

# Trellix

# Welcome!

Partner Tech Summit – Rome

Network Security



# Trellix

# Welcome



# AGENDA

- Welcome
- Latest Updates and Product Line Pitching
- Use cases and Demonstration Guidance
- SE Resources – How to Access
- POV Guideline and Process
- Trellix Differentiators
- Point of Contacts



# Trellix

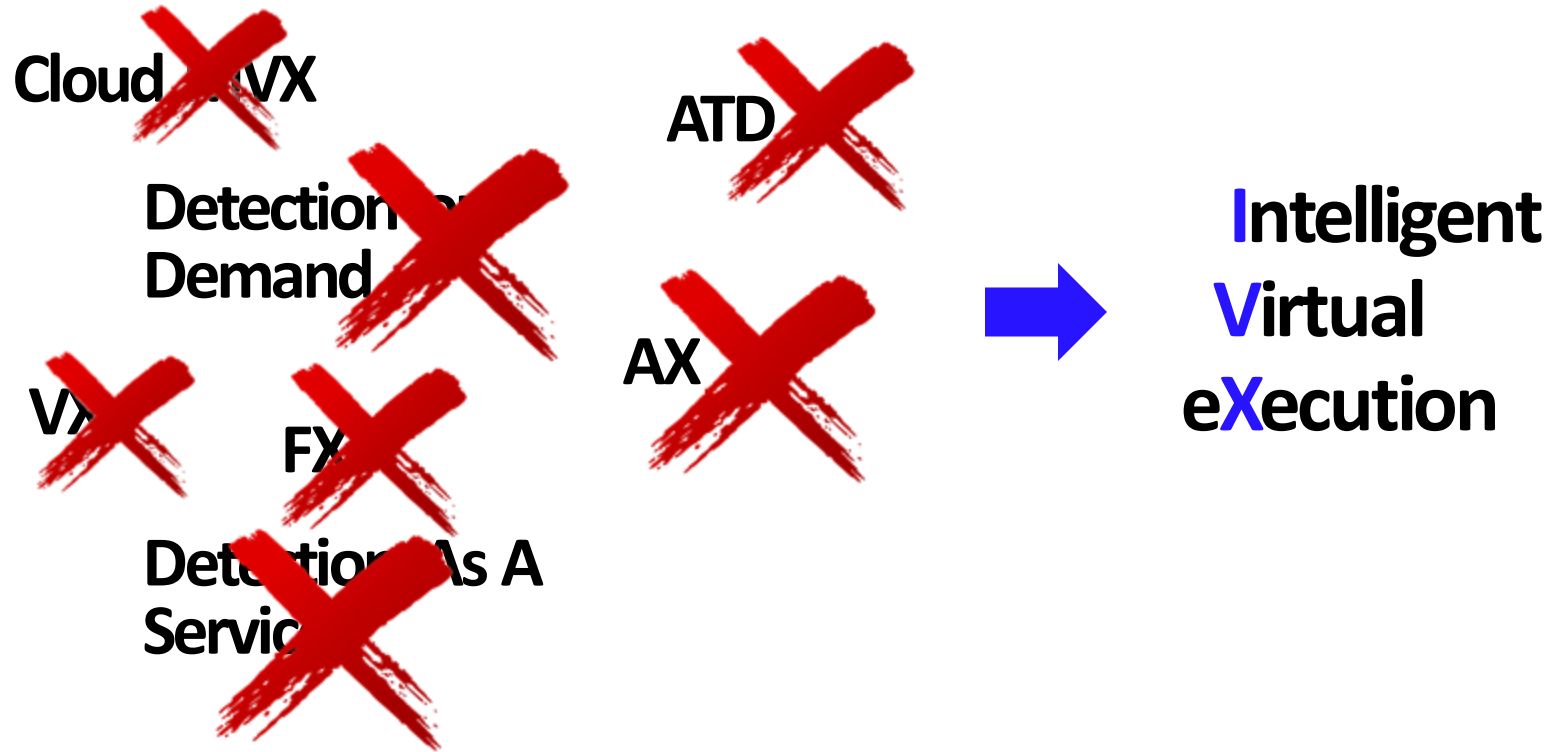
# IVX

Is this the Sandbox?



# Cleaning up our portfolio

We have a confusion of sandbox products available to customers today



# Proven technology to address three distinct use cases

## IVX for Products

---

Targeted for Trellix Appliances

MVX detection created the sandbox market.  
Detection is our founding competency

Flexible deployment options that scale for  
scanning throughput with Network Security,  
Email Security, Endpoint, etc.

Clustered architecture instrumented for 200  
potential simultaneous executions

**Product: Trellix IVX**

## IVX for Investigators

---

Targeted for the SOC

Used during investigative workflows

Detonate suspicious content

Reverse engineer malware

**Product: Trellix Malware Analysis**

## IVX for Collaboration Security

---

Targeted for Enterprise Applications

Organizations focused on digitizing their  
extended enterprise value chain

Integrates with enterprise applications

Mitigate the risk of working with external  
organizations and vendors

**Products: Trellix IVX Cloud  
Trellix File Protect**



**End of Sale**

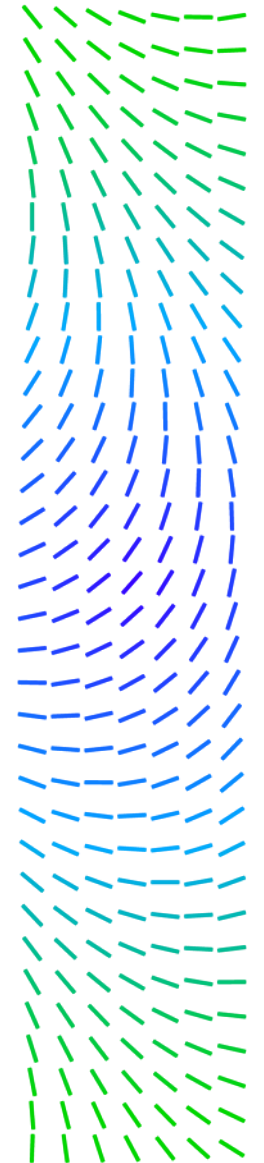
**End of Support for  
ATD / TIS**

**Trellix**

# ATD/TIS – EOS & Last Support Dates

Platform	End of Sale	End of Support
ATD 3100	31-Dec-20	31-Dec-25
ATD 6100	31-Dec-20	31-Dec-25
ATD 3200	30-Jun-23	31-Dec-25 with ATD* 30-Jun-28 with IVX
ATD 6200	30-Jun-23	31-Dec-25 with ATD* 30-Jun-28 with IVX

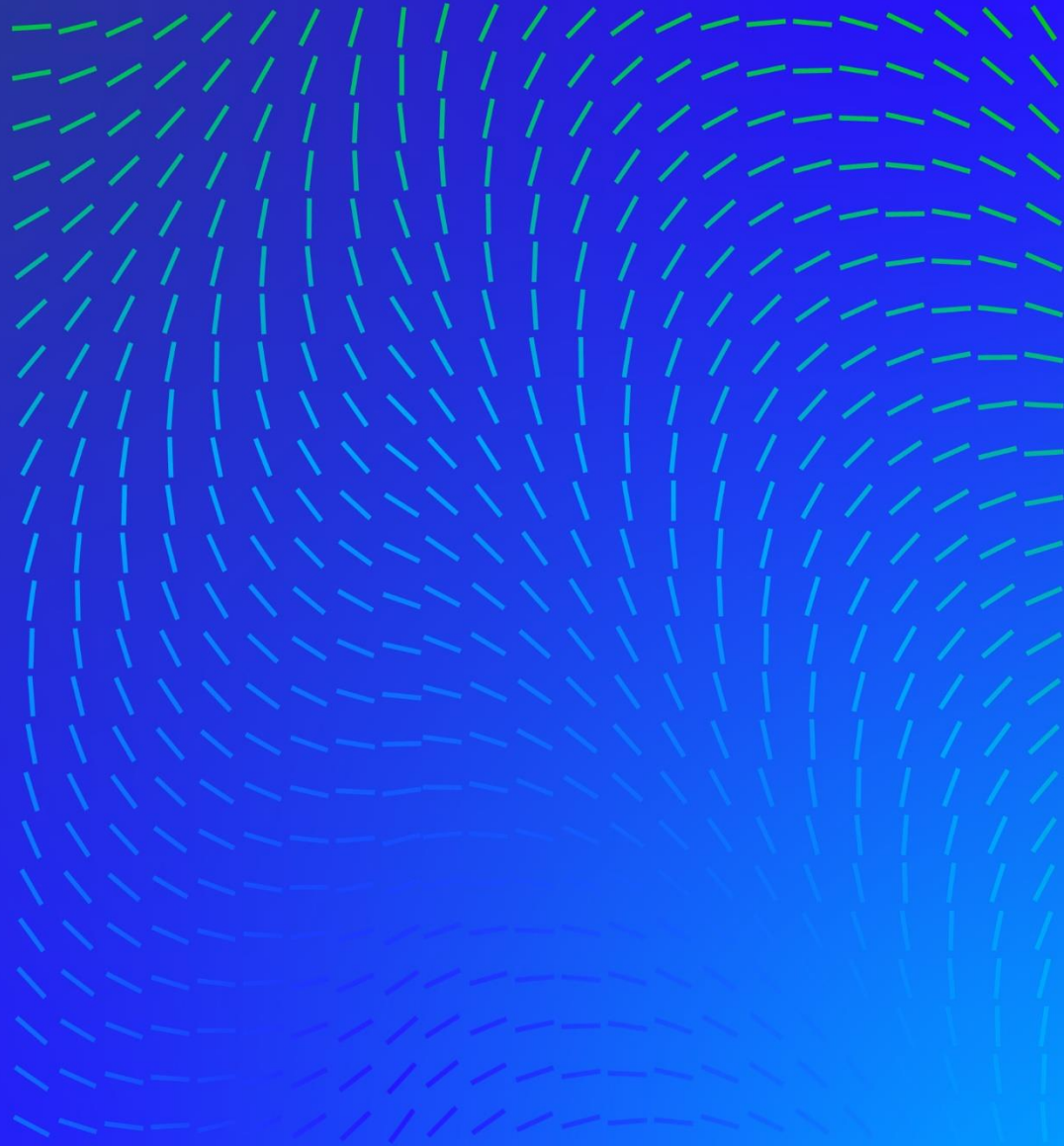
\* ATD -> IVX upgrade will be available in Q4'23





# Features Parity across Sandbox products

	Trellix ATD	Trellix IVX	Trellix IVX Cloud	Trellix File Protect	Trellix Malware Analysis
Hardware	✓	✓		✓	✓
Virtual	✓	Q4'23		✓	
Cloud		✓	✓	✓	
Web UI	✓	Q4'23	✓	✓	✓
macOS & Linux images		✓	✓	✓	✓
Live Mode Analysis	✓	Q4'23	✓		✓
File Share Scanning		via FX		✓	
Integration with ENS/EDR	✓	via TIE	via MVISION ePO		
Integration with Email		via EX	via ETP		
Integration with IPS	✓	✓	✓		
Integration with Skyhigh SWG	✓	✓	1H'24		
Integration with TIE	✓	✓	✓		1H'24
Integration with XConsole			✓		
ICAP Submission	via SWG	1H'24			



# IVX Appliances

Collaboration Security, powered by Trellix  
IVX

**Trellix**

# Trellix IVX (Formerly VX)

- Signature-less, dynamic analysis engine that captures and confirms zero-day, and targeted APT attacks
- Detonates files, URLs, web objects, and email attachments within proprietary hypervisor instrumented for over 200 potential simultaneous executions
- Static scanning includes object decomposition & emulation, machine learning and statistical analysis to conduct one-to-many analysis
- Integrates with Trellix Network Security, Trellix Email Security, Trellix File Protect and Trellix Endpoint Security
- Analyzes threats across Windows, macOS and Linux operating system environments

## Appliance



VX5600  
VX12600

Upto 15,840 files per day  
Upto 120,960 files per day



ATD3200  
ATD6200

Upto 19,320 files per day  
Upto 31,560 files per day

## Cloud

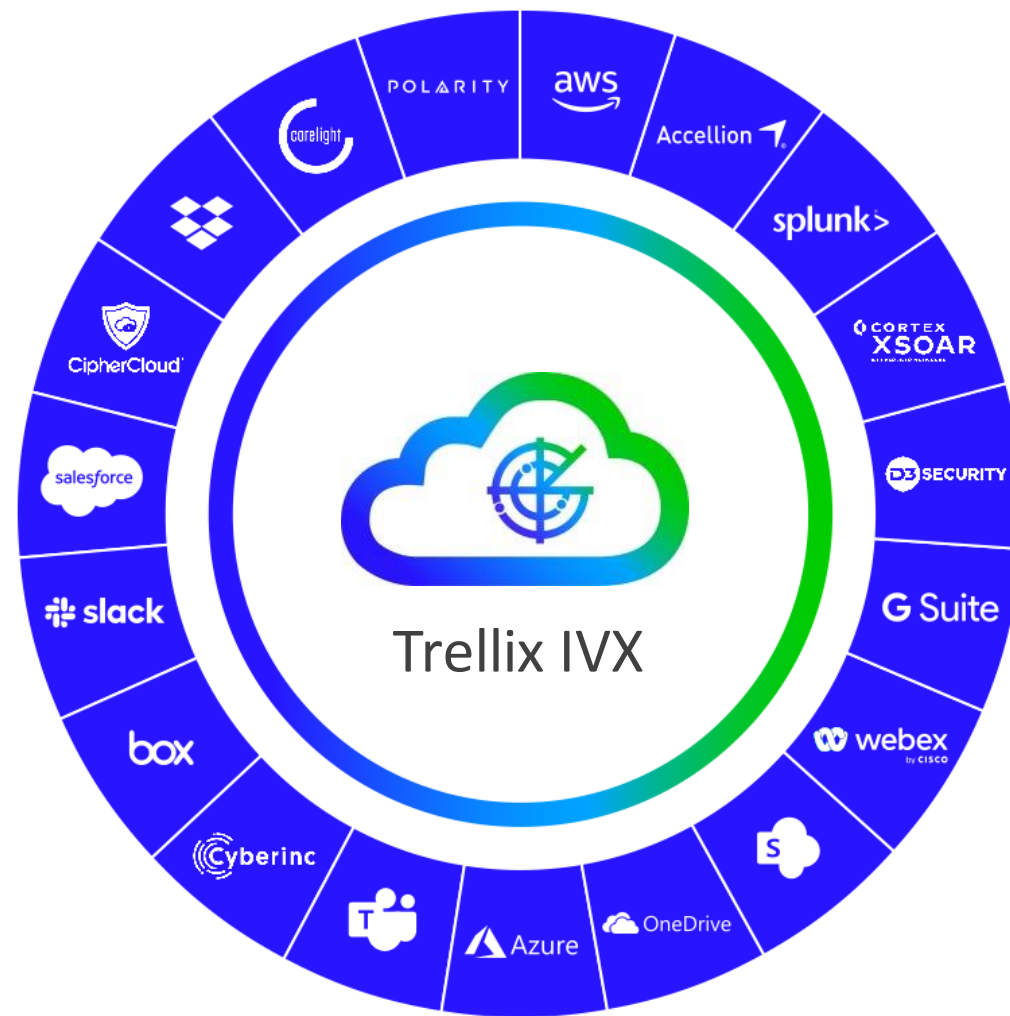


AWS Bare Metal  
c5.metal

Upto 150,000 files per day

# Trellix IVX Cloud (Formerly DaaS)

- Cloud-native service that delivers flexible file and content analysis capabilities to identify zero-day, and targeted APT attacks
- Integrate with security operations center workflow, SIEM analytics, data repositories, customer web applications, and more!
- Integrates with cloud services like AWS, Azure, Google, and cloud tools like Dropbox, Box, OneDrive and enterprise applications like Salesforce.com, Webex, Slack, Microsoft Teams and more!
- Compiles in-depth analysis details, including MITRE ATT&CK mapping, extracted objects, IOCs, memory dumps, pcap, screenshots and more!
- Available through Trellix channels or directly through the AWS Marketplace



File submissions rate at 100 per minute  
Hash submission rate at 200 per minute



# Trellix File Protect (Formerly FX)

- Secures data assets against attacks that originate from backups, online file transfer, cloud, and portable file storage devices
- Analysis of over 200+ file types such as Portable Executables, Documents, PDF, Scripts, Archives, and Multimedia files
- Provides continuous, scheduled, and on-demand scans of CIFS, NFS, SMB, WebDAV and compatible file shares
- Provides proactive protection for NetApp ONTAP, Amazon S3 buckets and Microsoft OneDrive & SharePoint
- Deploys in active Quarantine (protection) or Analysis (monitoring) modes
- Integrates with Trellix Central Management and Trellix Dynamic Threat Intelligence

## Appliance



**FX6600**

Scan upto 87,000 files per day

## Virtual Machine



**FX2500V**

Scan upto 50,000 files per day

## Cloud



**FX2500V**

Scan upto 50,000 files per day

# Trellix Malware Analysis (Formerly AX)

- Forensic analysis solution that gives security analysts hands-on control over auto-configured test environments
- Safely execute and inspect malware, zero-day, and APT attacks embedded in files, web pages and email attachments
- Reports changes to file systems, memory, and registry in OS and applications
- Offers live-mode or sandbox-mode to analyze zero-day exploits along with VNC viewer
- Analyzes threats across Windows, macOS and Linux operating system environments
- Integrates with Trellix Central Management, Trellix IVX Cloud and Trellix Dynamic Threat Intelligence

**Appliance**



**AX5600**

Upto 10,000 analyses per day



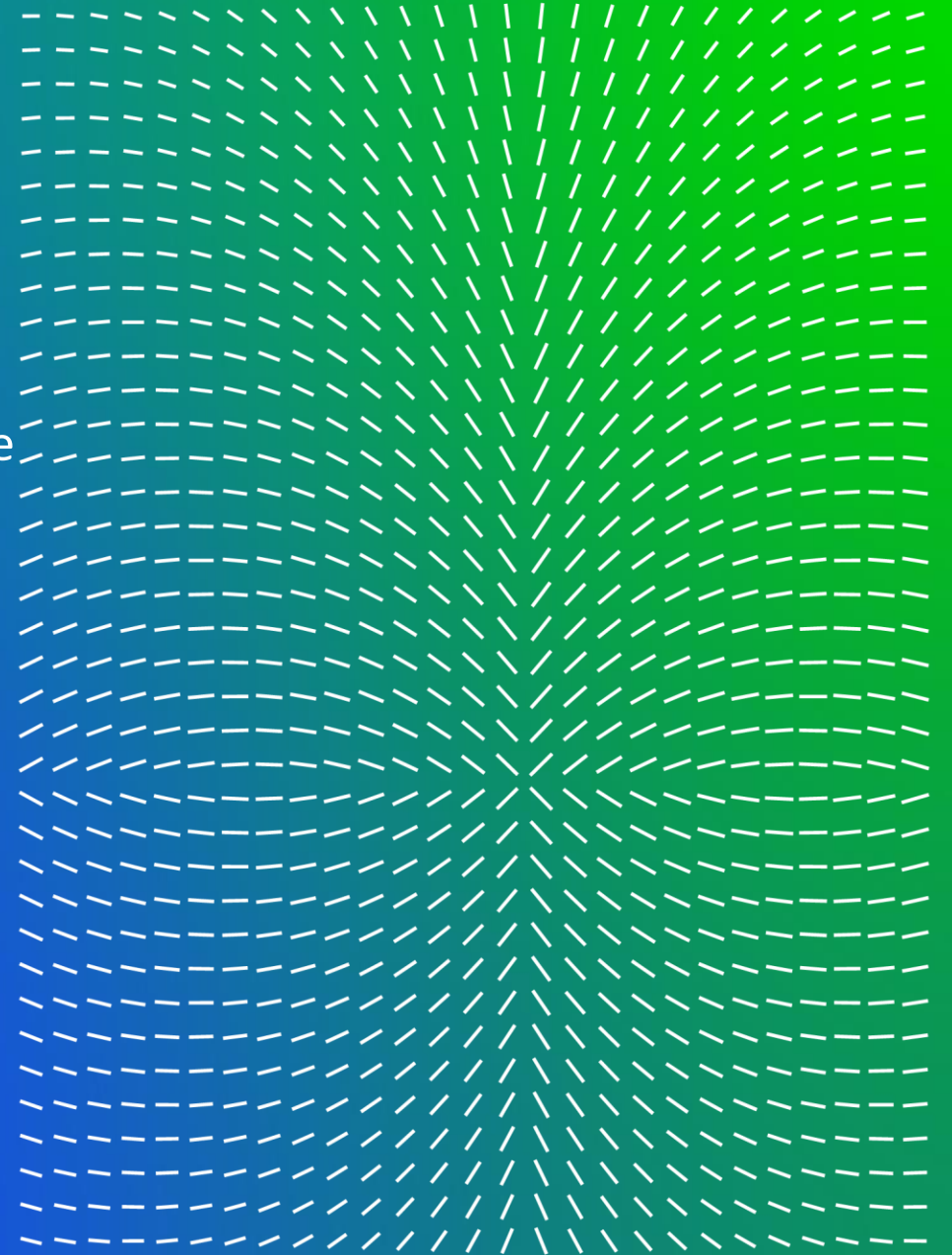
# IVX Roadmap

**Trellix**



## Safe Harbor Statement

This slide deck may include roadmap information, projections or other information that might be considered forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ





# Roadmap: Trellix IVX On-Prem

Detect the threats that matter. Detect the undetectable

## Recent

### Released 9.1.5 (Mar'23)

#### Improved Protection

Password protection archives extraction  
Support for OneNote samples  
Unpack UPX-packed binary ELF and macOS samples  
YARA rules support version 4.1.0

#### Platform Support

Faster database backup during appliance upgrade

#### Integrations

- On-Prem TIE Integration
- On-Prem Skyhigh SWG Integration

## Coming Soon

### Upcoming Release 10.x (Q4'23)

ATD -> IVX Upgrade Path  
Web UI for IVX (AX use case)

#### Improved Protection

Live mode in IVX  
Improved HTML attack detection

#### Integrations

- TIE SaaS Integration

#### Platform Support

- Virtual FX – KVM
- Virtual IVX – VMWare ESXi

## Exploring

### Improved Protection

Updates to Guest Images  
Google Suite Support

### Integrations

Private GTI Integration  
ICAP Support

### Management/Reporting

Web UI Enhancement (Cluster results)  
Dashboard improvements  
Improved Alerts Notifications

### Platform Support

Virtual IVX – Azure  
Virtual IVX – Nutanix

# Roadmap: Trellix IVX Cloud

Cloud-based sandboxing that detects known and unknown malware

## Recent

Released 2023.09.01 (Sep'23)

### Integrations

- XConsole Integration
- Trellix IAM Global Integration
- Skyhigh Integration

### Improved Protection

- GCP file scan size increased to 100MB
- URL Prefetch size increased to 100MB

### Management/Reporting

- Improved GCP and Teams Workflow

### Platform Support

- Oxylabs Proxy Support

## Coming Soon

### Platform

- Japan region availability
- Trellix-F to Trellix IAM migration

### Improved Protection

- Updates to Guest Images

### Management/Reporting

- Export option for Submissions and Alerts
- Set daily/monthly limit for subscriptions

## Exploring

### Improved Protection

- Updates to Guest Images
- Google Suite Support

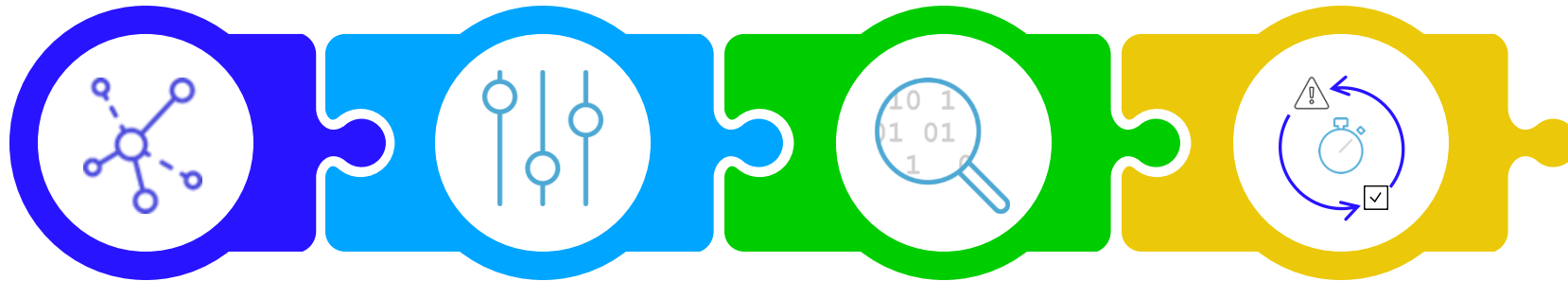
### Integrations

- ServiceNow
- Zoom

### Management/Reporting

- Generic Dashboard improvements
- Quota and key expiration notifications
- User login and submissions audit trail

## NDR Secures your Network at the Speed of the Adversary



### Visibility

- Level 7 Metadata
- Post-compromise
- Anomaly Detections

### Detect & Protect

Multiple detection methodologies aligned to the MITRE Attack framework

### Investigate

- Scope / Scale / Enrich
- Network Investigator
- Event-based packet capture
- Full packet capture

### Respond

- Ability to block traffic
- Isolate endpoints (XDR)
- Update firewall rules (XDR)

# Trellix

## Latest Updates

Network Security





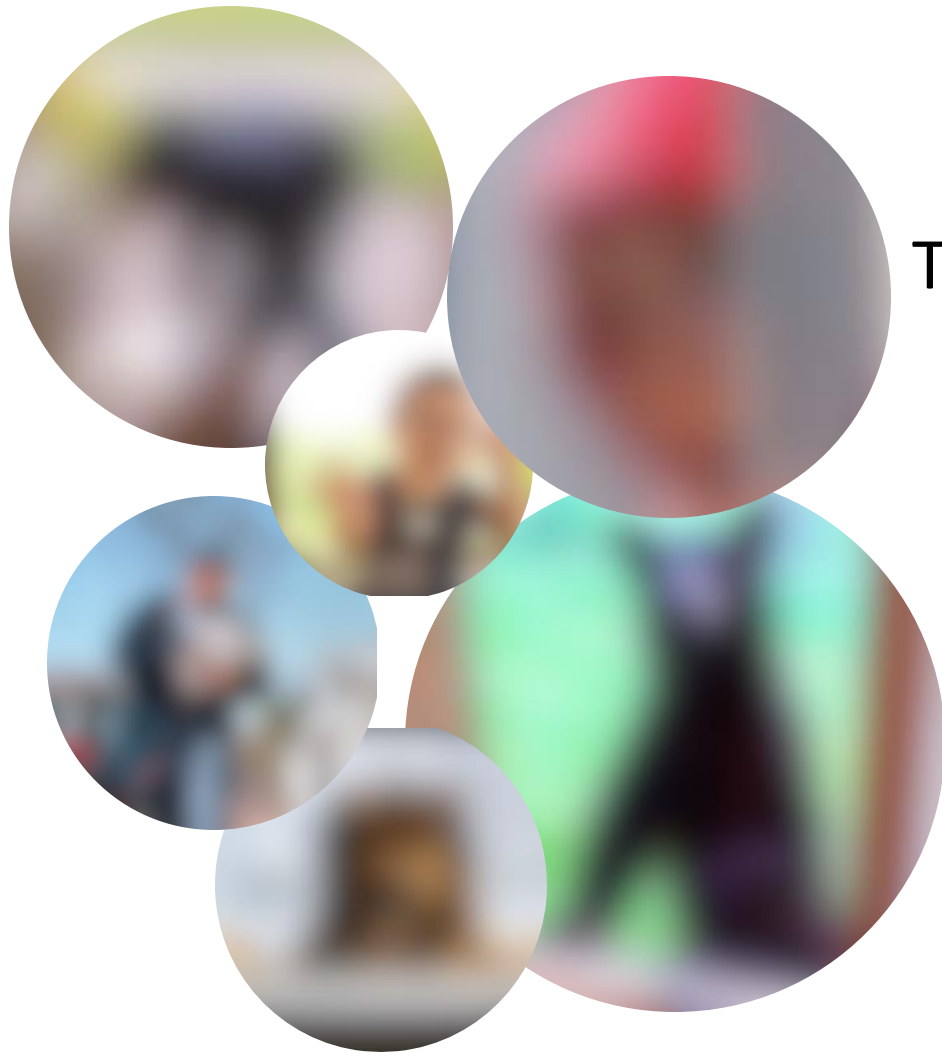
# Trellix

# Welcome!

Partner Tech Summit – Rome

Network Security





## The issue with traditional NDR

- Anomalies are signals – not detection
- Normal always changes – so you must constantly tune
- Time spent investigating inconsequential alerts
- Built for throughput, not deep inspection

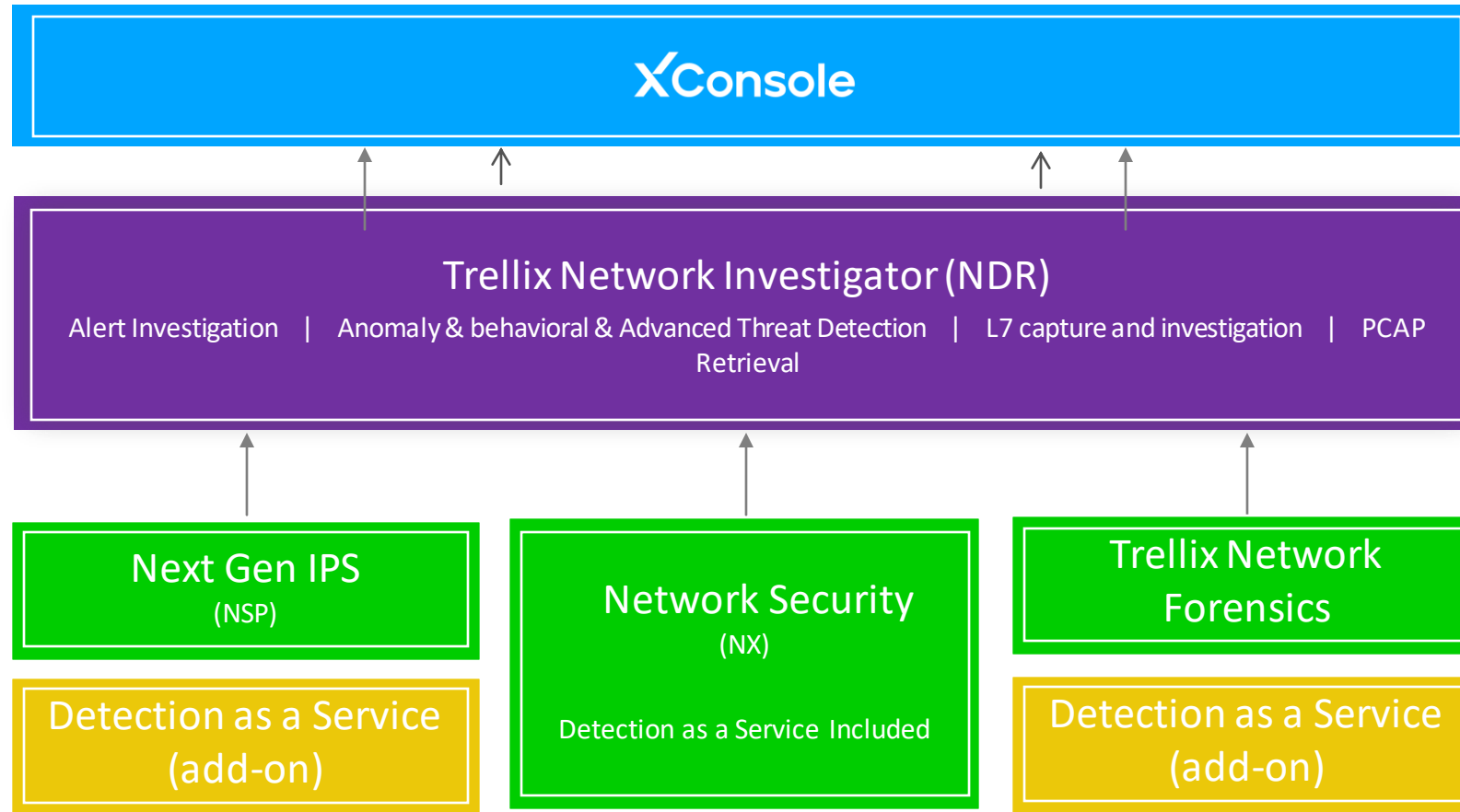


## Deep analysis reveals the threats that matter

- Detection is our founding competency
- Years invested tuning machine learning models
- Continually adapt as threats evolve
- Full, deep packet inspection across multiple threat vectors
- Layer 7 metadata provides additional context for investigation and hunting

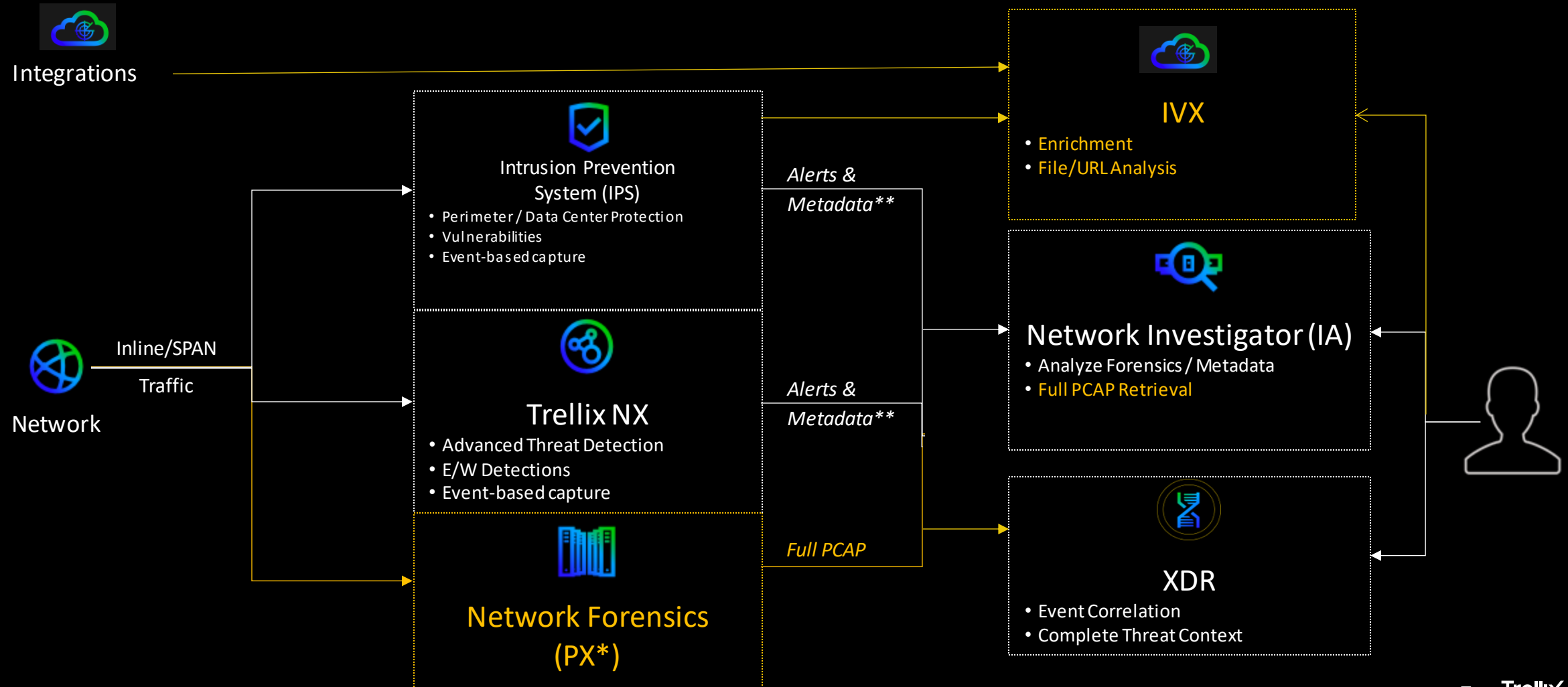
Customers value our high-fidelity alerts

# Bringing a SecOps perspective to NDR



- Leveraging our SecOps and Detection focus
- Consolidation of existing and new ML models in one module
- Supplemented with context decoration, hunting and PCAP acquisition

# NDR Solution Architecture

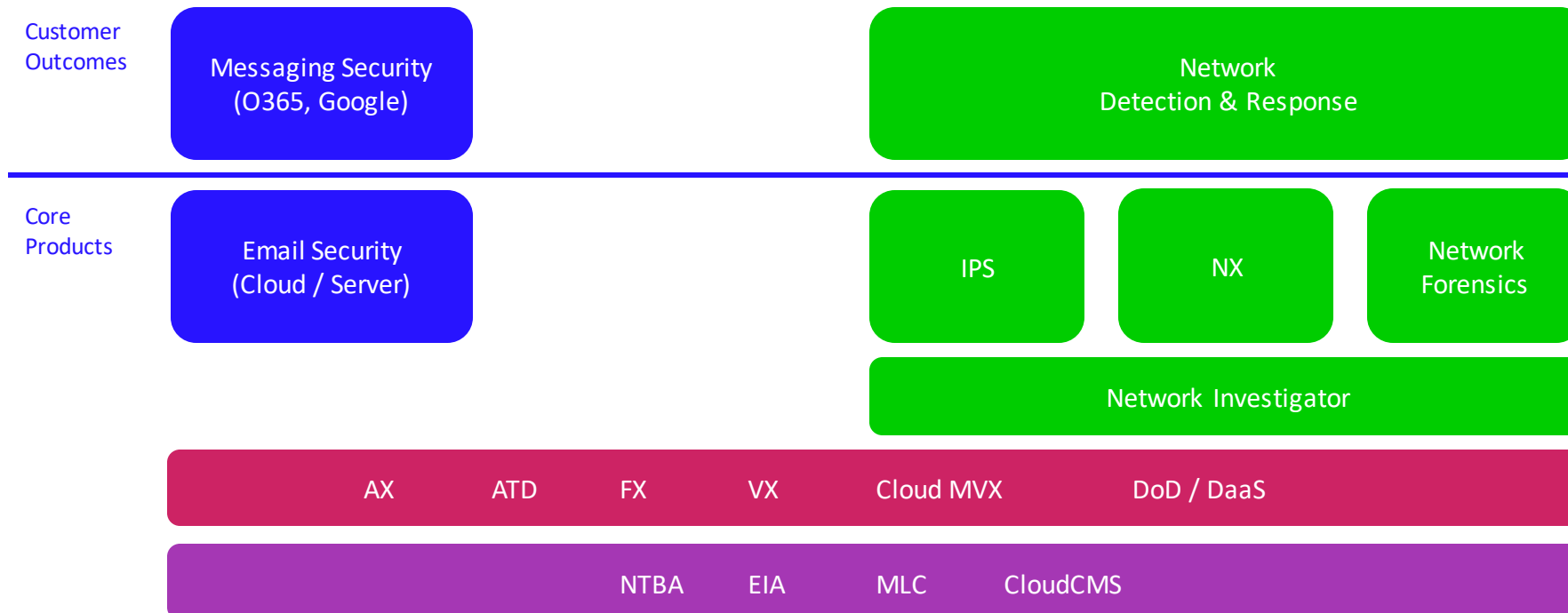


\*Optional Outcome

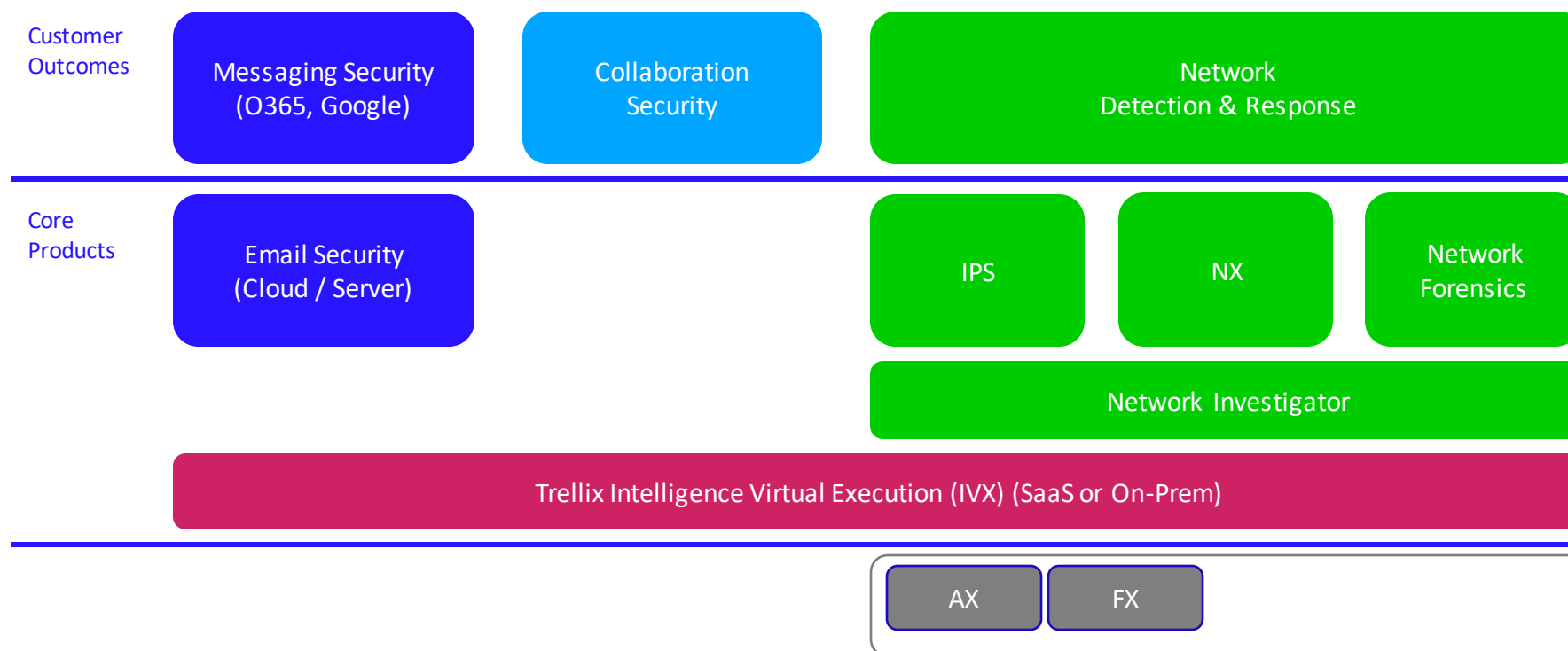
\*\* Metadata from either IPS or NX



# Network + Email Portfolio - Before



# Network + Email Portfolio - NOW



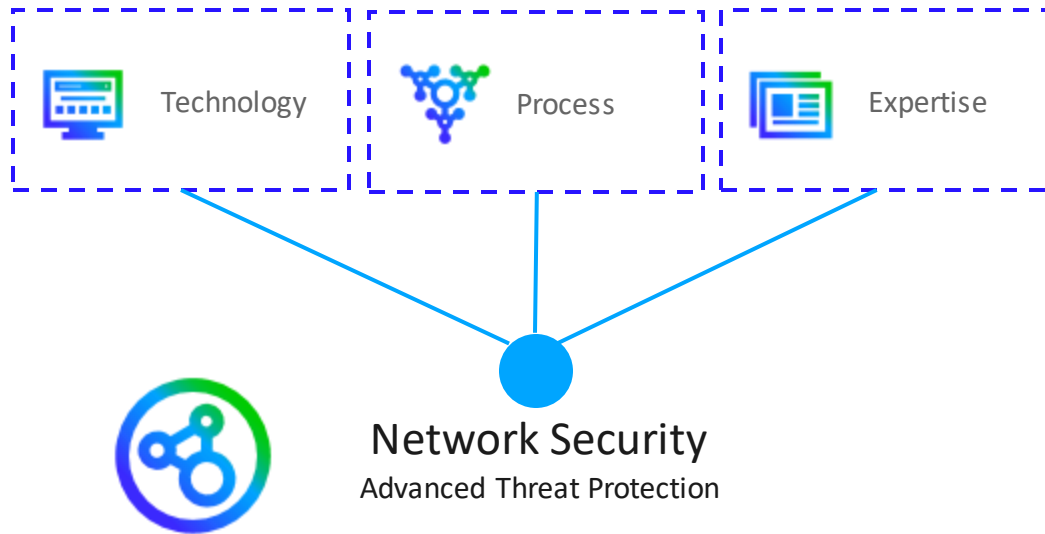
# Trellix

## NDR Components



# Network Security (NX)

# Trellix Network Security at-a-Glance



**Signatureless IVX engine** inspects suspicious objects to identify targeted, evasive and unknown threats

**Codified intelligence** for faster detection and resolution of newfound threats

**Dynamic threat intelligence** protects customers before they are aware a new threat is active

**Flexible deployment model** that scales and grows with your network

**Integrated IPS & SSL Decryption** improves efficiencies, while reducing costs



# Trellix

## IVX

Is this the Sandbox?



# MVX “The Sandbox”

## Trellix Hardened Hypervisor

- Custom hypervisor with built-in countermeasures
- Designed for threat analysis

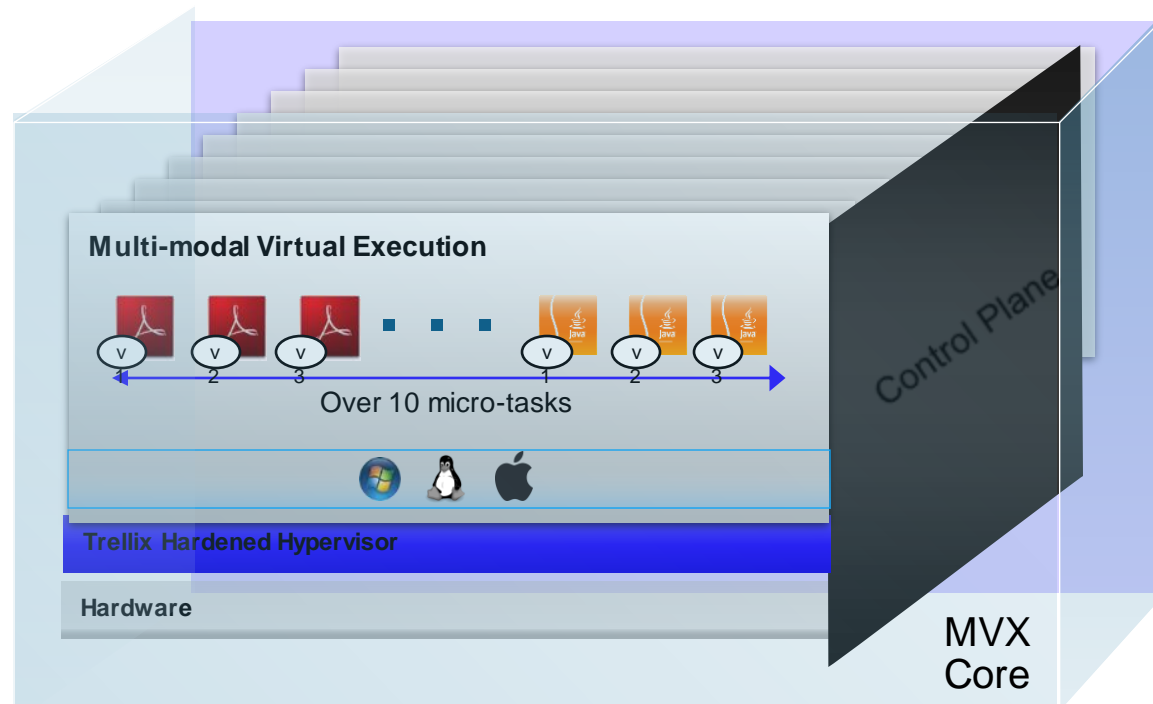
## Multi-modal Virtual Execution

- Multiple operating systems
- Multiple service packs
- Multiple applications
- Multiple file-types

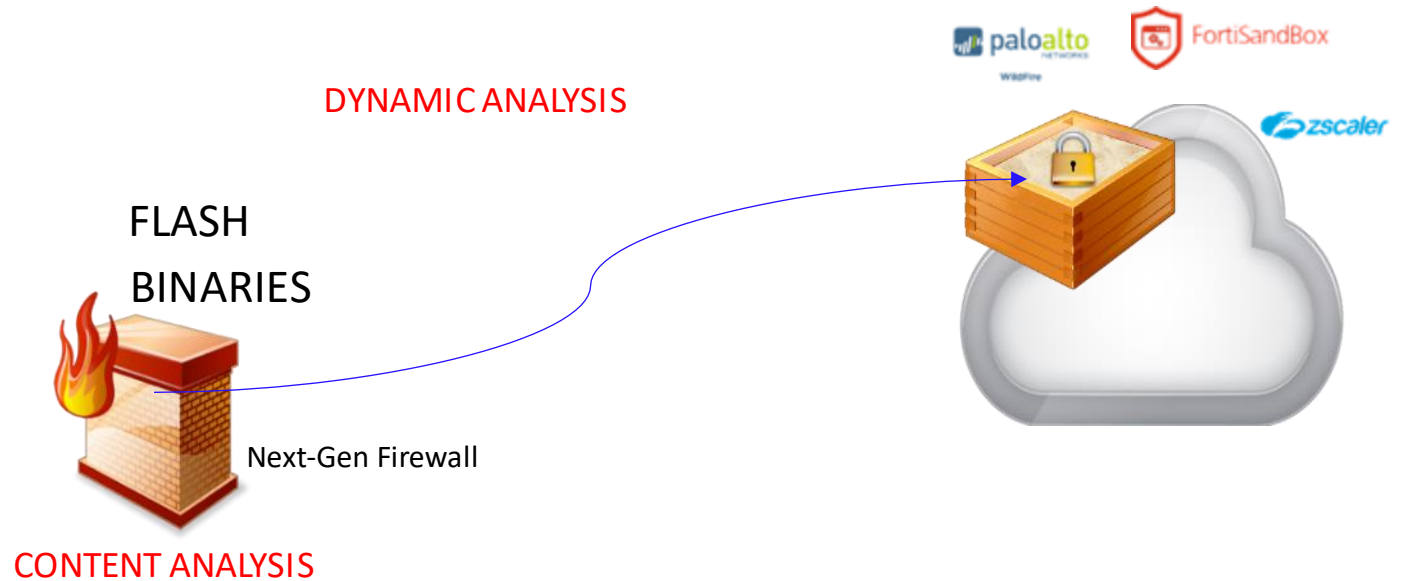
## Threat Protection at Scale

- Over 2000 simultaneous executions
- Multi-stage analysis

Nearly 200 execution environments



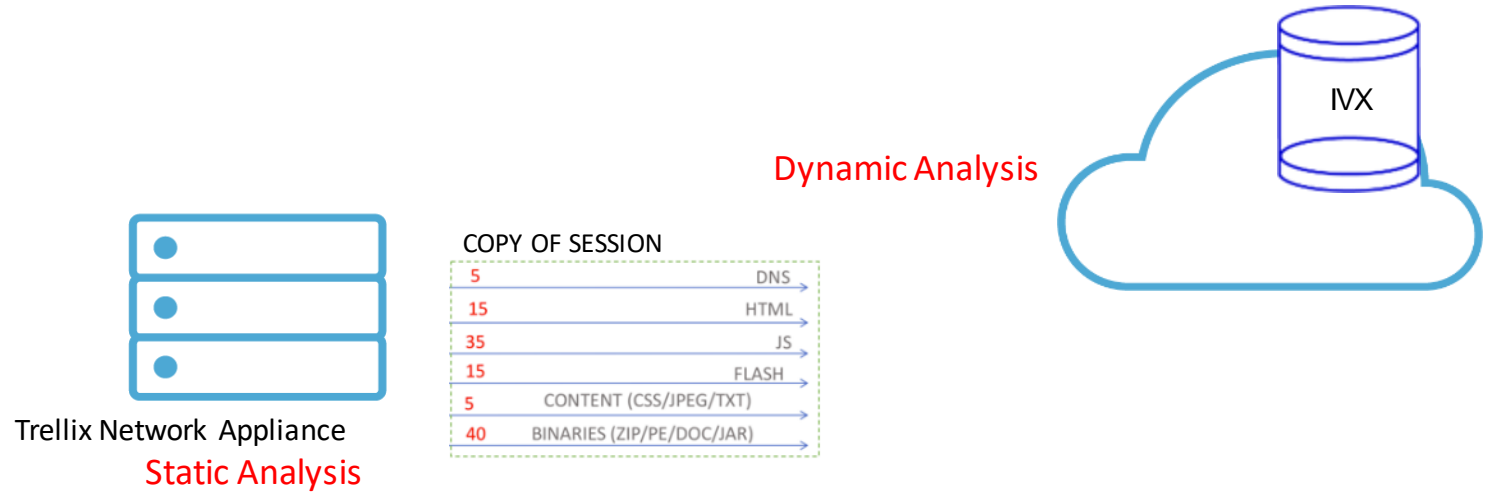
# Single-Flow (File-based) Analysis



- DNS
  - HTML
  - JS
  - FLASH
  - CONTENT (CSS/JPEG/TXT)
  - BINARIES (ZIP/PE/DOC/JAR)
- Blue arrows point from each item to the right, indicating the direction of traffic flow.



# Multi-Flow (Session-based) Analysis



DNS	5
HTML	15
JS	35
FLASH	15
CONTENT (CSS/JPEG/TXT)	5
BINARIES (ZIP/PE/DOC/JAR)	40

Total > 50



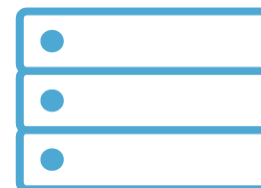
# IPS Difference

*Protecting Vulnerable Assets from Exploits*



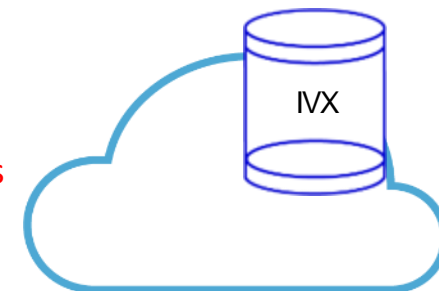
Attack against Vulnerability

---



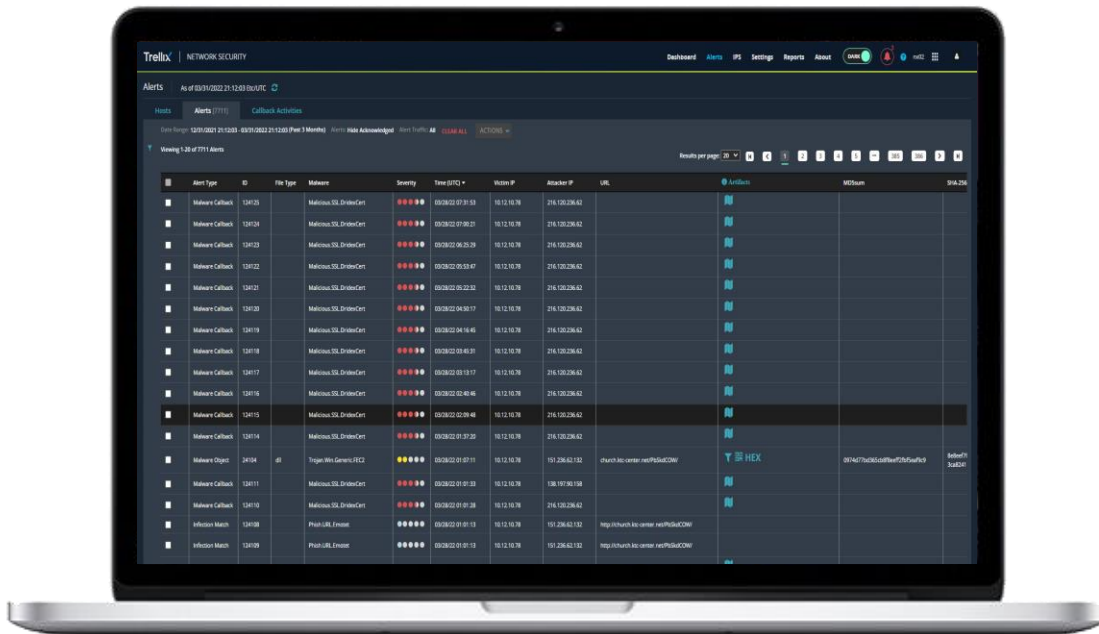
Trellix IPS  
Static Analysis

Dynamic Analysis





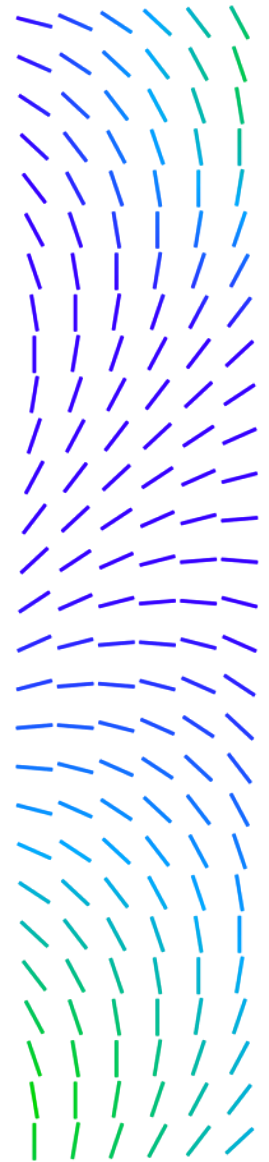
# Trellix Network Security Business Value



**Prevent Malicious Attacks** by catching threats that other solutions miss

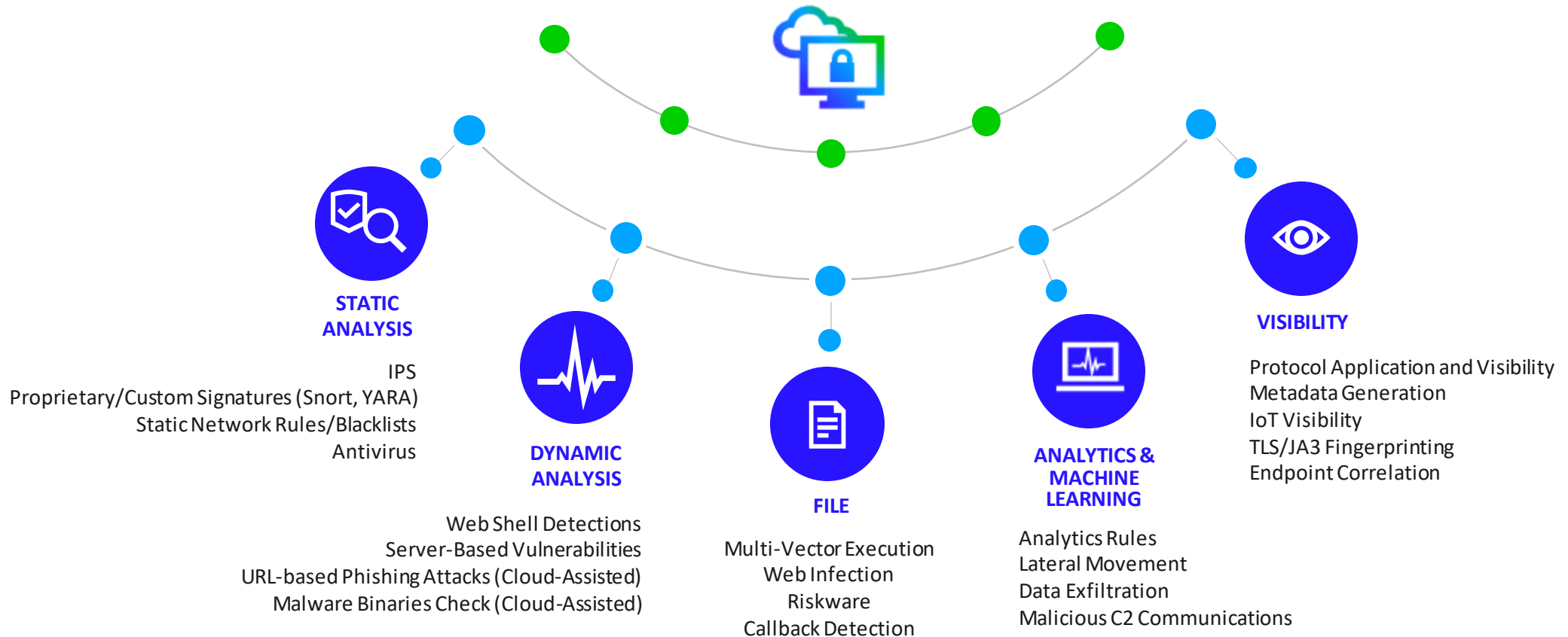
**Reduce Breach impact** by empowering expert decisions supported by multiple, dynamic machine learning, AI and correlation engines

**Improve Security Efficiencies** by eliminating noise and providing the alerts that matter



# Detection and Protection: How Network Security Does It Better

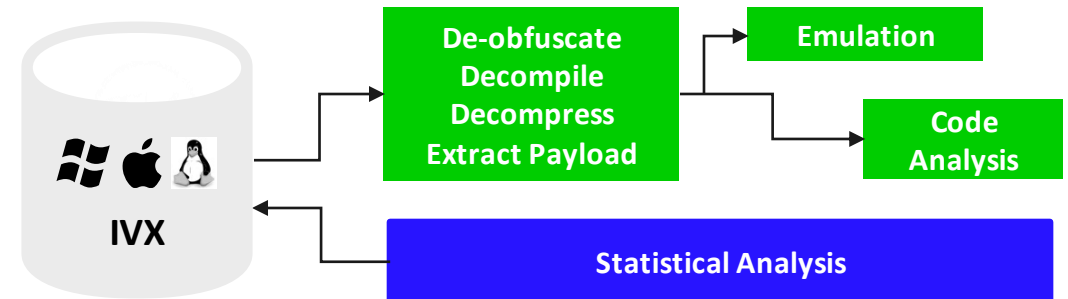
Content Updates – Signatures/ Threat Feeds  
Cloud Assist – Cache for File & URL Analysis  
Cloud Assist – File Sandboxing & Analysis



# Industry-Leading Malware Analysis

Adds a multitude of heuristics, deep code and content analysis, including:

- **Code Analysis:** includes Function analysis and Similarity analysis
- **Statistical Analysis:** includes N-gram analysis and Entropy analysis;
- **Embedded URL analysis capability**
- **Emulation Analysis:** includes Object emulation
- **Global cloud-based analysis** of known and unknown objects.



# SmartVision Lateral Threat Detection

180+ rules for lateral movement detection

Provides full kill chain detection that targets east-west, server-facing deployments

Machine learning framework with data-exfiltration detection

JA3 detection for identifying encrypted communication

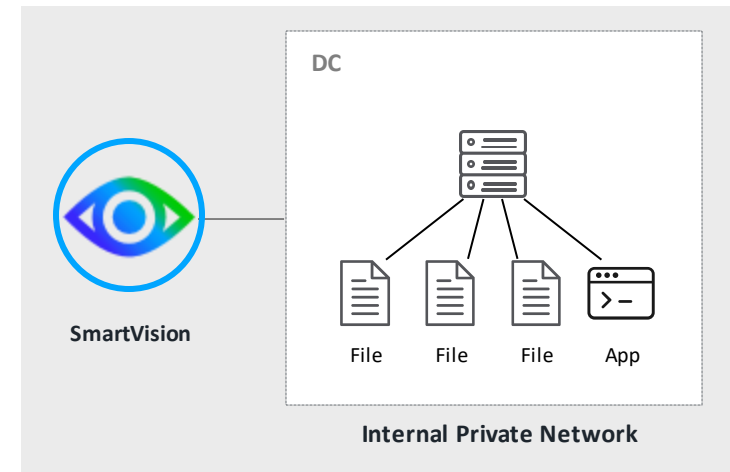
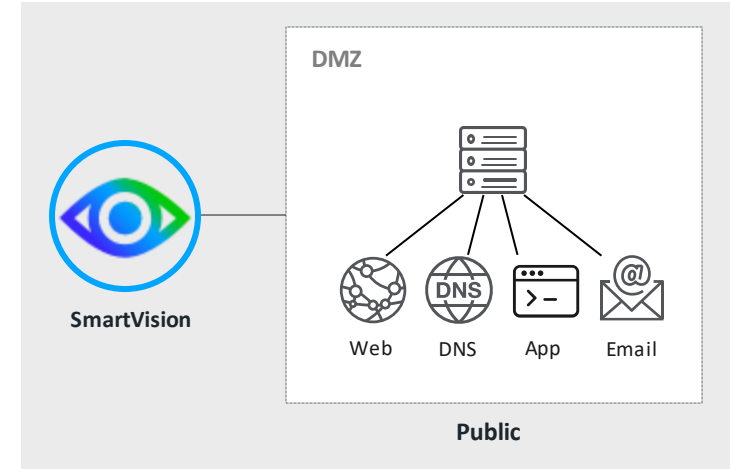
Web shell Detection (visibility into attacks on Webservers)

Lateral movement of malware (MVX detonation)

Provides L7 context around every real-time alert

Map adversarial techniques with the MITRE ATT&CK Framework

Ability to record and capture packets for SmartVision alerts



# SmartVision Techniques

Remote  
user/group/session  
enumeration

Remote share  
enumeration

Detect Mimikatz  
activity generically

NetFlow-based  
detection

Uploads of EXE,  
DLL, MOF files to  
C\$, ADMIN\$, etc.

Remote service  
launch

Remote registry  
service launch or  
access

Remote task  
scheduling via  
ATSVC

SSL/TLS JA3  
Fingerprinting

PsExec Activity

DNS Zone Transfer

WMI Remote Shell  
Launch



# Yes, there is a light IPS onboard NX:

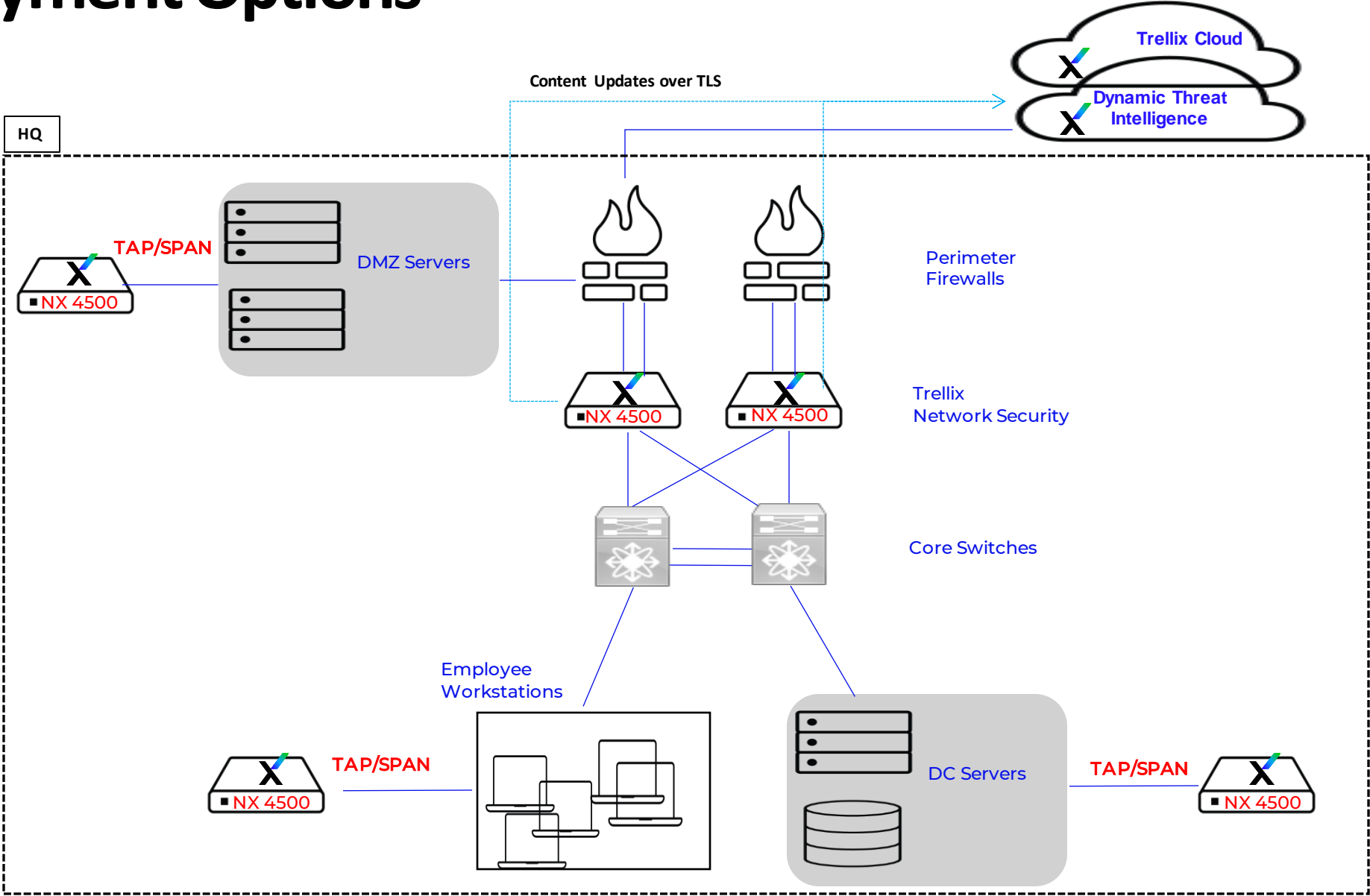
## Compliance Checkbox

- IPS – Single Packet detection – Low Fidelity
- IPS / IVX Confirmed – Single + IVX detonation – Higher Fidelity

<input type="checkbox"/>	06/02/22 20:01:44	10.12.10.41	10.12.12.15	●●●●●	15	Possible DCSync Detected	exploit	UNKNOWN	
<input type="checkbox"/>	05/18/22 08:03:02	10.12.21.12	10.12.19.134	●●●●●	28	Nmap Scanner Traffic Detected	recon	HTTP	
<input type="checkbox"/>	05/18/22 08:01:05	10.12.21.12	10.12.19.134	●●●●●	1	Scanning Activity - Nmap, SMB	other	SMB	
<input type="checkbox"/>	05/17/22 04:09:35	10.12.11.181	10.12.250.105	●●●●●	1	Malicious File Transfer - Mimikatz, Retrieval via Script	exploit	HTTP	
<input type="checkbox"/>	05/17/22 04:01:25	10.12.11.181	10.12.250.105	●●●●●	1	Malicious File Transfer - Mimikatz, Retrieval via Script	exploit	HTTP	<b>MVX</b>

*Use Trellix IPS for strict IPS & Data Center Protection*

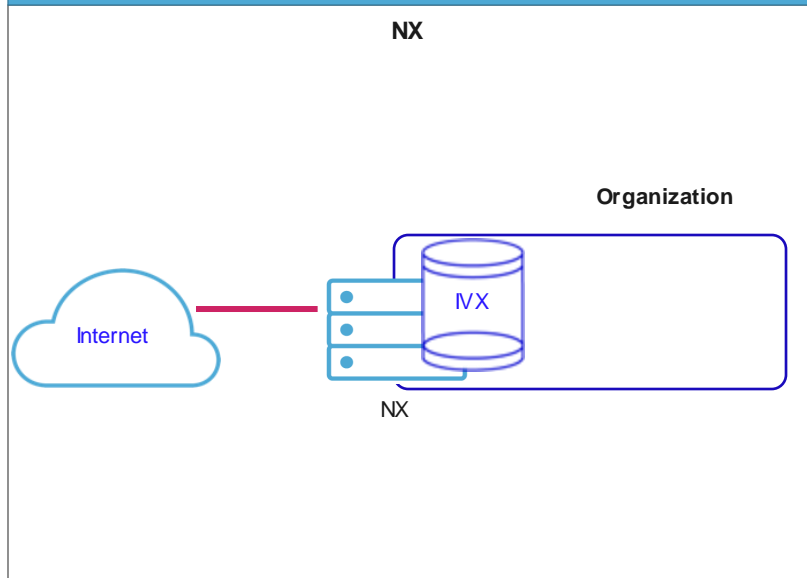
# Deployment Options



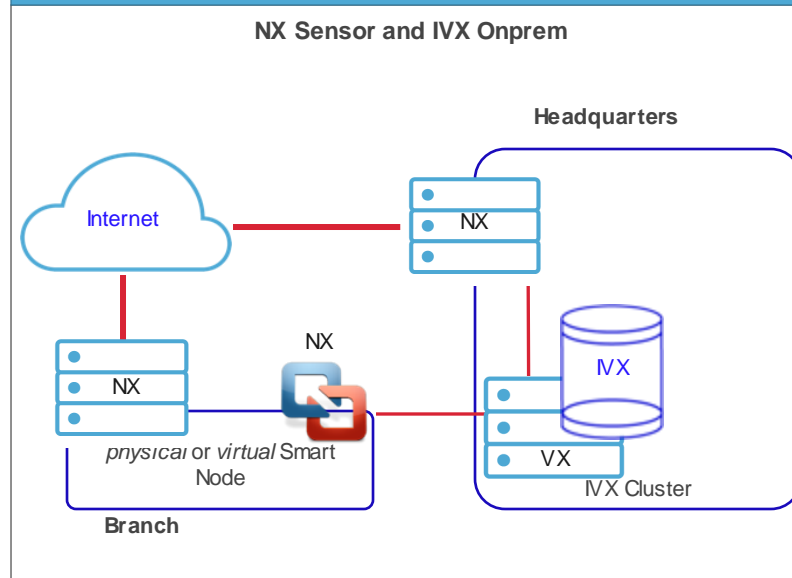
# NX Deployments Architectures

- Hardware Integrated
- Hardware / Virtual IVX-Onprem
- Hardware / Virtual IVX-Cloud
- Public Cloud (AWS / Azure)
- SaaS (iboss + Trellix)

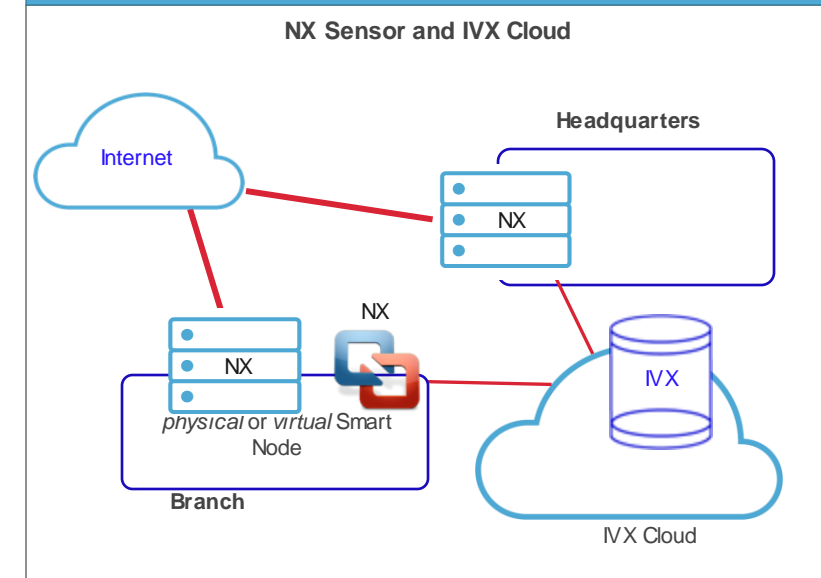
## Integrated Appliances



## Distributed with IVX Onprem

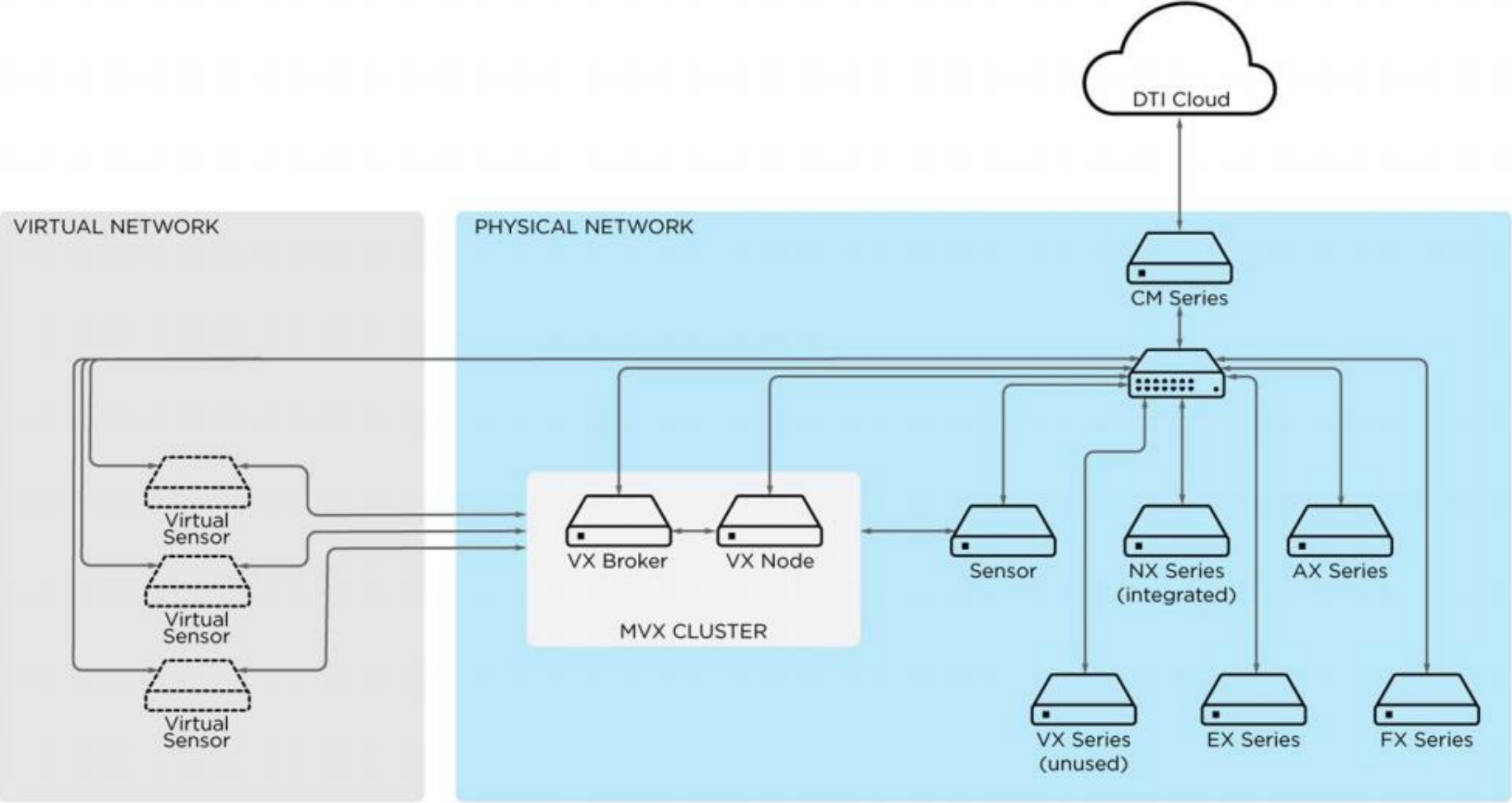


## Distributed with IVX Cloud



# IVX Separation

## VX Architecture (On-Prem)



# SmartVision Lateral Threat Detection

180+ rules for lateral movement detection

Provides full kill chain detection that targets east-west, server-facing deployments

Machine learning framework with data-exfiltration detection

JA3 detection for identifying encrypted communication

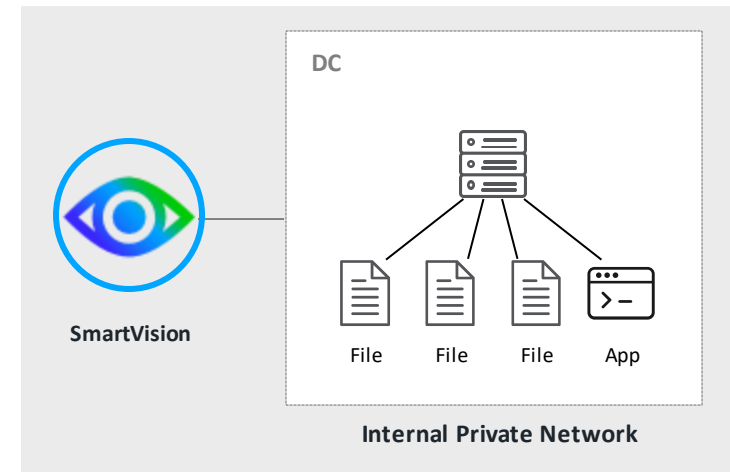
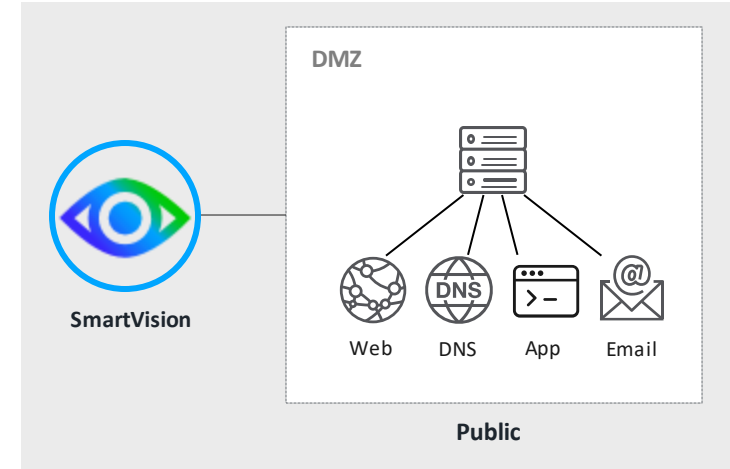
Web shell Detection (visibility into attacks on Webservers)

Lateral movement of malware (MVX detonation)

Provides L7 context around every real-time alert

Map adversarial techniques with the MITRE ATT&CK Framework

Ability to record and capture packets for SmartVision alerts



# SmartVision Techniques

Remote user/group/session enumeration

Remote share enumeration

Detect Mimikatz activity generically

NetFlow-based detection

Uploads of EXE, DLL, MOF files to C\$, ADMIN\$, etc.

Remote service launch

Remote registry service launch or access

Remote task scheduling via ATSVCS

SSL/TLS JA3 Fingerprinting

PsExec Activity

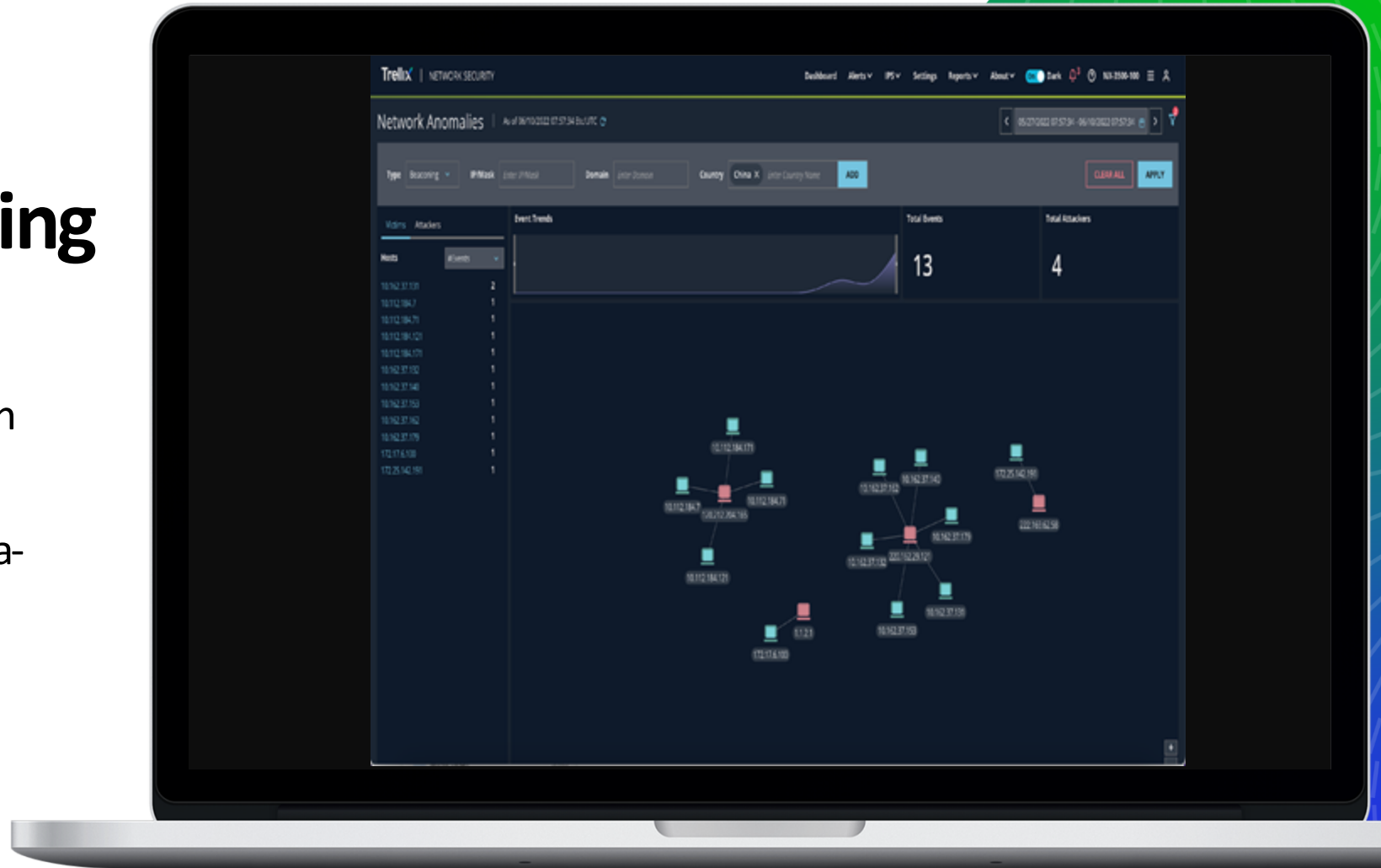
DNS Zone Transfer

WMI Remote Shell Launch



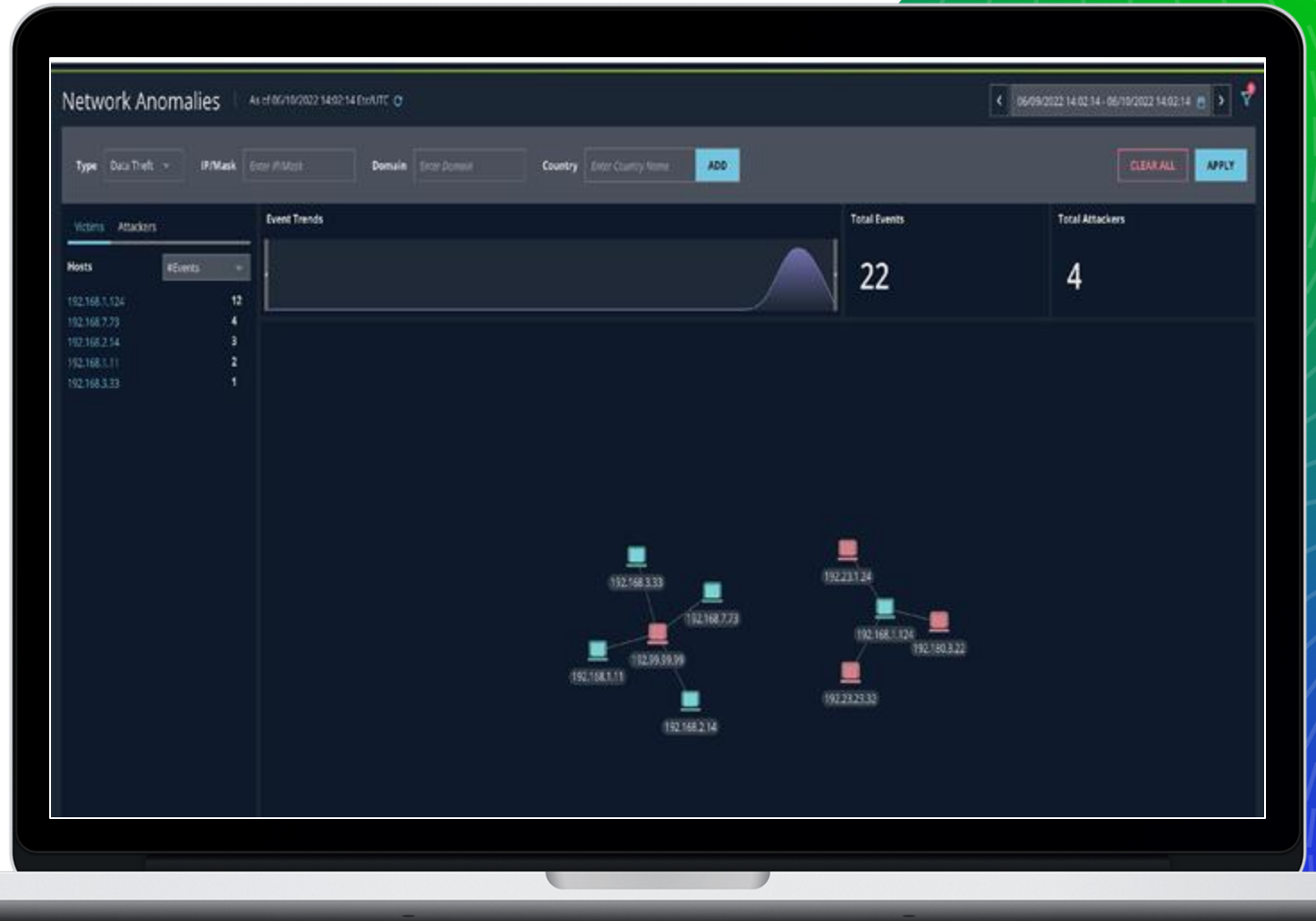
# Using ML to Detect Beaconing

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



# Using ML to Detect 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



# MITRE Alert Mapping

The screenshot shows the FireEye Network SmartVision dashboard. The top navigation bar includes 'NETWORK SECURITY', 'DASHBOARD', 'ALERTS', 'SETTINGS', 'REPORTS', and 'ABOUT'. The main content area displays a list of alerts. A table below the list shows detailed alert information:

ID	NAME	TYPE	ARTIFACTS	TIME	SOURCE IP (PORT)	DESTINATION IP (PORT)
97	Sysinternals PsExec Activity	T1035 / PsExec Activity	N/A	11/13/19 20:53:01	192.168.31.135 (49367)	192.168.31.163 (445)
96	Sysinternals PsExec Activity	T1035 / PsExec Activity	N/A	11/13/19 20:53:00	192.168.31.135 (49367)	192.168.31.163 (445)
94	Sysinternals PsExec Activity	T1035 / PsExec Activity	ASSOCIATED FILE ANALYSIS	11/13/19 20:52:59	192.168.31.135 (49367)	192.168.31.163 (445)

The popup window, titled 'Mitre Att&ck Mapping', displays 'MITRE ATT&CK™ details' for the 'Initial Access' category. The specific technique shown is 'Execution through API' (T1106).

**Execution through API**  
T1106

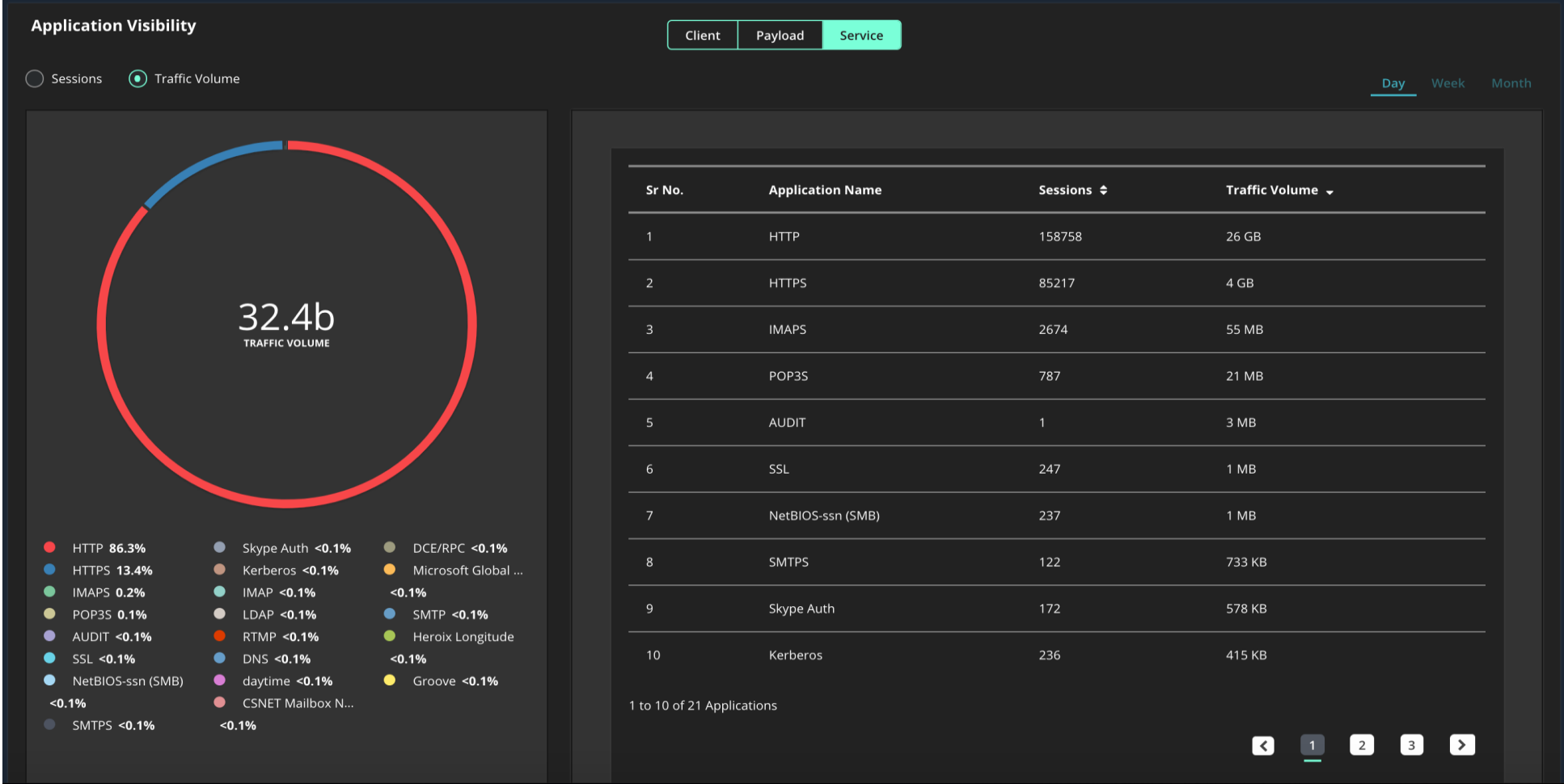
Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters. (Citation: Microsoft CreateProcess) Additional Windows API calls that can be used to execute binaries include: (Citation: Kanthak Verifier) \* CreateProcessA() and CreateProcessW(), \* CreateProcessAsUserA() and CreateProcessAsUserW(), \* CreateProcessInternalA() and CreateProcessInternalW(), \* CreateProcessWithLogonW(), CreateProcessWithTokenW(), \* LoadLibraryA() and LoadLibraryW(), \* LoadLibraryExA() and LoadLibraryExW(), \* LoadModule(), \* LoadPackagedLibrary(), \* WinExec(), \* ShellExecuteA() and ShellExecuteW(), \* ShellExecuteExA() and ShellExecuteExW()

**Rules Hit**

- Executable file created in suspicious location ; Process creating executable file in suspicious location

**MITRE Mapping to Alerts with details**  
[Map Alerts to MITRE ATT&CK: https://attack.mitre.org/matrices/enterprise/](https://attack.mitre.org/matrices/enterprise/)

# Application Visibility



**Dashboard view of Top Applications seen on Network  
(Client-side browsers, applications along with network usage)**

# Evidence Collector – Xconsole/XDR Integration

Whitelists

Notifications

Network

Custom Rules

YARA Rules

Riskware Policy

SmartVision Configuration

Guest Images

Certificates/Keys

SSL Intercept

Port Mirroring

ICAP

**Evidence Collector**

3rd Party Feeds

Appliance Backup & Restore

Appliance Licenses

Login Banner

Commbroker configuration removed successfully.

Input Type: syslog

Interface: ether1  
IP Address: 10.128.45.95

Protocol: TCP

Port:

ADD

Configuration List

Input Type	Interface	Protocol	Port	Action
syslog	ether1 (IP Address: 10.128.45.95)	SSL	514	

SSL Certificate Configuration | This configuration is mandatory for SSL protocol.

Server Certificate: web-cert\_new\_ssl

Root CA Certificate: rootCA\_cb\_new

Did not find certificate? [Add Certificate](#)

Require Client Certificate ⓘ

Allow Untrusted Client Certificate ⓘ

UPDATE

Enable Settings

OFF Tapsender

ON Commbroker

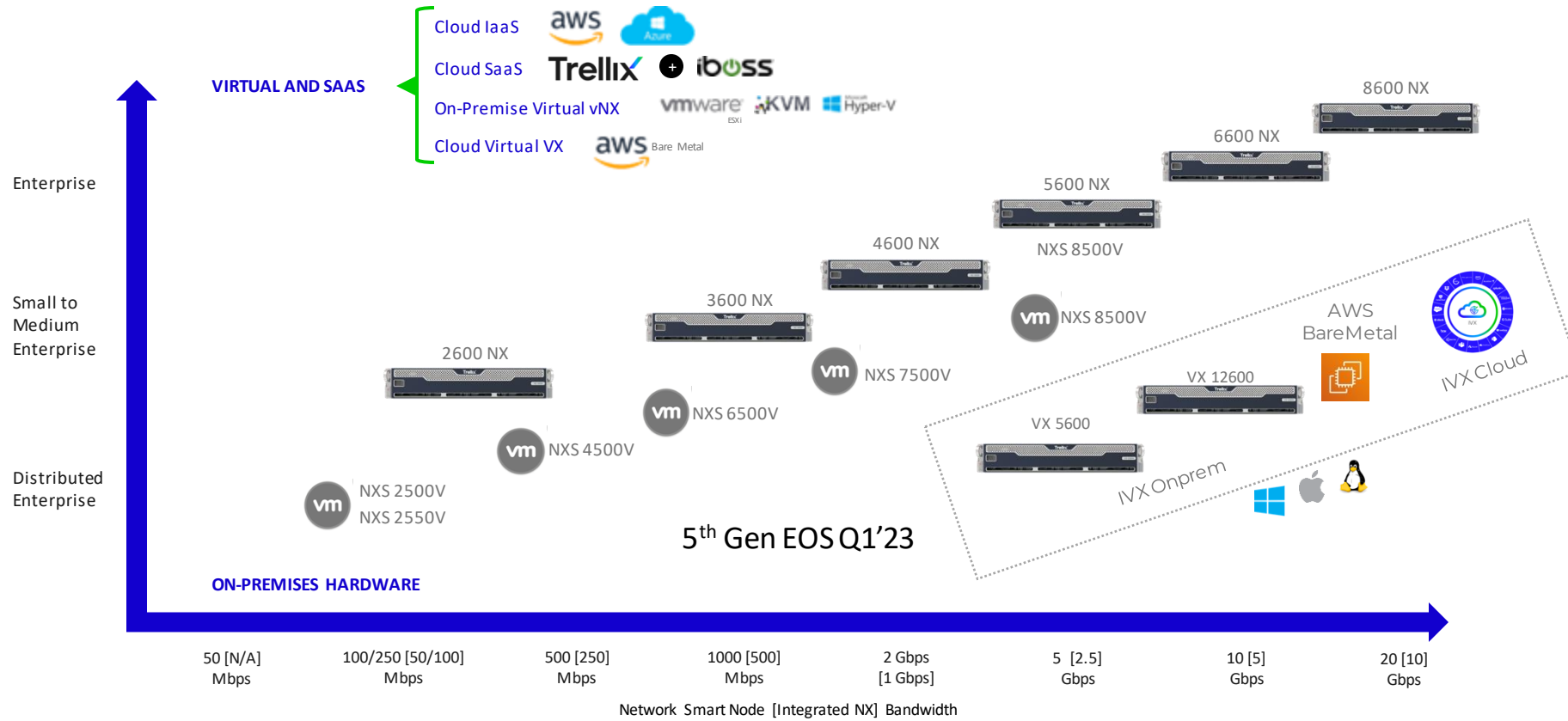
## More than a threat detection sandbox



- Riskware
- SSL Intercept
- TLS Fingerprinting
- Beaconing Detection
- Phishing Detection
- Data Exfil Detection
- Call back detection
- IoT Detection
- Webshell Detection
- IPS (for “compliance only”)
- Lateral Movement
- Metadata generation



# Trellix NX Scale and Flexible Deployment Options



# NX Sizing

```
Cumulative Stats in timespan 2018-12-15 15:58:48 to 2018-12-16 15:58:48
Submissions : Total : Rate/minute
Submissions(url) : 0 : 0.000
Submissions(file) : 6 : 0.004
```

## By Throughput

- Sensor mode is double Integrated

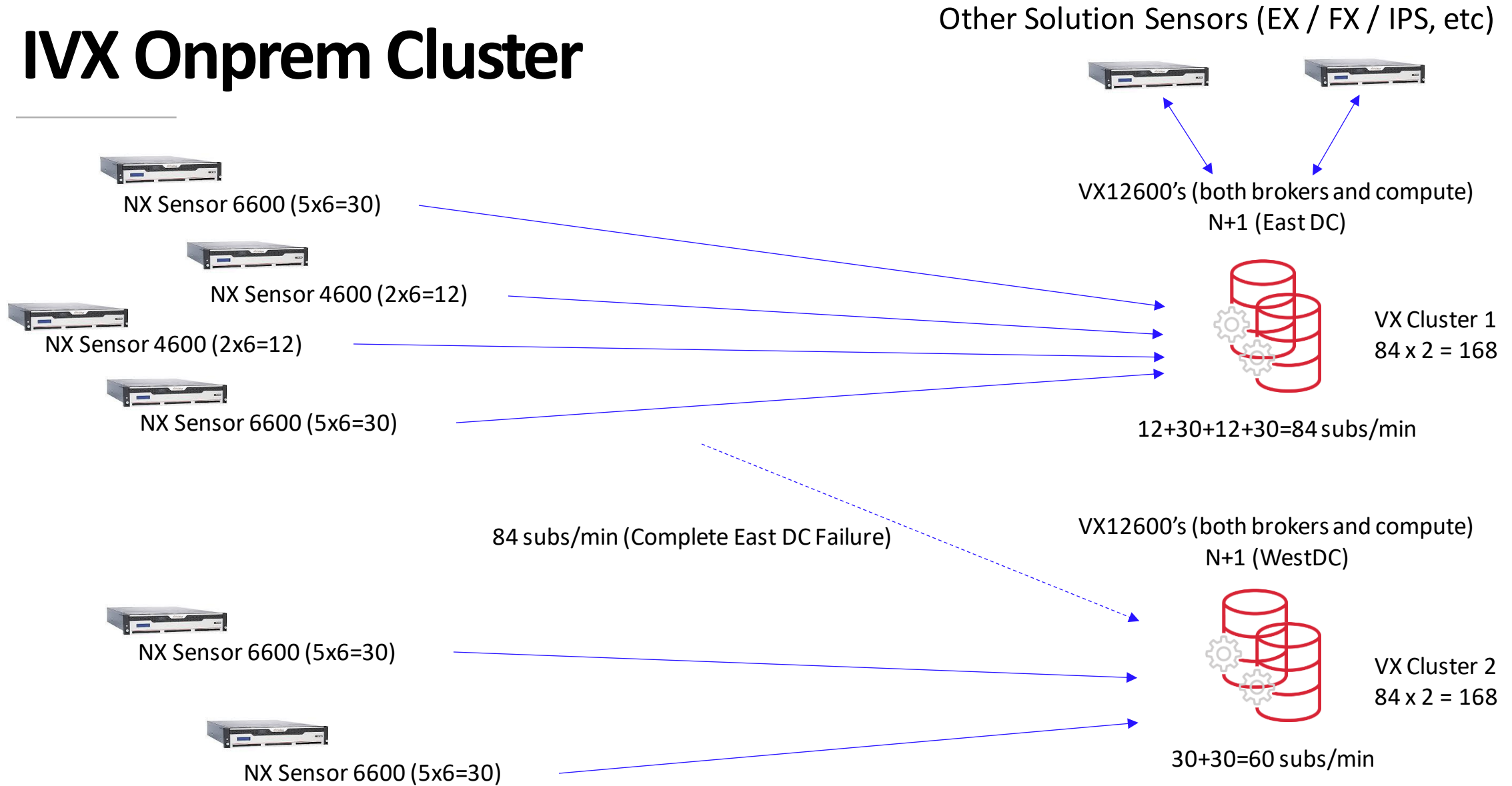
### Submissions

- show submissions
- Spec BW \* 6 = MaxSubmissions

### IVX Onprem

- True HA is 3 VX appliances
- At least 2 VX's should run as brokers.
- VX 5600 = 11 Subs/min
- VX 12600 = 84 subs/min
- Example – NX4600 in Sensor mode is 2 Gigs.  $2 \times 6 = 12$ .
  - 7 NX 4600's per VX126000 (max utilization, no geo HA considered)

# IVX Onprem Cluster



# Sizing Continues

SmartVision is a ~20% hit when not in dedicated SV mode.

- Ie. NX4600 sensor is now 1.6 Gigs instead of 2.

Evidence Collector ~ 5-10%

- Comm Broker alone 0% hit. Just syslog on mgmt.

SSLi

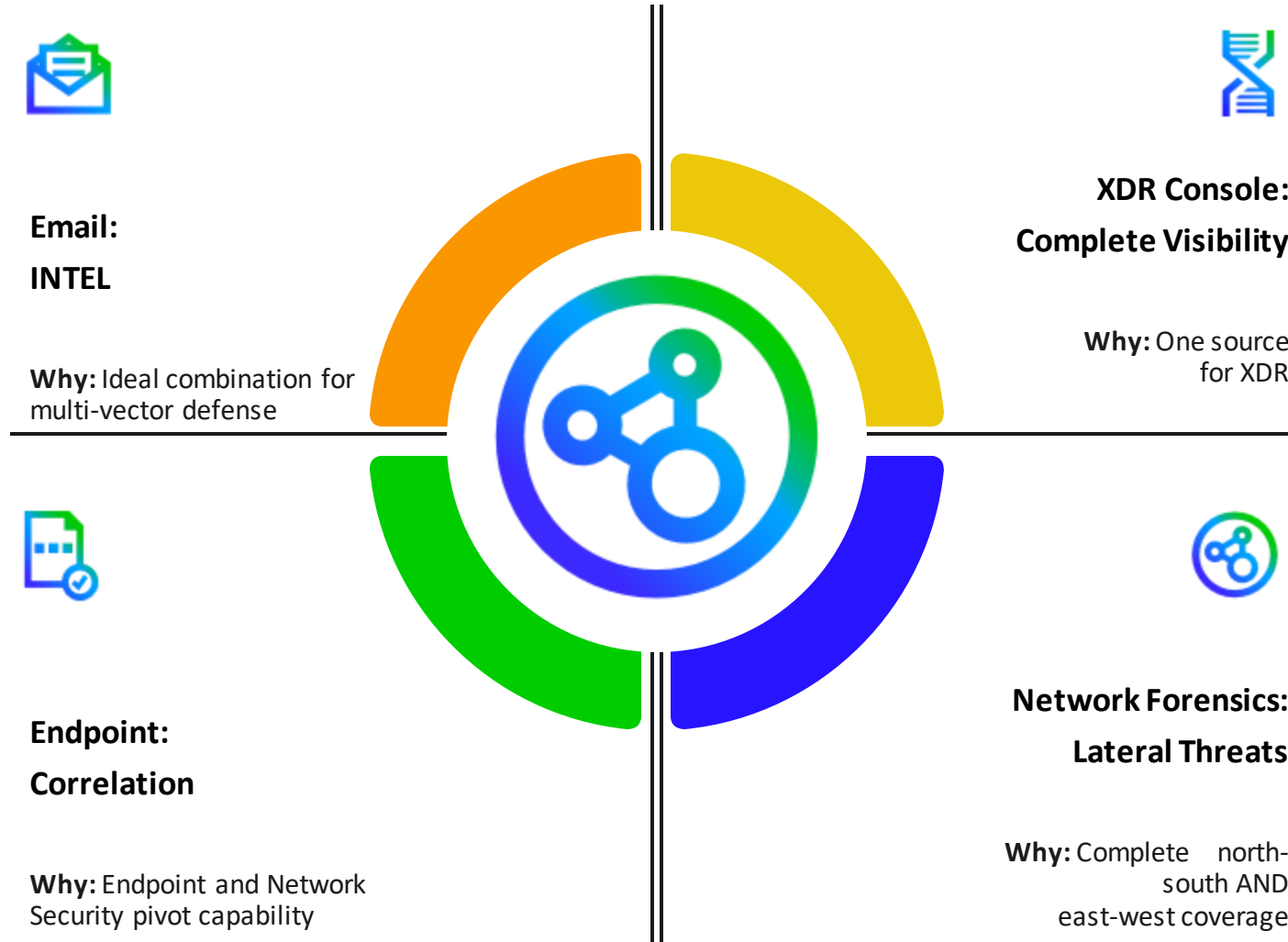
- Hit varies
- On integrated NX4600 (100% SSL is a 50% hit.)
- Not platinum coated SSLi (meant for smaller sites, Enterprise SSLi decrypt sandwich should be considered)

Unified Sizing guided located on Charepoint or siesmic

# SSL Sizing

NX HW & Mode	Rated HTTP Throughput	100% HTTPS Recommendations	100% HTTPS perf as % of rated HTTP	50% HTTPS
2500 int	100 Mbps	80 Mbps	80%	HTTPS: 40Mbps , HTTP: 60Mbps
2500 sensor	250 Mbps	200 Mbps	80%	HTTPS: 100 Mbps , HTTP: 150 Mbps
2550/ 2600 int	250 Mbps	200 Mbps	80%	HTTPS: 100 Mbps , HTTP: 150 Mbps
2550/ 2600 sensor	500 Mbps	400 Mbps	80%	HTTPS: 200 Mbps , HTTP: 300 Mbps
35/3600 int	500 Mbps	400 Mbps	80%	HTTPS: 200 Mbps, HTTP: 300 Mbps
35/3600 sensor	1 Gbps	400 Mbps	40%	HTTPS: 200 Mbps , HTTP: 700 Mbps
45/4600 int	1 Gbps	500 Mbps	50%	HTTPS: 250 Mbps, HTTP: 750 Mbps
45/4600 sensor	2 Gbps	1Gbps	50%	HTTPS: 500 Mbps, HTTP: 1.5 Gbps
55/5600 int	2.5 Gbps	1 Gbps	40%	HTTPS: 500 Mbps, HTTP: 2 Gbps
55/5600 sensor	5 Gbps	2 Gbps	40%	HTTPS: 1 Gbps, HTTP: 4 Gbps
65/6600 int	5 Gbps	1.5 Gbps	30%	HTTPS: 750 Mbps, HTTP: 4.25 Gbps
65/6600 sensor	10 Gbps	3 Gbps	30%	HTTPS: 1.5 Gbps, HTTP: 7Gbps
8600 int	10 Gbps	3.8 Gbps		
8600 sensor	20 Gbps	8 Gbps		
10550 int	4 Gbps	2 Gbps	50%	HTTPS: 1Gbps HTTP: 3Gbps
10550 sensor	8 Gbps	4 Gbps	50%	HTTPS: 2Gbps HTTP: 6 Gbps

# Integrations with Other Trellix Solutions

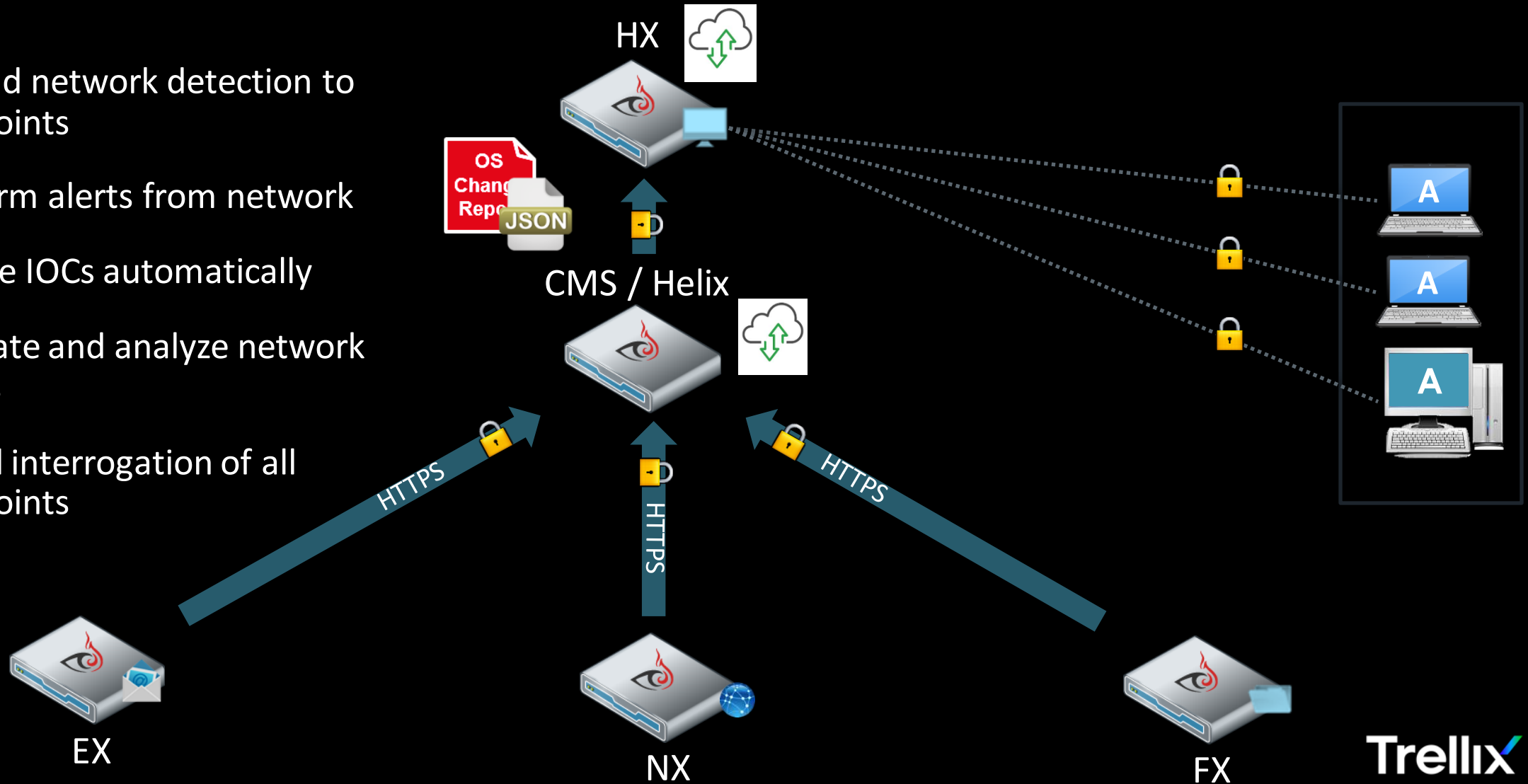




# Integration / Correlation with other Trellix Technologies

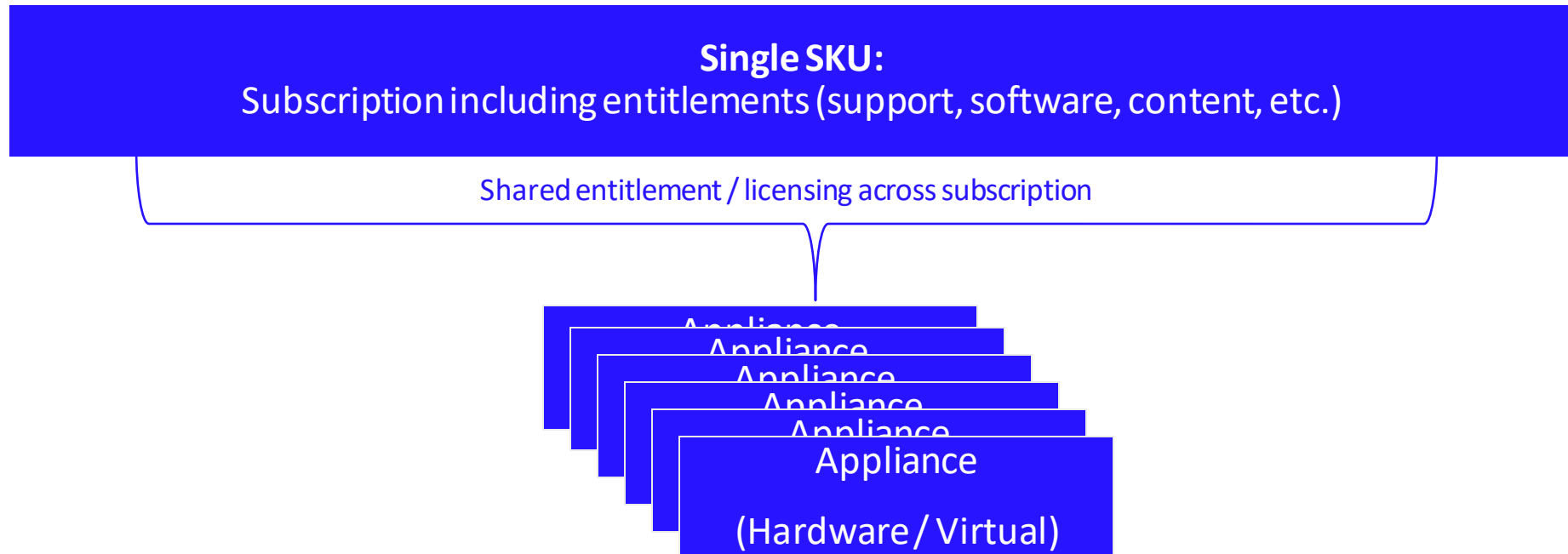
## Detect and Validate

- Extend network detection to endpoints
- Confirm alerts from network
- Create IOCs automatically
- Validate and analyze network alerts
- Rapid interrogation of all endpoints



# Overview of Hermes

- Subscription based pricing
- Buy what you plan to use vs. buy full capacity of appliance
- Usage “floats” over the account rather than being fixed to an appliance
  - Customer uses investment 24x7 rather than business hours of time zone deployed
  - Think **Family Share Plan** concept
- Separates entitlement and hardware value



# Plan per Device vs. Family Share Plan

(Classic/Capacity) | (Subscription/Consumption)

CELL SUBSCRIPTION

Aggregate Bill = \$180

2GB  
\$60

2GB  
\$60

2GB  
\$60



Per Phone Cost = \$799

CELL FAMILY SHARE SUBSCRIPTION

10 Gg - Family Share Plan = \$140

\$80

\$30

\$30



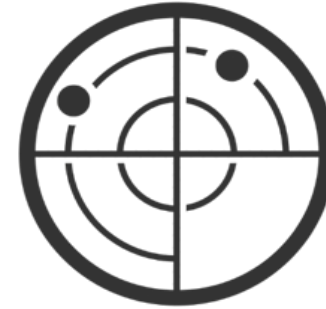
Per Phone Cost = \$140

# Network Security - Forensics

# Packet Capture (PX) and Investigation Analysis (IA) Relationship



- ◆ Packet Capture (PX) – a “Security Camera” to record and replay network traffic and flows



- ◆ Investigation Analysis (IA) – a source to manage multiple “security cameras” and rewind to view what led to the event, correlate events, and ask questions

# Network Forensics (PX)

## Key Features

**Up to 20Gbps** Continuous Lossless Packet Capture



**Intelligent Capture** for selective filtering



**Real-time indexing** of flow and connection metadata



**Ultra Fast Search** of indexed metadata



**Cost Effective Storage** Expansion options



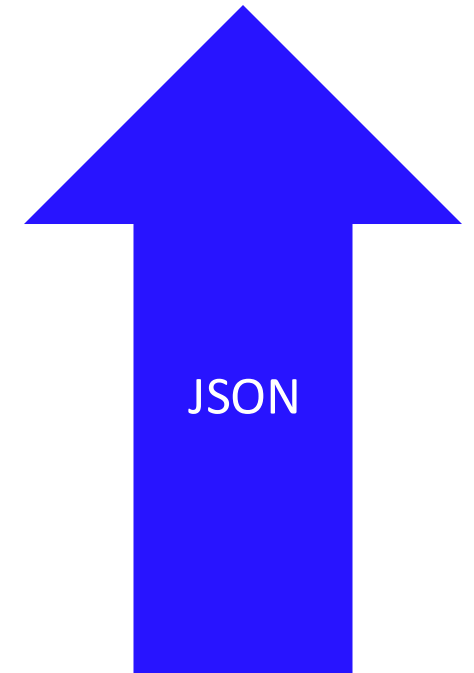
# IA and PX Functional Relationship

IA

- Central Search Across PXs and IAs
- Fast Search up to Layer 7
- Flow and Layer 7 Records
- Enhanced Visualization
- API with pivot to any PX

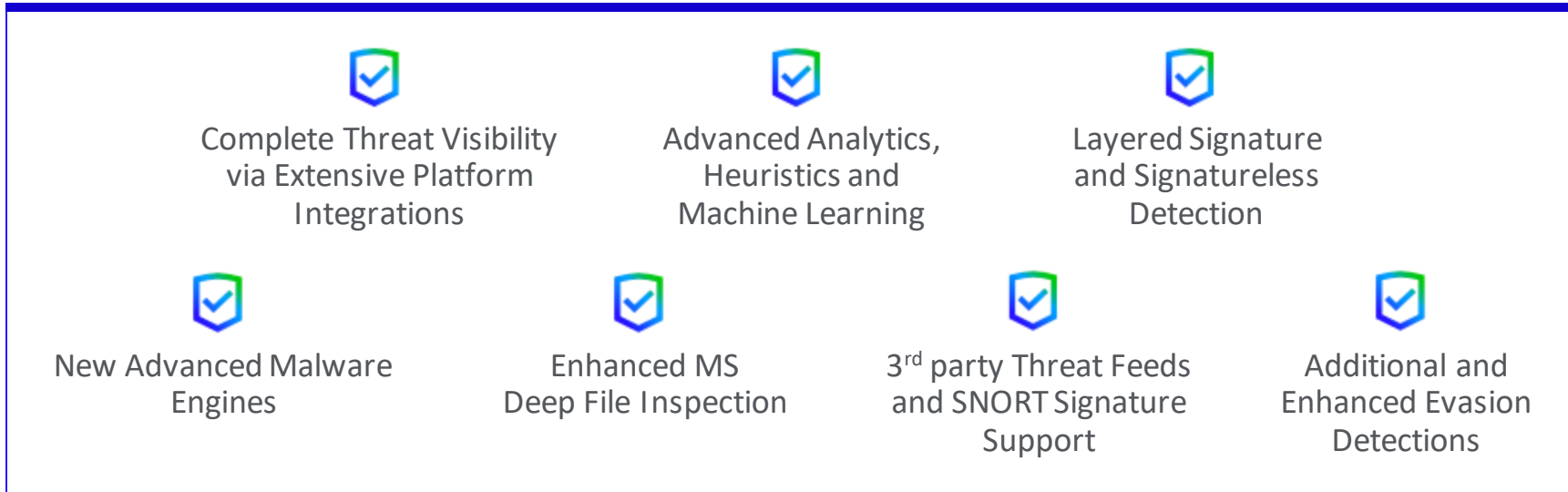
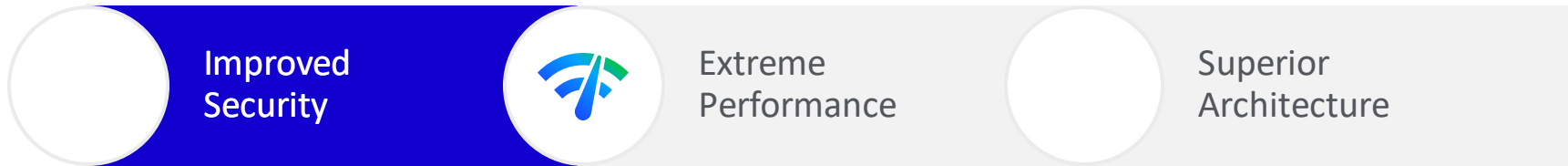
PX

- PCAP
- Fast Search up to L4
- API
- Limited Session Reconstruction




















# Network Security - IPS



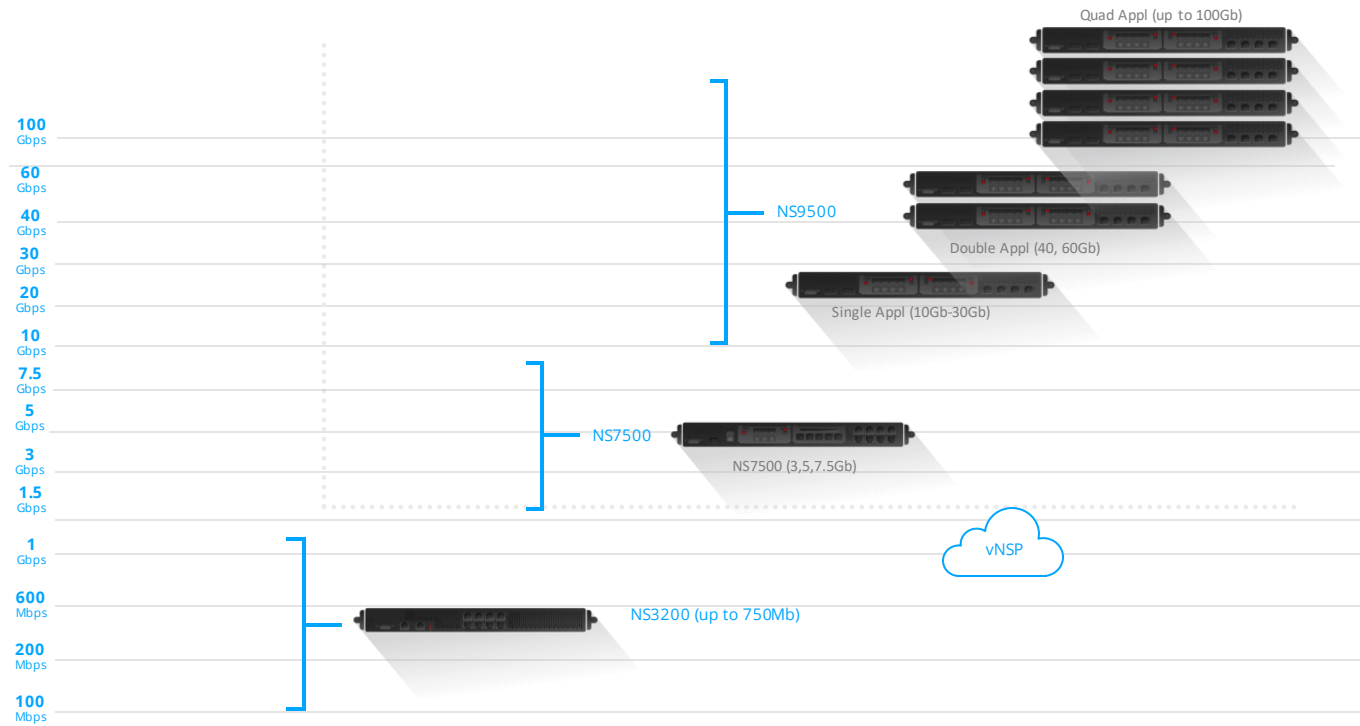
Improved Security    Extreme Performance   Superior Architecture

 100% SSL Traffic Visibility (Inbound & Outbound)	 Dynamic Key Support	 L7 Visibility and Analytics	
 Up to 100Gbps IPS Throughput	 Active Failover	 Built-in Passive Failover	 High Availability

Improved Security  Extreme Performance  Superior Architecture

-   
100Gbps Throughput
-   
Higher Throughput in a Smaller Form Factor
-   
Greater Power Efficiency
-   
Stackable – Add Capacity as Needed
-   
Seamlessly Secure Private, Public and Hybrid Cloud Environments  
(e.g., AWS, Azure, Oracle, VMware, OpenStack)
-   
Higher Port Density, Flexible Port Modules

# Trellix IPS – Sensor Overview



# NX vs. IPS Positioning

	Trellix IPS	Trellix NX	Trellix Network Forensics
<i>Primary Use-Case</i>	IPS, Virtual Patching, Vulnerabilities / Exploits	Advanced Threat Detection	Network Forensics
<i>Visibility</i>	Primarily Datacenter Traffic	Primarily End User Traffic	Any
<i>Dynamic Analysis Support</i>	Yes (Off Box)	Yes (On Box or Off Box)	Yes (Off Box)
<i>Behavioral Detections</i>	Planned - via add on	Yes - partial	Planned – via add-on
<i>Static Detections</i>	Vulnerability Protection, DoS, Recon, QoS, Data Center Protection, internal firewall	Web infections, Callbacks, malware, lateral movement, Data Exfil detection	Suricata
<i>Protocols</i>	All	Mainly outbound web and SMB	All
<i>L7 Metadata</i>	Yes	Yes	Yes
<i>Packet Capture</i>	Event Based	Event Based	Full Capture
<i>Appliance Scalability</i>	Up to 100 Gbps	Up to 20 Gbps	20 Gbps
<i>Competition</i>	NGFW at SMB, Best of breed IPS at large Enterprise (Cisco Sourcefire, Trendmicro Tippingpoint)	CSWG at large enterprise (Zscaler, Netskope), NGFW at SMB	NetWitness, SentryWire, Riverbead, Niksun

# Trellix

## Use cases



# Trellix NDR use-cases

## Detect Exploits and Zero-day Attacks

- Signature Based
- Non-signature Based
- URL's

## Block C&C

- Callbacks
- Beaconsing
- Behavioral Analysis

## Detect Lateral Movement

- East-West Traversal
- IVX Enrichment
- Data Exfil
- Behavioral Analysis

## Prevent and Detect Malicious Binaries

- Ransomware
- Callbacks
- Malicious Presence



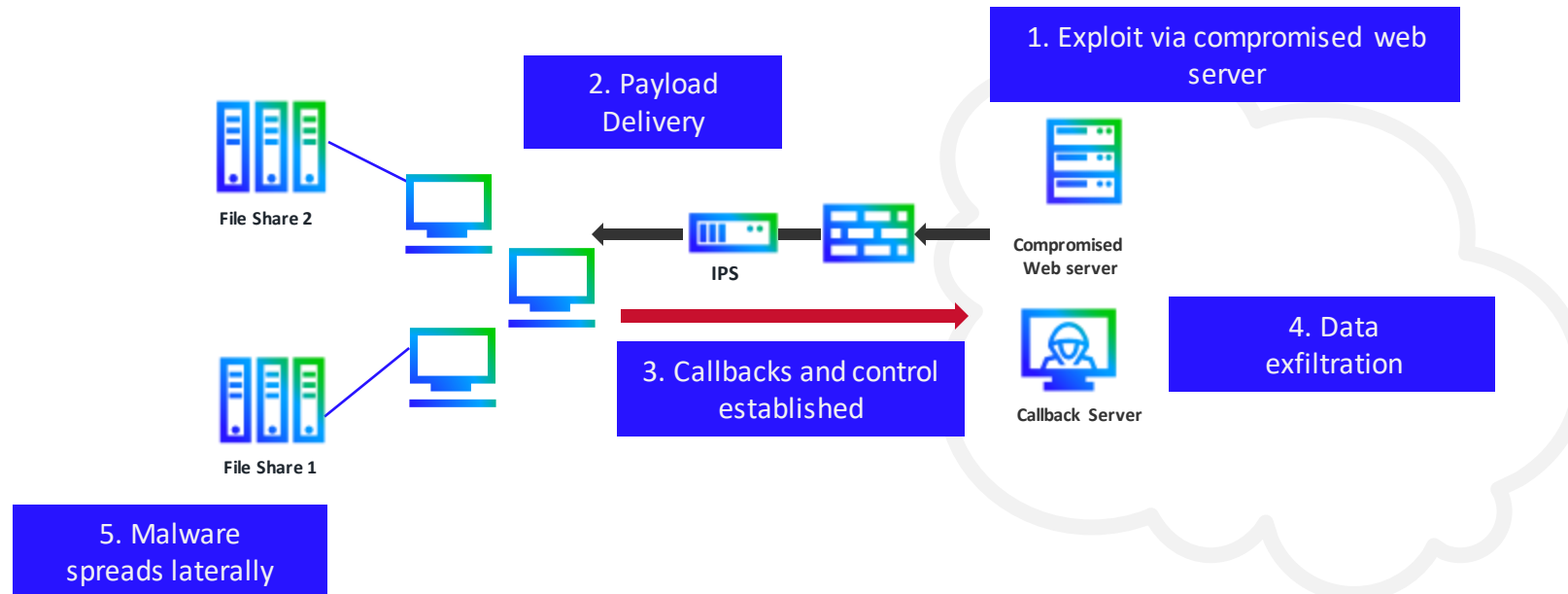
# Trellix

## Demonstration Guidance

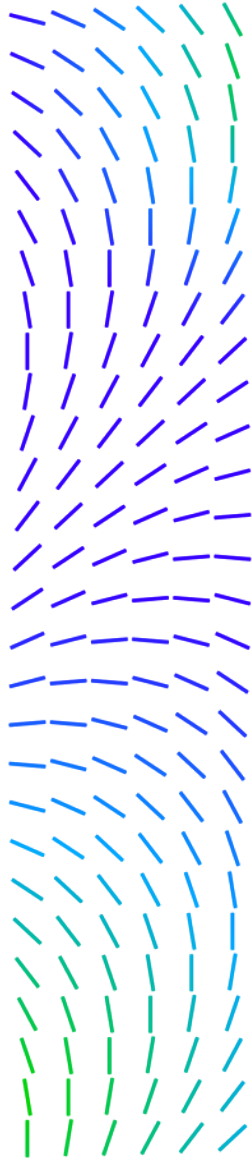
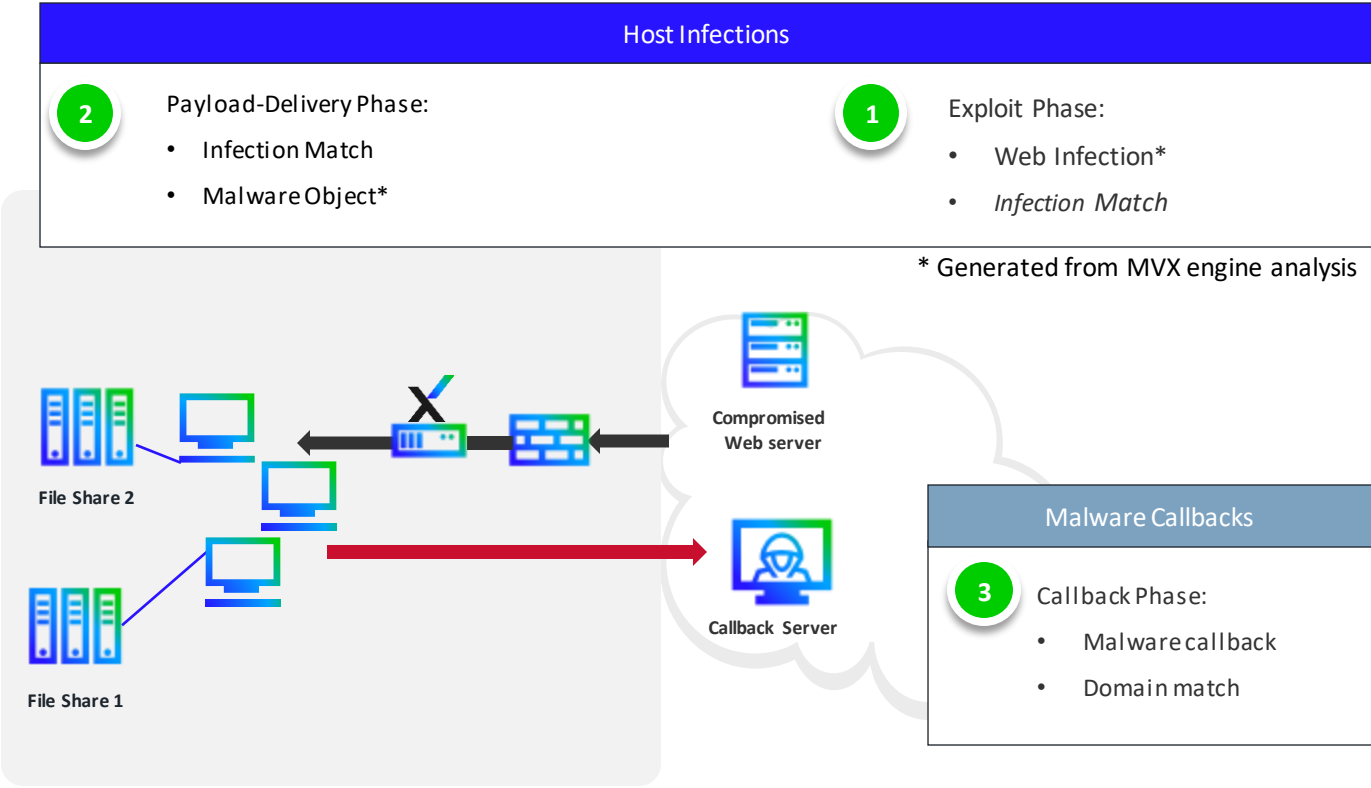
[Insert Trellix Product]



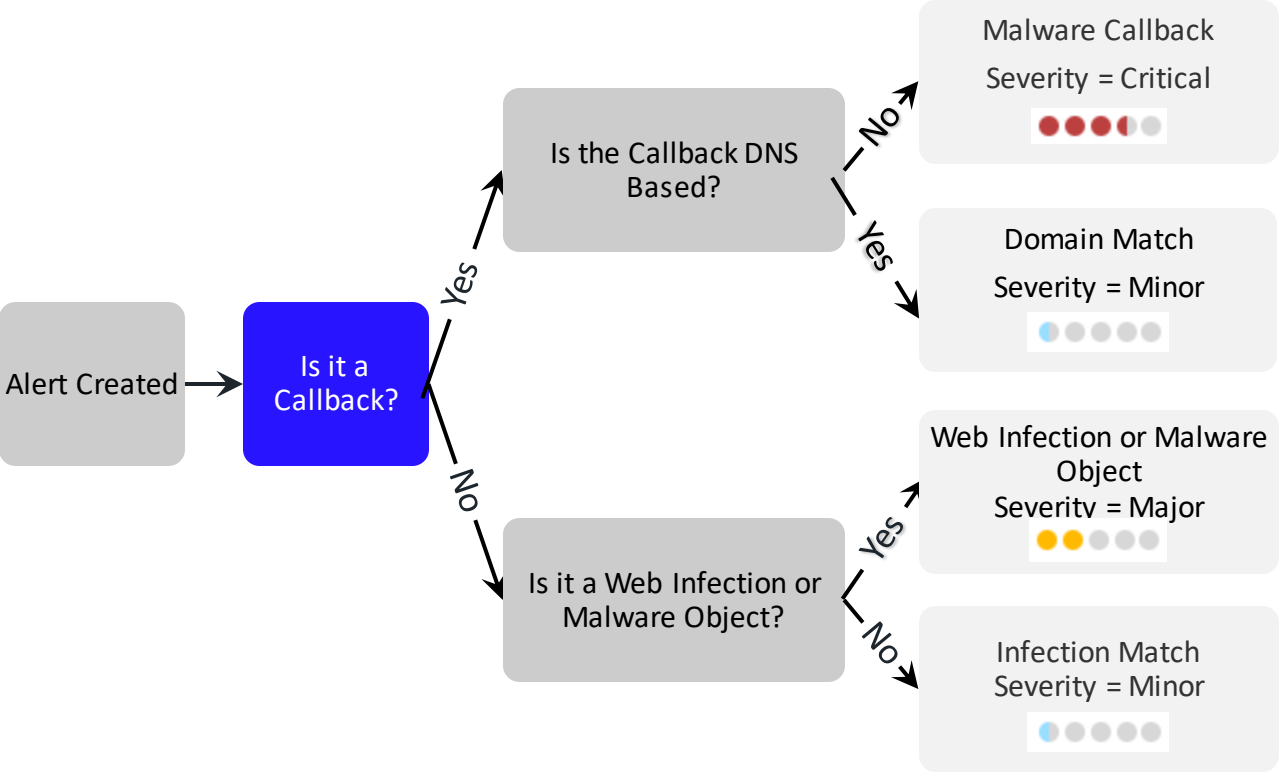
# Web Compromise



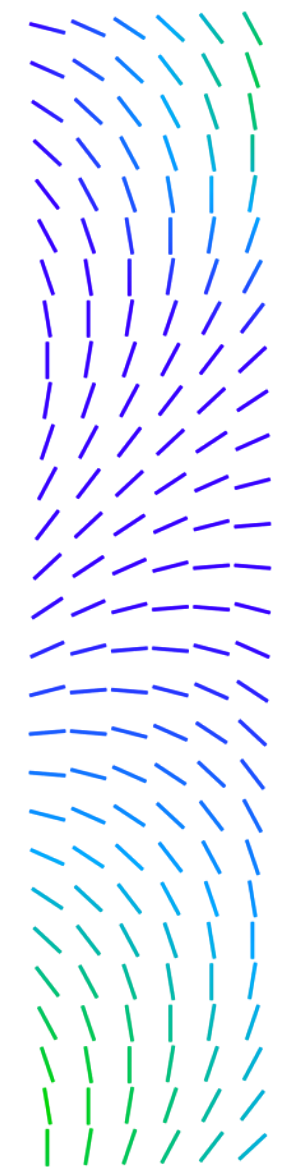
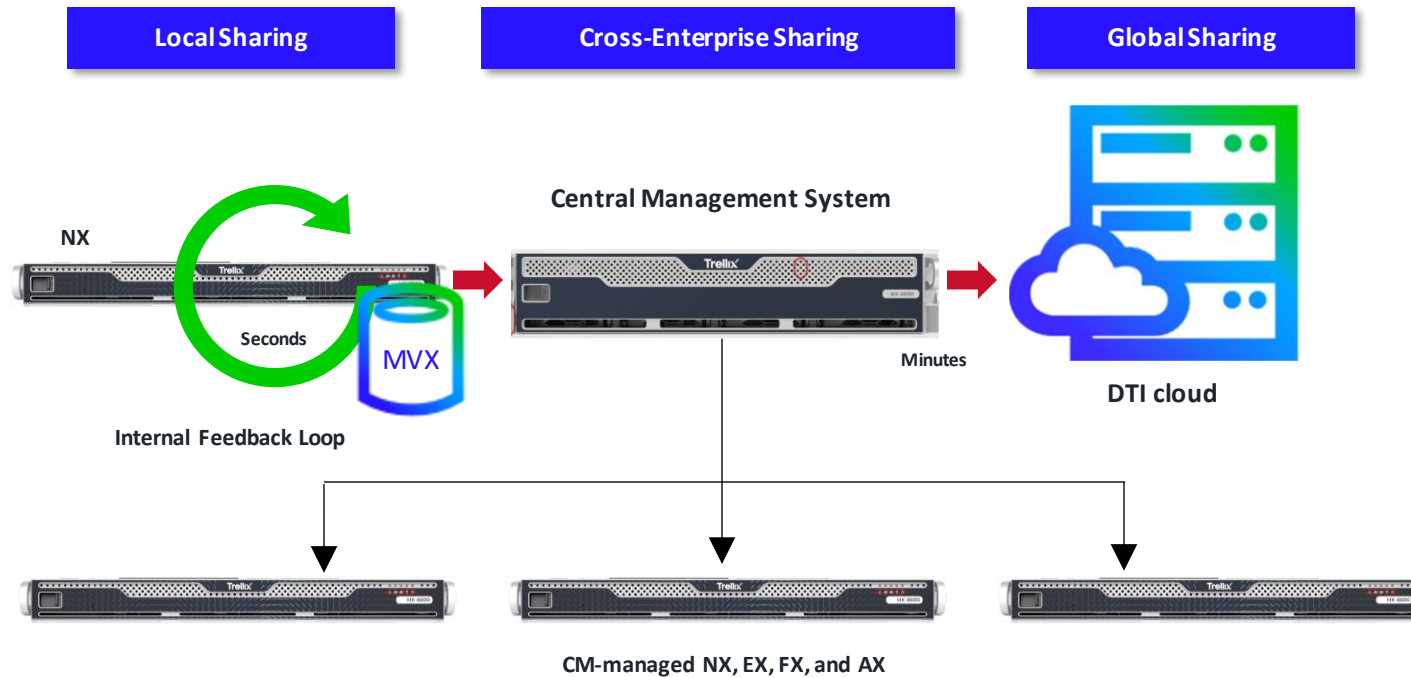
# Event Types



# Alert Severity



# Dynamic Threat Intelligence (DTI)



# Alerts – Hosts View

Hosts | As of 03/03/2019 12:29:54 Etc/UTC

Hosts [38] Alerts Callback Activities

Date Range: 02/17/2019 12:29:54 - 03/03/2019 12:29:54 (Refresh)

Viewing 1-20 of 38 Hosts

Results per page: 20

Host	Total	Infections	Callbacks	Blocked	Last Malware	Last Seen at (UTC)	Last Ack at (UTC)	Host Name	Badges
10.13.11.141	23	18	5	0	SocialEngine	03/03/19 01:39:05		10-13-11-84.victim.crossfire	
10.13.20.143						03/01/19 16:36:14		10-13-20-143.victim.crossfire	
10.13.20.139						03/01/19 08:42:27		10-13-20-139.victim.crossfire	
10.13.20.138						03/01/19 07:37:27		10-13-20-138.victim.crossfire	
10.13.10.61		1			Trojan.APT.GRILLMARK	03/01/19 07:33:02		10-13-10-61.victim.crossfire	
10.13.20.125		12	5	7	0	Trojan.APT.GRILLMARK	03/01/19 05:24:49	10-13-20-125.victim.crossfire	
10.13.20.136		4	2	2	0	Backdoor.Win.CYBERGATE	02/28/19 16:46:05	10-13-20-136.victim.crossfire	
10.13.20.133		2	0	2	0	Trojan.APT.GRILLMARK	02/28/19 03:51:16	10-13-20-133.victim.crossfire	
10.13.11.227		4	2	2	0	Backdoor.Win.CYBERGATE	02/27/19 09:03:31	10-13-11-227.victim.crossfire	
10.13.11.235		4	4	0	0	Backdoor.Win.CYBERGATE	02/27/19 09:01:20	10-13-11-235.victim.crossfire	
10.13.10.37		7	6	1	0	Trojan.Generic	02/27/19 08:46:51	10-13-10-37.victim.crossfire	
10.13.11.234		2	2	0	0	Backdoor.Win.CYBERGATE	02/27/19 07:57:04	10-13-11-234.victim.crossfire	
10.13.11.249		2	2	0	0	Malware.archive	02/27/19 03:08:27	10-13-11-249.victim.crossfire	
10.13.11.226		4	2	2	0	Backdoor.Win.CYBERGATE	02/26/19 09:12:40	10-13-11-226.victim.crossfire	
10.13.13.168		1	0	1	0	DTI.Callback	02/26/19 09:07:49	10-13-13-168.lateral.crossfire	

# Alerts – Alerts View

The screenshot shows an Alerts View interface with a table of alerts. Three callouts are present:

- Alerts [2096]**: A callout box highlighting the total number of alerts.
- Source IP: 10.13.11.84**: A callout box highlighting the source IP address of the selected alert.
- URL: http://www.themainappforflashredirectfree.icu/...**: A callout box highlighting the URL of the selected alert.

Alert Type	ID	File Type	Malware	Severity	Time (UTC)	Source IP	Target	SC Version	Location	Badges
Infection Match	98057		SocialEngineering.Exploit.FakeFlash	0-0-0-0-0	03/03/19 01:39:05	10.13.11.84	www.dtypeappleflashselect.icu/...	828.220		
Infection Match	98056		SocialEngineering.Exploit.FakeFlash	0-0-0-0-0	03/03/19 01:39:02	10.13.11.84	http://www.themainappforflashredirectfree.icu/...	828.220		
Infection Match		Malware.Binary.url		0-0-0-0-0	03/02/19 21:58:01	10.13.11.84	http://12promo.icu/i/10924?cid=155156177810...	828.205		
Infection Match		Downloader.Win.AZORult		0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	conscriptiondaddy.bingobundarasok.info/getve...	828.198		
Infection Match		Exploit.Kit.GrandSoft		0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	conscriptiondaddy.bingobundarasok.info/getve...	828.198		
Infection Match		Exploit.Kit.GrandSoft		0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	conscriptiondaddy.bingobundarasok.info/getve...	828.198		
Infection Match		Exploit.Kit.GrandSoftRedirect		0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	conscriptiondaddy.bingobundarasok.info/getve...	828.198		
Infection Match		zip	Malware.archive	0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	http://www.dtypeappleflashselect.icu/...	828.192		
Infection Match		Malware.Binary.url		0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	http://www.dtypeappleflashselect.icu/...	828.192		
Infection Match		pdf	Trojan.PDF	0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	http://www.dtypeappleflashselect.icu/...	828.192		
Infection Match		Malware	FETestEvent	0-0-0-0-0	03/02/19 21:23:00	10.13.11.84	http://www.dtypeappleflashselect.icu/...	828.192		







# Alert Filtering

The screenshot displays an alert management interface. On the left, a table lists alerts with columns for Alert Type, ID, File Type, Malware, and Severity. A funnel icon is circled in the top left. Two filter panels are overlaid on the right, each with an 'Expand all' button and 'CLEAR'/'APPLY' buttons at the bottom.

**Left Filter Panel:**

- Filters Expand all
- Date Range: 03/02/2019 15:35:06 - 03/03/20
- Alerts
- Critical Detection
- AV Alerts
- Malware Guard Alerts
- Custom Rules
- Alert Type
- Alert Traffic
- ID
- Distinguisher(UUID)
- File Type

**Right Filter Panel:**

- Filters Expand all
- ID
- Distinguisher(UUID)
- File Type
- Malware
- Severity
- Source IP/Mask
- Target IP/Mask
- URL
- Malware Hash
- Location
- SC Version
- Badges

**Alert Table:**

Alert Type	ID	File Type	Malware	Severity
Infection Match	96057		SocialEngineering.Exploit.FakeFlash	High
Infection Match	96056		SocialEngineering.Exploit.FakeFlash	High
Infection Match	96054		SocialEngineering.Exploit.FakeFlash	High
Infection Match	96053		Exploit.SocialEngineering.FakeFlash	High
Web Infection	35568		Malware.Binary.url	Medium
Malware Callback	96051		Downloader.Win.AZORult	Critical
Infection Match	96050		Exploit.Kit.GrandSoft	High
Infection Match	96049		Exploit.Kit.GrandSoft	High
Infection Match	96048		Exploit.Kit.GrandSoftRedirect	High
Malware Object	35185	zip	Malware.archive	Medium

**Table on the far right:**

SC Version	Location	Badges
828.220		
828.220		
828.204		
828.202		
828.198		
828.198	RJ	
828.198		
828.198		
828.192		

# Alert Details

Alert Details

Malware

- Backdoor.Win.CYBERGATE
- FE\_Backdoor\_Win32\_CYBERGATE

VXE Callback

- Backdoor.Win.CYBERGATE

Application Type

Windows Explorer

File Type

exe

Builtin AV

- Win.Trojan

Yara Rule

- FE\_Backdoor
- FE\_Evasion\_D
- FE\_VM\_Evasion\_

AV Suite

- Trojan.Rebhip.FEC3

Malware Guard

- fe\_ml\_heuristic

Malicious behaviour observed

IP Protocol

TCP

Victim Host

10-1

Victim IP

10

Victim Port

5

Target IP

1

Src MAC Address

00:1f:ad

Dst MAC Address

00:1f:ad

Communication

- [1]pcap 13921 bytes (text)
- [2]pcap 21831 bytes (text)
- [3]pcap 1936 bytes (text)

Captures

ID

35149

Distinguisher(UUID)

0987eaf6-551c-40a4-87e5-ad6ba636949f

URL

uiamp.org.ua/resources/w32tm.exe

Malware Hash

0ef4ccede47eaeefe88962817b385af5

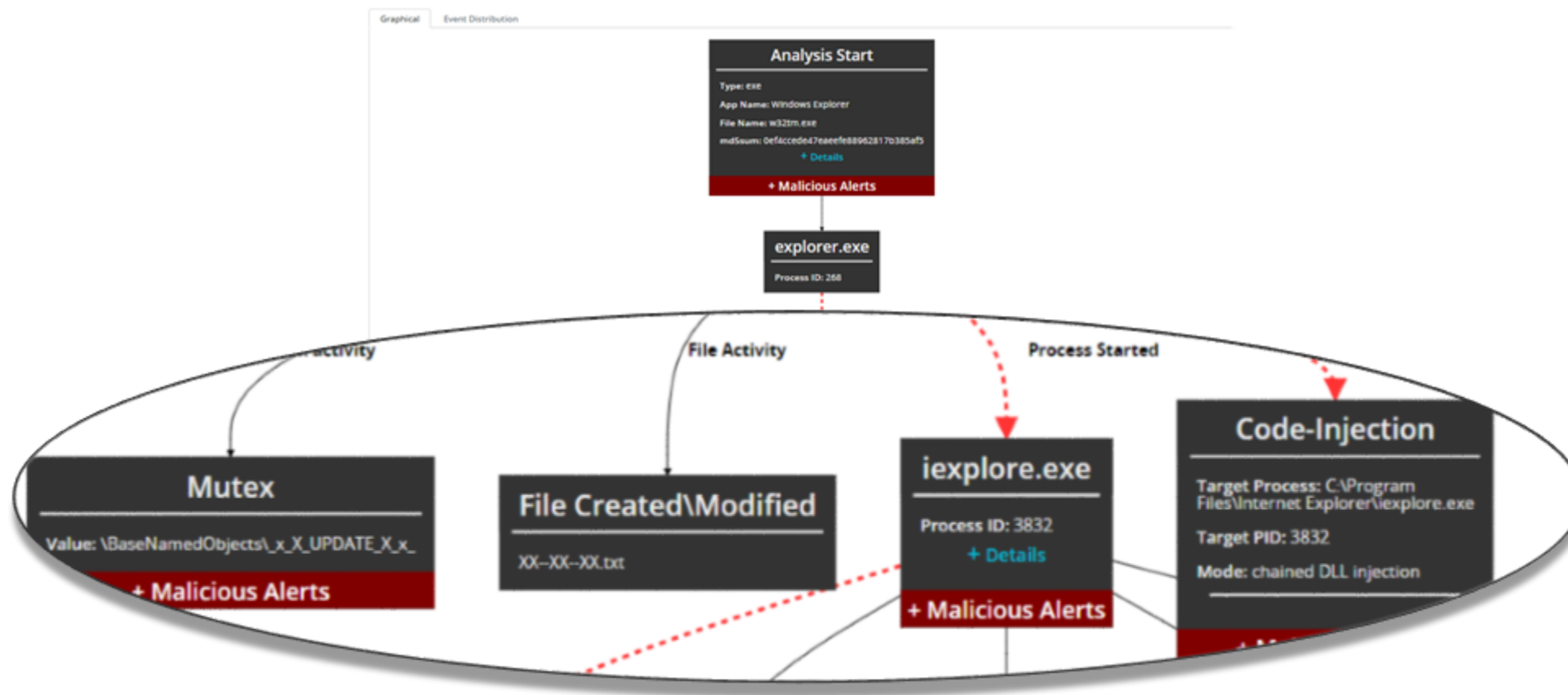
Archived Object

0ef4ccede47eaeefe88962817b385af5.zip

Ngulse Analysis

ngpulse analysis

# OS Change Detail – Graphical



# OS Change Detail – Report

Mutex		\BaseNamedObjects\X_X_UPDATE_X_X_	3836		
Malicious Alert	Malware Family	Message: Malicious Refros Indicator			
Mutex		\BaseNamedObjects\X_X_PASSWORDLIST_X_X_	3836		
Mutex		\BaseNamedObjects\X_X_BLOCKMOUSE_X_X_	3836		
Mutex		\BaseNamedObjects\***MUTEX***	3836		
File	Created	C:\Documents and Settings\admin\Local Settings\Temp\XX_XX_XX.txt	3836		
File	Closed	C:\Program Files\Internet Explorer\iexplore.exe Parentname: C:\Documents and Settings\admin\Local Settings\Temp\w32tm.exe Command Line: "C:\Program Files\Internet Explorer\iexplore.exe" MD5: b60ddd2d63ce41cb8c487fcbb6419e SHA1: eadce51c88c8261852c1903399dde742fba2061b			235356
Codeinjection	Chained Dll Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\w32tm.exe Target: C:\Program Files\Internet Explorer\iexplore.exe	3836 3848		
Malicious Alert	Suspicious Code Injection	Message: Code injection observed			
Codeinjection	Chained Direct Code Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\w32tm.exe Target: C:\Program Files\Internet Explorer\iexplore.exe	3836		
Codeinjection	Create Process Suspended Memory Write Code Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\w32tm.exe Target: C:\Program Files\Internet Explorer\iexplore.exe			
Codeinjection	Chained Direct Code Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\w32tm.exe Target: C:\Program Files\Internet Explorer\iexplore.exe	3836 3848		
Codeinjection	Create Process Suspended Memory Write Code Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\w32tm.exe Target: C:\Program Files\Internet Explorer\iexplore.exe	3836 3848		

# OS Change Detail – Event Distribution



# Trellix

## SE Resources How to Access

[Insert Trellix Product]



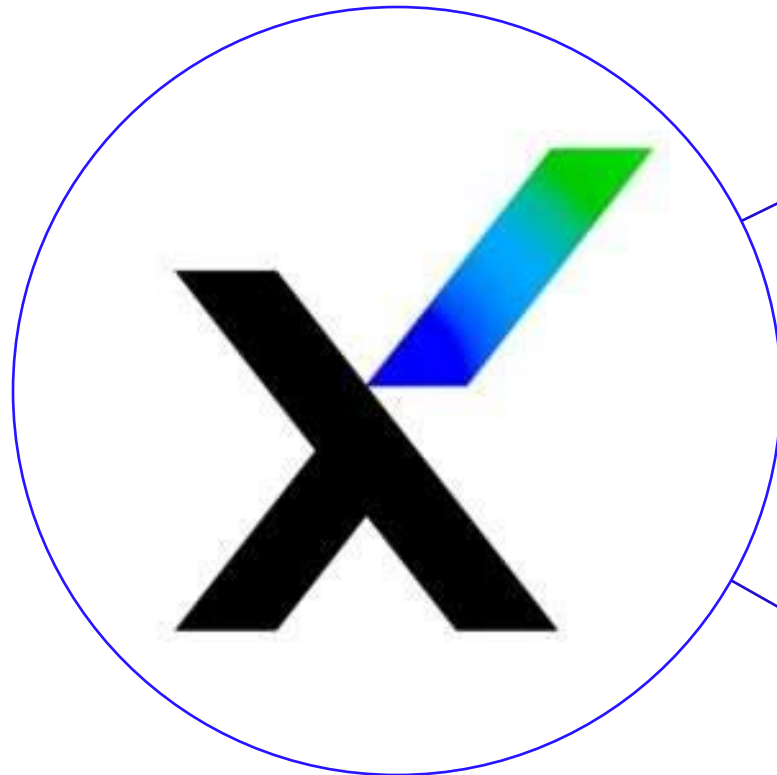




Partner Care Team here to help with:

[partnercareemea@trellix.com](mailto:partnercareemea@trellix.com)

[msspartnercare@trellix.com](mailto:msspartnercare@trellix.com)



Partner  
Care

- **Partner Portal & Service Portal**
- **Product/Licensing queries**
- Profitability programs
- Partner Registration
- Partner Update/Certification
- **NFR Depot**
- **NFR License**
- Reports
- **Training/Partner Onboarding**
- **Lab Access**

MSP  
Partner  
Care

- **iAsset access**
- **Partner training: iAsset, PBC, MSP program, Download center**
- Partner Business center (PBC), Reporting
- Product & Licensing
- BPS Portal
- Billing
- Tenant
- Name and address updation on MSP accounts



## Partner SE Technical Bookmarks



### Product Technical Documentation Portal

- Product Documentation:
  - <https://docs.trellix.com/>
- Administratorion Guides
- Deployment Guides
- System Security Guides
- Release Notes
- Hardware Guides



### Cloud Lab

- CrossFire (ASH):
  - <https://login.trellix.com/>



### Communication

Partner Care Team

- [partnercareemea@trellix.com](mailto:partnercareemea@trellix.com)
- MSP Partner Care Team
- [msppartnercare@trellix.com](mailto:msppartnercare@trellix.com)



### Expert Center

Knowledge Base

Forum

- Trellix-F Community:
  - <https://community.fireeye.com/>
- Trellix-M Community:
  - <https://communitym.trellix.com/>
  - Consolidation in progress...



# NFR (Not-or-Resell)

Based on Partnership Level\*, free NFR Licenses can be requested

COMPETENCY (Enablement)	Collaborate	Momentum	Growth	Distribution	MSSP
Access to Trellix University	✓	✓	✓	✓	✓
Trellix Annual Partner Conference (by Invitation)	✓	✓		✓	✓
Trellix Demo Center (formerly MPACT & Cross Fire)	✓			✓	✓
Not-for-Resell (NFR), Upon Request	✓	**		✓	
Trellix Evaluation Offering (partner requested POV)	✓	✓		✓	✓
Cyber League Specialization (Trellix University)	✓			✓	✓

BENEFITS NOTES: \*\* Support Varies by Region. Assumes completion of ICPA following acceptance of Trellix Partner Application.

Partner eXperience | Program Benefits table from Global Partner Program Guide  
<https://partners.trellix.com/partner/en-us/assets/guides/xtend-global-partner-program-guide.pdf>

Ready



Badge



Explore



**Thank you!**

**Your friendly bookmark for certification**

Trellix University  
<https://training.trellix.com>

**Trellix Sales Certified: Network Security (NX)**  
**Trellix Sales Certified: Detection as a Service**

**Trellix Certified Architect: Network Security (NX)**  
**Trellix Certified Architect: Detection as a Service**  
**Trellix Intrusion Prevention System Essentials**

**Trellix Service Provider: Network Security (NX)**  
**Trellix Service Provider: Detection as a Service**  
**Trellix Intrusion Prevention System Essentials**

# Trellix

# Trellix Differentiators

[Insert Trellix Product]



# Awards and Certifications



2022 GLOBEE Gold Award for Network Detection and Response



2021 KuppingerCole Leadership Compass Overall Leader for Network Detection and Response



2021 Network Analysis and Visibility Recognized as a Large Vendor



Market Leader for Advanced Threat Protection



Common Criteria Certification



FIPS 140-2 Certification



SOC 2 Type 2 Certification for Security and Confidentiality



ISO 27001 Certification



First security solution to receive the US Department of Homeland Security SAFETY Act Certification





**Thank You**