
Trellix
APJ Partner Summit'24
Partnering for a Secure Future
Join us at the APJ Partner Summit
Phuket, Thailand
10-12 JULY 2024

Trellix

Trellix NDR Solutions

APJ Partner Summit 2024

July 8, 2024

Speakers for Today

Ron Wang
Sr Director, APJ SE

Hidemitsu Sakurai
Sr Director, Japan SE

Manish Sinha
Director, India SE

Carl Thaw
Global Enablement

Trellix

Copyright © 2024 Musarubra US LLC. | All Rights Reserved - Trellix Confidential

What are the most common pain points your customers experience with traditional network security solutions?

Copyright © 2024 Musarubra US LLC. | All Rights Reserved - Trellix Confidential

Agenda

1) **Why the need for Trellix NDR solution?**
   Challenges it solves

2) **How does Trellix solve the problem?**
   How we are different

3) **About the Trellix solution**
   Overview & Demo

4) **Personas**
   Who to target

5) **Proof Points**
   Customer Case Study

6) **Product Packaging**
   Product SKUs

7) **Upsell and Cross-Sell**
   Positioning the solution to customers

Trellix

Copyright © 2024 Musarubra US LLC. | All Rights Reserved - Trellix Confidential

Trellix

Why Trellix NDR Solutions

The challenges

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

Required Capabilities to Solve It

Eliminate Blind Spot

Visualizing traffic patterns, covering various types of network traffic, discovering and classifying assets, extending the visibility

Disrupt attackers at each stage

Detecting unknown, hidden or stealth threats by utilizing a multi-layered approach that uses AI and threat intelligence alongside sandboxing

Speed investigation and response

Accelerate and streamline threat investigation and response by prioritizing alerts, correlating signals, and contextualizing impacts on the business/network

Trellix

But what if we dont change - status quo?

Increased security blind spots

increase of security blind spots as the IT team does not know where their network traffic is going.

Increased breaches / cyber attacks

Golden Opportunity for Hackers to spread their presence in the network to steal data or to breach sensitive systems

Lack of information for investigation

Unable to make a determination on the remediation action due to lack of information

Trellix

Trellix

How Trellix NDR Solves It

How we are different

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

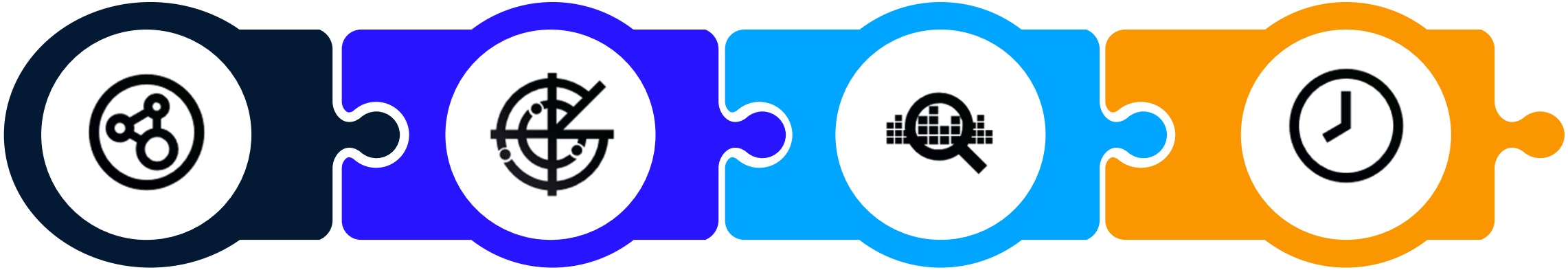
Speed investigation and response

- 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

Trellix NDR Reveals Hidden Threats



Networks have significant blind spots

Continuous analysis of alerts, netflow, and L7 metadata **reveals hidden threats**

Attackers move quickly along the cyber kill chain

Multi-layered detection aligned to MITRE ATT&CK framework **disrupts attackers at every stage**

Investigating a cyberattack is complex

Automated enrichment and guided workflows **accelerate investigations**

Mean Time to Remediate (MTTR) is critical

Remediate root causes to **reduce risk of future compromise**

Trellix

Visibility in Complex Networks

Blind spots are often identified during incident post-mortem

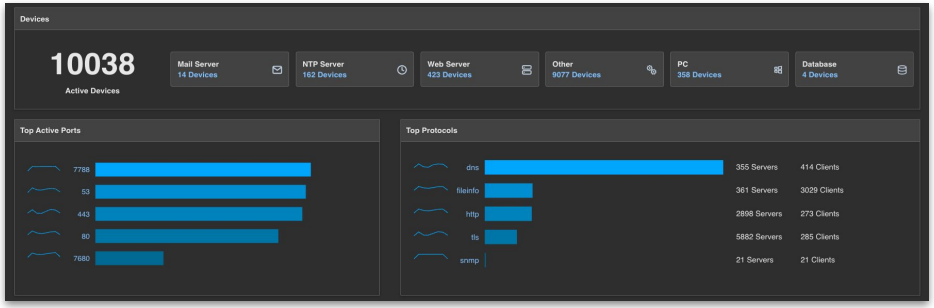
Digital transformation increases complexity and risk to secure network environments

Customers need visibility to secure:

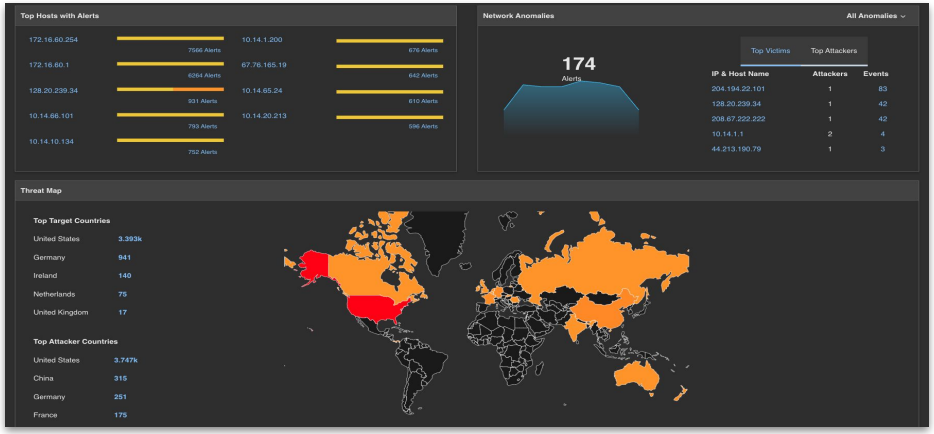
- On-prem, cloud, hybrid, and OT networks
- High-throughput data centers and user workplaces
- Network packet and app-layer visibility

Trellix NDR leverages existing investments and increases actionable visibility:

1. New capabilities like Asset Discovery



2. Intuitive dashboards for app layer visibility



Trellix

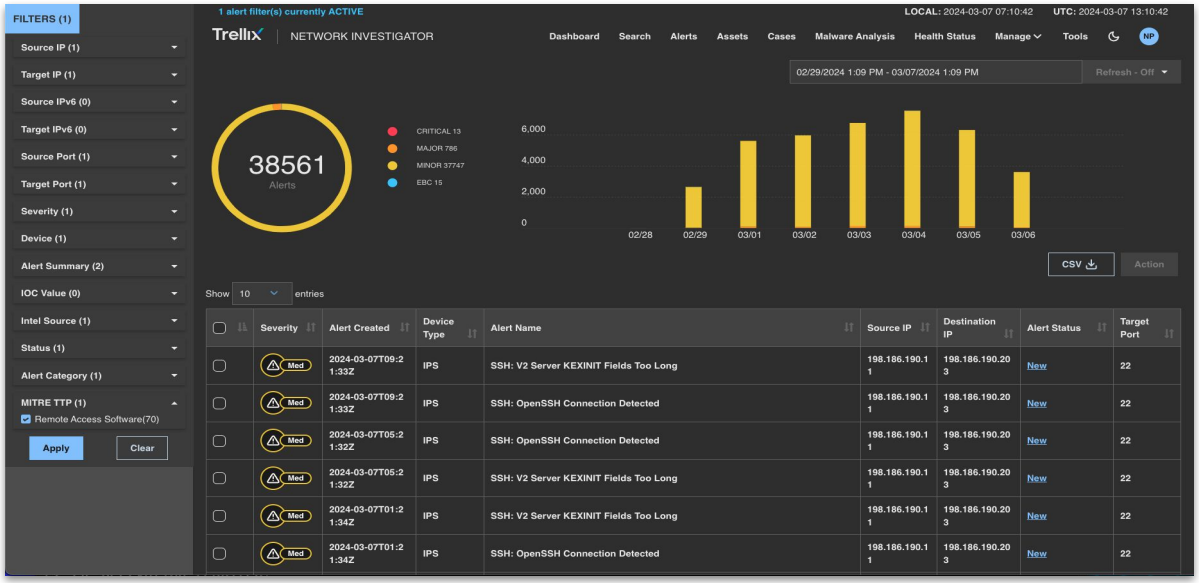
Sophisticated Attacks Evade Detection

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:



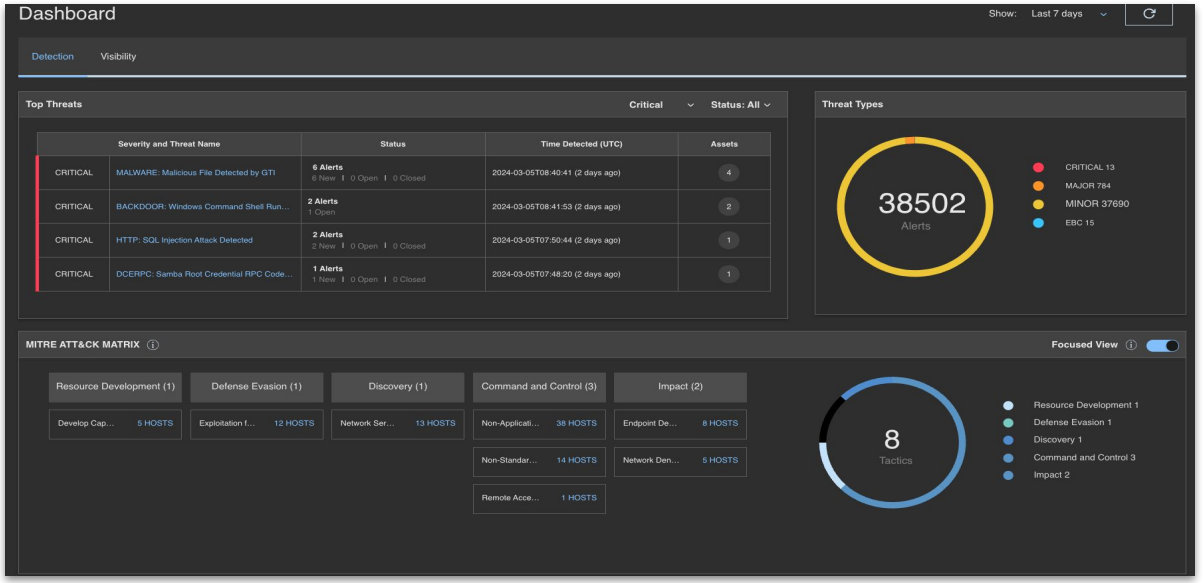
Trellix

Attack Mitigation Takes Too Long

Visibility and context help Security Operation Center (SOC) analysts respond quickly

Mitigation is dependent on the ability to quickly detect, contain, and remediate a threat *BEFORE* the business is disrupted.

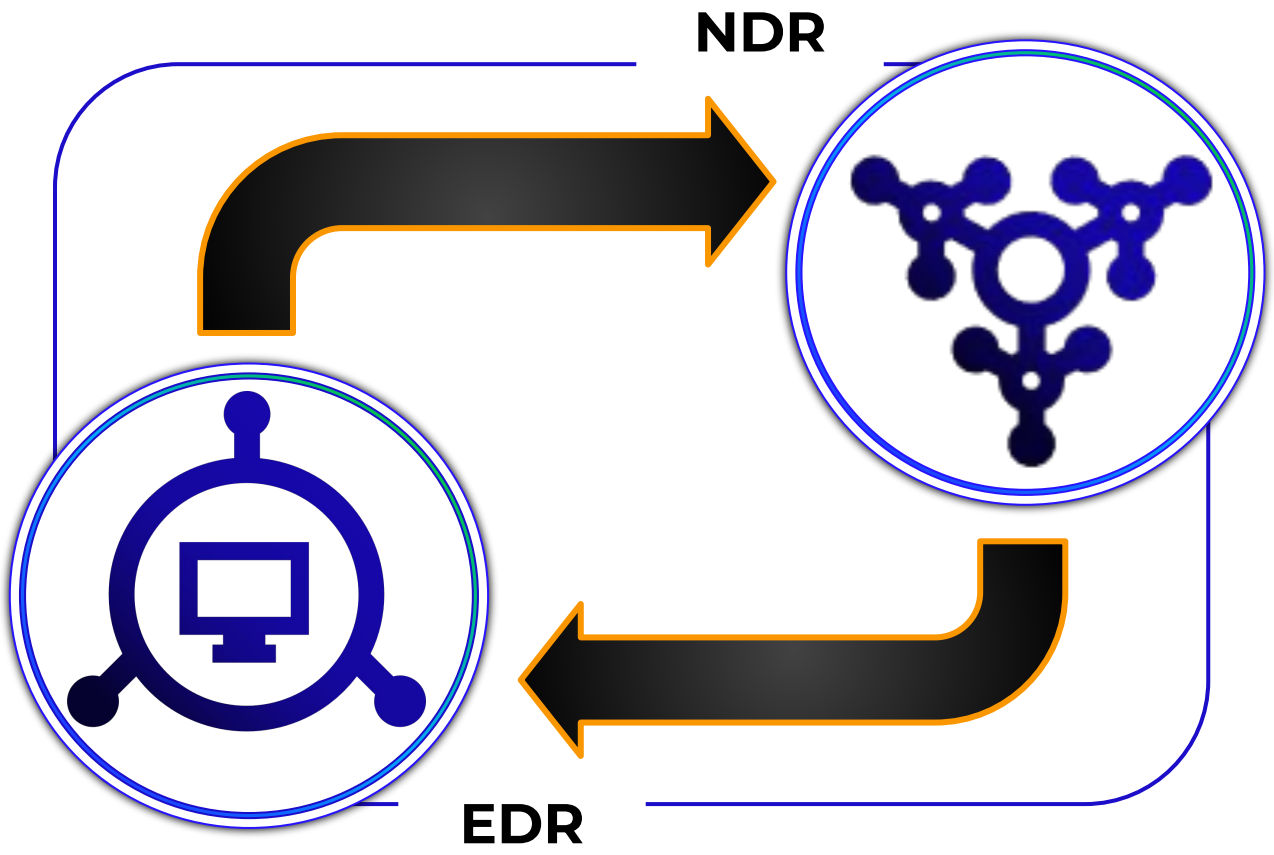
- Too many alerts cause alert fatigue, which leads to slower responses.
- Lack of context in network events slows down responses to disrupt an attack



Trellix NDR SOC workflows give analysts situational awareness and context needed for efficient investigations.

Trellix

The Perfect Complement to EDR



NDR enables and accelerates key SOC playbooks to:

- 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 exfil and reconstruct stolen material
- Respond to block ransomware and vulnerability exploitation

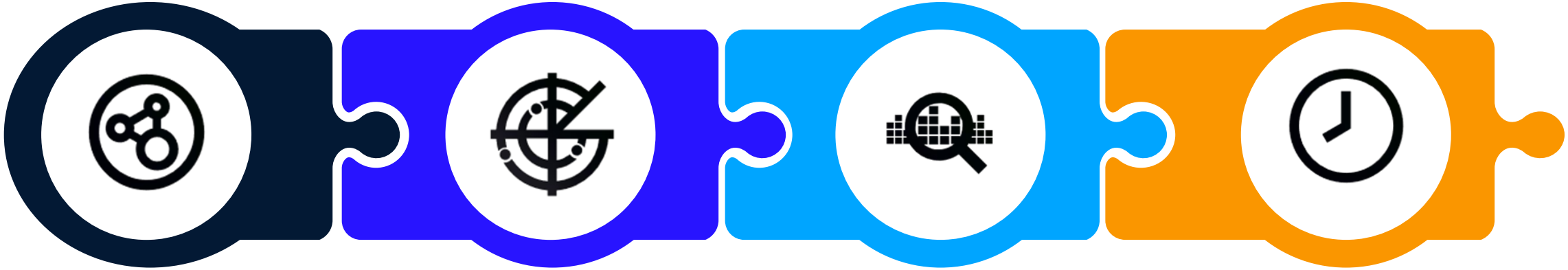
Trellix

Trellix

About Trellix NDR Solution

Overview and Demo

Trellix NDR Reveals Hidden Threats



Networks have significant blind spots

Continuous analysis of alerts, netflow, and L7 metadata **reveals hidden threats**

Attackers move quickly along the cyber kill chain

Multi-layered detection aligned to MITRE ATT&CK framework **disrupts attackers at every stage**

Investigating a cyberattack is complex

Automated enrichment and guided workflows **accelerate investigations**

Mean Time to Remediate (MTTR) is critical

Remediate root causes to **reduce risk of future compromise**

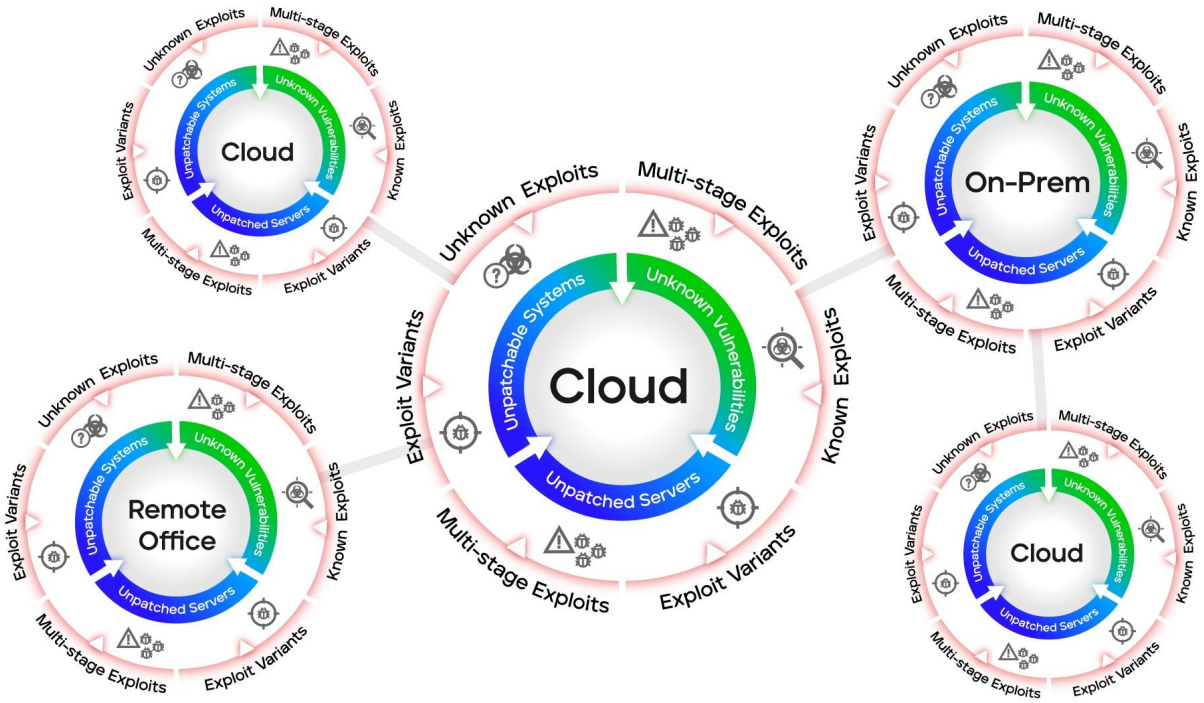
Trellix

Eliminate Blind Spots

Extended Security Visibility: Achieve unparalleled visibility across data centers, hybrid clouds, branch offices, and corporate campuses.

Comprehensive Coverage: Ensures monitoring of N/S (North/South) and E/W (East/West) network traffic, critical for detecting lateral movements and other sophisticated attack vectors.

Advanced Asset Discovery: Identifies and classifies assets within the network, facilitating a comprehensive understanding and management of network resources.



Seamlessly integrates with Trellix Network Security (IPS, NX, PX)

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

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

Multi-layered Detection

Combined techniques detect known, unknown, and emerging threats

Signature-less Detection
"Find unknown bad"
Executes suspected malicious code in a safe environment

- Web Shell Detections
- Server-Based Vulnerabilities
- URL-based Phishing Attacks (Cloud-Assisted)
- Malware Binaries Check (Cloud-Assisted)

Behavioral Analysis
"Reveal suspicious patterns"
Machine learning identifies characteristics similar with known bad behaviors

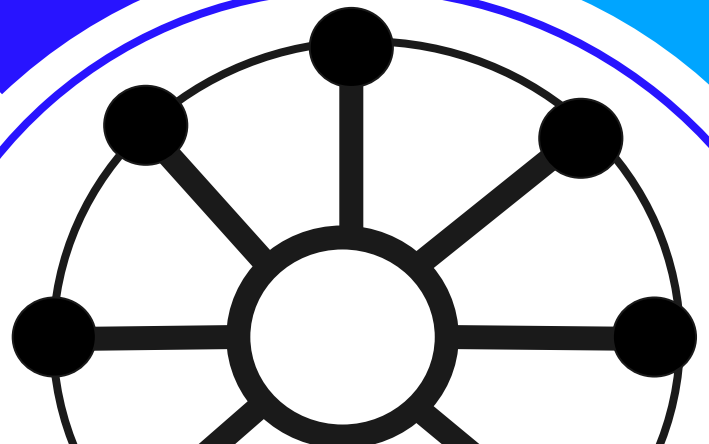
- Analytics Rules
- Lateral Movement
- Data Exfiltration
- Malicious C2 Communications

Signature-based Detection
"Find known bad"
High speed analysis at scale

- Proprietary / Custom Signatures (Snort, YARA)
- Static Network Rules / Blacklists

Traffic Analysis
"Visibility when perimeter protections fail"

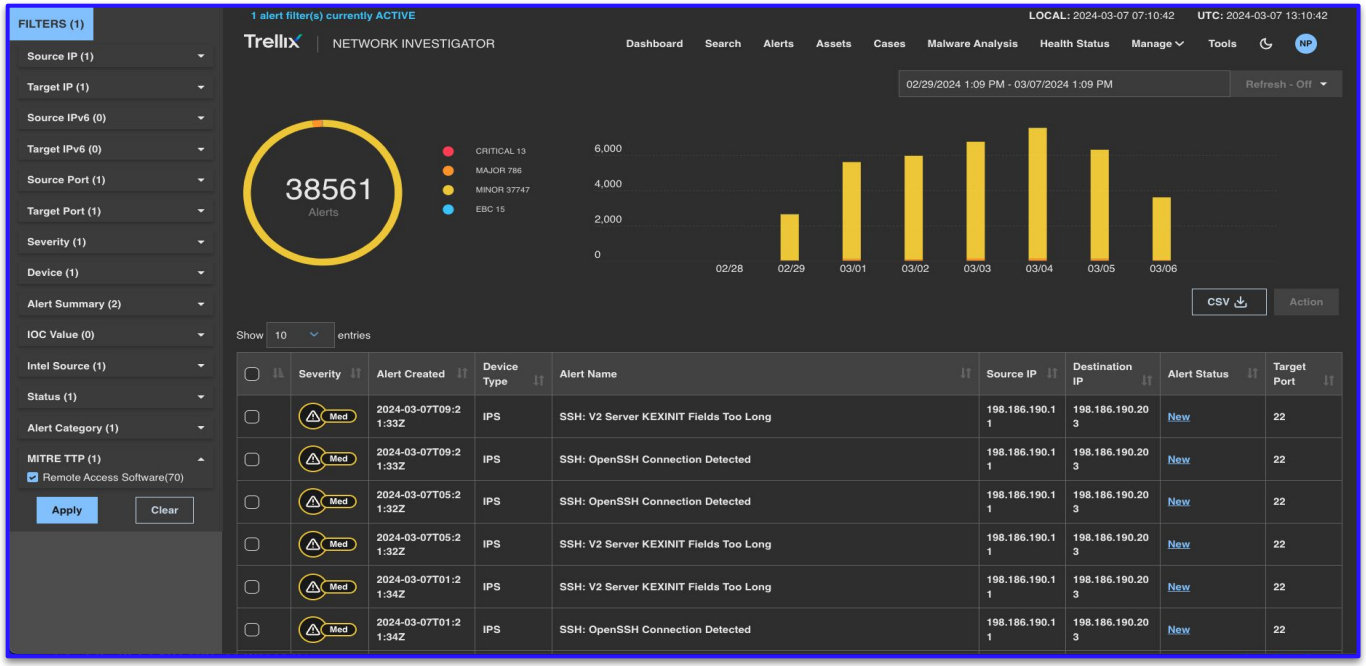
- Protocol Application and Visibility
- Metadata Generation
- Lateral Movement
- Full-packet capture



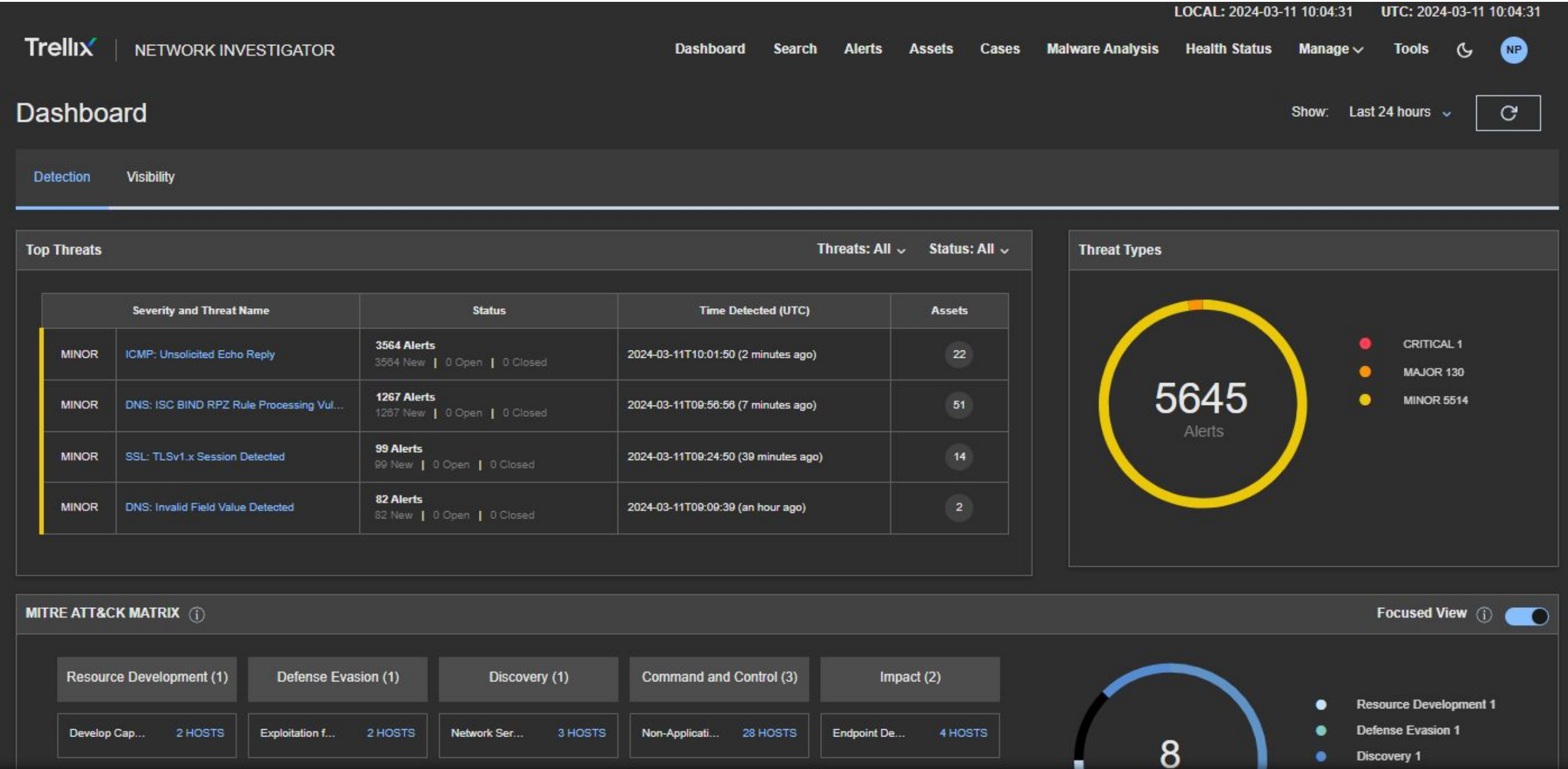
Trellix

Trellix Network Detection and Response

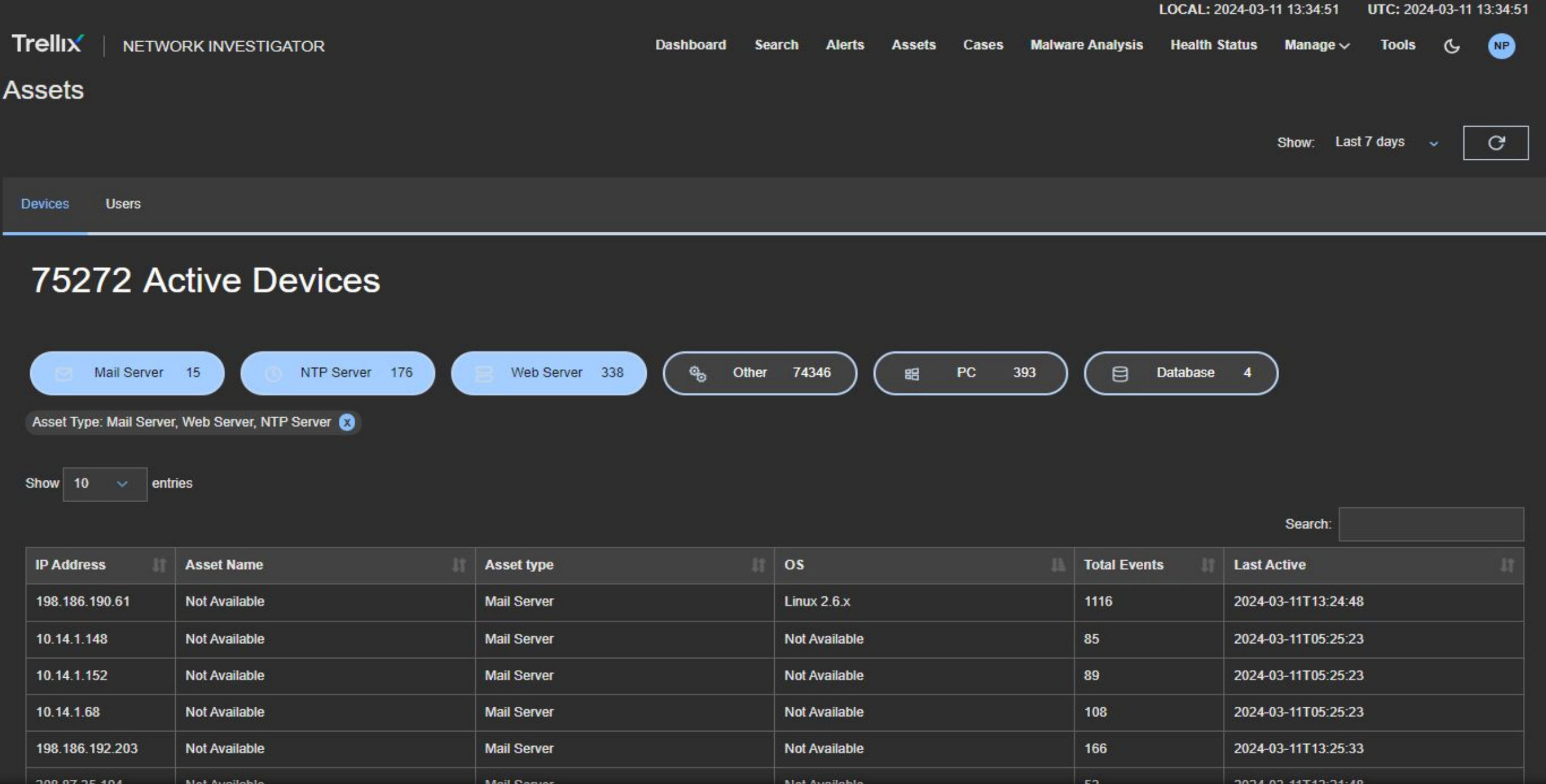
- Collects alerts, netflow and L7 metadata from NX, IPS, and PX
- Uses correlation and behaviour analysis across multiple sources
- Leverages advanced analytics and MITRE mapping for enrichment and prioritization
- Asset discovery
- Detection and visibility views
- Customizable dashboards
- Drill down to packet-level detail



Trellix



NDR Threat Reporting



NDR Threat Reporting

LOCAL: 2024-03-11 13:41:48 UTC: 2024-03-11 13:41:48

Trellix | NETWORK INVESTIGATOR

Dashboard Search Alerts Assets Cases Malware Analysis Health Status Manage Tools NP

10.14.1.200

Other

Show: Last 24 hours

Summary Asset Map Alerts

Host Details Tue, 05 Mar 2024 14:52:49 GMT

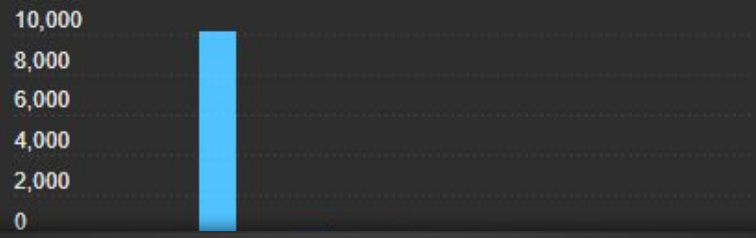
IP Address	10.14.1.200
Host Name	api-edruse.edruse.ccs-trellix.com
Op System	Not Available
MAC address	00:0C:29:E7:2D:74
Open Ports	52673,53,88,389,135,49669,445,123,57271,0
First seen	Tue, 05 Mar 2024 14:52:49 GMT
Last seen	Mon, 11 Mar 2024 13:40:59 GMT
Alerts	110287

What kind of traffic is on the asset?

0 B
External Traffic

1.12 MB
Internal Traffic

Traffic Distribution by Protocol

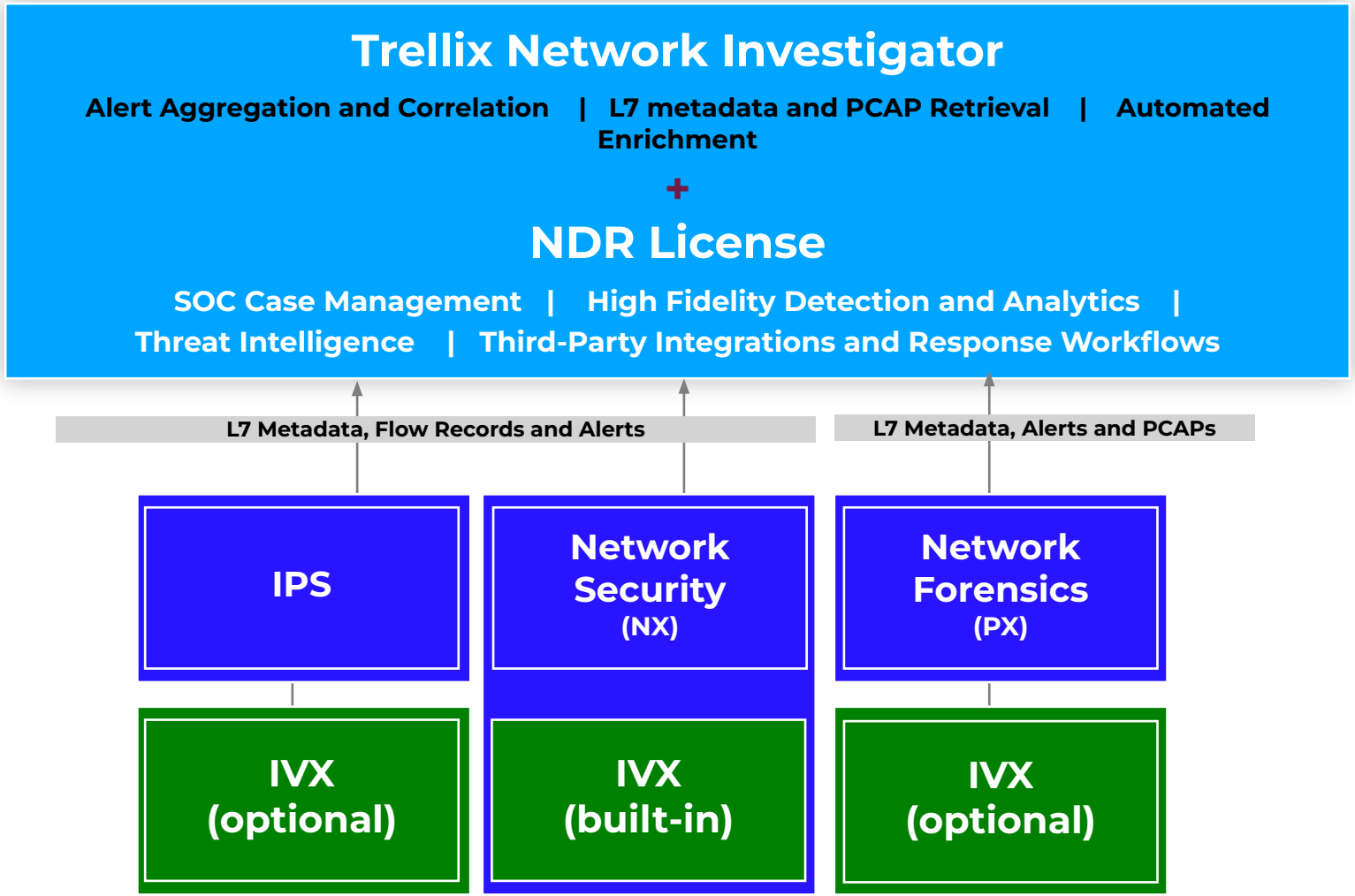


What kind of alerts are on the asset?

NDR Threat Reporting

NDR Solution Architecture

NDR adds value to existing IPS, NX, and PX Deployments



SOC focused workflows for investigation and response

Intuitive visualization of network telemetry

Enrichment and analytics for **higher fidelity** alerting

More context through **correlation** of **multiple data sources**

Improved Security posture with forensic understanding of **scope** and **root cause of incidents**

Trellix

Trellix NDR

Multi-layered visibility, detection, investigation and response

- ✔ Delivers security visibility across the extended enterprise
- ✔ Detects, prevents and prioritizes high impact threat incidents
- ✔ Speeds investigations with high fidelity detections and alert enrichment
- ✔ Adapts to the constantly evolving threat landscape
- ✔ Improves the security operations program by reducing noise and risk
- ✔ Elevates the value of existing Trellix network security investment

Trellix NDR detects threats and helps defenders investigate and respond to threats across the cyber kill chain.

Trellix

DEMO

Trellix

Trellix

Personas

Who to target

Chief Information Officer (CIO)

Economic Decision Maker

"How do I leverage technology to transform the business, while securing infrastructure and assets from external threats?"

Success Metrics:

- Reducing risk (financial, compliance, reputation, brand)
- Ensuring ongoing compliance with industry mandates and regulations
- Perceived as a business enabler
- Doing more with less

Key Responsibilities:

- Keeping the business running, making sure systems are always available, and ensuring solution design and deployment are correctly implemented
- Planning and aligning IT initiatives with business strategy; exploiting digital technology to transform the business, and improving environments
- Securing infrastructure and assets from external threats while ensuring the best possible user experience for all
- Managing IT budget to control cost and improve efficiency, *"I'm constantly looking for new more cost-effective solutions"*
- Evolving the role of technology, helping to implement agile business processes and digital transformation that integrate with legacy systems
- Communicating with the board and satisfying their expectations in terms of IT security and business strategy

Before Scenario:

- Struggle to adapt legacy infrastructure to evolving business initiatives.
- Unable to meet operational metrics and targets

Positive Business Outcomes:

- Add measurable impact to the business
- Valued for enabling business transformation and expansion
- Ability to do more with limited resources

Negative Consequences:

- Business perceived organization as creating friction rather than being a key partner / enabler
- Budget overruns and frustrated staff
- Failed audits
- Never really sure the organization is safe
- Negative impact to customers, employees, brand and professional reputation

Key Influencers:

- Chief Information Security Officer
- Security Architect
- VP, Global IT Infrastructure
- Director, Security Operations
- Security Architect

Chief Information Security Officer

Economic and Technical Decision Maker

"I want to support as many partner digital touch points as possible, without risking loss of our mutual trust due to an incident."

Success Metrics:

- Help grow the business without taking on unnecessary cyber risks.
- Effectiveness of inspection (false negatives; false positives; alert fatigue)

Key Responsibilities:

- Deliver meaningful value to the business by balancing technology innovation **with security posture**
- Protect intellectual property and customer data; identify key risks and share mitigation strategies with stakeholders
- Maintain an overall security strategy and roadmap; overseeing development and compliance with security mandates
- Ensure teams have the right skills, technology and tools while maintaining cost efficient operations
- Communicate security risks and impact to the board; influence crisis communications if major breach occurs

Before Scenario:

- With more stakeholders participating in the value chain, the attack surface has expanded.
- Network complexity prevents end-to-end network visibility; I can't protect what I can't see
- Attackers lay in wait on the endpoint

Positive Business Outcomes:

- Support business agility without fear of increasing cyber risk
- Early, hi-fidelity, detection eases burden on the SOC.

Negative Consequences:

- Malware dwell time increases if malware isn't detected as early as possible.
- Decline in revenues, loss of partner and customer trust, loss of IP, brand impersonation.
- Sanctioned tools are too slow, unwieldy due to security interventions so users use shadow IT to 'get stuff done'

Key Influencers:

- Board of Directors
- C-Suite
- Security Architect
- Director, Security Operations
- VP, Global IT Infrastructure

"How do I ensure I have needed visibility to detect and respond to incidents in my network environments before they cause business impact?"

Success Metrics:

- Complete visibility
- Minimize incidents
- Pass audits
- No impact to network throughput/availability

Security Architect (Office of the CISO)

Technical Influencer

Key Responsibilities:

- Design infrastructure needed to achieve strategic security goals within budget
- Maximize network visibility, minimize blind spots, address coverage gaps
- Conduct assessments of security architecture identify vulnerabilities, assess security risk, and develop design and mitigation strategies
- Satisfy compliance mandates and address audit failures

Before Scenario:

- Unknown blind spots and gaps in coverage
- Legacy-siloed security solutions limit effectiveness
- Existing network solutions miss suspicious activity. COMPLEXITY
- SOC teams complain about generic alerts
- Failed audits due to gaps in coverage

Positive Business Outcomes:

- Confidence about needed depth of network visibility.
- Efficient SOCs mitigate incident impact with actionable alerts.
- No performance complaints from network teams.
- Audits passed without issues

Negative Consequences:

- Breaches occur due to blind spots
- Missed alerts due to lack of context
- Decrease in SOC productivity

Key Influencers:

- SOC Manager/Director
- Threat hunting, Incident Response, and Pen Testing teams
- Network Operations

Security Operations Director

Technical Influencer

"How do I ensure my teams have the tools they need to detect and respond to network threats efficiently and effectively?"

Success Metrics:

- Meet SLAs and KPIs (e.g. MTTD/MTTI/MTTR)
- Minimize incidents
- Operationalize security teams and solutions

Key Responsibilities:

- Operationally effective usage of security solution
- Incident Response Metrics: MTD/MTI/MTR
- Minimize impact to business through security incidents or security tools

Before Scenario:

- Lack coverage and blind spots
- Inefficient alert triage
- Non-actionable alerts, missing context
- Inefficient investigations and more reactive firefighting
- Existing tools impact performance

Positive Business Outcomes:

- More actionable alerts, faster investigations
- Better situational awareness for scope of network to be protected
- Less impact from incidents
- Minimized business impact due to finding breaches sooner
- Situational awareness for scope of network to be protected

Negative Consequences:

- Breaches occur due to blind spots
- Missed alerts due to lack of context
- High impact due breaches / incidents
- Alert fatigue, staff burnout turnover

Key Influencers:

- Chief Information Security Officer
- SOC Analysts
- Incident Response team

Buying Committee

CISO / Sec Architect are the key targets

- **Initiates finding a solution**
- ***Owns about* 60% of the buying decision**

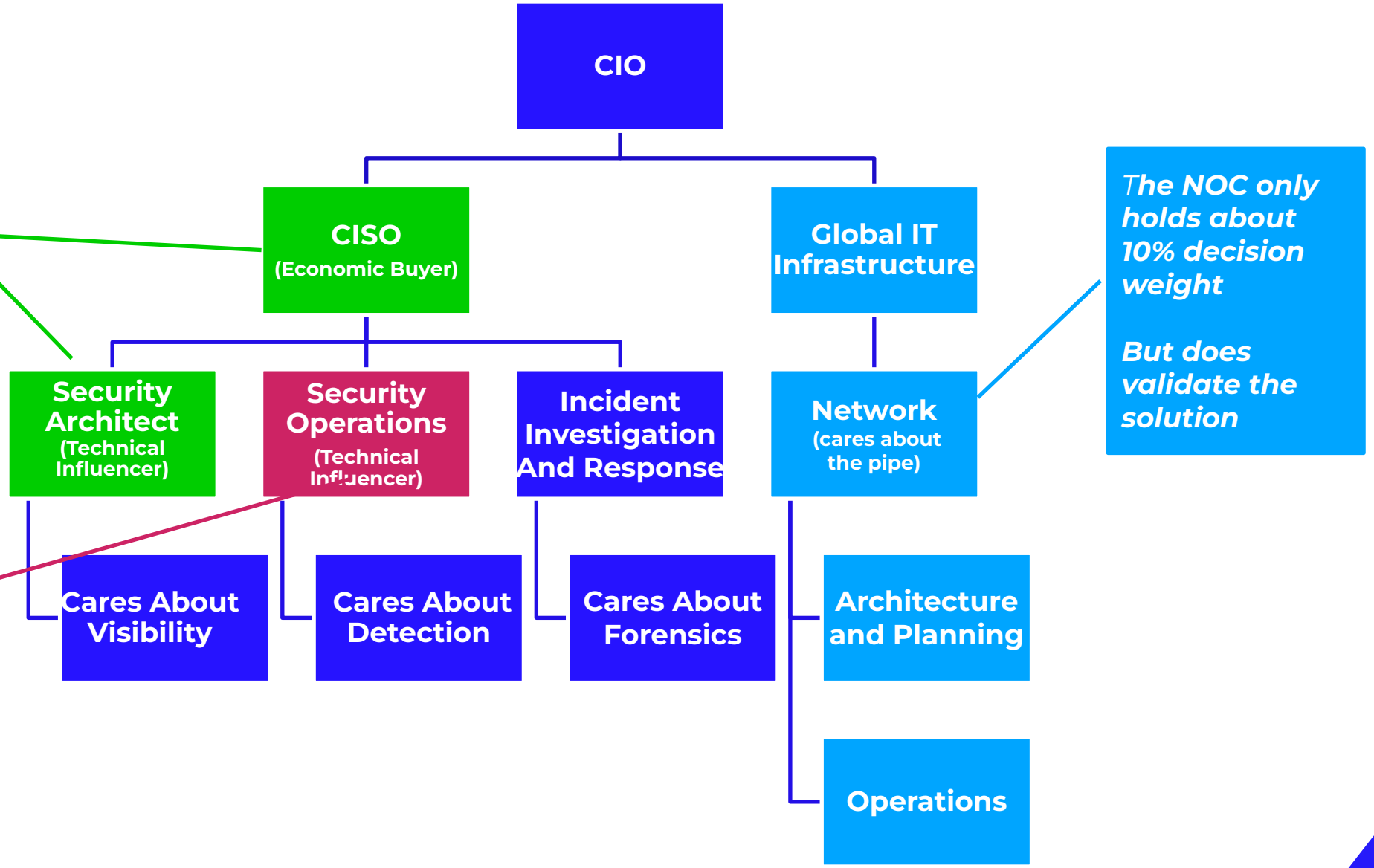
Pains

- **Sec Arch initiates, worries about incomplete visibility**
- **Knows what they're missing / viz gaps**

SOC Director 30%

- **May point out need but does not hold budget**
- ***Owns about* 30% of the buying decision**

- **Wants NDR**
- **Validates the solution**
- **Will value high-fidelity alert story**



The NOC only holds about 10% decision weight

But does validate the solution

Pain Points & Discovery Questions

Pain Points	Discovery Questions
Network security blind spots	• How do you currently identify security blind spots in your network? • Do you feel like your current network security tools provide complete visibility? • How do you track unknown or unmanaged assets on your network? • How do you manage Internet of Things (IoT) security in your network? • Do you monitor east / west traffic within a network segment for threats? • How do you know if there are endpoints vulnerable to sophisticated threats? • Do you have visibility into outbound network traffic?

Trellix

Pain Points & Discovery Questions

Pain Points	Discovery Questions
Sophisticated threats continue undetected	• How do you detect multi-stage attack campaigns? • Can you identify lateral movement within your network? • How do you defend against zero-day exploits? • How do you detect anomalies in network behavior? • How do you operationalize your threat intelligence within network sensors? • How do you manage the evolving attack surface? • Where do you have gaps in detection for example against MITRE ATT&CK framework?

Trellix

Pain Points & Discovery Questions

Pain Points	Discovery Questions
SOC inefficiencies	• How much time does your Tier-1 SOC team spend determining if an alert is a false positive or a detection requiring attention? • Do you struggle with the speed of threat detection? • What percentage of alerts goes unacknowledged? • How do security analysts understand the extent of an attack? • What additional tools do security analysts use to get more context for alerts? • What's your approach to threat hunting? • How do you remediate and make sure it does not happen again? • How do you detect attacker use of legitimate system admin tools?

Trellix

Trellix

Proof Points

Customer Case Studies

Customer Story 1 - US Federal Agency

Improving threat detection and investigation across multiple threat vectors

Industry: **Public Sector**

Trellix Products:
Existing; HX, CMS, and EX
Added: NX, PX/NI, and IVX
Future: NDR

CHALLENGES

- Meet EO 14028 requirements for investigation and response
- Build centralized investigation - CSIRT team required to investigate across threat vectors
- Correlation and investigation lacking at the network layer

SOLUTIONS

- Existing: Trellix HX, EX, and CMS products heavily used and optimized for investigation
- Added: Trellix NX, PX/NI and IVX for improved network threat detection, investigation, and forensics
- Future: NDR for comprehensive and integrated network visibility, detection, and investigation

RESULTS

- Improve network threat detection and telemetry correlation
- Time savings from alert enrichment and SOC-focused workflows
- Deep visibility and threat intelligence for investigation and hunting across the network

Customer Story 2 - US Armed Forces

"Trellix® Network Security with SmartVision™, had the best performance based on the criteria of the challenge, which focused on artificial intelligence (AI) and machine learning (ML) technologies that detect adversarial campaigns by monitoring network observable behaviors or by analysis of data collected across an enterprise."
— NAVWAR AI-ATAC CHALLENGE 2 Results

Industry:	**U.S. Dept. of Defense (DoD)**
Trellix Products:	**Trellix NDR (Trellix NX, PX, NI, IVX, and CM)**

CHALLENGES

- Maintaining advanced network detection and visibility on ashore + afloat, disconnected environments
- Multi-vendor solution requires integration and partnership
- Lack of unified visibility into the cyber posture of the DOD and ability to respond and recover

SOLUTIONS

Trellix NDR (Trellix NX, PX, NI, IVX, and CM)

Trellix Platform connects multiple Trellix technologies and other tools to support a seamless SecOps user experience

Trellix NDR platform covers numerous use-cases (IDS/IPS sensor node, PCAP, and L7 metadata, lateral movement, network sandbox, data exfil, beaconing, callback detection, web infection)

RESULTS

Trellix NX awarded First Place in AI-ATAC Challenge

Trellix solutions proposed for unified DOD sensor grid and user interface for the next 10 years across 300+sites

Open and extensible platform with flexible deployment options afloat and ashore

Trellix

Customer Story 3 - Global Financial Provider

Increase visibility in a global hybrid environment

Industry: **Financial**

Trellix Products: Trellix ENS, Data Loss Prevention (DLP), ePolicy Orchestrator (ePO), NX, ETP

CHALLENGES

- Increased blind spots as more workloads are moved to the cloud
- Too many egress points create a challenge with analyzing logs to identify suspicious activity.
- East/West traffic visibility is a challenge when misconfigured FW rules allow potential malicious traffic

SOLUTIONS

With Trellix Network Security, NX can be deployed in AWS by using native integrations with AWS gateway load balancing and other egress points to gain visibility

Trellix NX can be deployed in the user segments for E/W visibility using advanced detection techniques for lateral movement, suspicious call back traffic, and exfiltration

Trellix NDR is the central point to correlate these events and telemetry for enhanced visibility and response workflows

RESULTS

Increased awareness of suspicious traffic in the cloud and traditional on-premises networks

Reduce the noise with advance ML/AI models to detect suspicious E/W traffic.

Increased visibility with NDR with a centralized point for correlating our network alerts and telemetry

Trellix

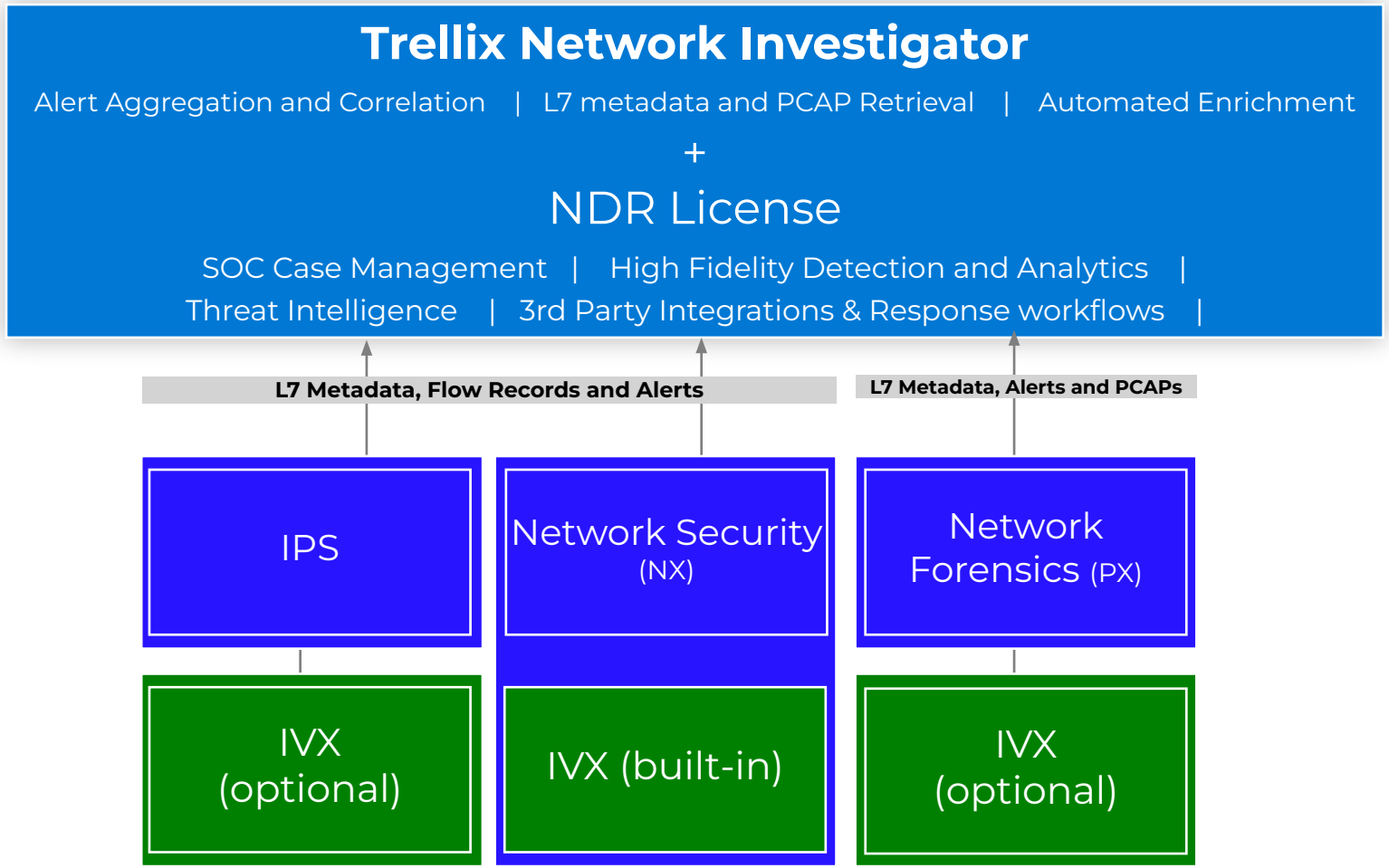
Trellix

Product Packaging

What SKUs

NDR Solution Architecture

NDR adds value to existing IPS, NX, and PX deployments



SOC focused workflows for investigation and response

Intuitive visualization of network telemetry

Enrichment and analytics for **higher fidelity** alerting

More context through **correlation** of **multiple data sources**

Improved Security posture with forensic understanding of **scope** and **root cause of incidents**

Network Portfolio Review

	Trellix Intrusion Prevention System (IPS)	Trellix Network Security (NX)	Trellix Packet Capture (PX)
Primary Function	**Server / Datacenter workloads** **High-throughput traffic**	**User Devices,** **Web and SMB traffic**	**Visibility for Forensics,** **Compliance**
Scalability	100 Gbps (200 Gbps planned)	20 Gbps	40 Gbps
Security Capability	**Deep packet inspection:** Exploit protection / virtual patching, advanced malware engines, DoS / DDoS, deep-file inspection, C&C, reputation, and L7 visibility	**Advanced Threat Detection:** Lateral movement, web infections, callbacks, beaconing, data exfiltration, basic IPS, L7 visibility	**Full packet capture:** Lossless packet capture, Session decoder, indexing and fast search
Zero-Day Suspicious File Detonation	Integration with IVX	On-box or via IVX for clustering	Integration with IVX
Deployment Options	Physical, Virtual, Public and Private Cloud, Integrations with AWS Load Balancer		

Trellix

Upsell and Cross-Sell

How to position to customers

Cross-sell Paths to NDR

Secure the base and help customers with network security maturity journey

IPS

- Improved detection (beaconing, data exfil)
- Improved UI for SOC Workflows
- Asset Discovery

NX

- Improved UI for SOC Workflows
- Asset Discovery

EDR / Email

- Unify network and endpoint / email detection
- Improved SOC Workflows
- Asset Discovery

NDR

- SOC Workflow Optimization
- Intuitive, actionable Visualizations
- Alert Aggregation and Correlation
- Automated Enrichment
- Asset Discovery
- Intelligent VIrtual Execution (IVX)

Trellix

Trellix NDR for NX Customers

Target Customers:

- Current NX customers looking for NDR to increase actionable visibility and control beyond core protection
- Trellix NX customer that also have Trellix EDR or email

Customer Benefits:

Get more value from existing Trellix NX by aggregating network telemetry from multiple sensor types to better enrich and correlate telemetry from NX with other sources like Trellix IPS and PX to provide deeper and more actionable detections in a centralized console to more effectively monitor and respond to incidents before they cause damage

Solution	Value Messaging	Customer Positive Outcomes and Benefits	Discovery Questions
NDR	Gain deeper and more actionable visibility and detection in a centralized console to more effectively monitor and respond to threats	• **Eliminate blind spots:** Intuitive dashboards and visualizations deliver comprehensive situational awareness, along with asset discovery to provide security visibility of network connected devices • **Disrupt Attackers:** achieve rapid and accurate threat detection across the extended network with multi-layered detection including advanced threat detection engines, powerful analytics and machine learning algorithms • **Accelerate Investigation and response:** bring to the foreground the most critical threats enabling analysts to triage alerts and respond faster and more efficiently	• What additional tools do security analysts use to get more context for alerts? • How do security analysts understand the extent of an attack? • How do security analysts detect lateral movement when attackers pivot and expand further into the network; what tools do you use for that additional visibility? • How do you quickly scope an incident?
EDR	Unify endpoint and network detection for comprehensive security coverage	Enhance threat detection and response capabilities by leveraging NDR with EDR to, achieve tighter security coverage and significantly reducing the risk of breaches across endpoints and network	How do you pivot from an endpoint alert to determine attacker activity across the network?
Email	Enhance threat detection across email and network for optimal protection	Bolsters protection against sophisticated threats, ensuring a robust security posture with improved detection and response capabilities across both network and email vectors	How do you currently detect and respond to email-based alerts by leveraging network telemetry for compromised hosts?


Trellix