
Trellix
APJ Partner Summit'24
Partnering for a Secure Future
Detect Undetectable and Evasive Network Attacks
Trellix NDR

Speaker Intro

Principal Solutions Architect

Gus Arias

Detect Undetectable and Evasive Network Attacks

Why you need a strong NDR platform to protect against stealthy, evasive & advanced network attacks and the importance of right network visibility.

- Introductions
- Why NDR?
- Disrupt attackers at Every Stage
- Speed up investigations with Multi-Layered Detection
- Q&A

Are you only seeing half the picture?

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

69%
[2]Unknown, poorly managed assets

16 days
[1]Global median dwell time

35%
[3]Ignored alerts

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

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

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

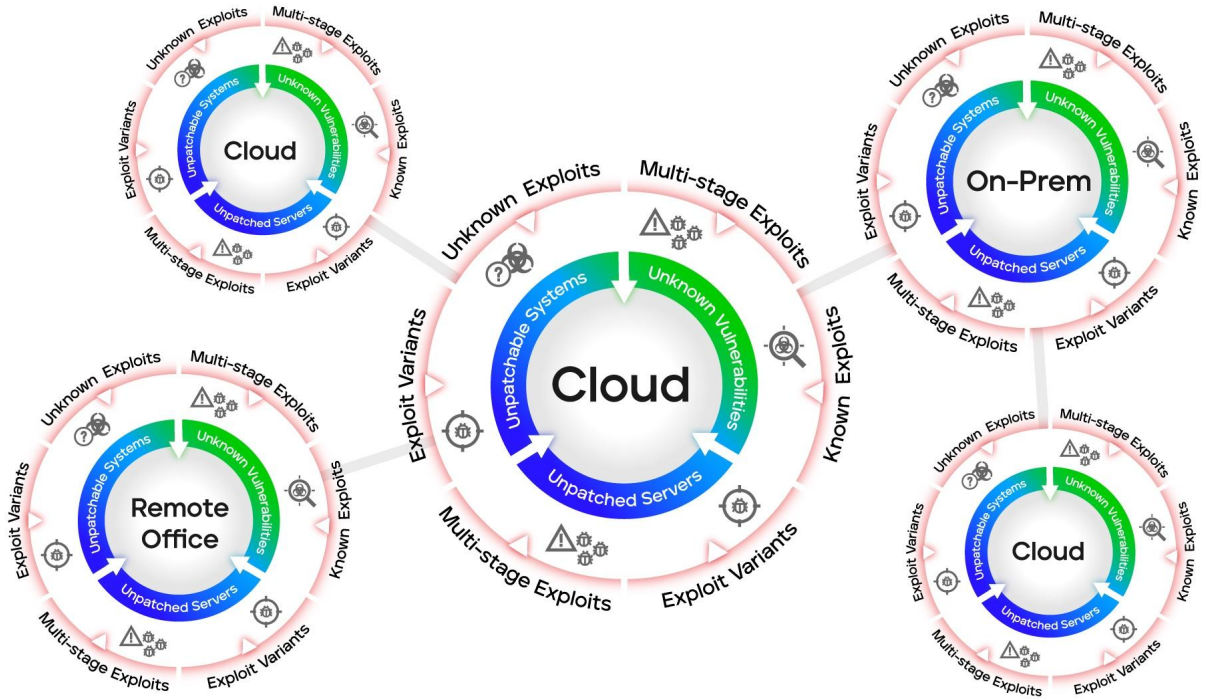
[4]JupiterOne 2023 (The 2023 State of Cyber Assets Report)

Networks today

More complexity, more workloads, more risk

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

Your Network – How many ways in?

Not just unpatched systems, vulnerability exploits, and email…

Vulnerabilities

Vulnerabilities in known and unknown assets on our networks.

Email

Still the primary attack vector. Over 90 % of cyber attacks begin with phishing.

Collaboration Platforms (Google Drive, Teams, etc.)

Allow us to freely share information, but do not ensure the integrity of what is being shared

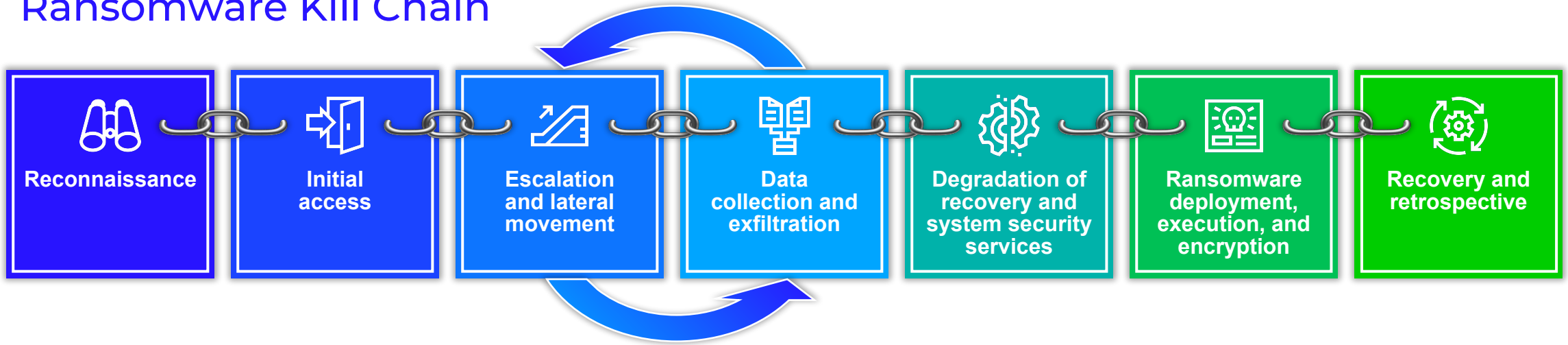
Enterprise Applications (Workday, Salesforce etc.)

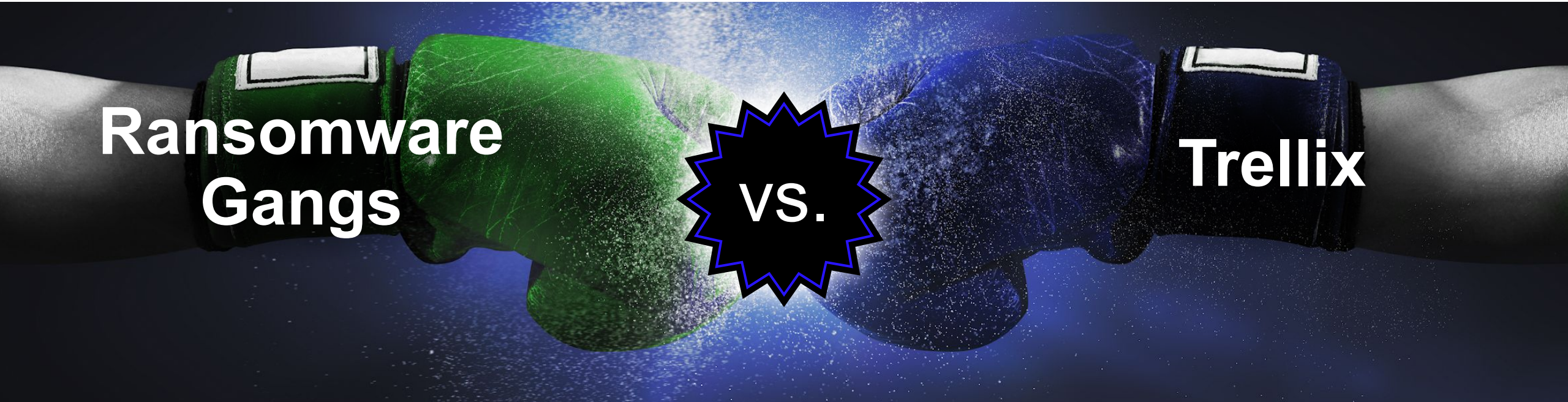
Digital transformation initiatives grant access to suppliers, vendors, customers – and threat actors

Trellix

The Phases of a Ransomware Attack

Ransomware Kill Chain

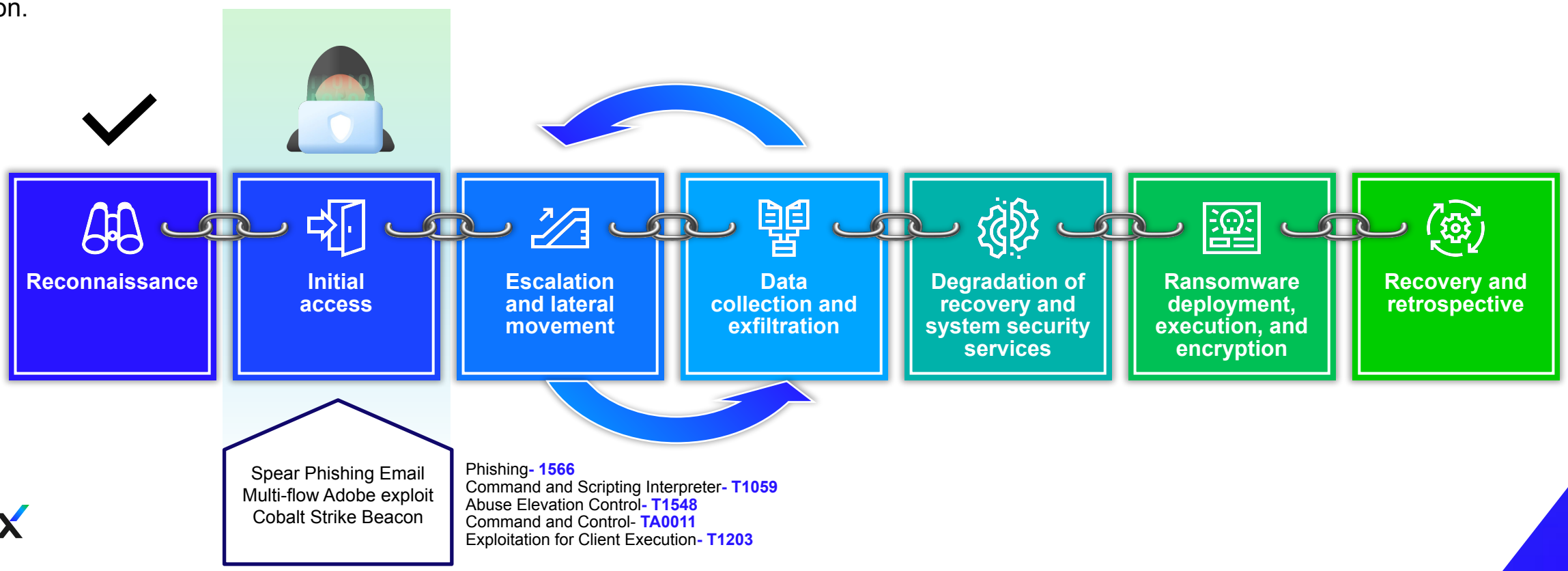




One missguided click and they are in...

Getting In

Email is still a common entry point for initial compromise, phishing emails trick recipients into clicking malicious links or downloading infected attachments. These emails often impersonate trusted entities to lower the guard of the targets. An arbitrary code execution vulnerability identified in Adobe products enables attacker with user interaction to achieve arbitrary code execution to execute powershell beacon.

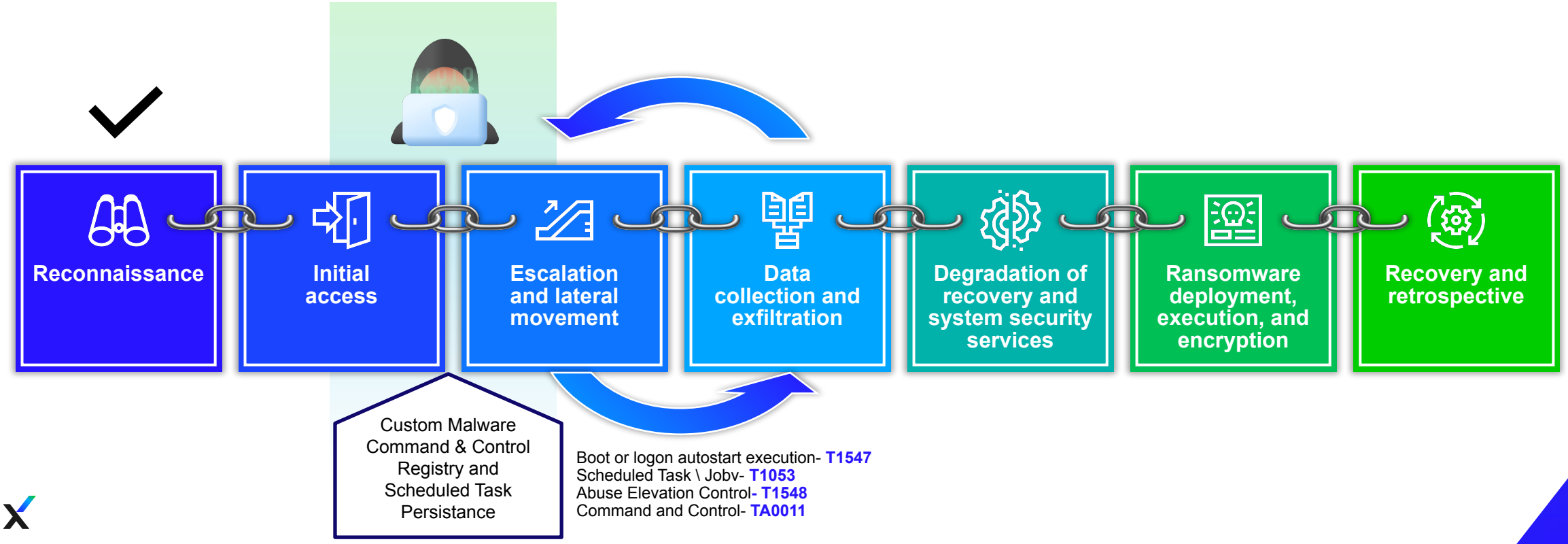


Trellix

Then they establish themselves...

Establishing Foothold

The infected endpoint will connect back to the Attacker's command and control infrastructure. Additional Payload is downloaded on the target machine. Registry and scheduled tasks to help maintain access

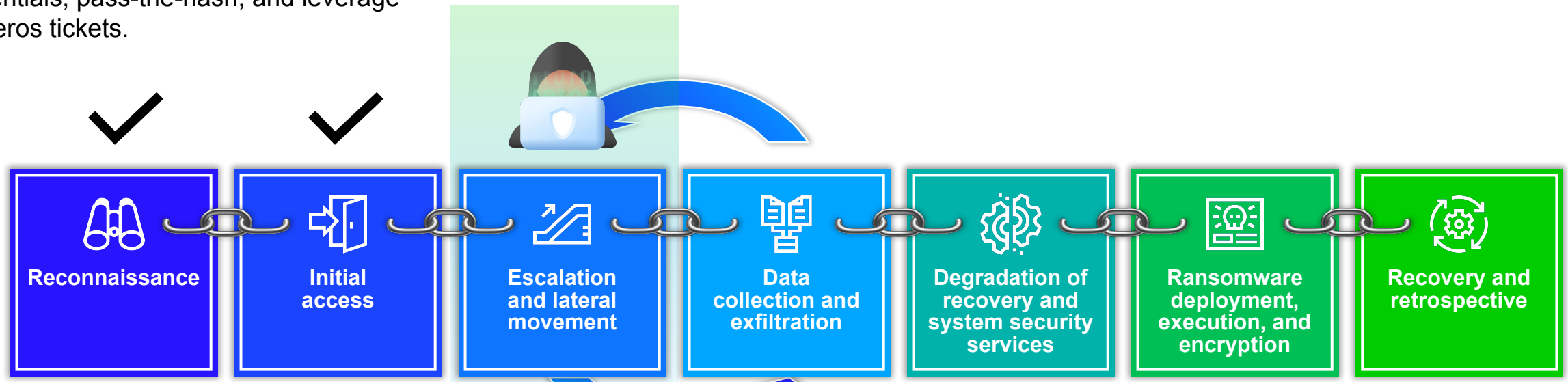


Trellix

Moving laterally...

Attack Dwell Time

Living-Off-The-Land and Command-Line tools are used to map the internal network, find relevant services and move laterally. Beacon has automation for this too. The psexec, psexec_psh, winrm, and wmi commands are present. Like other Cobalt Strike features, these tools run in the Beacon agent. Don't worry, the ability to leverage different trusts is present. Beacon can steal tokens, use credentials, pass-the-hash, and leverage Kerberos tickets.



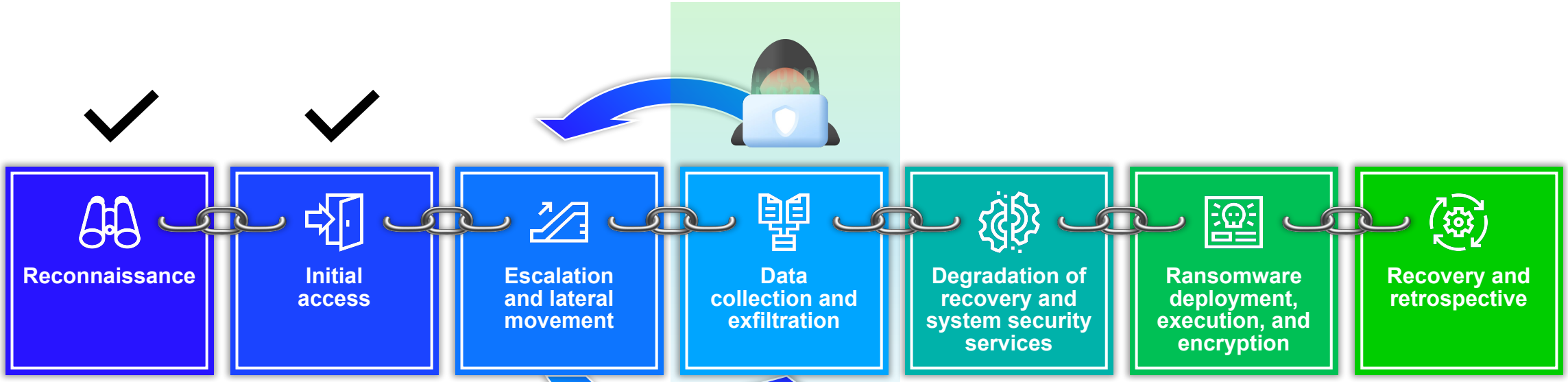
Adfind - Remote System Discovery - **T1018**
PsExec - Lateral Tool Transfer - **T1570**
Mimikatz - OS Credential Dumping - **T1003**
Remote Management Tools (Anydesk, Todesk, RuDesktop, TeamViewer, TightVNC, Aletera)- Remote Services: VNC - **T1021.005**
Net- Remote Services: SMB/Windows Admin Shares - **T1021.002**

Trellix

Exfiltrating organization's data..

Collection and Exfiltration

Additional Living-Off-The-Land tools and non-malicious cloud storages are used to collect and exfiltrate company's data.
Slow exfiltration to Cloud Storage is done using Cobalt Strike as the C2 Framework



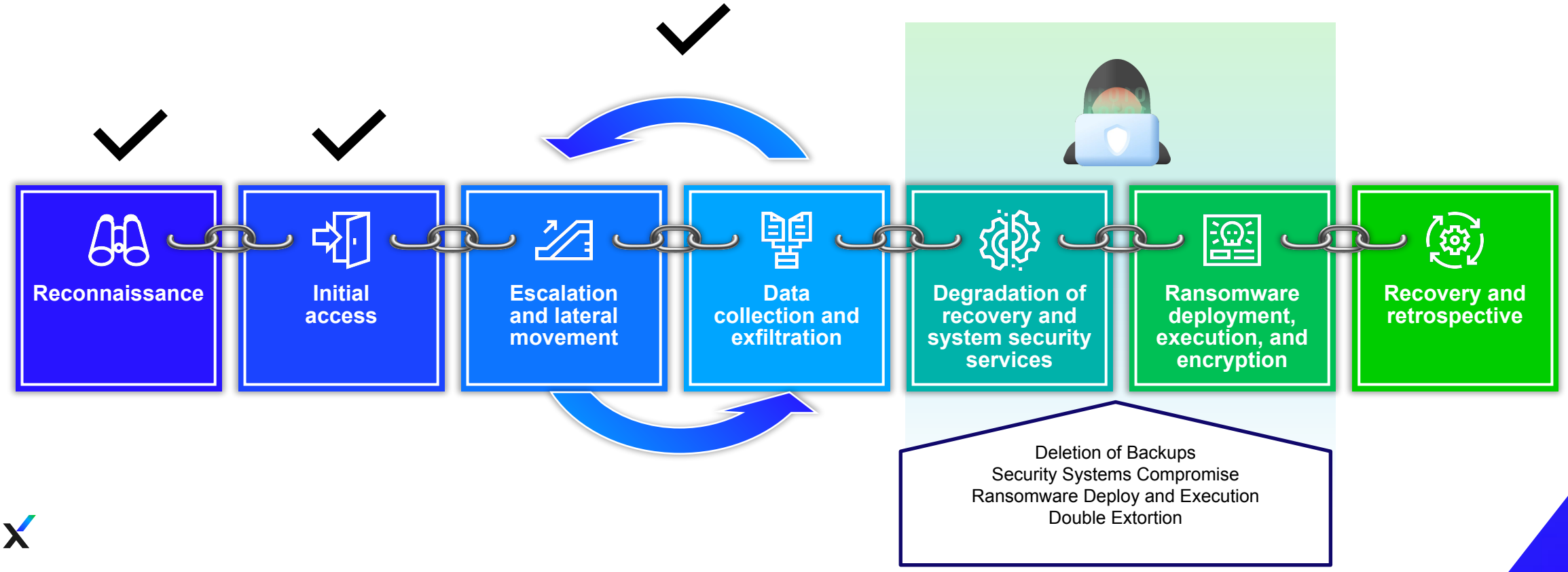
7-Zip- Archive Collected Data - **T1560**
DtSearch - File and Directory Discovery – **T1083**
Rclone/Megasync - Exfiltration to Cloud Storage – **T1567.002**
WinSCP/SFTP/FileZilla - Exfiltration Over C2 Channel - **T1041**

Trellix

Until they reach the goal..

Destroy your Business

Modern ransomware encrypts data and exfiltrates sensitive information.
Dual purpose: it allows criminals to demand ransom for decrypting the data and not disclosing the stolen information.



Trellix

NDR - The Trellix Approach

Eliminate blind spots

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

Disrupt attackers at every stage

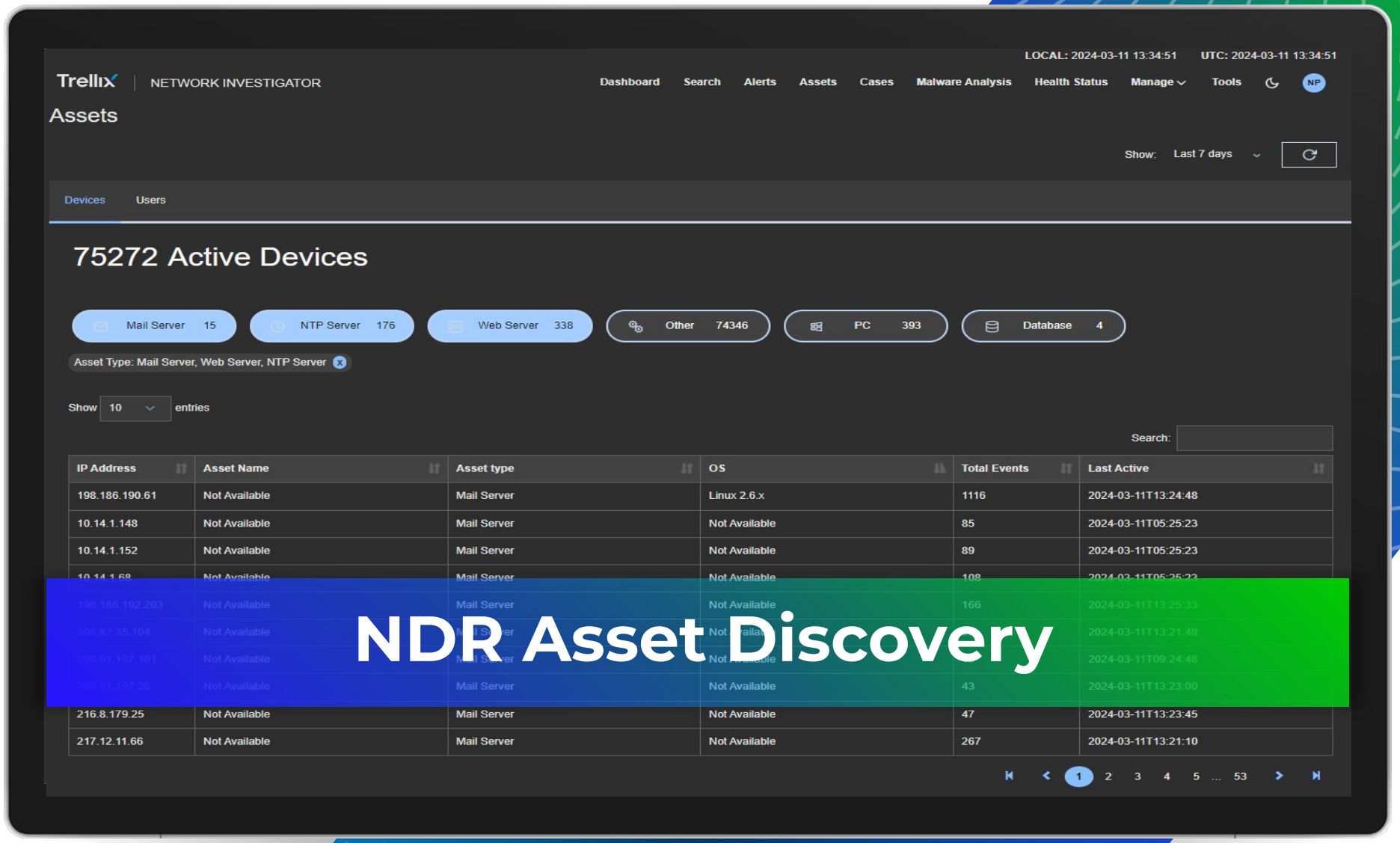
- Not just initial compromise
- Multi-layered ML based approach
- Detection of known, unknown, and emerging threats

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



NDR Asset Discovery

Trellix

Multi-layered approach to disrupt attackers

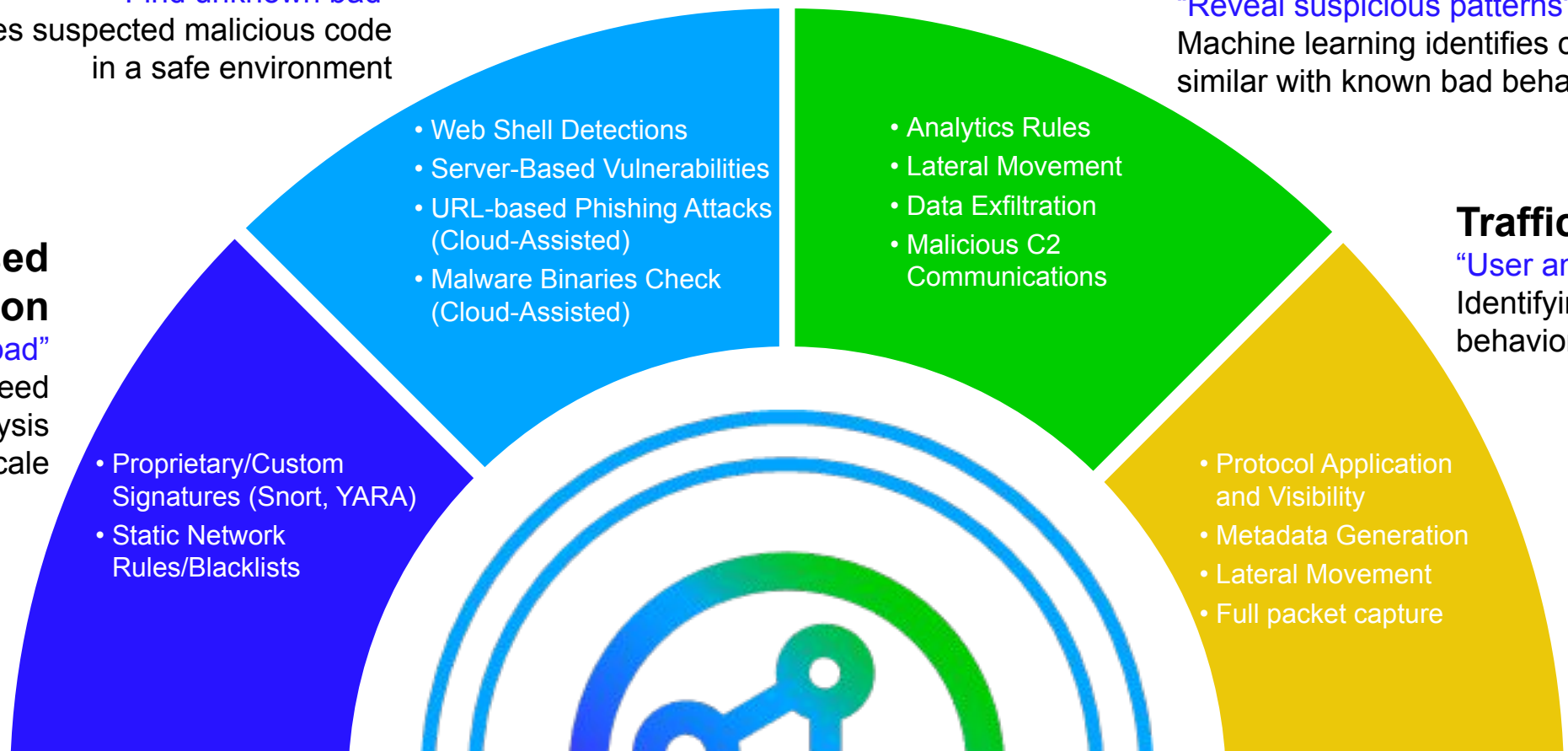
Combined techniques detect known, unknown, and emerging threats

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
"User anomaly detection"
Identifying unlikely behaviors



Trellix

Disrupt attackers... at every stage

Traditional Network Perimeter Security

Trellix Network Detection and Response

- Reconnaissance attack detection

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

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

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

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

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

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

Leveraging multiple detection and AI approaches

Trellix

Connect the dots, gain additional visibility, correlation, Threat Intelligence and advanced ML analytics features with Trellix Network Detection and Response. Fully integrated in the XDR Workflow

Network Investigator

Protect your Enterprise Network with high performing Intrusion Prevention Systems

Intrusion Prevention

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

Network Security

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

Network Forensics

Trellix

Trellix Network Portfolio

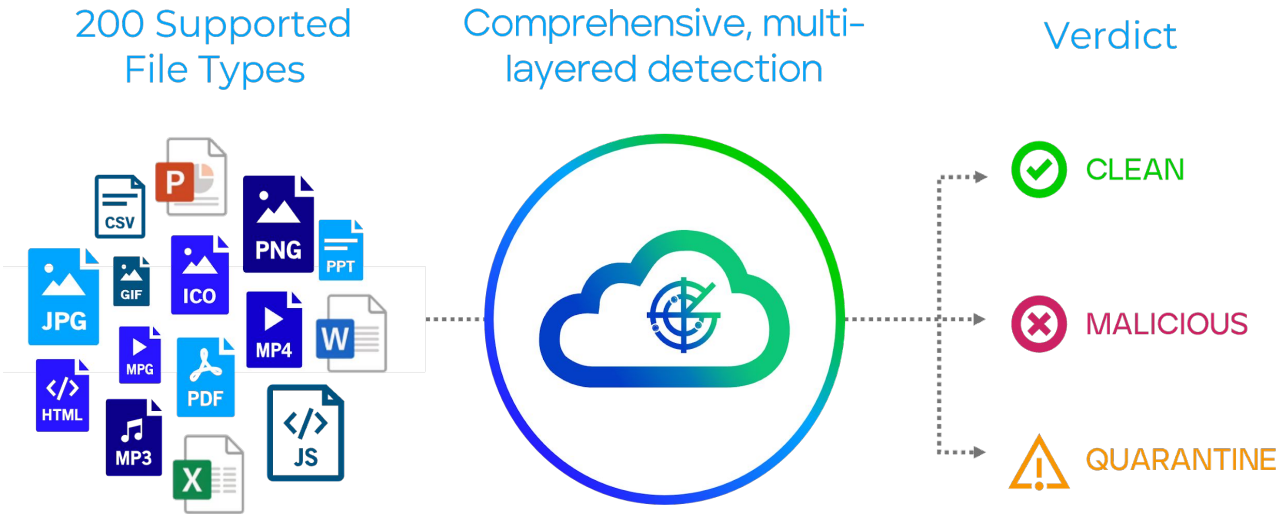
	Trellix Intrusion Prevention System (IPS)	Trellix Network Security (NX)	Trellix Packet Capture (PX)
Primary Function	**Server / Datacenter workloads High-throughput traffic**	**User Devices, Web and SMB traffic**	**Visibility for Forensics, Compliance**
Scalability	100 Gbps (200 Gbps planned)	20 Gbps	40 Gbps
Security Capability	**Deep packet inspection:** Exploit protection / virtual patching, adv. Malware engines, DoS/ DDoS, deep file inspection, C&C, reputation, 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
	Integration with IVX	On-box or via IVX for clustering	Integration with IVX
Zero-Day Suspicious File Detonation			
Deployment Options	Physical, Virtual, Public and Private Cloud, Integrations with AWS Load Balancer		

Trellix

For that zero-day evasive attack

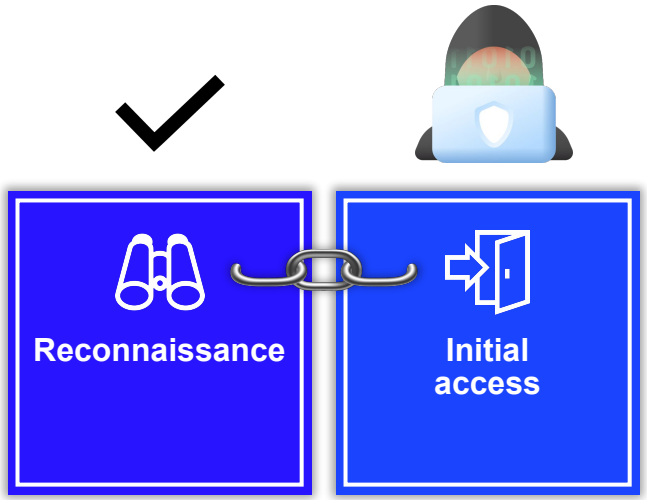
IVX detection sandbox pinpoints known and unknown malware

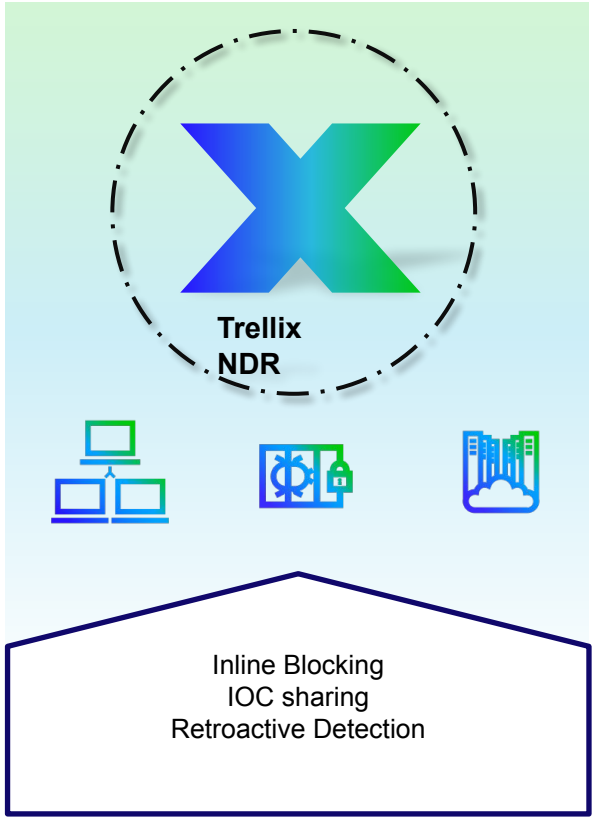
- Reduce dwell time: continually inspect and convict content upon entry
- Identify unknown and zero-day threats:
  using multiple analysis techniques including
  static, dynamic, URL,
  and behavioral analysis
- Supplements SOC Hunting: high fidelity alerts ensure analysts focus on the threats that matter



Trellix

NDR disrupts initial access



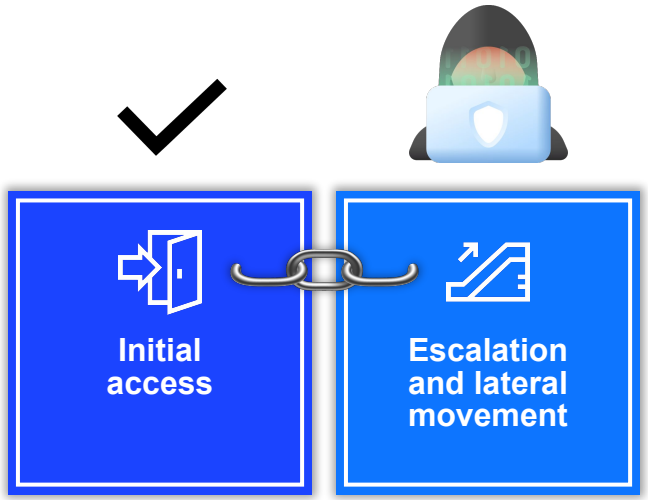


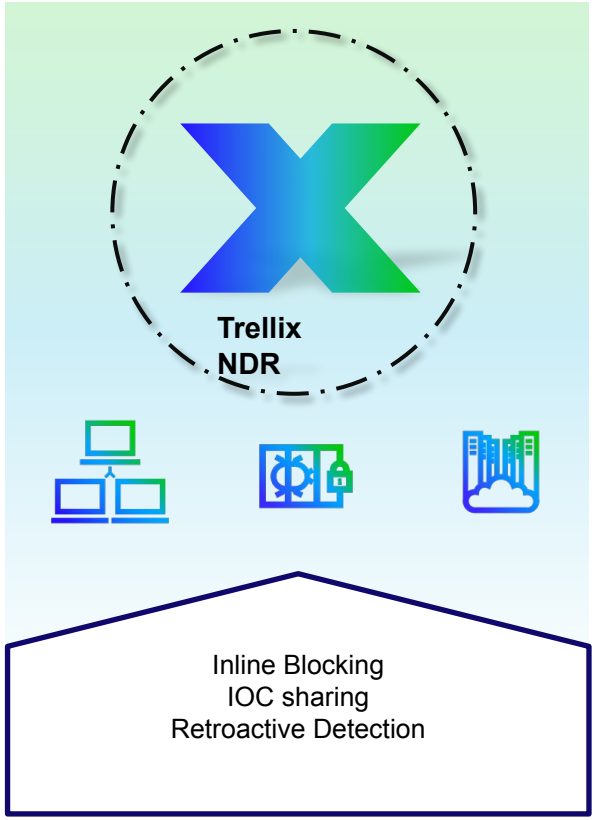
- ✔ Full protocol analysis
- ✔ Domain/URL Blocking
- ✔ Phishing Detection
- ✔ Signature based intrusion prevention
- ✔ Dynamic Analysis
- ✔ C2 Detection

- ✔ Telemetry and L7 Metadata sent to NDR

Trellix

NDR detects lateral movement and escalation



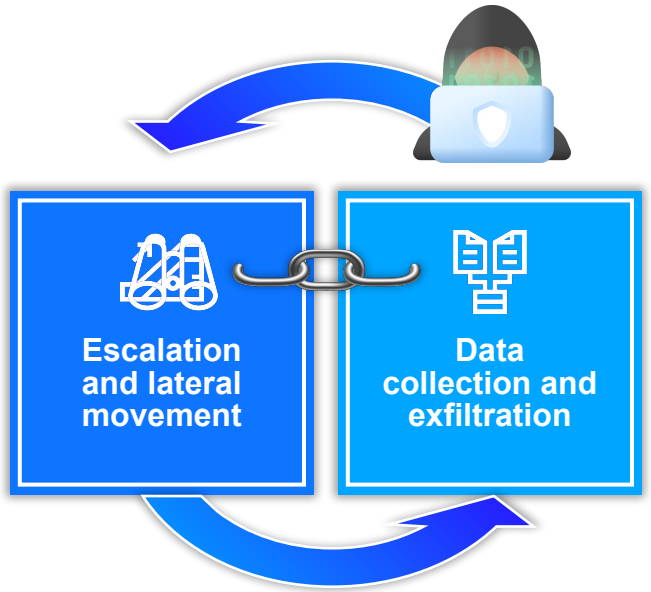


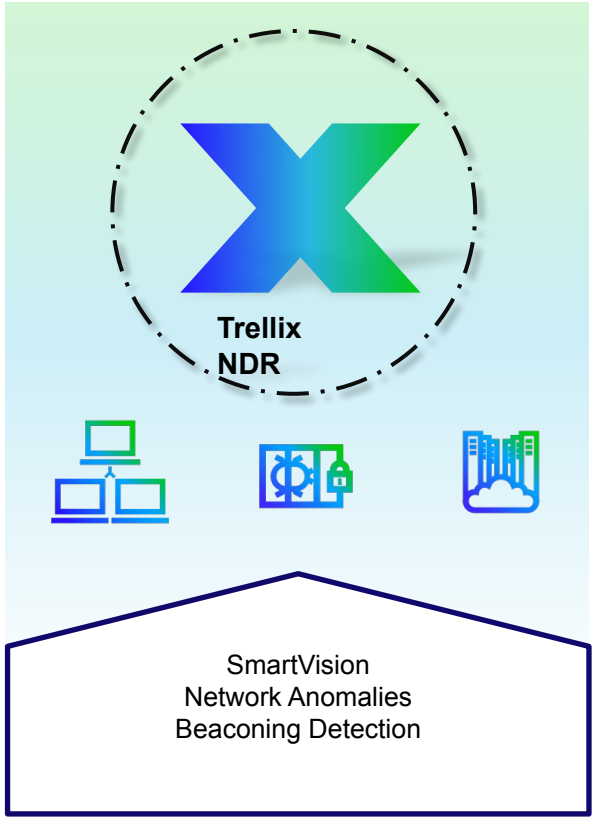
- ✔ **Pass the Hash**
- ✔ **Credential Dumping**
- ✔ **Fileless Malware Detection**
- ✔ **Host Enumeration**
- ✔ **User Enumeration**
- ✔ **Network Mapping**

- ✔ **Telemetry and L7 Metadata sent to NDR**

Trellix

NDR provides the visibility to detect their activities





- ✔ ML Unusual File Transfer
- ✔ Malware-in-Motion
- ✔ Dynamic Analysis
- ✔ Anomaly Detection
- ✔ Data-Exfiltration signature Based
- ✔ DNS Tunnelling
- ✔ Forensics Analysis

- ✔ Telemetry and L7 Metadata sent to NDR

Trellix

NDR Threat Reporting

Trellix

Accelerate investigation and response

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

Provides visibility and alert priority to respond quickly

Trellix

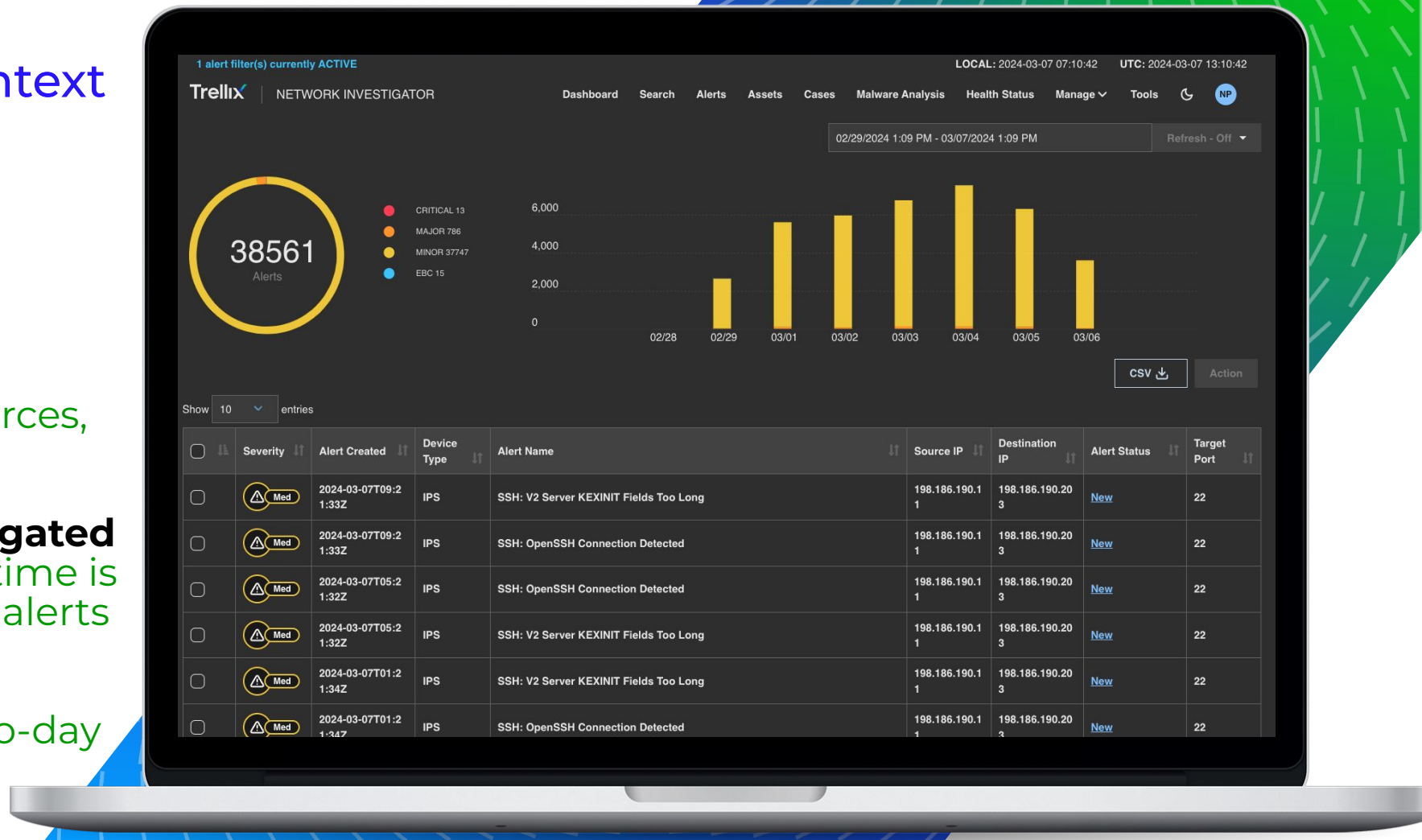
High-fidelity NDR Alerts provides scope and context

Overwhelmed Analysts
- NDR prioritises alerts
- Address most critical first
- No fear of missing

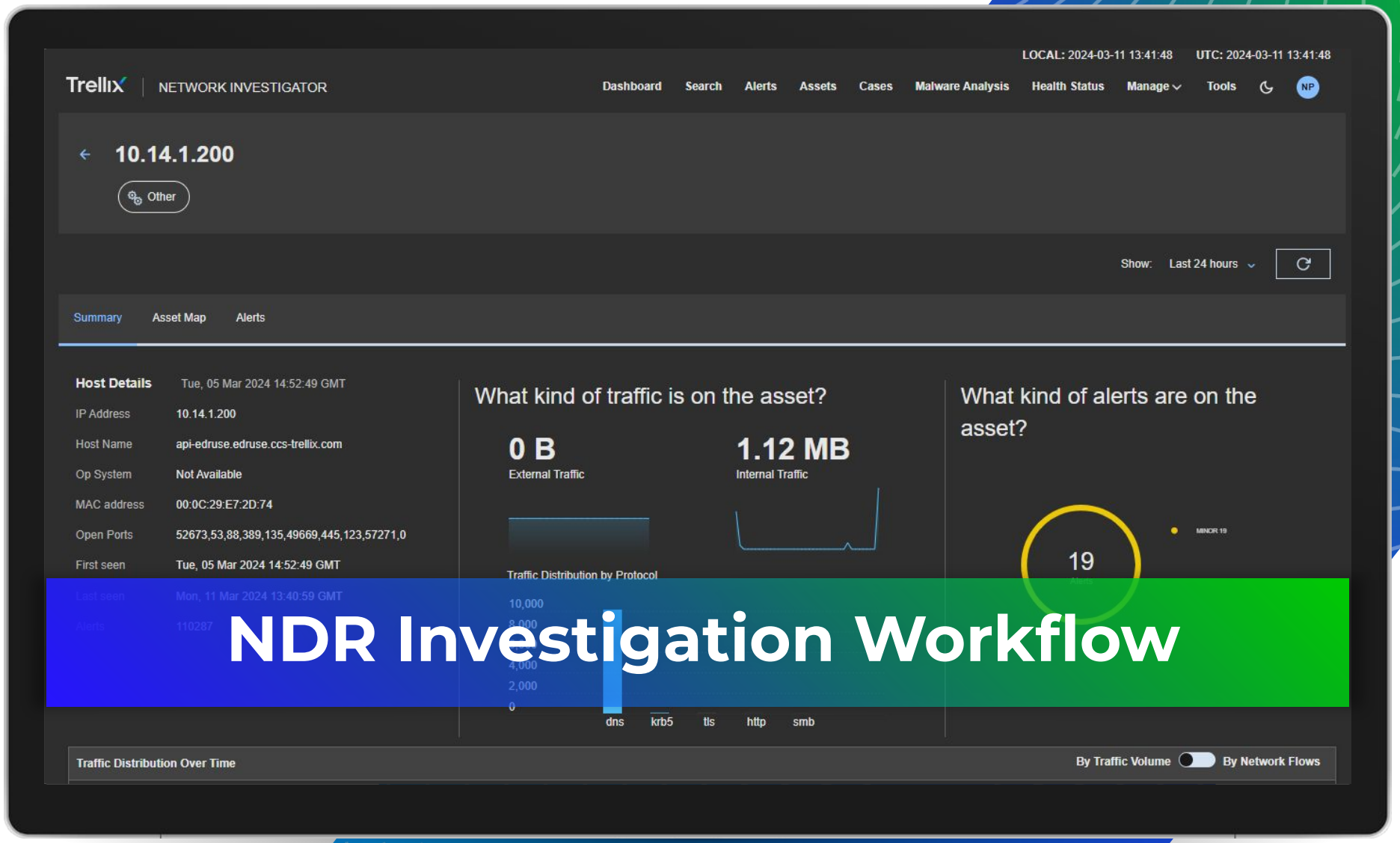
Time lost tuning policies
- NDR lets you turn on all sources, NDR will correlate

Only the obvious bad investigated
- NDR ensures investigation time is spent on the most valuable alerts

Focusing on known bad
- Uncovers unknown and zero-day threats



Trellix



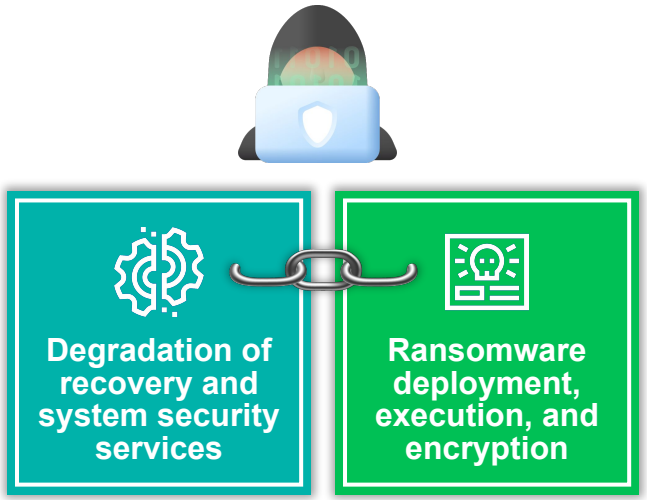
NDR Investigation Workflow

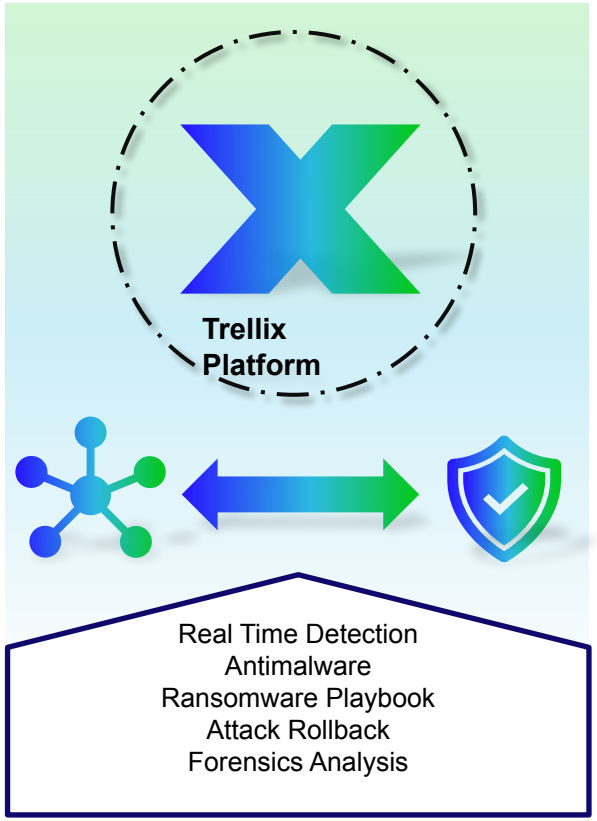
Trellix

A Perfect Complement to EDR

The perfect match

By integrating NDR with EDR, SOCs can respond more effectively to block ransomware attacks and prevent the exploitation of vulnerabilities. This complementary relationship between NDR and EDR ensures a more resilient defence against a wide range of cyber threats, enabling faster and more effective decision-making and response actions within key SOC playbooks.





- ✔ **Discover unmanaged endpoints and IOT devices**
- ✔ **Hunt for unusual user behaviour**
- ✔ **Identify suspicious file transfer**
- ✔ **Determine potential C&C traffic & compromised devices**
- ✔ **Rapidly scope an incident**
- ✔ **Identify lateral movement attempts**
- ✔ **Perform forensics analysis**
- ✔ **Rollback attack**
- ✔ **Automatically contain hosts**
- ✔ **Reduce MTTD and MTTR**
- ✔ **XDR Integration**

Trellix

Trellix NDR - See the whole picture

- ✔ 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

Multi-layered visibility, detection, investigation and response

Trellix

Thank You

Trellix

Trellix NDR

Complete network detection, protection and visibility

Visibility Dashboards
Track changes in Network Activity, Explore Ports, Protocols and Assets for advanced threat hunting

Detection Dashboards
Intuitive visualization of traffic patterns on attacker scope and techniques. Integration with Threat Intel and MiTRE ATT&CK Mapping

Asset Discovery
Extend visibility and automatically map discovered assets to device type, including new devices. Additional correlation with sensor telemetry

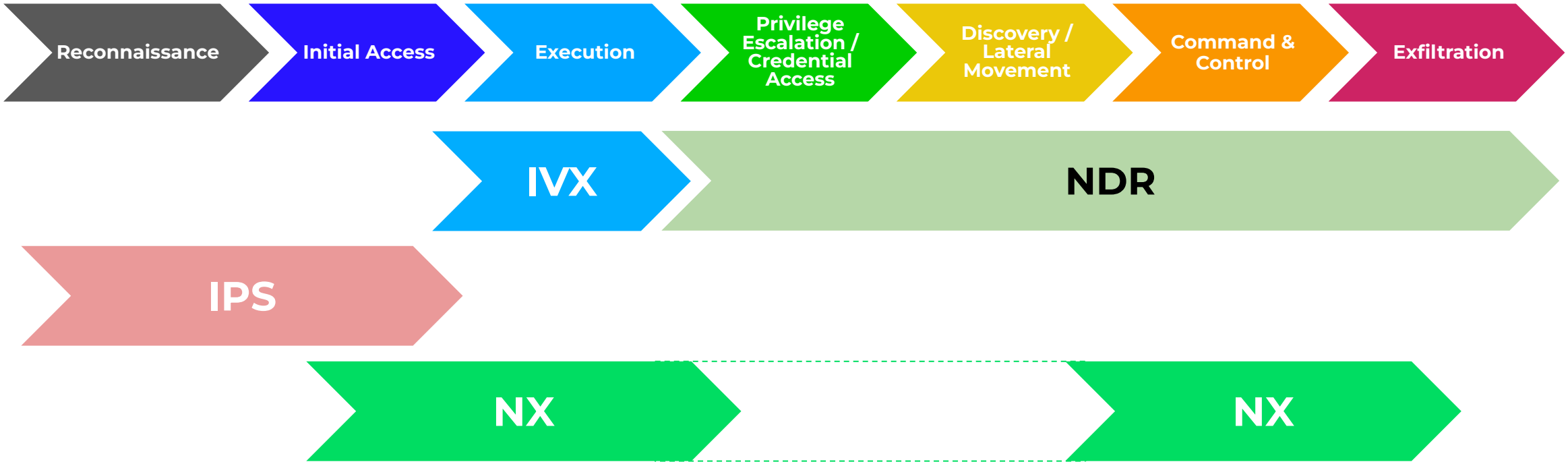
Analytics & Correlation
Continue to innovate differentiated high fidelity detection technologies building on a proven foundation of adaptable technologies

Enrichment & Prioritization
Improves situational awareness and risk posture for SOC Analyst.
Enriches network data with threat modelling based on attacker Tactics and Techniques

Investigative Workflow
Alerts combine into Incidents that are actionable. Incident workflow leverages XDR elements

Trellix

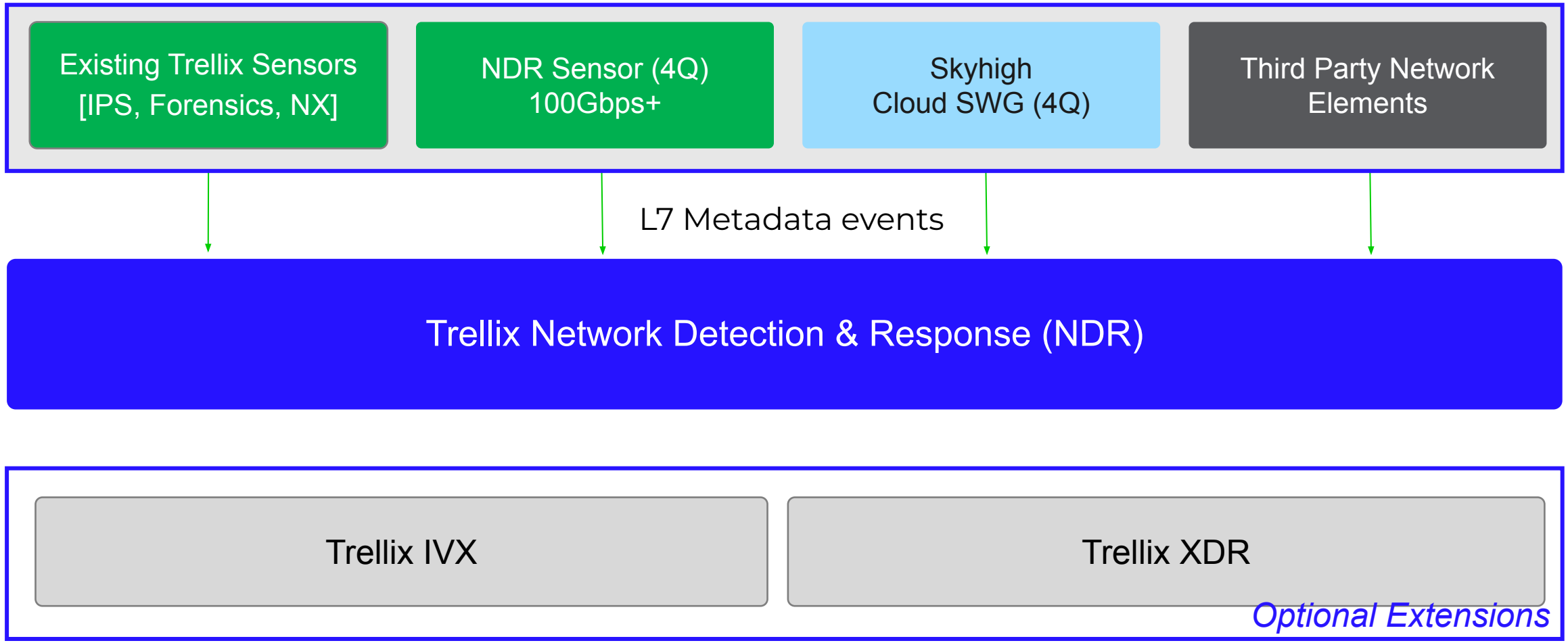
For existing customers



NDR provides post-compromise detection

Trellix

Leverage Existing Your Investment



Trellix