Trellix

Elevating Network Security

With NDR

Owen Edwards
Director, Network Product Management

November 10, 2023

Your Network Is Under Siege

Complex Networks vulnerable to attacks

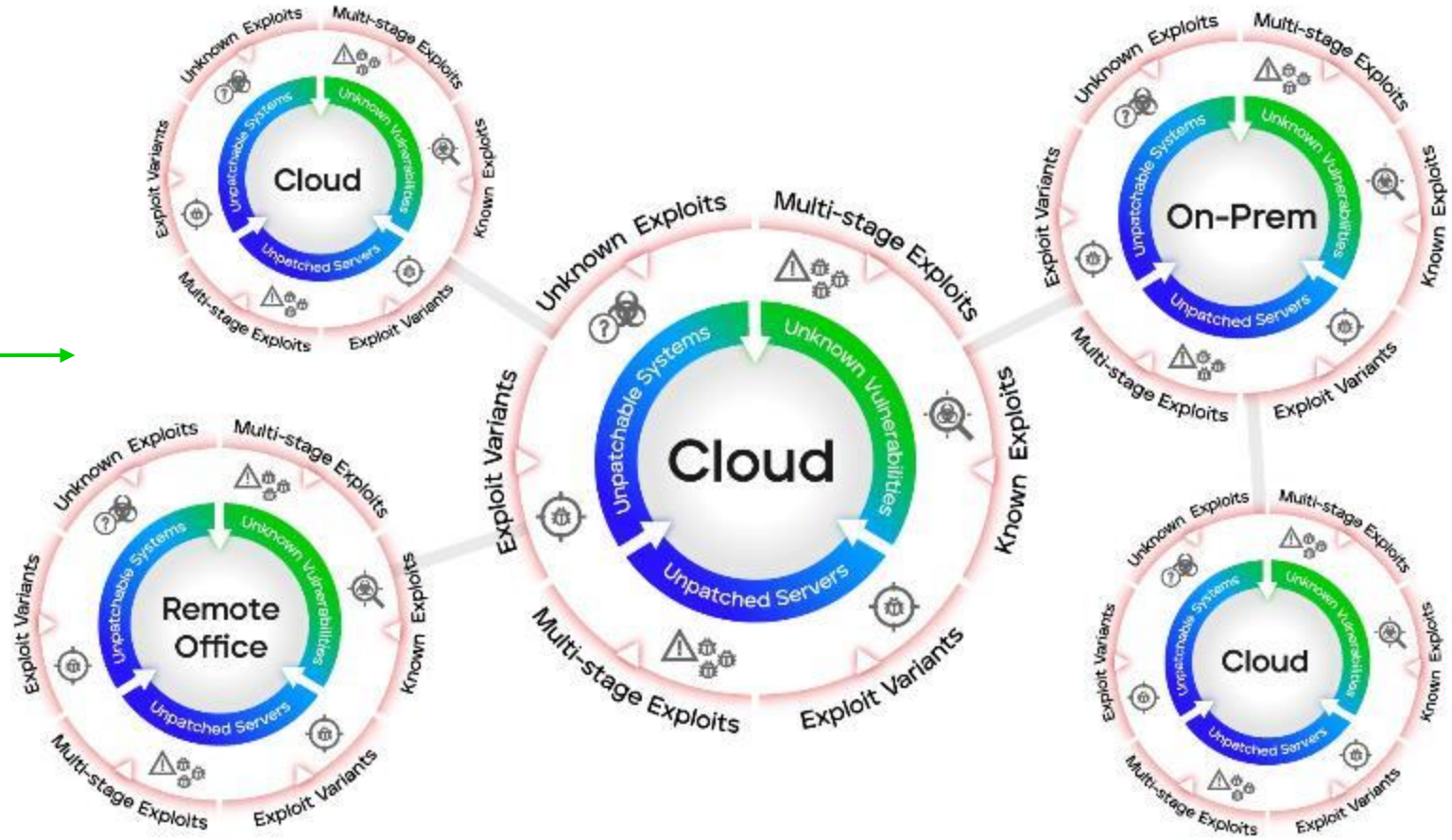
Known and unknown vulnerabilities, exploits and attackers are a constant risk on complex networks

Sophisticated attacks evade defenses

Sophisticated attackers continue to evade signature-based and anomaly-based detection causing impact to customers

More Alerts Overwhelming SOCs

SOCs are overwhelmed with alerts that generate noise and make investigations less efficient

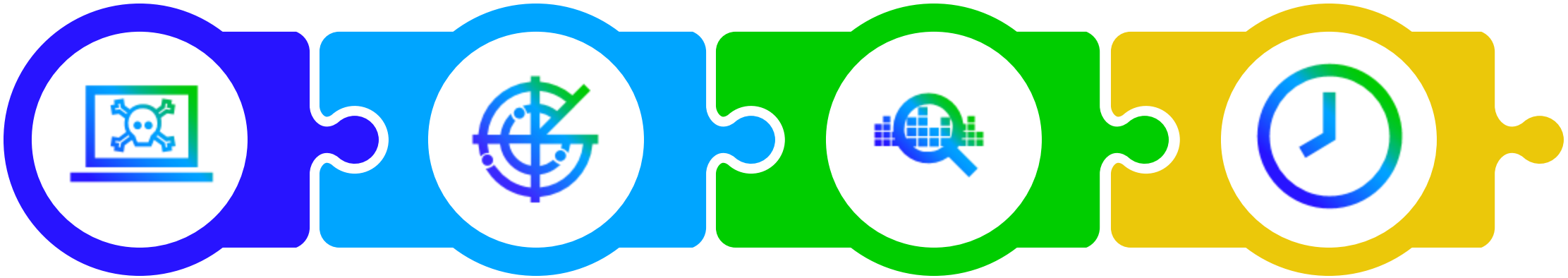


The time to respond is of essence

Trellix

More is needed for advanced cyberbreach protection

Network Security needs to be elevated



Keep known threats out

Detect unknown, emerging threats

Investigate the breach

Respond Quickly

We need Network Detection and Response

Trellix

“The escalating sophistication of threats requires organizations to use multiple sources of data for threat detection and response.

Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents.”

Gartner Research

Applying Network-Centric Approaches for Threat Detection and Response

Trellix

The Promise of NDR

Monitor environments in real time and address important incidents the moment they arise

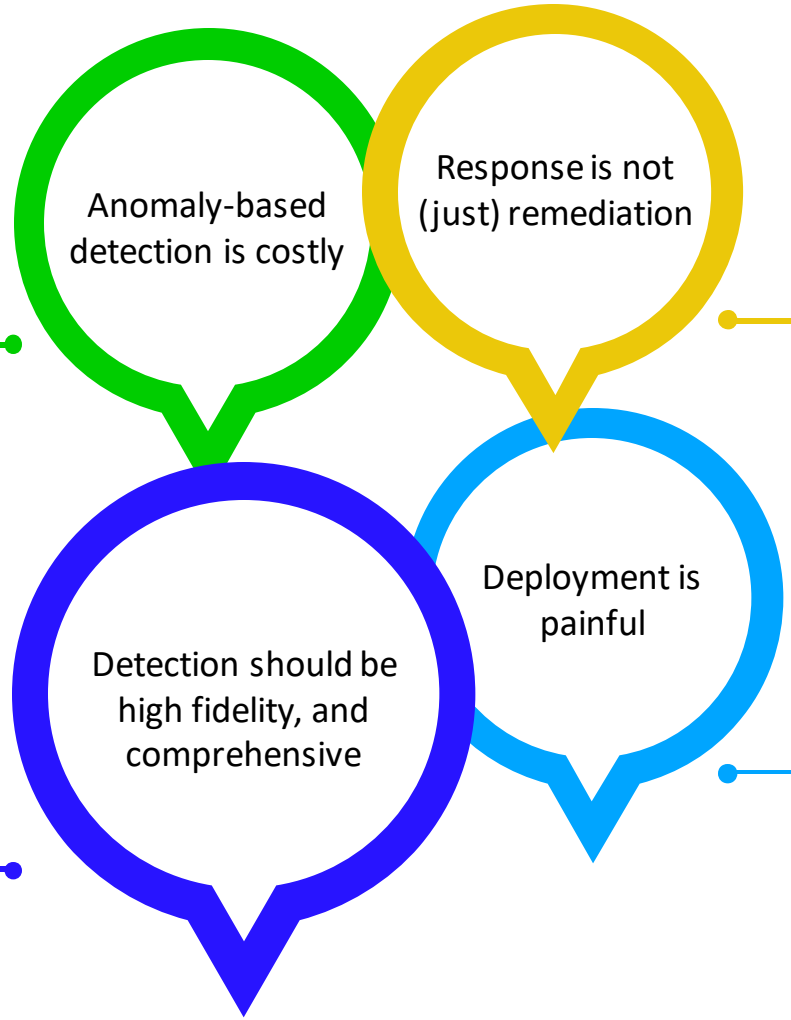
- ✓ **Detect** priority cybersecurity events from multiple sources
- ✓ **Enrich** alerts into actionable threat incidents
- ✓ **Prioritize** critical events for faster response
- ✓ **Optimize SOC workflows** like hunting, forensics and incident response
- ✓ **Improve key SOC metrics** like MTTD and MTTR
- ✓ **Integrated response** capabilities should be simple and straightforward

NDR - a security tool that detects abnormal behaviour by applying behavioural analytics to network traffic data – Gartner Definition

Trellix

But what we're hearing from our customers

Current solutions with NTA-based approaches increase workloads without reducing risk



Baselining is problematic and time consuming

Anomalies add noise for our SOC team without reducing risk

Support required for investigation actions (scoping, call back analysis, lateral move)

Resurgence of IPS/signature features for "virtual patching"

Correlation between NDR, EDR, Identity and Messaging is powerful

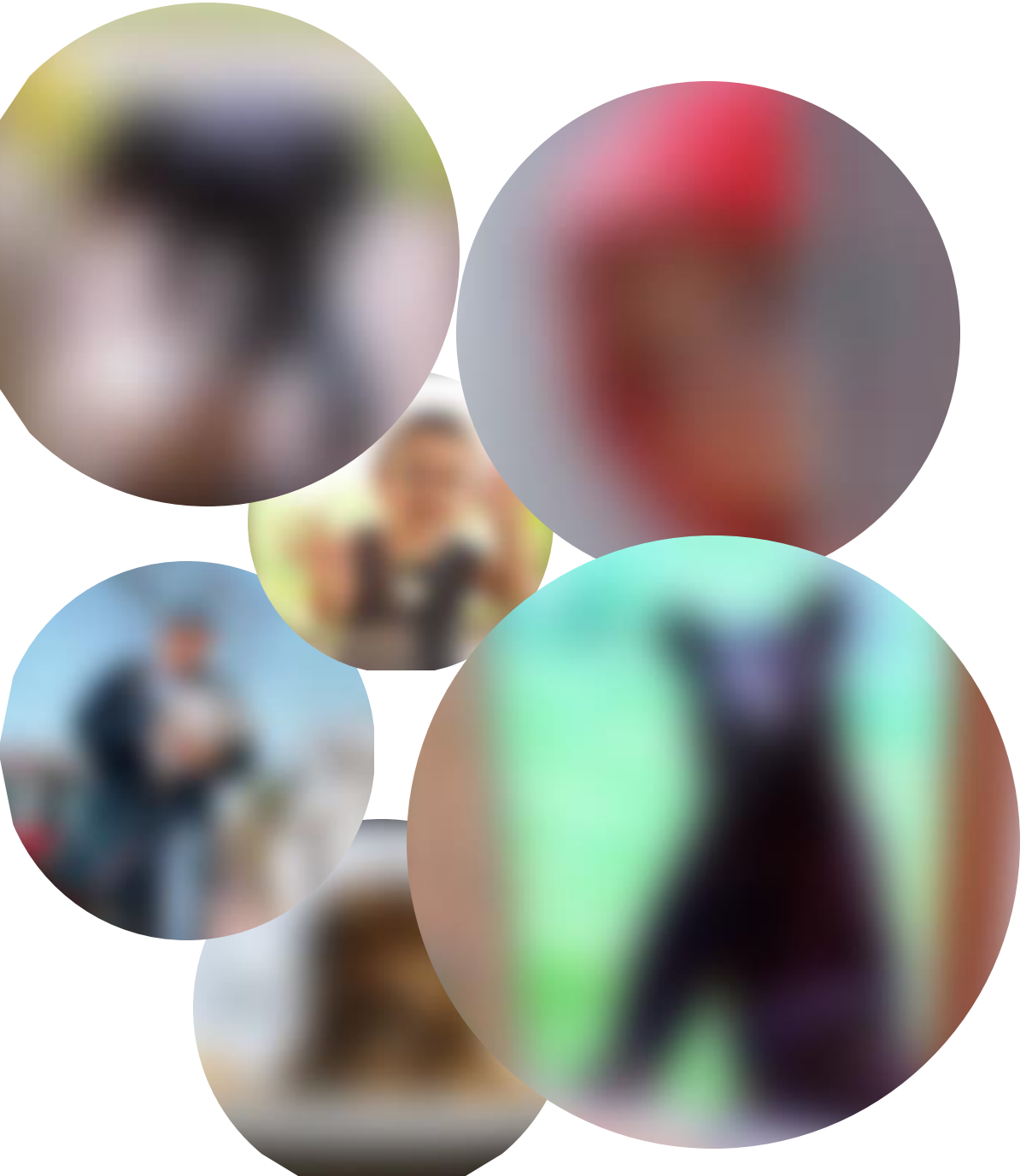
We receive too many false positives

Need coverage for all stages of attack framework.

We want to leverage existing network sensors, not deploy additional devices

TCO concerns with deploying new technology is a barrier to adoption

Trellix



The issue with traditional NDR

- Anomalies are signals – not detection
- Normal always changes – so you must constantly tune
- Alerts lack actionable context
- Too much time spent investigating inconsequential alerts

We want to detect and mitigate cyberattacks faster with less resources.

Trellix

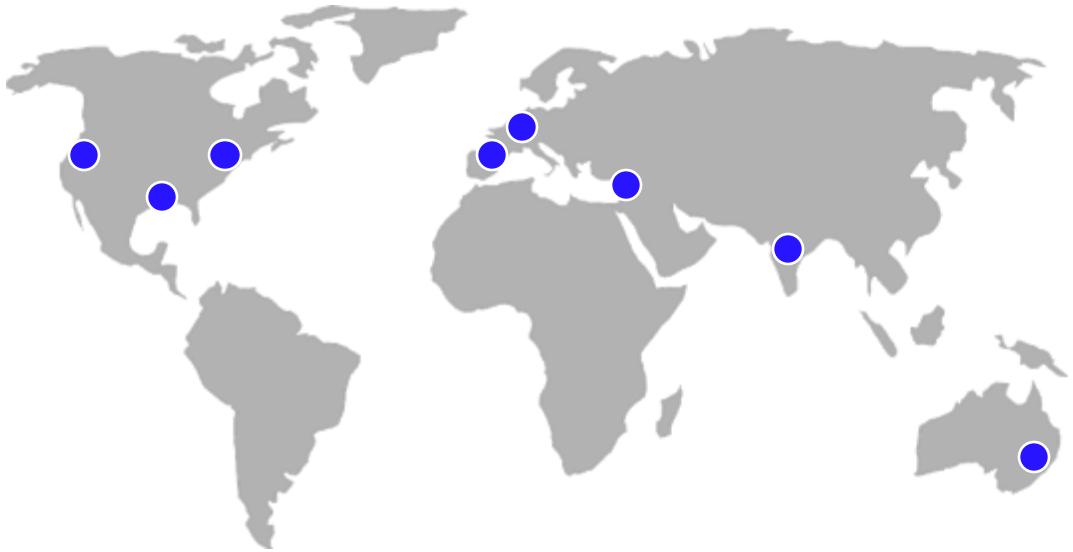
Deep analysis reveals the threats and context that matter

- Detection is our founding competency
- Years invested tuning machine learning models
- Detection that continually adapts as threats evolve
- Full, deep packet inspection across multiple threat vectors for hunting, investigating, and forensics

Customers value our high-fidelity alerts

Trellix

Global Threat Intelligence Group



- Located in multiple time zones, 24/7 coverage.
- 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
- Top Publications on current threats and tactics
- Leveraging telemetry from endpoint, email, network, sandbox, XDR

+50
TI Analysts

+200
researchers

Data-driven research from intel to products

Trellix

Broad Detection Stack Exposes Threats

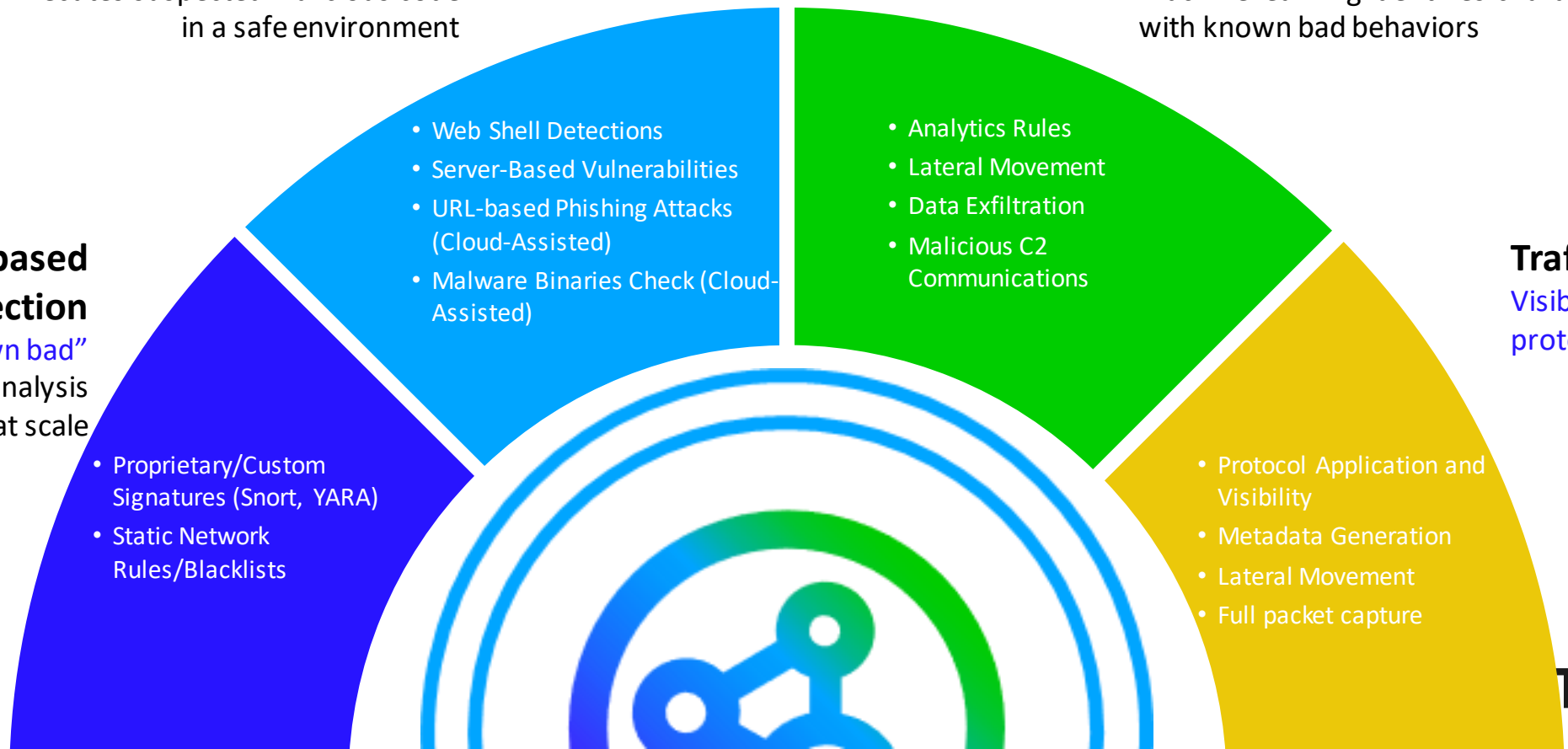
Prioritizes incidents that need attention

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

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

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

Traffic Analysis
Visibility when perimeter protections fail



Trellix

Detecting Threats Across The Kill Chain

Comprehensive threat model-based approach to detect threats

- 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

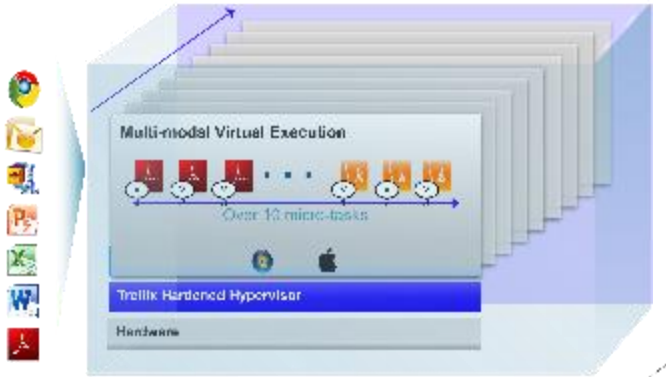
Coverage across the kill chain detects more and enables faster responses

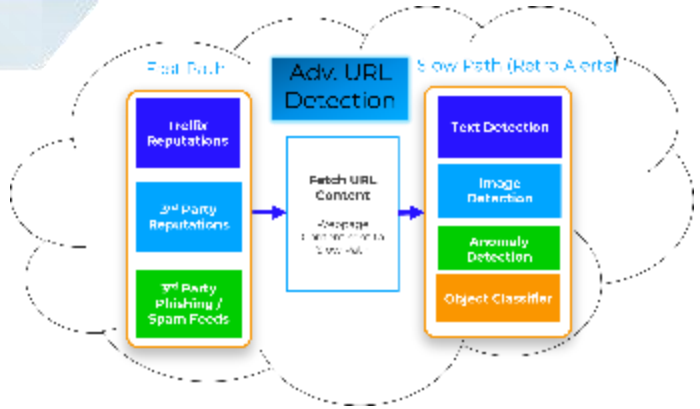
Trellix

Proven Innovative Detection

Foundational and Innovative technologies that adapt with the attackers

- Intelligent Virtual Execution
- Advanced URL Detection Engine
- SmartVision





Trellix

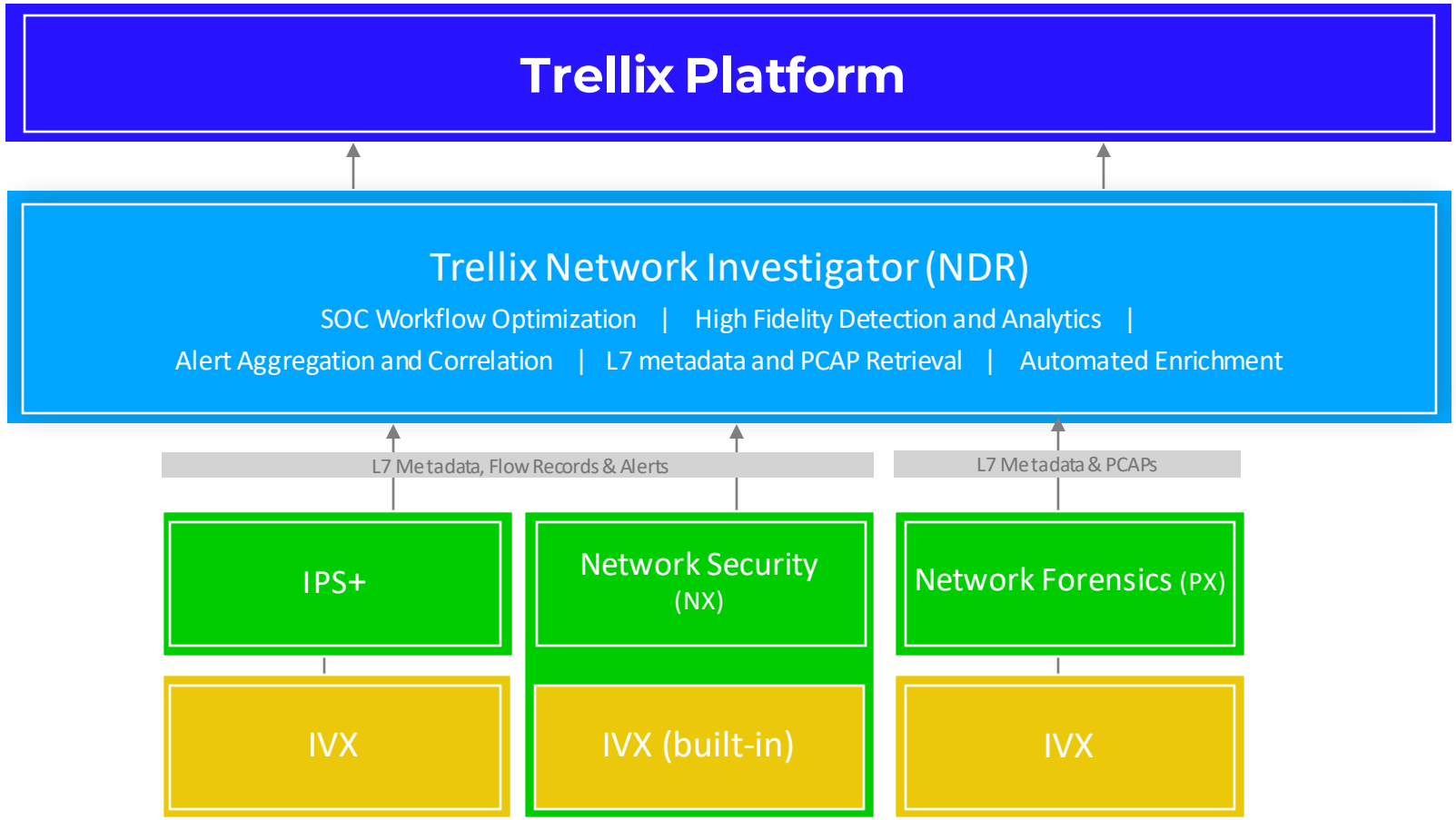
Trellix NDR

Elevate your Network Security

Trellix

Trellix Network Detection and Response

Complete network protection comes together in full NDR



- Leveraging our **SecOps and Detection focus** to speed investigations
- Trellix's **detection-first strategy** ensures SOC analysts receive **actionable alerts** from day one for faster responses
- **Intuitive Visualizations** of network activity
- **High fidelity alerting** through alert aggregation and advanced analytics and ML models

Trellix

Supporting the Incident Response workflow

NDR Threat modelling for the SOC Analyst

Advanced Threat Detection	Hunting	Investigation	Scoping	Containment & Remediation
Advanced signatures, ML/AI and behavioral analysis detect emerging threats	Full PCAP, L7 metadata, and flow data visibility for adv. 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	Expedite responses with XDR, SOAR playbooks and ticketing system integrations

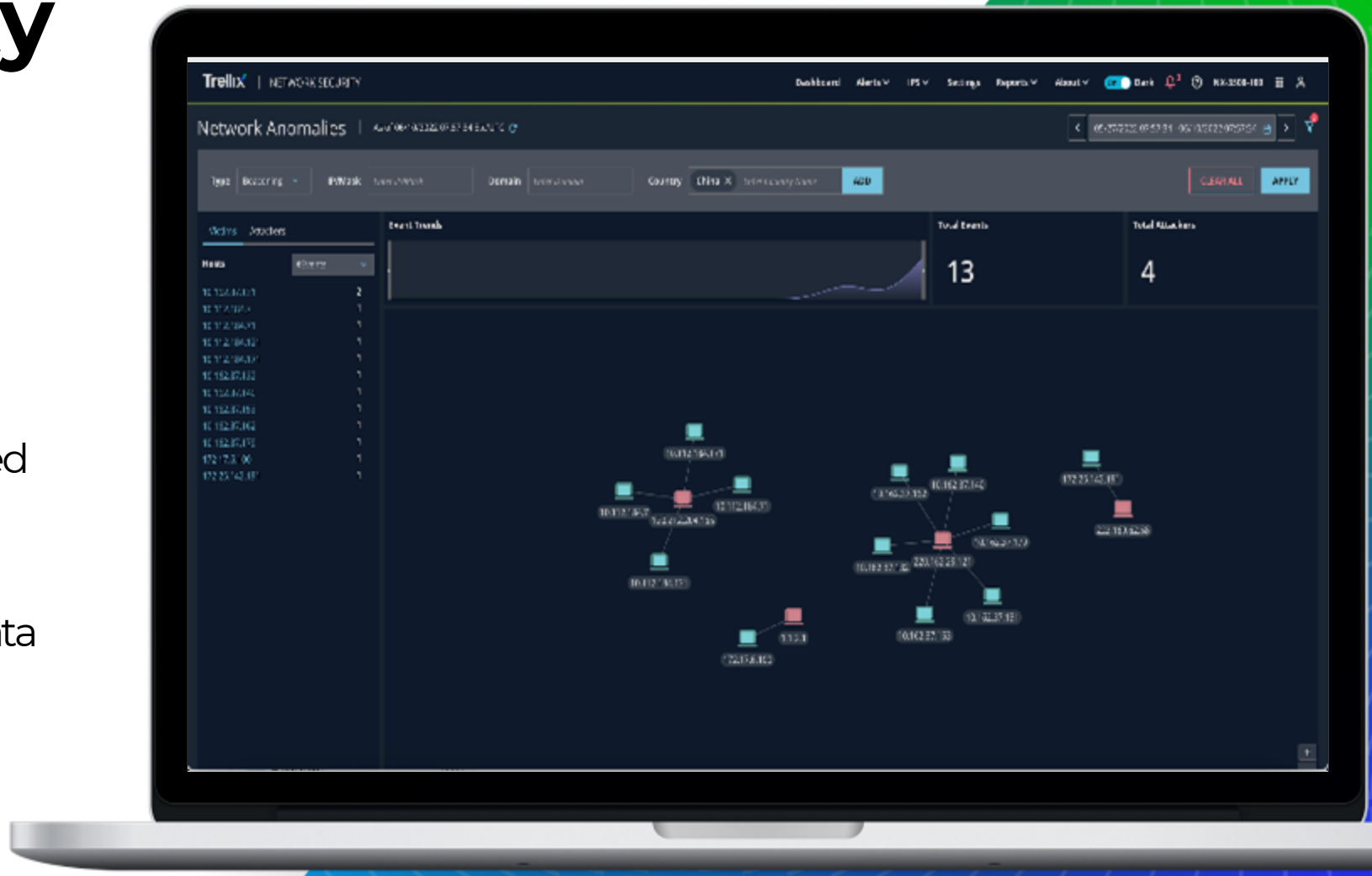
Provides visibility and alert priority to respond quickly

Trellix

High-Fidelity Detections:

Beaconing

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

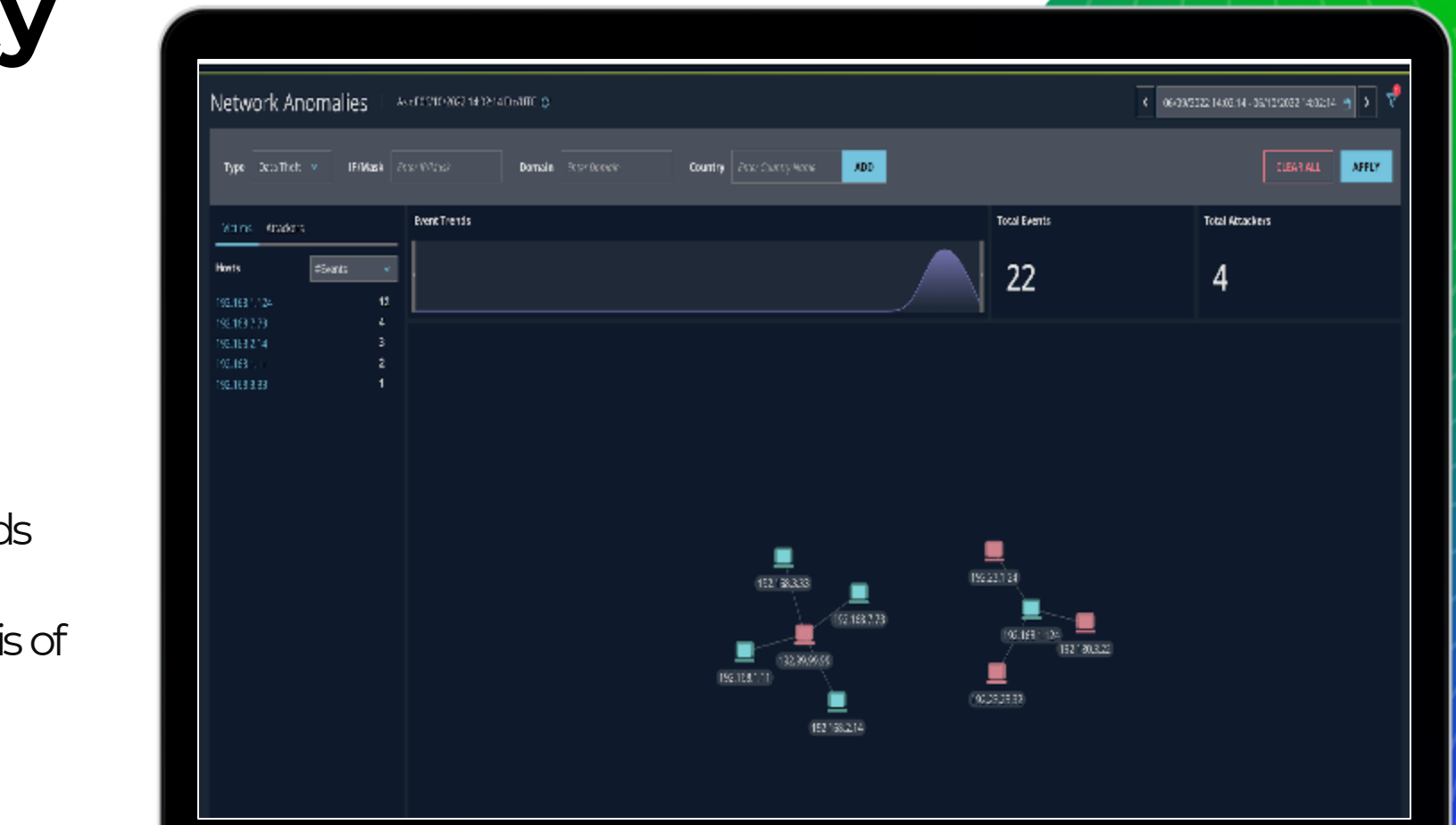


Trellix

High-Fidelity Detections:

Data Exfiltration

- Bi-directional net-flow records from Suricata engine
- ML-based volumetric analysis of flow data
- Learning mode to develop network baseline
- Adjusts to different size networks & traffic patterns to best baseline



Trellix

Trellix IPS/NX/Forensics

Value Enhanced with NDR

Trellix

Trellix IPS

High fidelity Intrusion Prevention at Scale

Powerful Protection with Deep Packet Inspection

- Prevents initial incursion
- Prevents C&C traffic and exfiltration
- Prevents exploits

High performance visibility

- 100% SSL visibility
- L7 Visibility and Analytics
- 100 Gbps throughput for high load north-south network traffic

Rich source of network activity for Network Detection and Response

Trellix

Signature + Signature-Less Technology

IPS + engines keeps known threats out

Signature-Based DPI

User-defined, custom, Snort Signatures

STIX Allow list/block list

Threat Reputation

Global Threat Intelligence

File, IP, and URL reputation

Deep File Analysis

Adobe PDF, Flash, JavaScript inspection

Real-time Emulation

Gateway Anti-Malware Browser (GAM) Emulation

Botnet Detection

Botnet and malware callback protection

Detects known and unknown threats and emerging techniques

Trellix

Trellix Network Security (NX)

High fidelity network visibility and advanced threat detection

Multiple Engine Network Detection

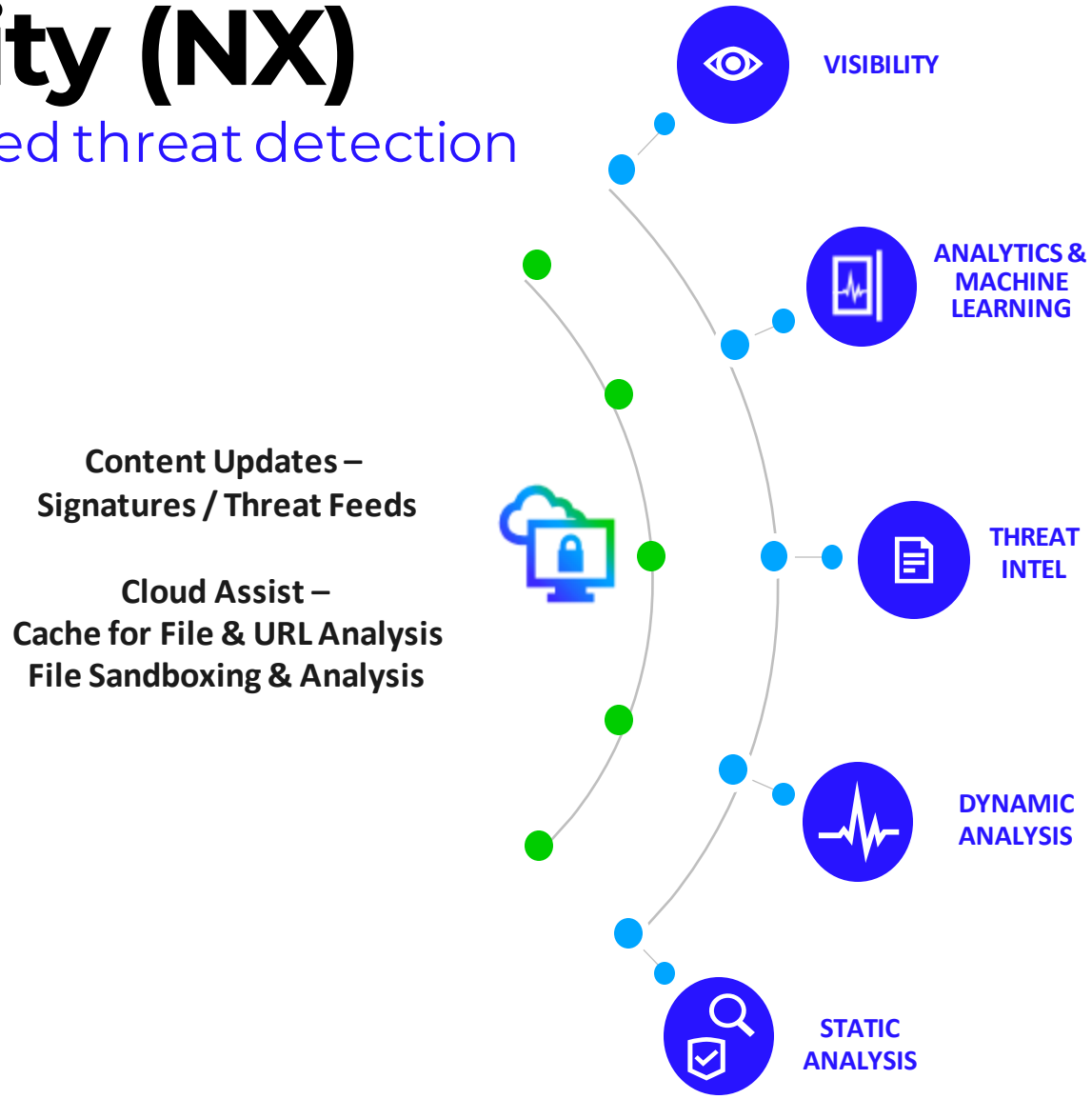
- East-west traffic detection; lateral movement, privilege escalation, C&C, beaconing, exfiltration, etc
- Built-in IVX detects new and emerging threats
- Multi-flow attack detection

Rich network visibility analytics

- 10 minutes L7 metadata around every alert
- TLS 1.3 SSL decryption

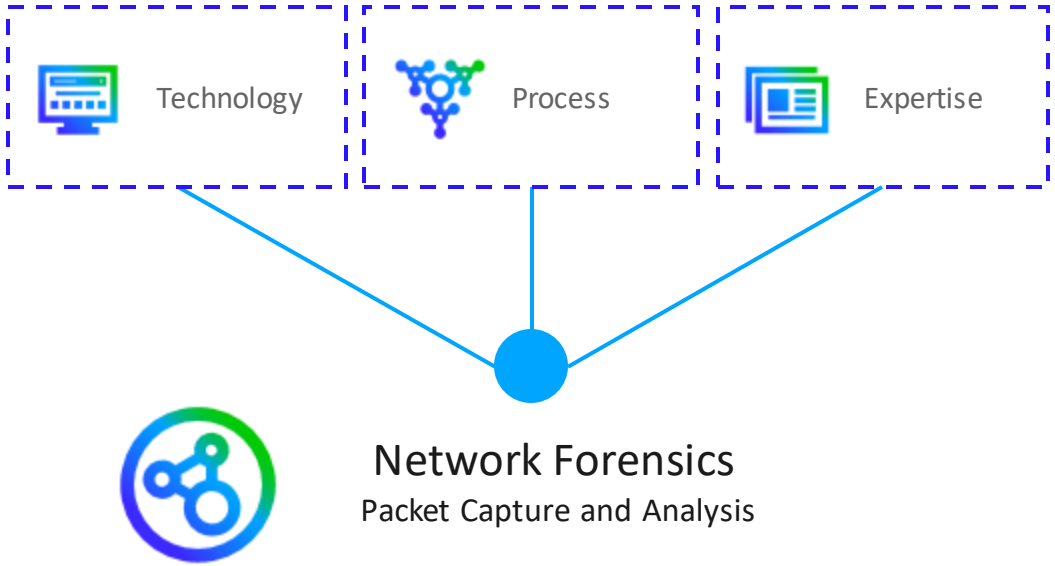
Operational efficiency

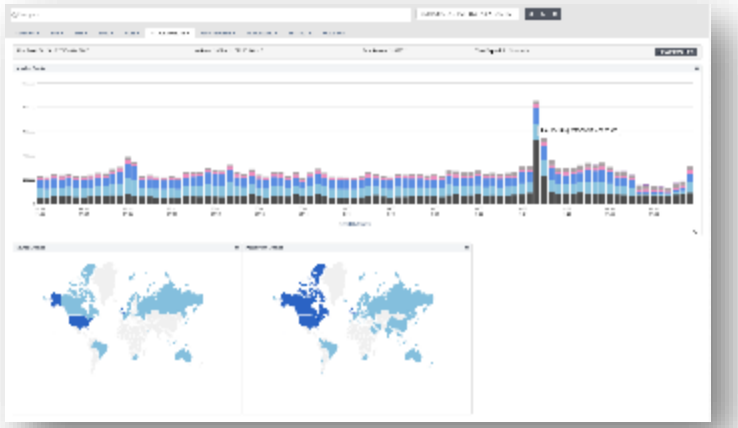
- On-prem, virtual, private and public cloud



Trellix

Trellix Network Forensics





Lossless packet capture provides vital data into effective network forensic investigations

Extensive Visibility session decoder to view and search web, email, FTP, DNS, SSL connection details and file attachments

Ultrafast search leverages unique indexing architecture for fast answers

Easy drill down allows analysts to quickly respond to alerts that matter

Flexible deployment model that scales and grows with your network

Trellix

Trellix IVX

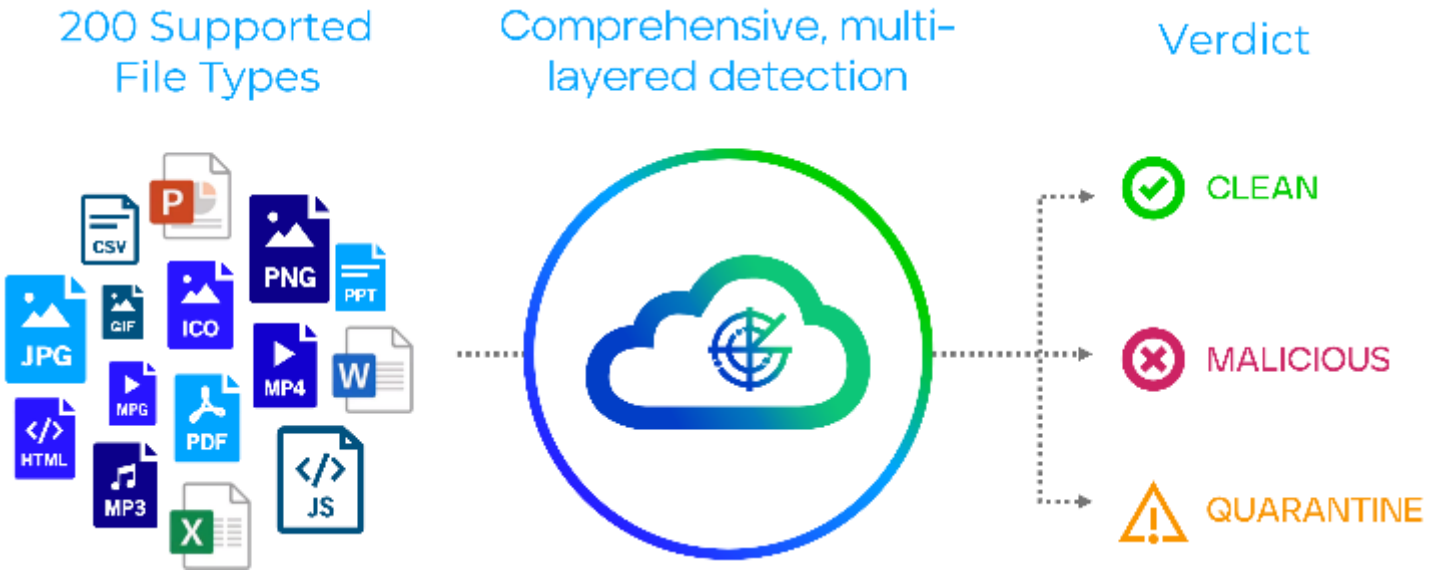
Supplementing network detection

Trellix

Trellix Intelligent Virtual eXecution (IVX)

Threat detection sandbox that pinpoints known and unknown malware

- Reduce dwell time: continually inspect and convict content upon entry
- Identify unknown and zero-day threats: using multiple analysis techniques including static, dynamic, URL, and behavioral analysis
- Supplements SOC Hunting: high fidelity alerts ensure analysts focus on the threats that matter

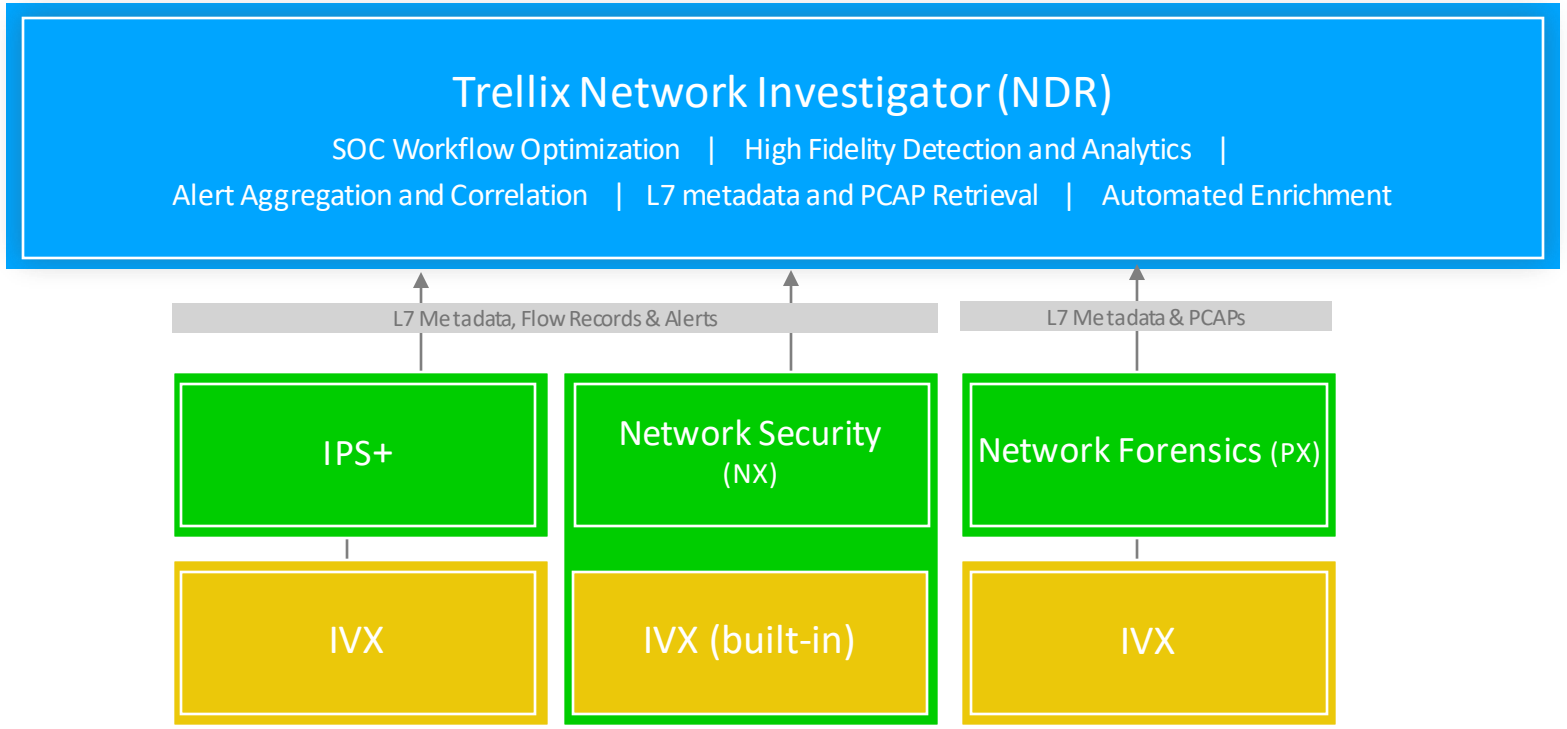


Accelerates investigation and response with visibility into unknown attacks

Trellix

Trellix Network Detection and Response

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**

Trellix

Trellix NDR

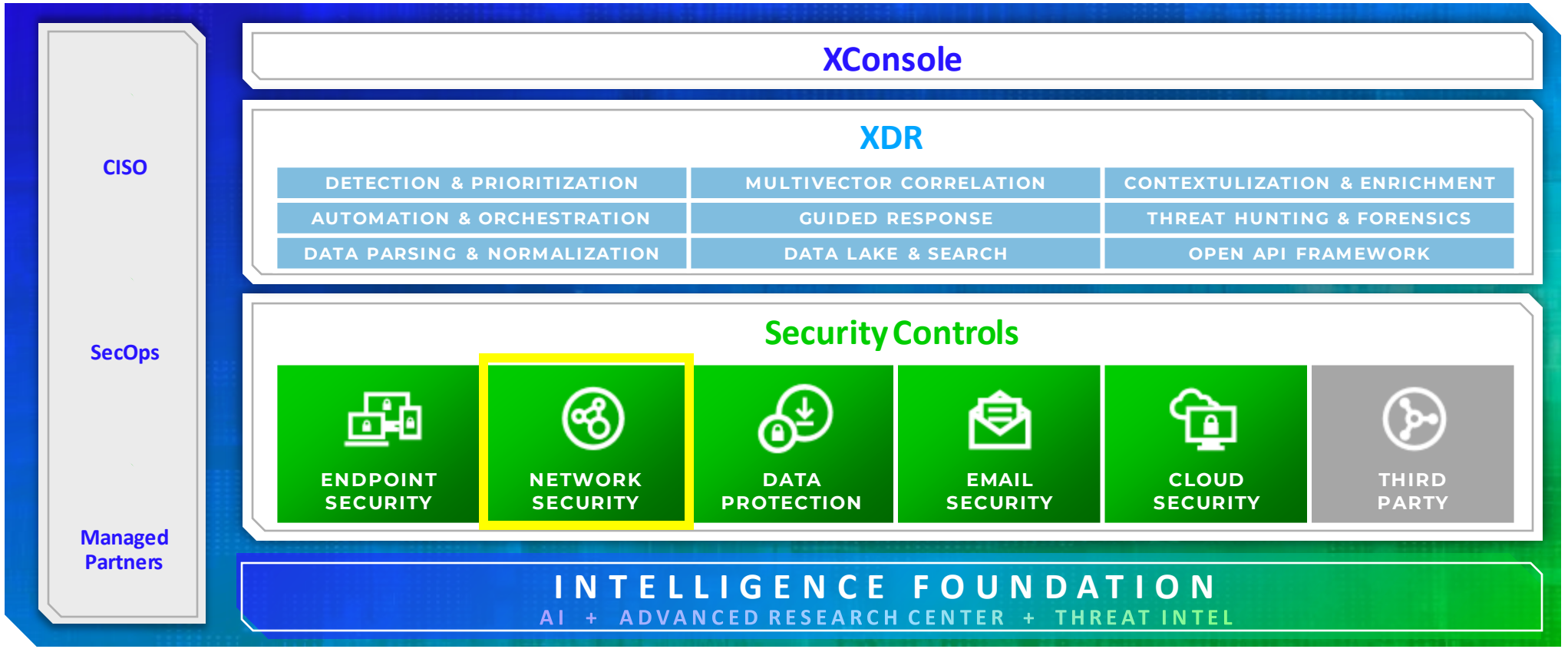
Threat model-based detection and response

- ✓ Detects, prevents and prioritizes high impact threat incidents
- ✓ Speeds investigations with high fidelity detections and alerts
- ✓ Adapts to the constantly evolving threat landscape
- ✓ Improves the security operations program by reducing noise and risk
- ✓ Elevates the value of existing network security investment

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

Trellix

A key component of our XDR Platform



Most Open XDR Platform

Best of Breed Security Controls

Strong Threat Intel Foundation

Trellix

Trellix

Thank You!

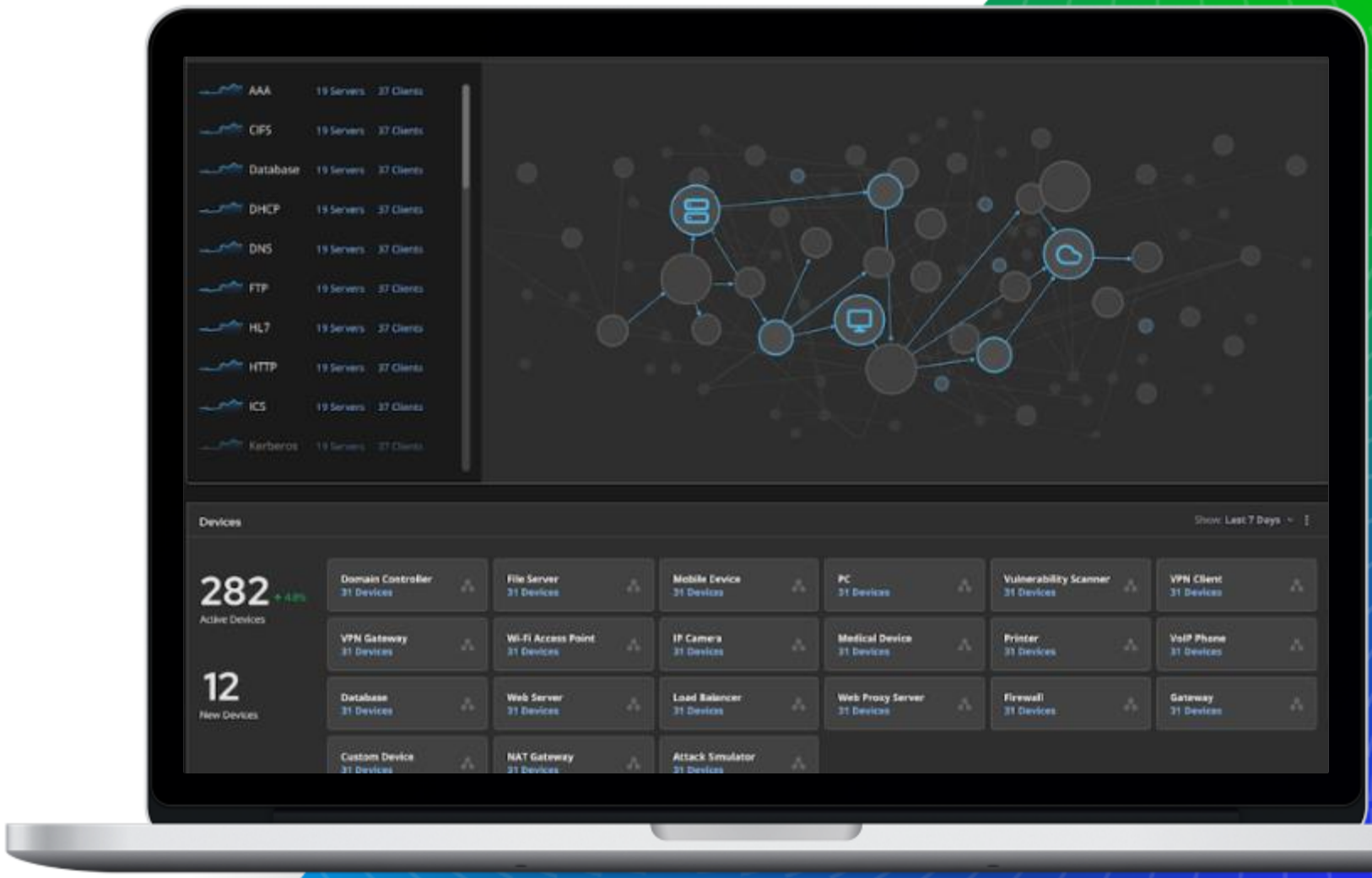
Asset Discovery

Identify all nodes in a network

- Allow for endpoint agent upsell
- Identify critical nodes
- Identify rouge nodes
- AD Integration available

Future iterations

- Validate IPS CVE coverage against current target threats
- Identify lateral move activity
- Map risk/exploit paths using identify & service data
- Integrate with third-party apps for response actions



Trellix

Machine Learning Models

Module name	Learning Type	Deployment	Description
Data Exfiltration	Unsupervised	Appliance	The data exfil model detects anomalies in network traffic based on data volume and historical behavior
Beaconing	Unsupervised	Appliance	The unsupervised beaconing model detects when a program exhibits a beaconing-like behavior, based on time series data.
PhishEye	Supervised	Cloud	PhishEye is a CNN based model for detecting phishing URLs using screenshot for the webpage.
NeURL	Supervised	Cloud	NeURL gives a prediction score of suspicious HTTP headers based on N-Grams and character distributions in a URL.
Profeta	Supervised	Cloud	Profeta leverages multiple data sources (data plugins) to classify an URL as C2 communication
Kraken	Supervised	Cloud	Kraken's focus is on detecting social engineering pages using image & string similarity techniques
Domphin	Supervised	Cloud	DOMphin uses characteristics of the document object model to find social engineering pages

Machine Learning Models

Module name	Learning Type	Deployment	Description
DGA	Supervised	Cloud/appliance	DGA detects dynamically generated domains which could be used for C2 communication
DNS Tunneling	Supervised	Appliance	The unsupervised beaconing model detects when a program exhibits a beaconing-like behavior, based on time series data.
Headshot	Supervised	Cloud	Headshot uses static features extracted from the URL structure and from the HTTP request.
Einstein	Supervised	Cloud	Machine Learning detection plug-in that makes use of time-based features extracted from data collected during crawling

Trellix

Lateral Detection – East / West Traffic

SmartVision provides four primary features

- Advanced correlation engine
  - 180+ rules for post-exploitation and malicious activity detection in the internal network
  - Provides detection across the attack lifecycle and expands NX value into east-west and data center traffic inspection
  - Goes beyond signatures and includes a comprehensive correlation and analytics engine
- Detonation of executables transferred over SMB
- Machine-learning data exfiltration module
- 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