, data exfil, and C2
- Traffic analysis in **distributed environments**

Centralized Operational Efficiency

- **Reduce manual analysis (Context, AI)**
- Enrich threat intel across multiple network segments
- **Identify threat trends and risk exposure**

SOC Workflow Integration

- **Enrich context for investigations**
- **Forensics** - Detection to PCAP reconstruction
- Threat Hunting (IOC's, Threat Intel)
- **Integrate with Sandbox/EDR/SIEM/SOAR**

SOC Maturity

- Enable **Tier 1 and 2 analysts for faster triage**
- Reduce the need for packet analysis skills
- Provide rich network data up to L7
- **Contextual alert aggregation across sensors**

Trellix

NDR Architecture, Design & Integrations

Duration - 20 Minutes

NDR Reference Architecture

NDR Console

AI/ML and Correlation Detection – Risk-Based Scoring

- Threat Intelligence
- Hyperautomation
- Trellix WISE™
- AttackPath Discovery
- Asset Discovery

L7 Metadata, Flow Records and Alerts	L7 Metadata, Alerts and PCAPs	Trellix Integrations	Third-Party Integrations
NDR Sensor	Network Forensics	ePO/HX (EPP/EDR)	splunk> a cisco company, SIEM
IVX		CMS[1], IPS	NOZOMI NETWORKS[2], VPC Flow Logs[2]
		Malware Analysis (AX)	CROWDSTRIKE[2]
		Helix	tenable

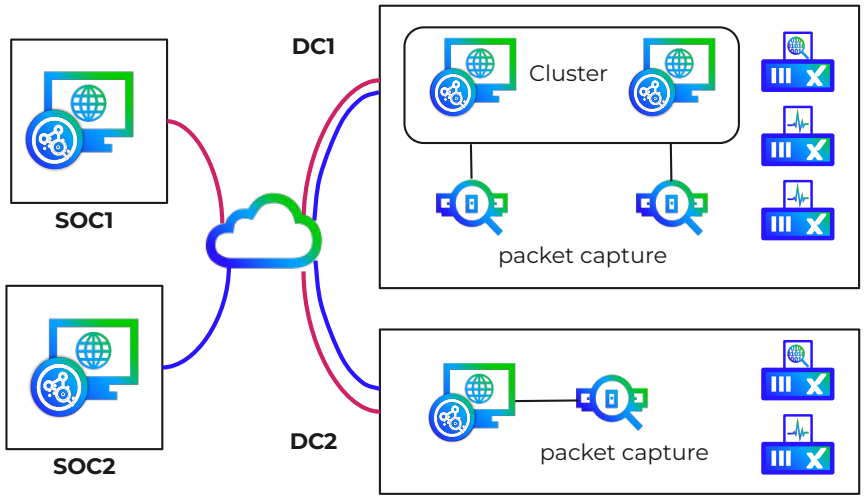
1. *EX, HX Alerts Only*
2. *Roadmap 2HCY25*
3. *Same as an NX Appliance*

Trellix

NDR Console / Analyst Workbench

Focus on most critical alerts and assets while avoiding alert fatigue

- Intuitive Analyst Experience
  - Analyst-centric design empowers a confident and rapid response.
  - Intuitive workflows deliver information and context, when and where you need it
  - AI-guided investigations and automated responses, are informed by elite security practitioners
- Scalable NDR System
  - Flexible multi-node deployments and clustering with distributed search with aggregated investigation and analysis
- Integrations Hub (Trellix and Third Party)
  - Seamless integrations with Trellix and third-party vendors
  - SIEM, Threat Intelligence, SOAR and more...



Trellix

NDR Portfolio

NDR Console
NDRC-2600-T

NDR Operations for security analytics and threat detection

- Network metadata process and alert analysis with Trellix Wise™ AI
- Central search across PX and NDR consoles
- AI / ML detections
- Flow and Layer 7 Records with fast search
- Event enhanced MITRE, CVE, and IOC Detection

NDR Sensor (NX Series)[1]
NDRS-x600 Series, NX-x600 Series

NDR Sensor Virtual[1]
VA-NXS series (Cloud, ESXi - KVM - HyperV)

NDR Sensor (IPS NS Series)[1]

Forensics (PX Series)

Detect and Block E-W and Advanced Threats

- Built-in Intelligent Virtual eXecution threat detection detects new and emerging threats
- Integrated ML Engines for Data exfiltration, DGA, Beaconing and more
- Event-based capture, generation & tagging
- TLS Onboard, SSL Anomalies
- C&C, reputation, L7 visibility
- Flexible operation modes: defend, boost, flare

Perimeter Protection and N-S In-Line Response

- Full IPS for Perimeter / Data Center Protection
- Event-based capture
- TLS Onboard
- Event generation & tagging
- DoS/ DDoS, Deep file inspection
- C&C, reputation, L7 visibility

Forensics and Compliance

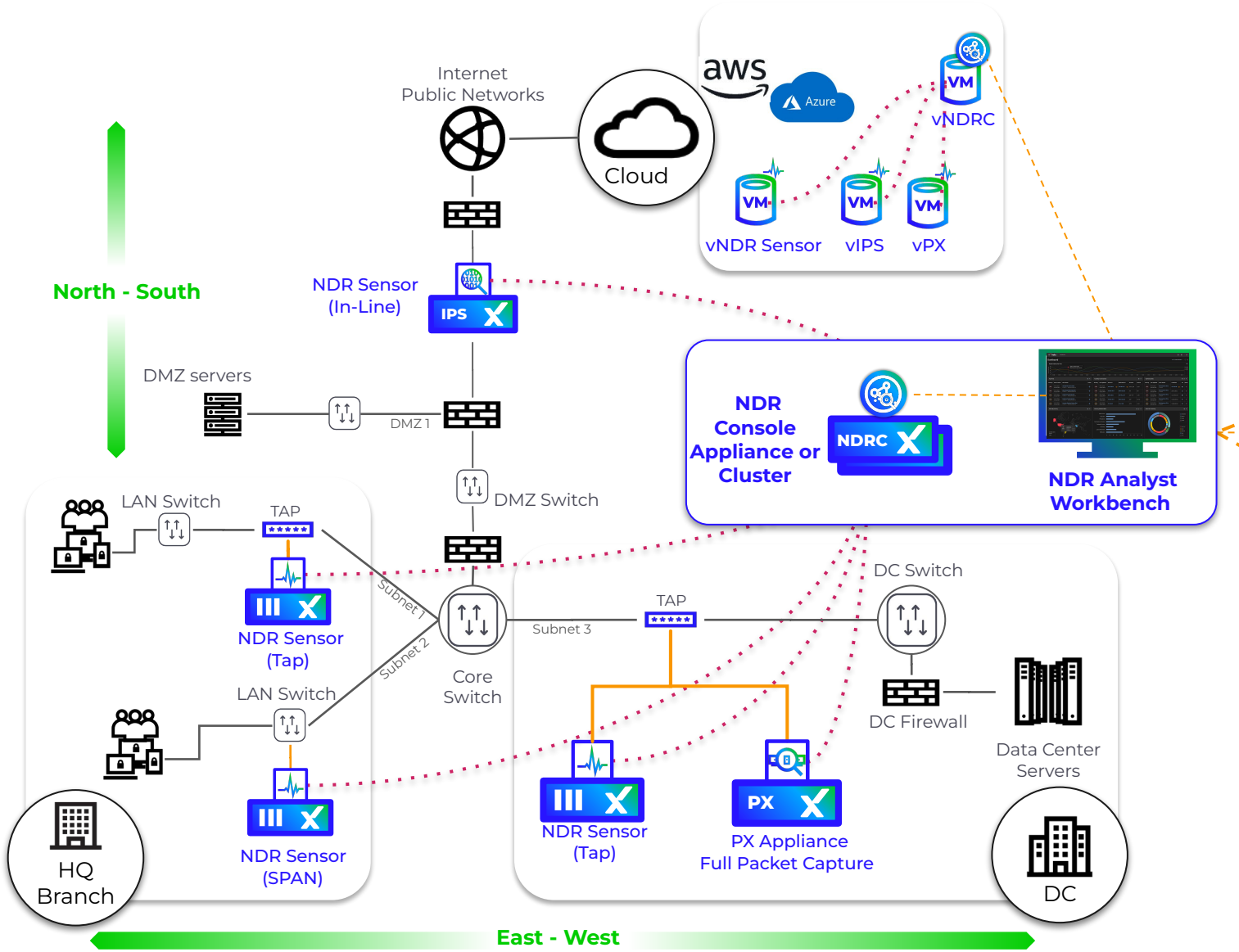
- 24x7 recording of all network traffic
- Data exfiltration capture
- TLS Onboard
- Full, Lossless Packet Capture (PCAP)
- Fast Search up to L4
- Real-time L4-7 Metadata and Indexing

Physical, Virtual, Public and Private Cloud

1. Existing Trellix customers can switch on NDR without interrupting network operations after a simple software release upgrade to v11.x or newer. More information is available in Network Security (NX) Datasheet

Trellix

NDR - IT Deployment Architecture



Trellix Integrations

- ePO - Context &Tasking
  HX Server - IP to Host Map
  CMS - Alert aggregation
  (HX/EX)
- TLC/AD - IP Host/User Mapping
- Sandbox - Malware Analysis
- Helix/Hyperautomation - SecOps and Automation

SOC

Third-Party Integrations

SIEM

tenable

VPC Flow Logs [1]

NOZOMI NETWORKS [1]

1. Roadmap 2HCY25

- **NDR Analyst Workbench**
- **NDR Console Appliance**
- **NX Series NDR Sensor**
- **IPS Series NDR Sensor**
- **PX Series Packet Capture**
- **Virtual NDR Console**
- **Virtual Appliance** (Sensor, IPS, PX)

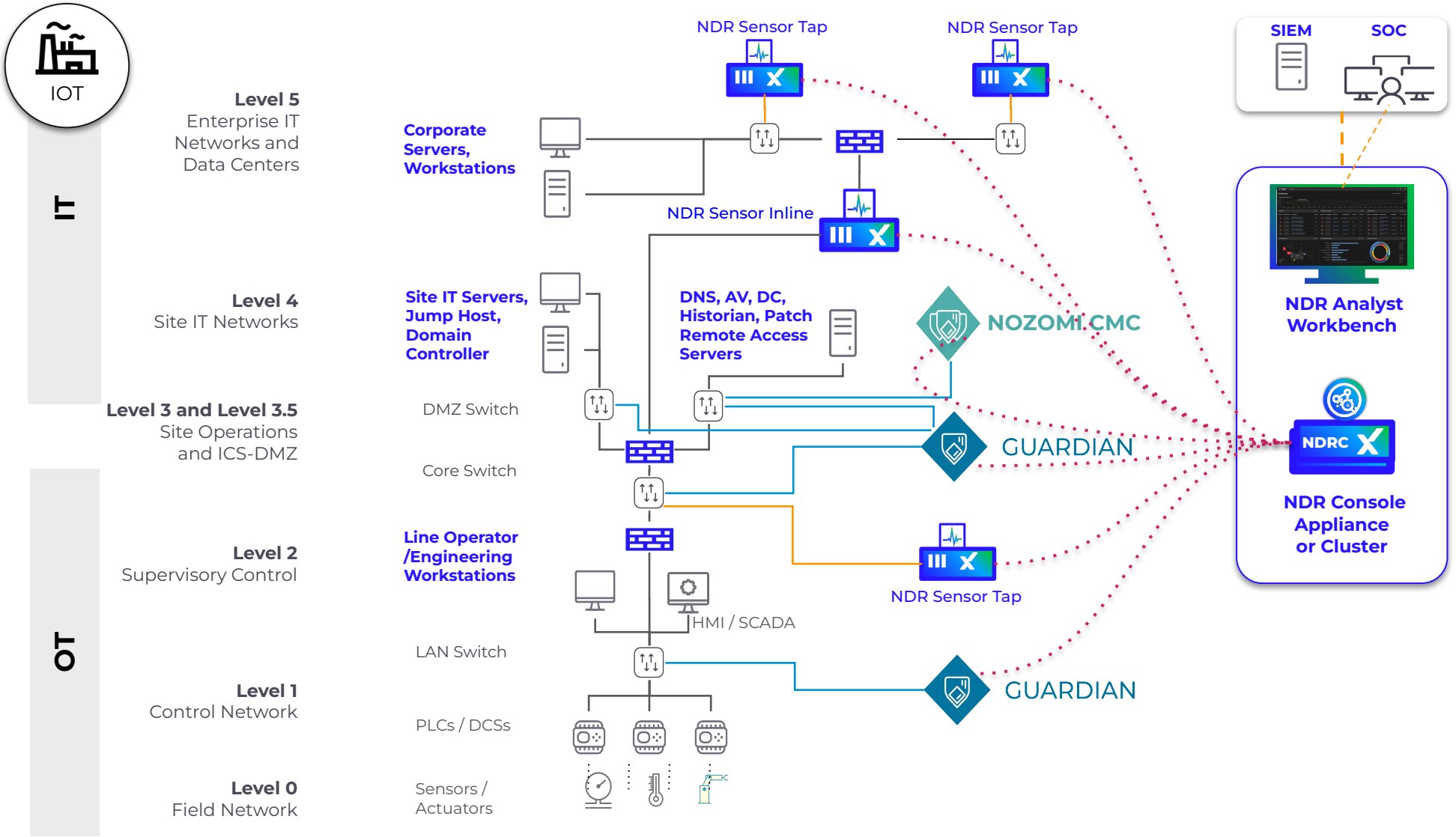
Alerts, L7, Netflow

Network Packet Broker (TAP) Link

Integrations

User / UX experience

NDR - OT Deployment Architecture (Wired)



NDR Analyst Workbench

NDR Console Appliance

NX series NDR Sensor

NOZOMI CMC

GUARDIAN

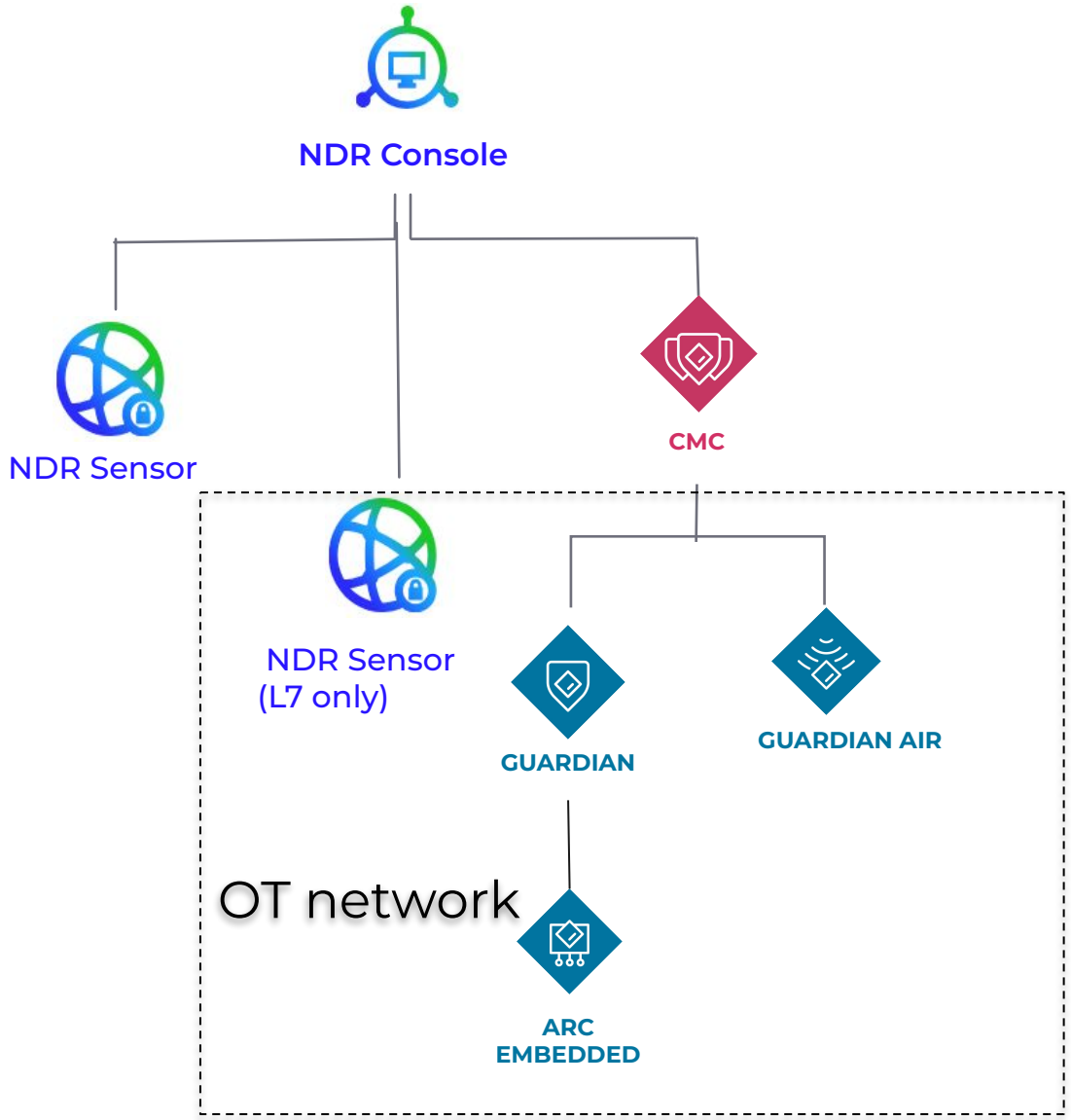
Alerts, L7, Netflow

Network Packet Broker (TAP) Link

Integrations

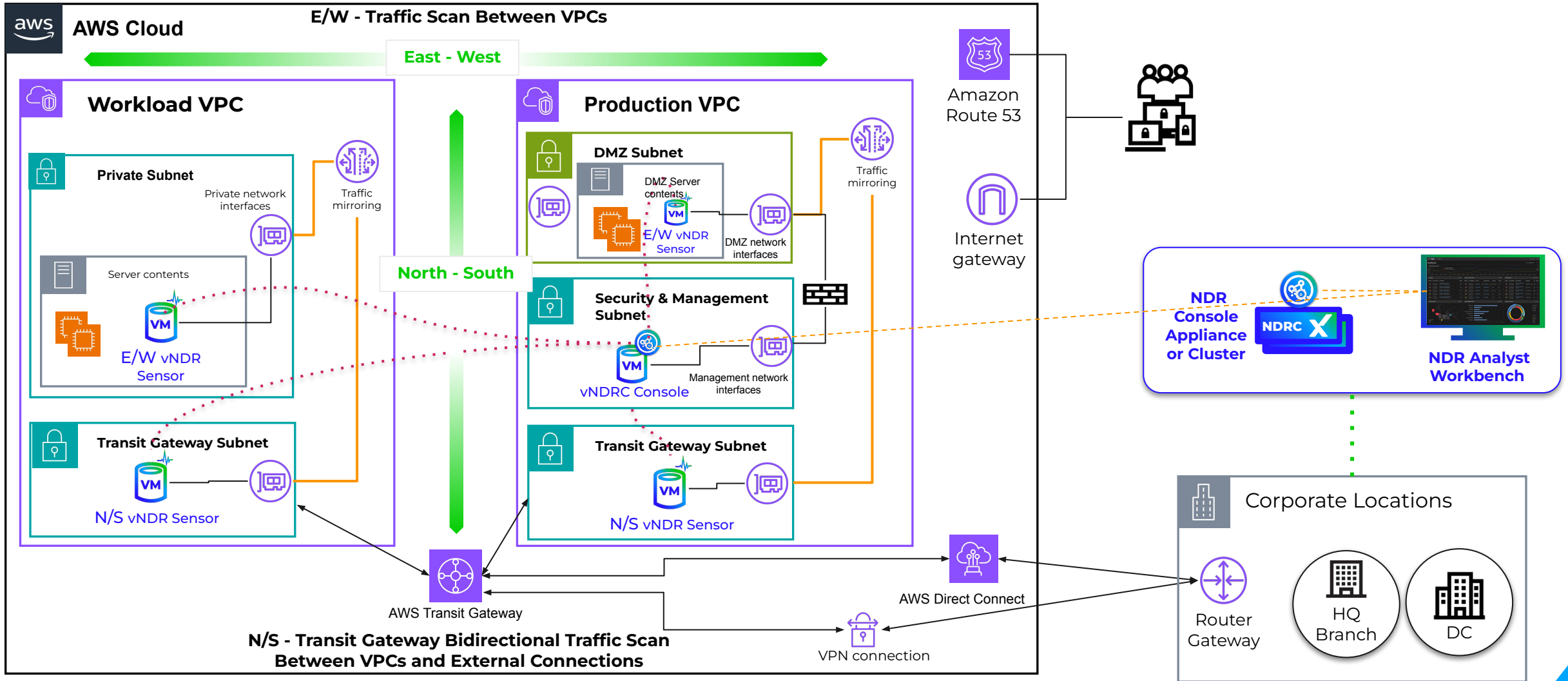
User / UX experience

Trellix NDR + Nozomi OT Integ Architecture

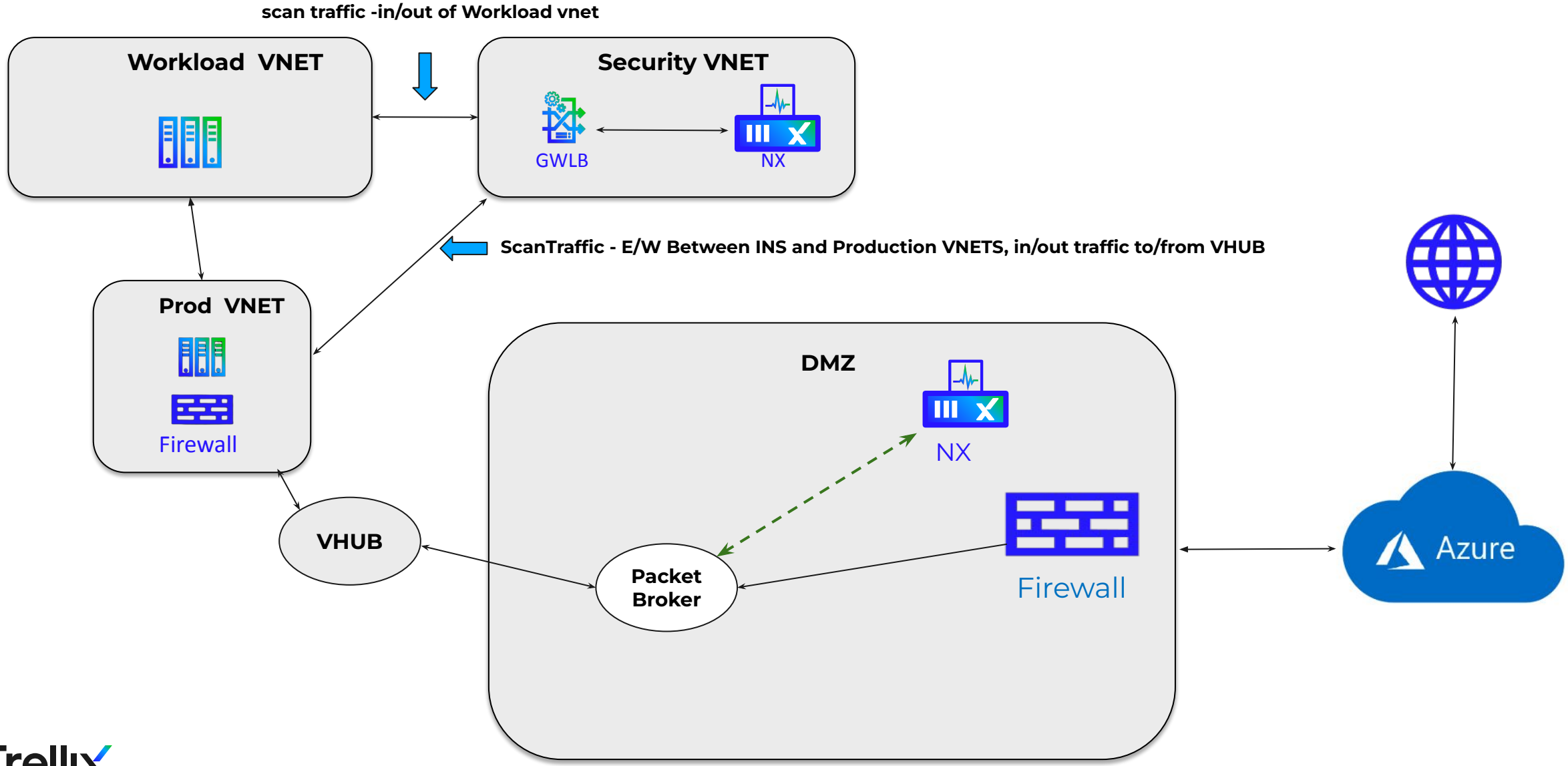


Trellix

AWS Deployment Architecture



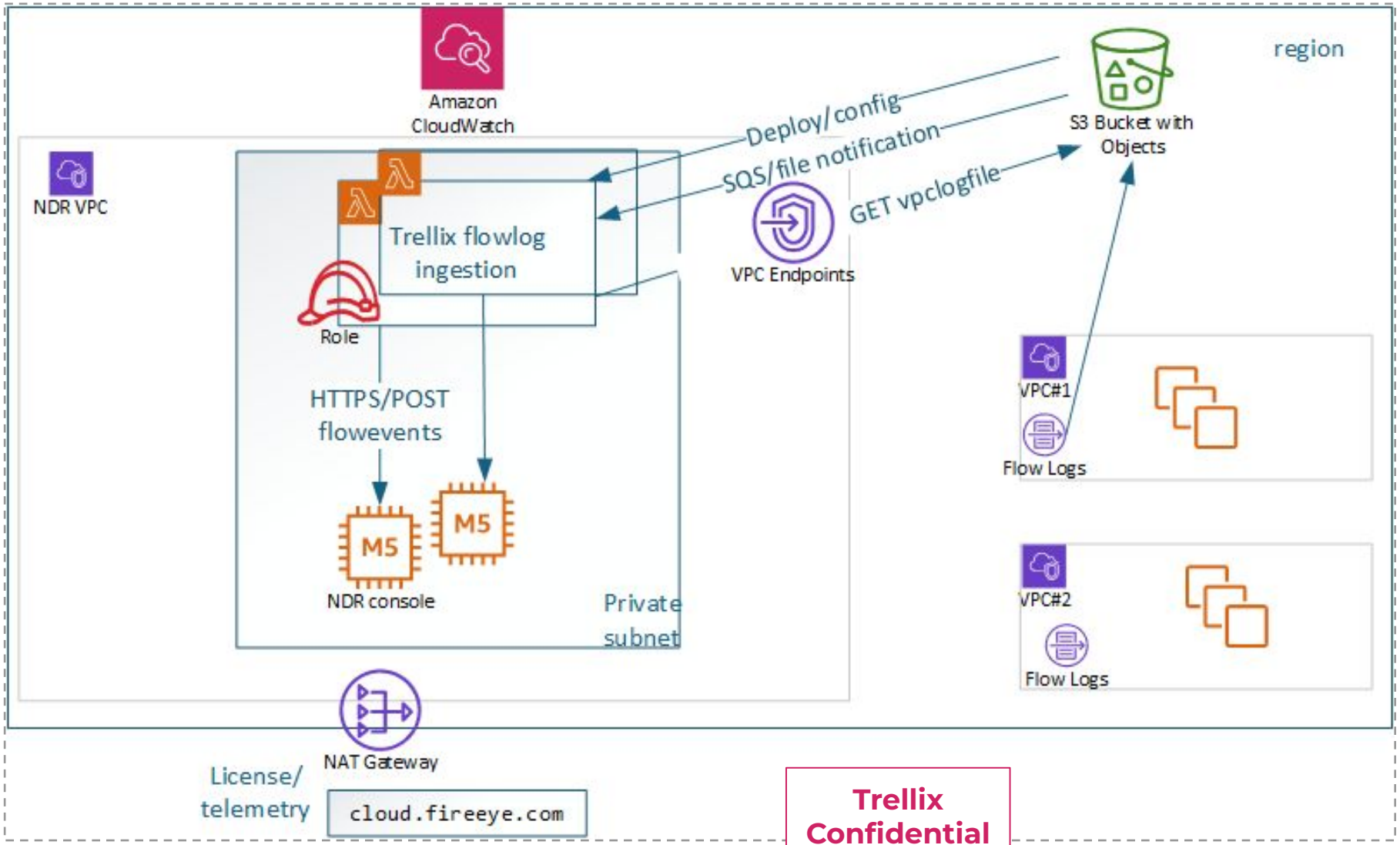
NX Azure Deployment Architecture



Trellix

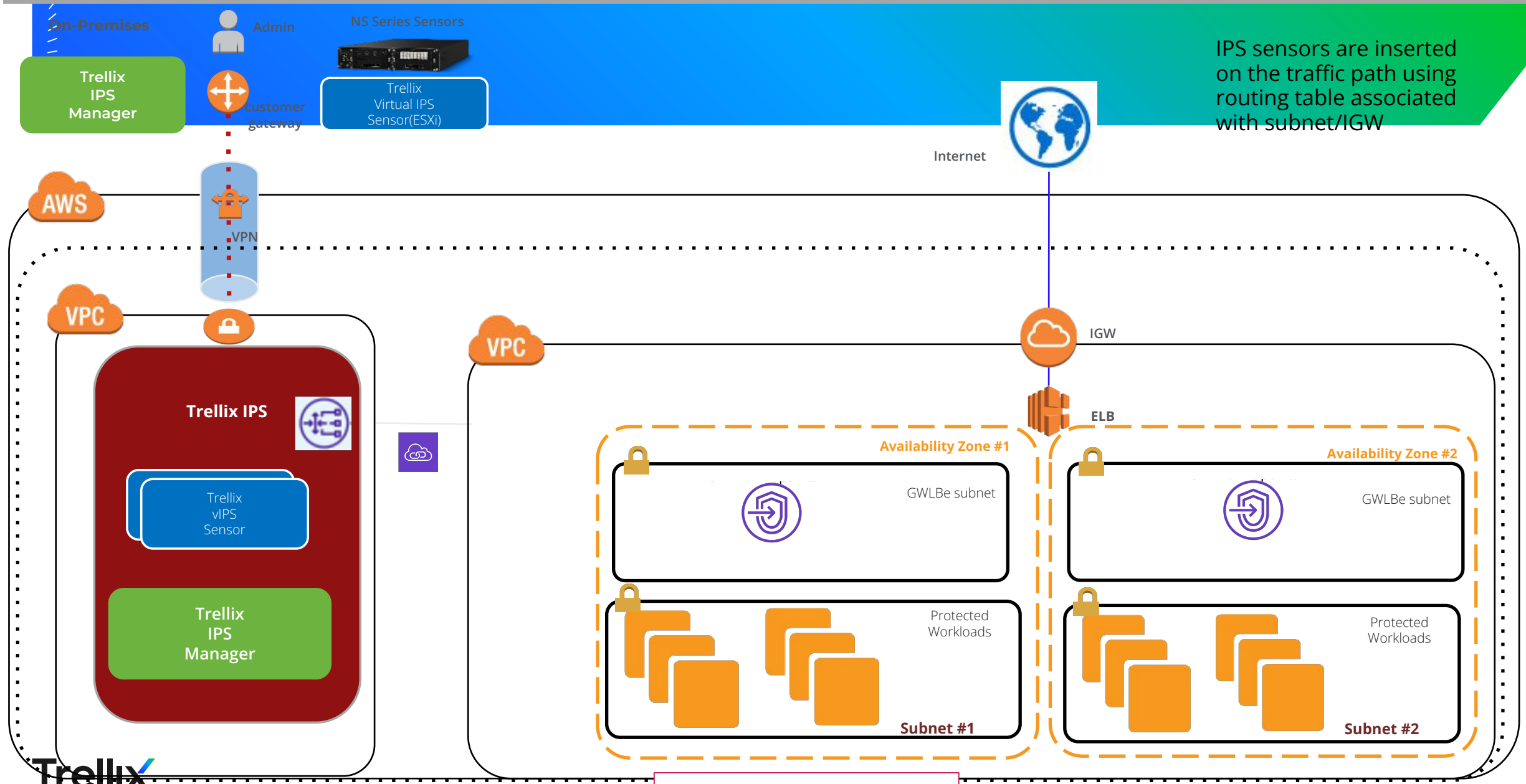
Proposed Network Detection and Response (NDR) architecture for VPC flow ingestion

Roadmap - Internal Only

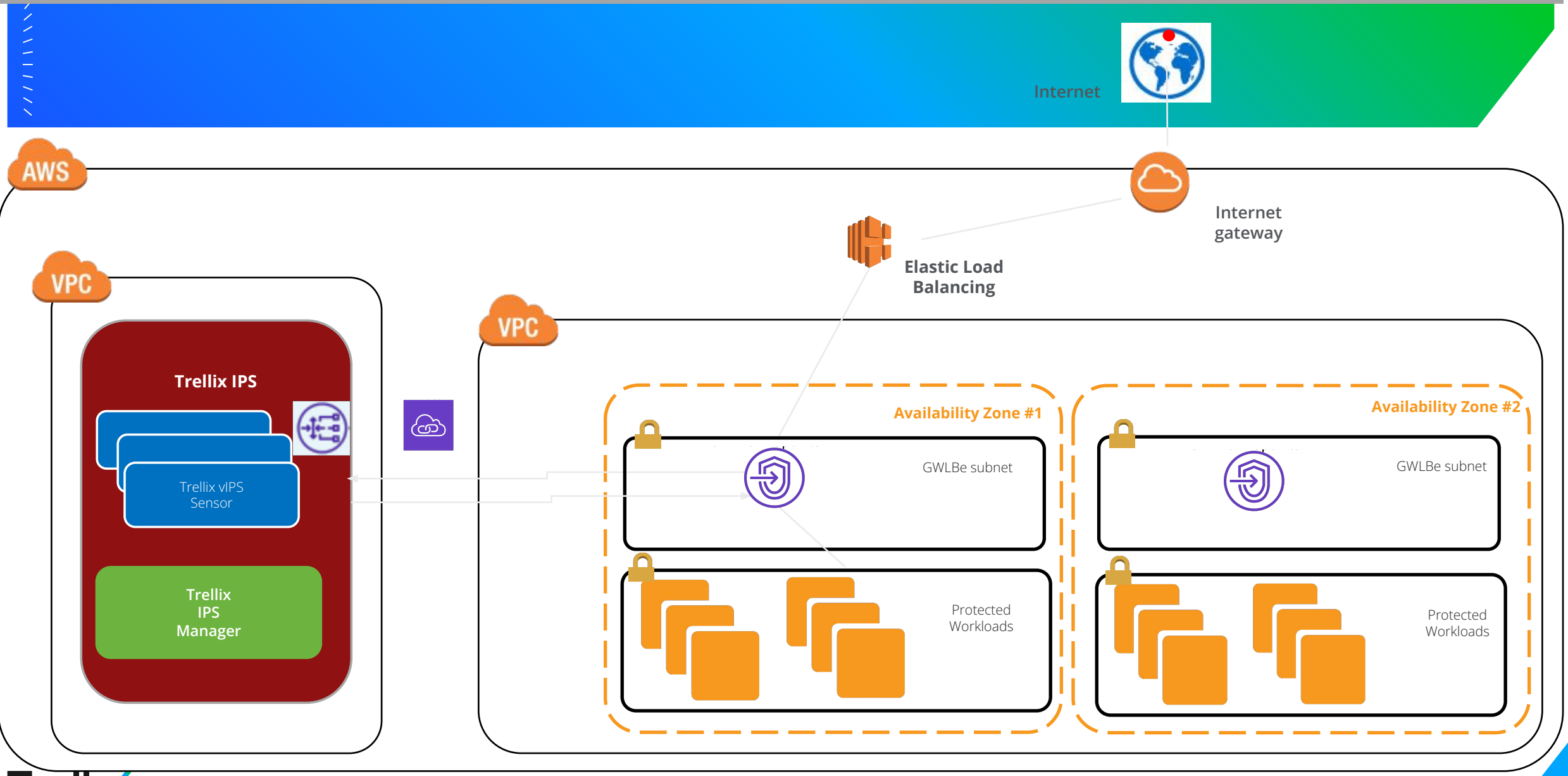


Trellix Confidential

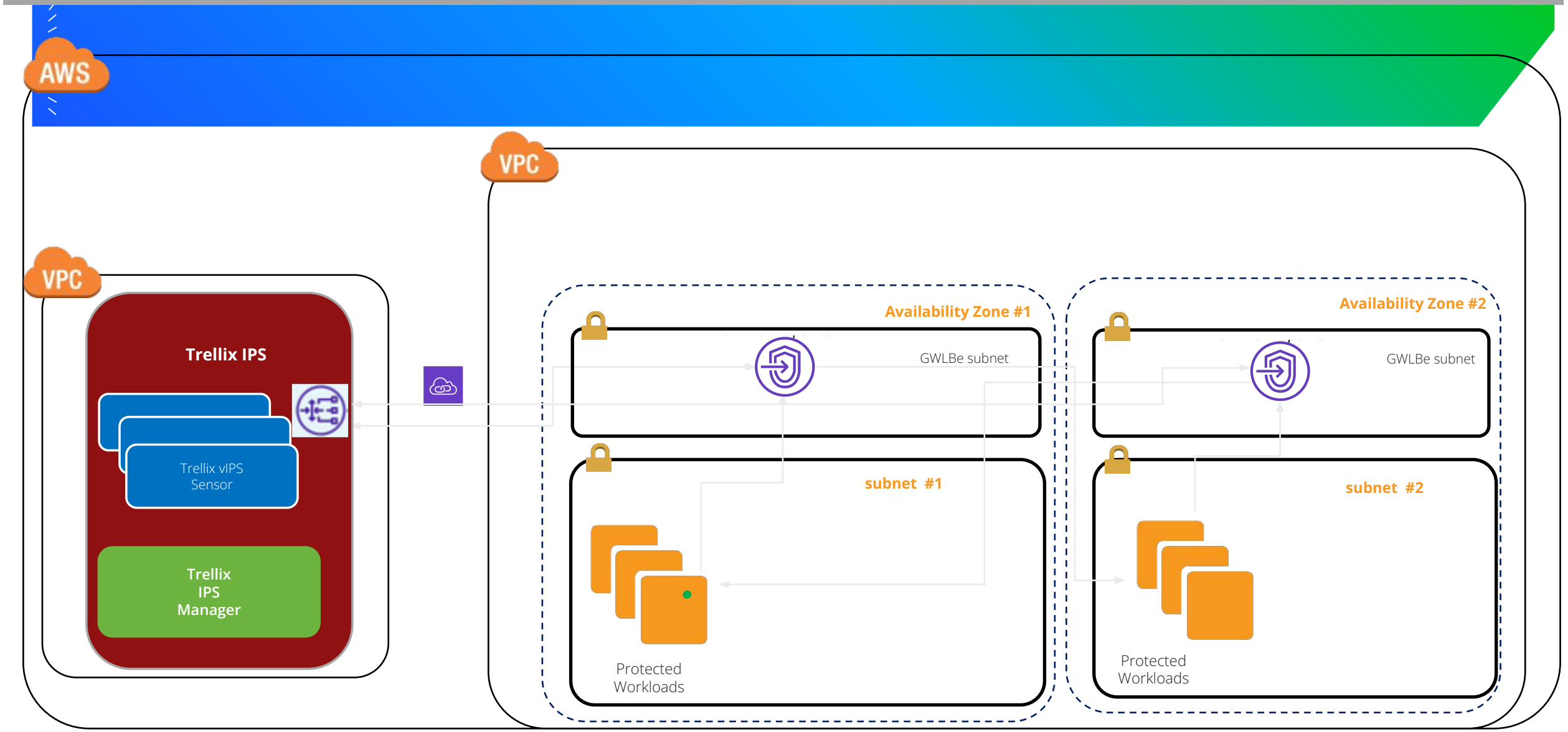
vIPS solution components (AWS as an example)



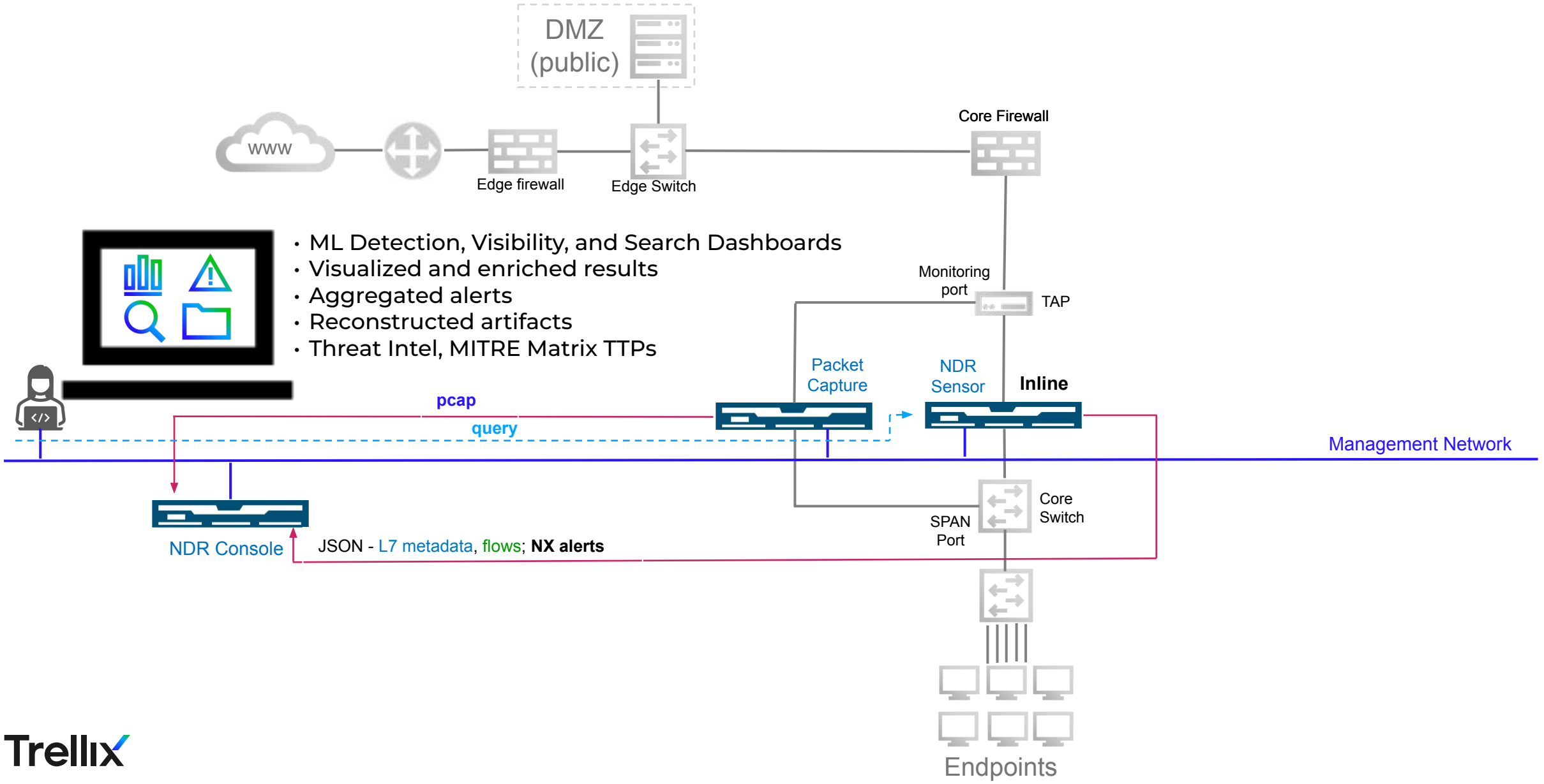
vIPS Protection for North-South Traffic



vIPS Protection for East-West traffic

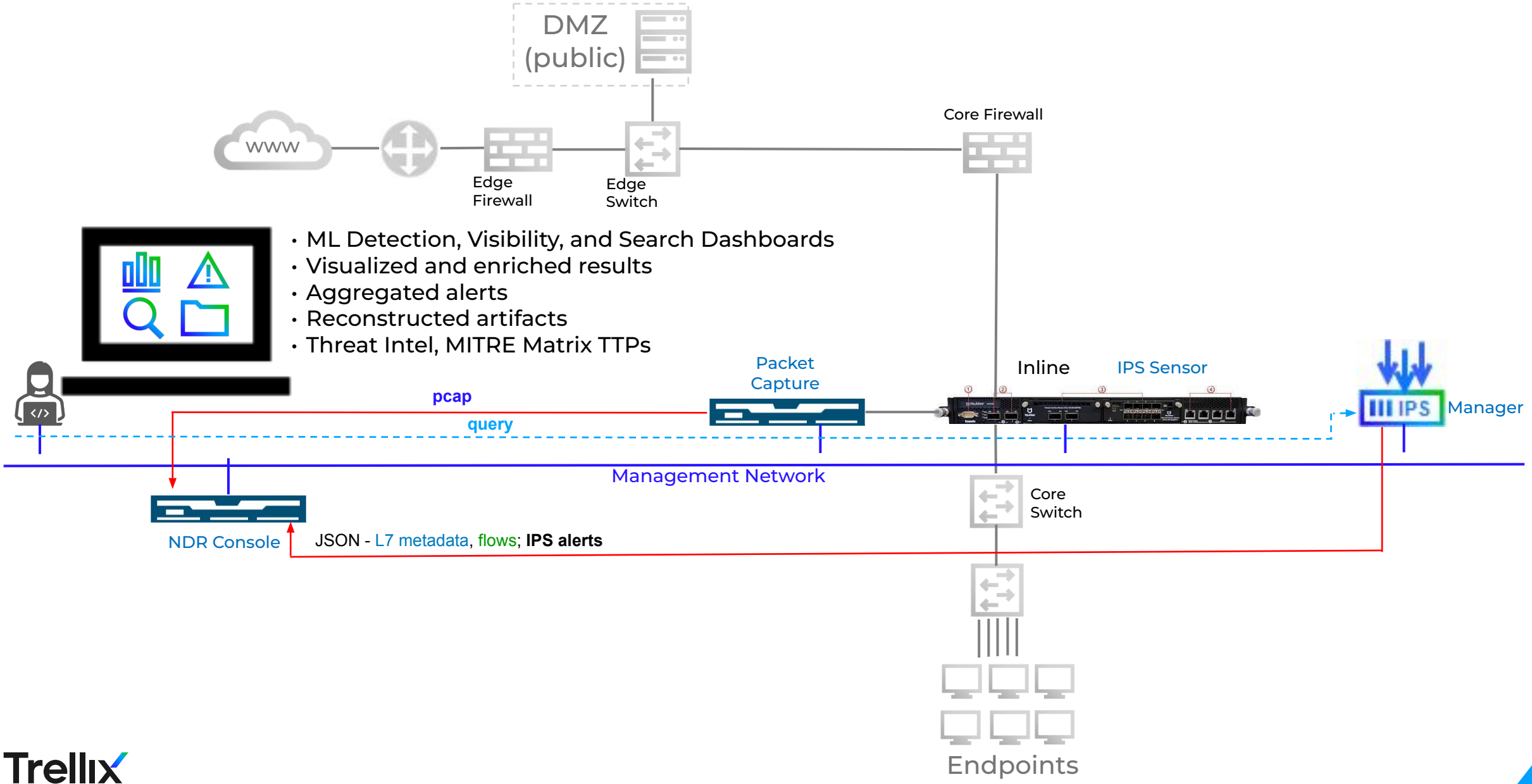


NDR Deployments: NDR Console, PX and NDR Sensor



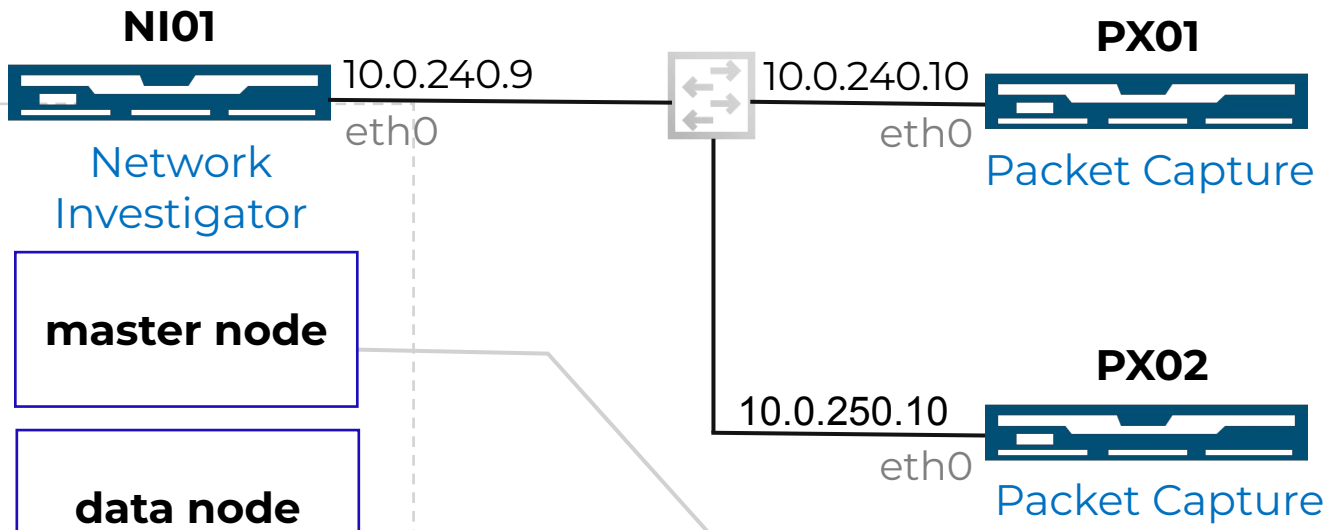
Trellix

NDR Deployments: NDR Console, PX and IPS



NDR Console Configuration: Standalone Deployment

A standalone (single-box cluster) contains two internal nodes with no other external NDR Console appliance as part of the cluster.



Stores metadata distributed by the connected *master node* and allows the metadata to be searched.

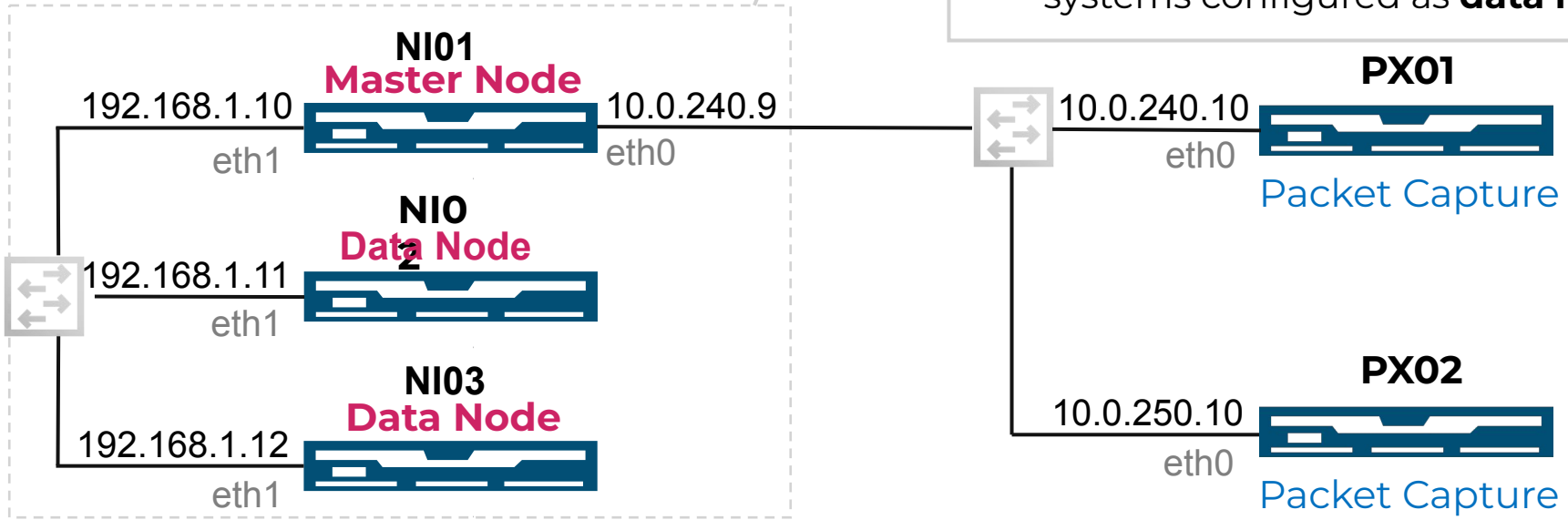
- Collects metadata from one or more connected Packet Capture systems
- Evenly distributes the data load between it and the other internal *data node*

Trellix

NDR Console Configurations: Multi-Box Cluster Deployment

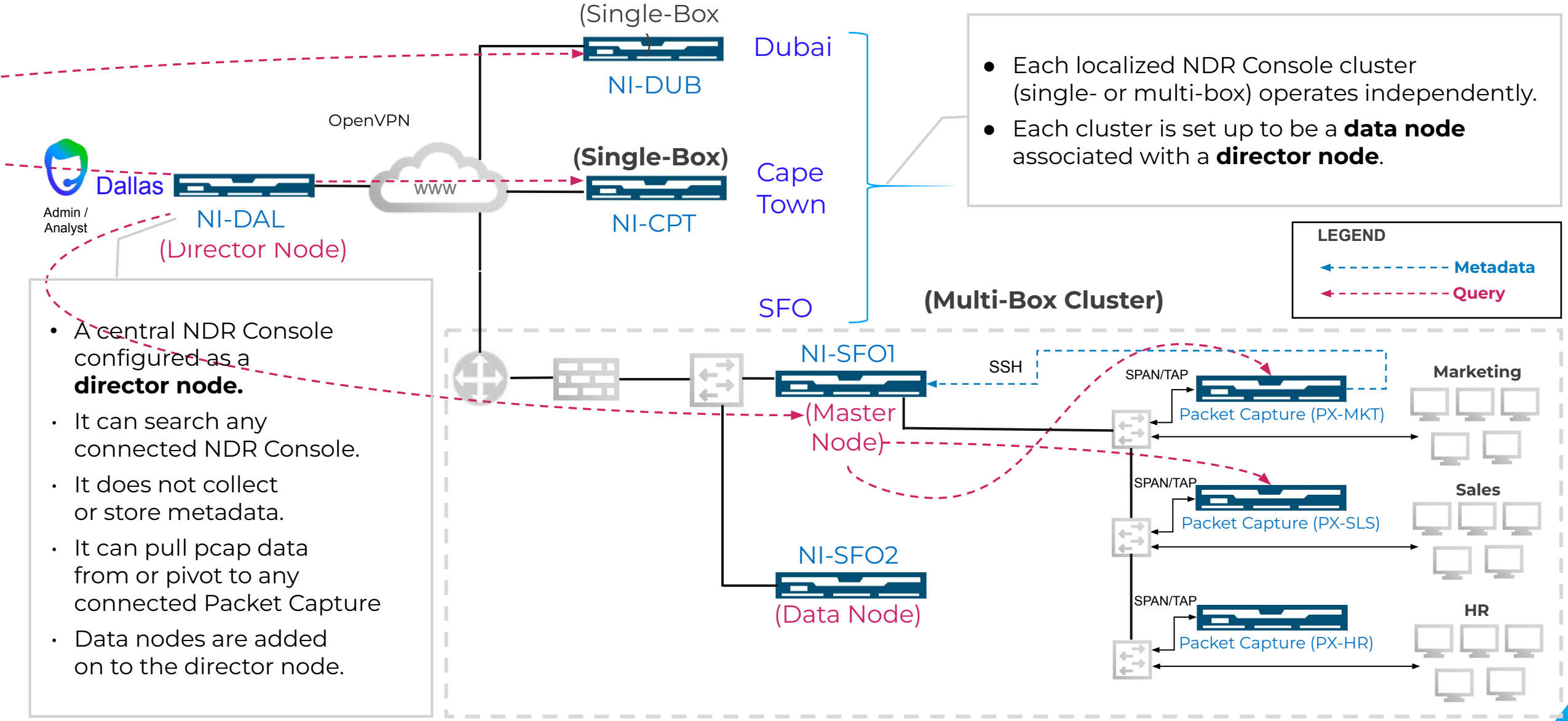
A single NDR Console appliance is configured as the master node, while additional NDR Console appliances act as data nodes in a multi-box cluster.

- A multi-box cluster significantly increases storage and search capacity
- One **master node** connects to one or more Packet Capture systems
- Clustered with one or more Network Investigator systems configured as **data nodes** only



Trellix

NDR Console Configurations: Distributed Search Deployment



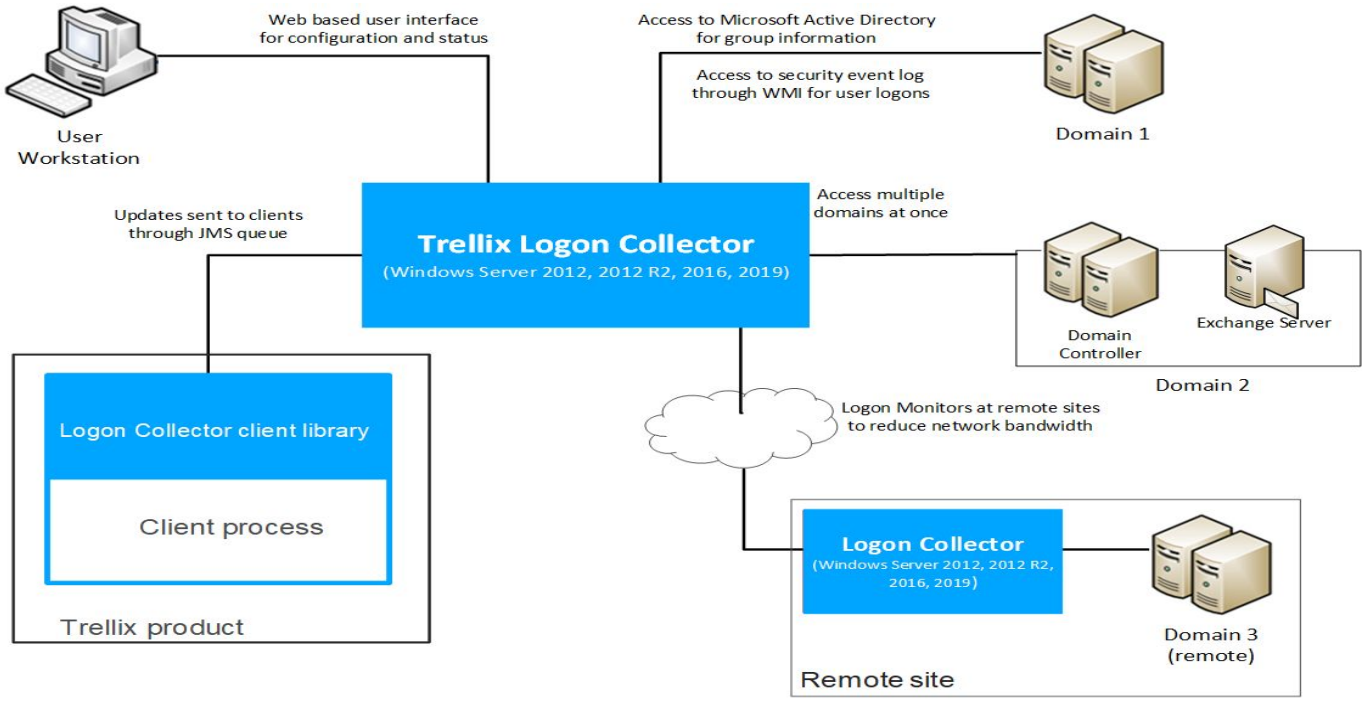
- Each localized NDR Console cluster (single- or multi-box) operates independently.
- Each cluster is set up to be a **data node** associated with a **director node**.

- A central NDR Console configured as a **director node.**
- It can search any connected NDR Console.
- It does not collect or store metadata.
- It can pull pcap data from or pivot to any connected Packet Capture
- Data nodes are added on to the director node.

Trellix

Trellix Logon Collector (TLC) Integration

- User and hostname details are essential for improving contextual understanding of security incidents
- Layer7 metadata and netflow events from downstream security devices usually lack user and hostname information
- TLC connects to Domain controllers to monitor user logon events
- Integration enables Network Investigator to associate user and hostname information for IP addresses
- Network Investigator enriches security events, Layer7 metadata events and netflow events with user and hostname information
- Assets page in Web UI has a separate section listing all active users in the network



Tenable Security Integration

Feature highlights

- NDR **enriches alerts** and **asset details** with **vulnerability scan findings** from **Tenable Security Center**.
- **Tenable vulnerability scores** are integrated with **NDR's network activity analysis** for **holistic asset risk assessment**.
- **Assets** with **high network risk** and **significant vulnerabilities** are identified for **prioritized investigation**.

Customer Value

This integration enhances risk visibility by combining network threat data with Tenable vulnerability assessments, **enabling proactive risk mitigation.**

Competitive Relevance

This integration provides **superior contextual awareness**, going beyond basic network data by adding **vulnerability insights** for a richer security picture. It enables **deeper investigations**, correlating vulnerability data with network behavior, which many competitors lack.

Trellix

ePO Integration

Feature Highlights

- **NDR** enriches its **asset details** with **endpoint data** from **ePO On-Prem**, providing details such as **operating systems, installed products, and agent status**, for a broader context.
- Enables **analysts** to initiate **endpoint containment actions** directly in **ePO On-Prem** from the **NDR interface**, speeding up **response to threats**.
- **Correlates network-based detections** with **ePO's endpoint data**, offering a **unified view of assets** and their **security posture**.

Customer Value

- Allows analysts to quickly **identify, understand, and contain compromised endpoints** by leveraging **ePO actions** directly from **NDR**.

Competitive Relevance

- Showcases **strong integration capabilities** with existing **Trellix solutions**, enhancing value for customers using **ePO**.
- Provides **superior endpoint control capabilities** directly from the **NDR platform**, which gives an edge over less integrated **competitive offerings**.

Trellix

Splunk Integration

Feature Highlights

- NDR Console forwards **enriched metadata and alert data** to **Splunk** for centralized logging and analysis.
- Allows **Splunk users** to correlate **NDR detections** with **other security data** within their **Splunk environment**.
- Enables **custom dashboards and reporting** in **Splunk** based on **NDR data**.

Customer Value

- Allows customers to leverage **existing Splunk investments** fully by adding **NDR's network detection data**.

Competitive Relevance

- Robust integration with Splunk caters to a broad customer base that relies on it as a central SIEM..

Trellix

SIEM Integration

Feature Highlights

- **NDR** forwards **rich, detailed logs** including **alerts, metadata, and context** to the SIEM platform for centralized analysis.
- Enables **SIEM users** to **correlate NDR data** with **other security events** from diverse sources within the SIEM environment.

Customer Value

- It allows for **cross-correlation of NDR insights** with other security data, enriching the **threat detection** capabilities of the SIEM.
- This enables customers to maximize their **SIEM investment** by adding **detailed NDR visibility** to their existing analysis workflows.

Competitive Relevance

- Provides **enhanced threat detection and response** by complementing the SIEM's logs with **rich NDR data** for deeper insights.
- Grants **customer flexibility** by allowing them to analyze **NDR data** within their pre-existing security ecosystem, offering a significant advantage over less open integrations.

Trellix

Trellix

NDR Roadmap

Duration - 20 Minutes

NX Evolution

Advanced Threat point product to NDR solution

ATD Point Product

- Dynamic File Analysis
- Multi-flow Attack Detection
- Multi-engine ATD Detection
- Lateral Movement (Smart Vision)
- IDPS detection

Same Great Sensor Only Better

NDR Solution

- More detections (ML & AI)
- Cross sensor correlations
- AI-driven investigations
- Risk-based prioritization
- Automated response

+

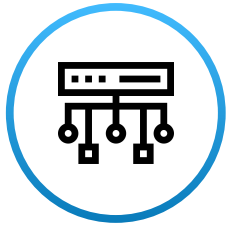
- Dynamic file analysis
- Multi-flow attack detection
- Multi-engine ATD detection
- SmartVision lateral movement

Trellix

Network Detection & Response Roadmap

DONE

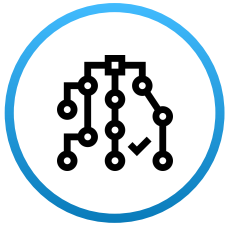
NDR v4.0



Asset discovery, risk profiling, encrypted traffic analysis, DNS anomalies, DGA and credential steal.

DONE

Attack Path Discovery



Integration with Trellix Endpoint and vulnerability tools/data for risk identification and reduction.

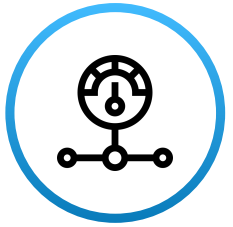
Q4'25

NDR v4.1

Extended control to ICS/OT environments, hyperautomation, user anomalies engine, and cloud workloads.

H1'26

Next-Gen NDR Sensor



Consolidated NDR sensor for active control with SSL, 60 Gbps per sensor, stacking to 300 Gbps.

Simplified Integrations | Hybrid Operations | Data Federation

Trellix

NDR Outcome & Feature Roadmap

- GREEN - Scoped & WIP
- BLUE - Partially Done
- ORANGE - Scoped
- BLACK - To be Scoped

Phase	Q3 2024	Q2 2025 (April)			
Analyst Experience - DFIR Workbench	**Outcome : Enable users to bring down the time to understand, derive context and respond to threats quickly, leveraging GenAI**				
	• Actionable insights & summaries with Trellix Wise • Improved alert summarisation • Interactive MITRE ATT&CK dashboard • Analyst Springboard	• Risky Conversations • Risky Assets • Top Alerts • Asset Details • MITRE / Asset OS / Geo widgets	• Asset List • Alert List • User List • Alert Details	• Selective Packet capture • Alert Acknowledgment	
Detection & Analytics	**Outcome : Reduce time and effort users spend analyzing event data throughout the different stages of its life cycle.**				

	• Passive Asset Discovery
	• DNS tunnelling
	• DGA
	• Reputation detection (GTI/DTI):
	  ○ Malicious URLs
	  ○ Malicious IP
	  ○ Malicious Domain
		• Risk Based Aggregation Part 1 (Sensor, User Defined Criticality Focus)
		• SSL Anomalies (Expired, Weak Cipher, Self Signed)
			• Tor Activity
			• Traffic similar to (not same) as known Malicious traffic
			• Risk Based Aggregation Part 2 (Plugin Focus)
				• ICMP Tunnel
				• Lateral Movement
				• Successful Phish (Phishing Exfil) / Credential Steal
					• Scanning Activity
					• Integration of Network sensor alerts
					•Communication with Newly Registered Domain

NDR Sensor & NDR Forensics	**Outcome : Provide customers with increased network visibility with an NDR sensor optimised with traffic profiles for the traffic segment achieving 100 Gbps**				
	• vNX Sensor (8.5 Gbps) - ESXi • NDR Sensor HW - 20 Gbps • Traffic Profiles (E/W, N/S) • Security Content/DTI Integration	• Metadata Generation • NDR Sensor HW - 30 Gbps Inspection Mode • Virtual NDR Sensor - 10 Gbps - ESXi, KVM	• Alma Linux • OS Fingerprinting • Selective Packet Capture		
Integrations & Ecosystem	**Outcome : Expand organisation's security posture by sharing security events across their networks and assets through integrations**				
	• MS Active Directory • Trellix Logon Collector	• Asset Enrichment (Tenable Security Center) • Notifications (SIEMs, Splunk)	• Attack Path Discovery	• Asset Enrichment and Containment Tasking (ePO On-prem)	• Trellix Hyperautomation for NDR
Platform, Management & Monitoring	**Outcome : Enable proactive product support**	**Outcome : Reduce the total-cost-of-ownership (TCO) of the NDR module by optimizing performance** **Outcome : Improve product experience through user behaviour analysis**			
	• Health and Detection Telemetry • Data Lake - Elastic • Federated Search [Elastic]	• Pendo (User experience analysis) • Entitlement & Licensing Module (NDR Packages)	• Sensor - Registration & Activation	• NDR Module Performance	

NDR Outcome & Feature Roadmap

Phase	Q4 2025	Q1+ 2026	
Analyst Experience - DFIR Workbench	**Outcome : Enable users to bring down the time to understand, derive context and respond to threats quickly, leveraging GenAI**		
	• Hyperautomation • Alert Details, Recommended mitigation actions • Alert Policy Exception • Safe Suricata Rule Builder	• Retrospective Analysis (90 Days) • Captured packet Analysis • User alert feedback (Thumbs Up / Down)	• Asset details - Severity of conversation • Asset details - Trellix Insights •MITRE D3FEND knowledge-graph • Compliance Value reporting
Detection & Analytics	**Outcome : Reduce time and effort users spend analyzing event data throughout the different stages of its lifecycle**		
	• Domain Controller Attacks/Anomalies ○ Golden Ticket ○ Silver Ticket ○ DC Shadow ○ DC Sync ○ Kerberoasting • DNS Anomalies ○ Rebinding ○ Poisoning ○ Hijacking ○ TypoSquatting ○ FastFlux • Malicious use of RMM ○ RDP ○ NetSupport ○ Teamviewer + 30+	• User Anomaly ○ Improbable Travel time ○ Login from UnManaged device ○ Login from UnUsual Host ○ Password Guessing ○ Password Spray ○ Distributed Password Spray ○ SuccessFul Password Guess	•HTTP Anomalies •HTTP Tunneling •VPN Anomalies •Communication with Unusual Location •Traffic Pattern Anomalies •Exploit Correlated OS and patch level • User Visibility Enhancements • Cloud Visibility Enhancements • Endpoint Visibility Enhancements • User Community Anomaly • Asset Community Anomaly
NDR Sensor & NDR Forensics	**Outcome : Provide customers with increased network visibility with an NDR sensor optimised with traffic profiles for the traffic segment achieving 100 Gbps**		
	• Qualify new NDR Sensors (Virtual & HW) • IPv6 Compatibility • Cloud NDR Sensor -10Gbps (AWS/Azure/GCP)	• New Gen High-end HW model • Virtual NDR Sensor - 10 Gbps - Hyper - V • vNDR sensor perf improvements - ESXi, KVM	• HW Enhancements - SAS ports for full pcap storage - Replaceable components - Switch based architecture - All in one appliance
Integrations & Ecosystem	**Outcome : Expand organisation's security posture by sharing security events across their networks and assets through integrations**		
	• Native Response Tasking (Palo Alto FW, Cisco FW, CheckPoint, Forti) • IoT/ICS Ingestion (Nozomi Guardian) • Qualys, Rapid7 • SIEM and EDR (Crowdstrike, Chronicle, SentinelOne)	• Asset Enrichment and Containment Tasking (MS Defender) • Asset Enrichment (Rapid7) • Palo Alto NGFW	• Asset Enrichment and Containment Tasking (SentinelOne) • ZTNA Ingestion (Zscaler ZPA, ZIA) • WIZ Cloud risk visibility and virtual patching
Platform, Management & Monitoring	**Outcome : Improve operational excellence**		
	• NDR Module Performance • Migrate Phase 4.0 Pages to React.js	• Beachhead • New Hardware - Console • NDR Console Base Platform •Console RBAC & User Management	• User audit trail • Value Reporting • Multi Factor Authentication (MFA) • Titan Dashboard

Trellix

Time for a Break !

Duration - 30 Minutes

Trellix

NDR Demonstration

Duration - 40 Minutes

Trellix

NDR Licensing

Duration - 10 Minutes

NDR Packages

Essentials

Threat Monitoring

New Alert UI for NX customers

- NDR Console Licence
- Analyst Workspace
- IVX for Network Traffic
- Detections, threat intel, blocking, etc. capabilities as per NX
- Trellix Wise Essentials
- Virtual NDR Console
- 5 Virtual NDR Sensors
- 2 Virtual Central Manager

Upgrade from NX SKUs

Core

Detect, Investigate, Respond

Full NDR

- NDR Console Licence
- NDR Sensor Licenses per Appliance
- Trellix Wise Core
- Trellix Insights Freemium
- Threat Intelligence
- Threat / ML/AI Anomaly Detections
- Asset Discovery
- Hyperautomation
  - Trellix Response Actions

Enterprise

Advanced Detection, Deep Investigation

Core, Plus

- Trellix Wise Enterprise
- Trellix Insights
- IVX Manual API Submission
- Attack Path Discovery
- Hyperautomation for NDR (SOAR)
- Full NDR Forensics
- 5 Additional Virtual NDR Sensors

NDR Packages - Future

IOT/ICS NDR Addon

Nozomi Guardian

- IoT/ICS Asset Visibility & Threat Detections

Requires NDR Core or NDR Enterprise

IVX Enterprise NDR Addon

- Manual File Analysis
- File Protect

Trellix

NDR Trellix Wise (AI)

NDR Essentials

- 100 Requests per Month
- Available Requests:
  - Summarize this alert
  - MITRE findings

NDR Core

- 100 Requests per Month
- Available Requests:
  - Summarize this alert
  - MITRE findings
  - Remediation steps
  - Knowledge graph

NDR Enterprise

- 1000 Requests per Month
- Available Requests:
  - Summarize this alert
  - Top affected entities
  - MITRE findings
  - Remediation steps
  - Knowledge graph
  - Sequence diagram

Trellix

NDR Packages (Breakdown by feature, Page 1)

	NDR Essentials	NDR Core	NDR Enterprise
NDR Console	✅	✅	✅
NDR Sensors	✅5 Virtual Appliances	✅ 5 Virtual Appliances	✅ 10 Virtual Appliances
Analyst Workbench	✅	✅	✅
NDR Detections & Correlations	❌[1]	✅	✅
Threat Intelligence (DTI)	✅[1]	✅	✅
IVX for NDR	✅[2]	✅[2]	✅[2]
IVX (API Submission)	❌	❌	✅[3]
IVX (File / Manual Submission)	❌	with IVX Enterprise Addon	✅
SSL Traffic Decryption	✅	✅	✅
Active Sensor (inline blocking)	✅	✅	✅
Asset Discovery	❌	✅	✅
Attack Path Discovery	❌	❌	✅
Trellix Response Actions	❌	✅	✅
IoT/ICS Detections	❌	with IoT/ICS Addon	with IoT/ICS Addon
3rd Party Integration (Ingestion and Enrichment)	❌	✅	✅

Trellix

1 Only NDR console detections are not available. Detections, threat intel, blocking, etc. capabilities as per NX or IPS are available.
2 Integrated with NDR Sensor or additional IVX Enterprise appliance purchase or CloudMVX
3 Available on separate IVX Enterprise appliance

NDR Packages (Breakdown by feature, Page 2)

	NDR Essentials	NDR Core	NDR Enterprise
Hyperautomation for NDR[1]	❌	Workflow automation with Trellix Products	✅
Trellix Insights[1]	Freemium	Freemium	✅
Trellix Wise	Freemium [Summation / MITRE]	Freemium [Summation / MITRE / Knowledge Graph / Remediation Steps]	✅
Netflow Session Reconstruction	❌	✅	✅
Retroactive Analysis - Behavioural [1]	❌	❌	✅
Retroactive Analysis - DPI [1]	❌	❌	✅
Event Based Packet Capture [1]	❌	✅	✅
Selective Packet Capture	❌	✅	✅
Continuous Full-Packet Capture	❌	with Forensics (PX) NDR Addon	✅
Full-Session Reconstruction	❌	with Forensics (PX) NDR Addon	✅
CMS (Management)	❌	✅ 2 Virtual CMS	✅ 2 Virtual CMS

Trellix

1 Roadmap

Upgrade Path for Existing Clients

Customer Owns ⇩	I want to Upsell or Cross Sell		
	NDR Essentials	**NDR Core**	**NDR Enterprise**
NX	Available for purchase	Available for purchase	Available for purchase
PX	Not available for purchase	1. Available for purchase. 2. Only NDR Core subscription is included for detections, visibility and response capabilities. 3. Forensics subscription is still separate. 4. Need to associate the IAs from existing PX Hermes or Classic deployments to NDR subscription for the IA to get NDR core license and feature functionality.	1. Available for purchase. 2. Forensics subscription is included 3. Need to associate PX and IA appliances to the NDR Enterprise subscription for the new licenses.
IPS	Not available for purchase	1. Available for purchase. 2. Please reach out to PM team to include the IPS license as part of the NDR Core subscription. 3. IPS doesn't have all NDR Sensor features, customer may require to deploy additional NDR sensors depending on the use-case.	1. Available for purchase. 2. Please reach out to PM team to include the IPS license as part of the NDR Enterprise subscription. 3. IPS doesn't have all NDR Sensor features, customer may require to deploy additional NDR sensors depending on the use-case.

Trellix

Trellix

NDR Differentiators

Duration - 20 Minutes

Vendor_zZ

Or Zz?

- They only analyzes metadata without capturing full packets. Trellix advantage: Supports complete L2-L7 packet capture and inspection Impact on security: Comprehensive forensics and threat investigation capabilities.
- They have no SSL/TLS decryption capabilities, only analyzes encrypted traffic metadata. Trellix advantage: Supports both in-line and out-of-band SSL/TLS decryption Critical difference: Ability to inspect encrypted traffic content vs. just metadata
- They leverage unsupervised learning can generate higher false positives. Trellix advantage: Advanced machine learning models with contextual analysis Key difference: Precision in threat detection vs. purely behavioral analysis.
- They rely solely on behavioral analysis without DPI. Trellix advantage: Combines DPI with advanced behavioral analysis Impact: More comprehensive threat detection and analysis

Trellix

Vendor_Xx

Or xX?

- Their platform requires integration with third-party security tools like firewalls or SOAR platforms to implement blocking actions. Trellix offers built-in blocking: Our platform provides native Intrusion Prevention System (IPS) with immediate threat mitigation capabilities Direct response actions: Trellix can automatically isolate compromised devices and block malicious IPs without requiring additional integrations.

- Their scope is limited: Focuses primarily on network protocol analysis with support for about 70 enterprise protocols. Trellix's broader coverage: Our platform combines network, endpoint, and multi-vector threat intelligence for comprehensive protection Advanced analytics: We utilize machine learning and behavioral analytics across multiple security domains

- They rely primarily on protocol analysis and behavioral detection based on network traffic patterns. Trellix's advantage: Uses advanced machine learning and behavioral analytics across multiple security domains Enhanced detection capabilities: Our platform can identify sophisticated threats that may not be visible through network analysis alone

- They're focused solely on network detection and response (NDR). Trellix's advantage: Provides an integrated security platform covering network, endpoint, and cloud security Unified management: Single console for managing multiple security functions vs. multiple point solutions

Trellix

Vendor Yy

Or yY?

- detection-only solution, no prevention, no containment, no enforcement. It relies entirely on third-party systems (SOAR, firewalls, etc.) to take action. Trellix includes native prevention through IPS, sandboxing, and behavioral blocking.
- sees only network telemetry. Trellix platfomize network, endpoint, email, and cloud telemetry into a unified detection surface — with correlated alerts and incident views across domains.
- Offers good detection starting point, but real-world tuning is required for efficacy. Customers often describe “a sea of logs” without guided prioritization. Trellix offers pre-built, context-rich detections and threat scoring out of the box
- provides network logs, but no malware sandboxing or full-packet retrospective forensics. Trellix offers deep inspection of suspicious files with MVX and retains packet-level data with PX.
- Alerts lack enrichment or correlation, forcing analysts to manually investigate each signal across disconnected tools and surfaces.
- no native mechanism to correlate activities across stages of an attack

Trellix

Vendor Aa

Or aA?

- Their platform requires integration with third-party tools like firewalls and SOAR platforms to implement blocking actions
- No native SSL/TLS decryption capabilities, relies only on metadata analysis. Trellix's advantage: Full SSL/TLS decryption support for real-time inspection of encrypted traffic. Complete visibility: We can detect threats hidden in encrypted traffic that metadata analysis might miss
- Relies solely on metadata analysis without full packet capture capabilities. Trellix's advantage: Complete packet inspection and capture for comprehensive threat analysis. Enhanced forensics: Detailed packet-level data for thorough incident investigation
- Focuses primarily on behavioral analytics and metadata analysis. Trellix's advantage: Combines behavioral analysis with deep packet inspection and advanced ML detection. Multi-vector detection: Our platform identifies threats across multiple attack vectors

Trellix

Trellix NDR Differentiators

- In-line L2 deployment with blocking
- Full, deep packet inspection for hunting, investigations, and forensics
- Leverages IPS engine with detection and prevention mode
- On-prem sandboxing engine, faster detection and blocking, no data share with cloud
- Malware Callback detection and blocking
- Webshell & Beaconing Detection
- Uses statistical analytics, supervised and unsupervised machine learning
- SSL Inspection engine or use JA3 signatures
- SMB Detonation of files/objects
- Detection of fileless malware (i.e. Mimikatz)
- Extend visibility and automatically map discovered assets to device

Trellix

Trellix

Q & A

The final Leg

Trellix

Thank you for your TIME


Trellix