

Trellix

# Detect Undetectable and Evasive Network Attacks

Trellix NDR

**Presenter Name**

Presenter Title

April 9, 2024



# Speaker Intro



**Owen Edwards**

Director, Network Product Management



**Fabrizio Rega**

EMEA Solutions Engineer

# 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%**

<sup>4</sup>Increase in number of assets to protect

**69%**

<sup>2</sup>Unknown, poorly managed assets

**16 days**

<sup>1</sup>Global median dwell time

**35%**

<sup>3</sup>Ignored alerts



<sup>1</sup>Mandiant. 2023. [M-Trends 2023 Mandiant Special Report](#)

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

<sup>3</sup>FireEye 2021 (IDC InfoBrief "The Voice of the Analysts: Improving Security Operations Center Processes Through Adapted Technologies")

<sup>4</sup>JupiterOne 2023 (The 2023 State of Cyber Assets Report)

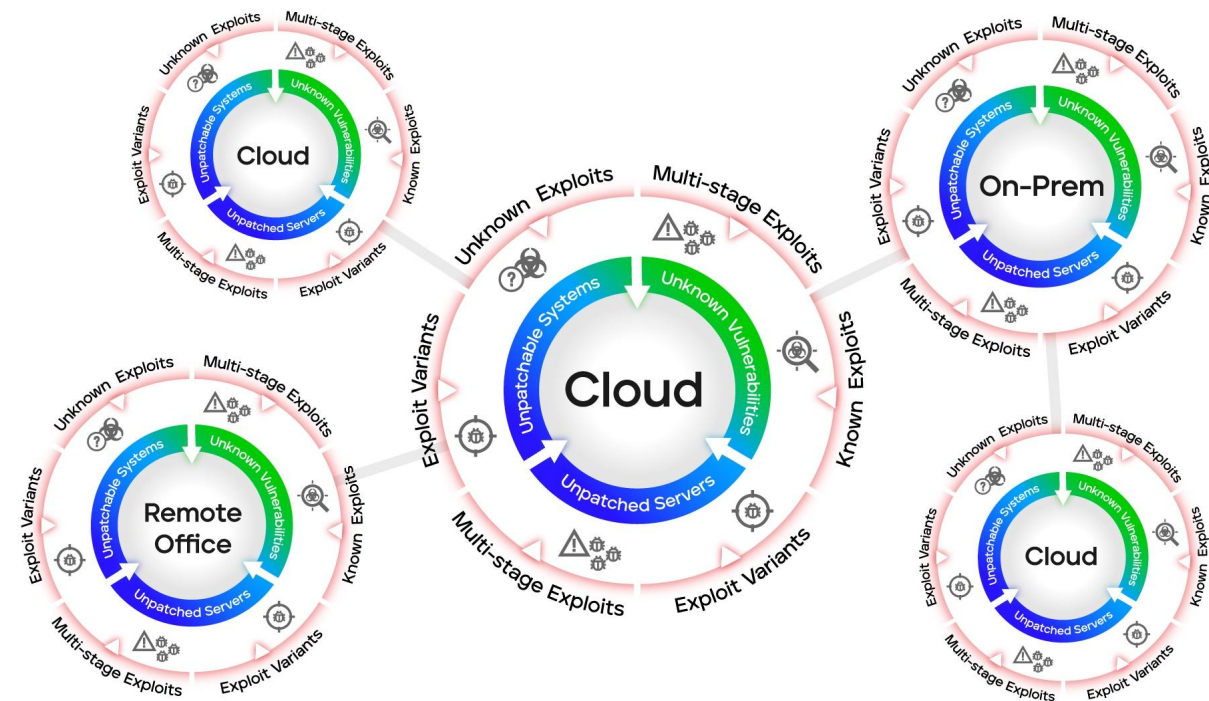


# Networks today

## 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



# 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

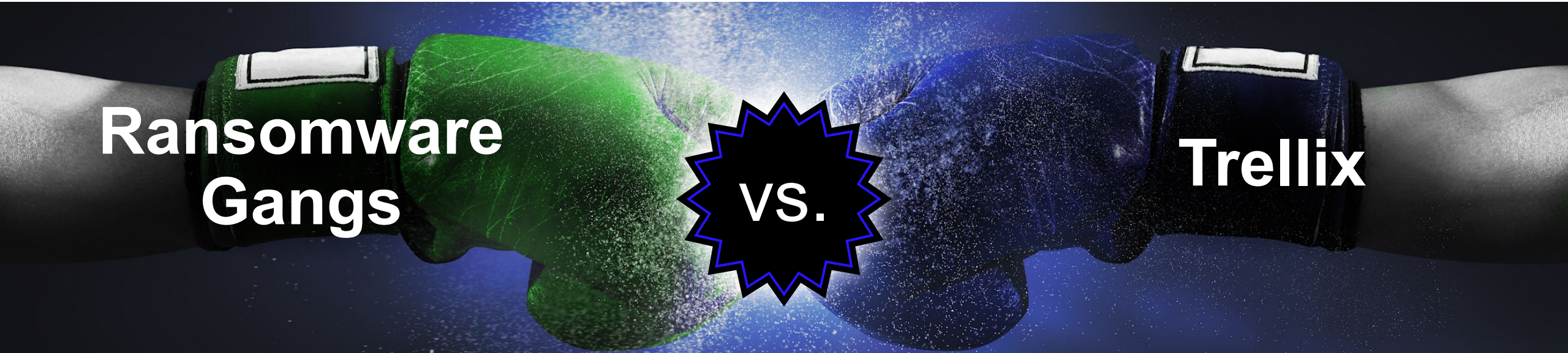
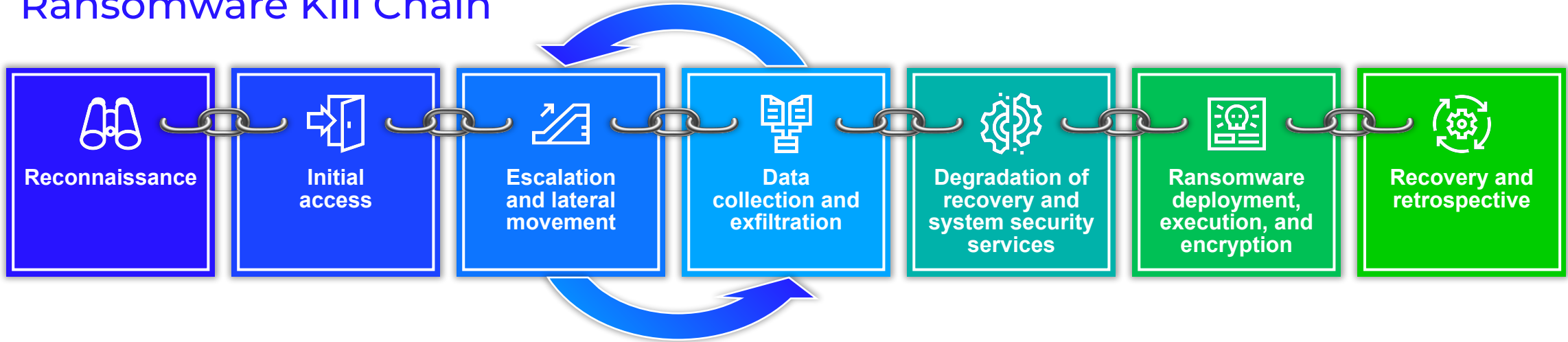


## Enterprise Applications (Workday, Salesforce etc.)

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

# The Phases of a Ransomware Attack

## Ransomware Kill Chain

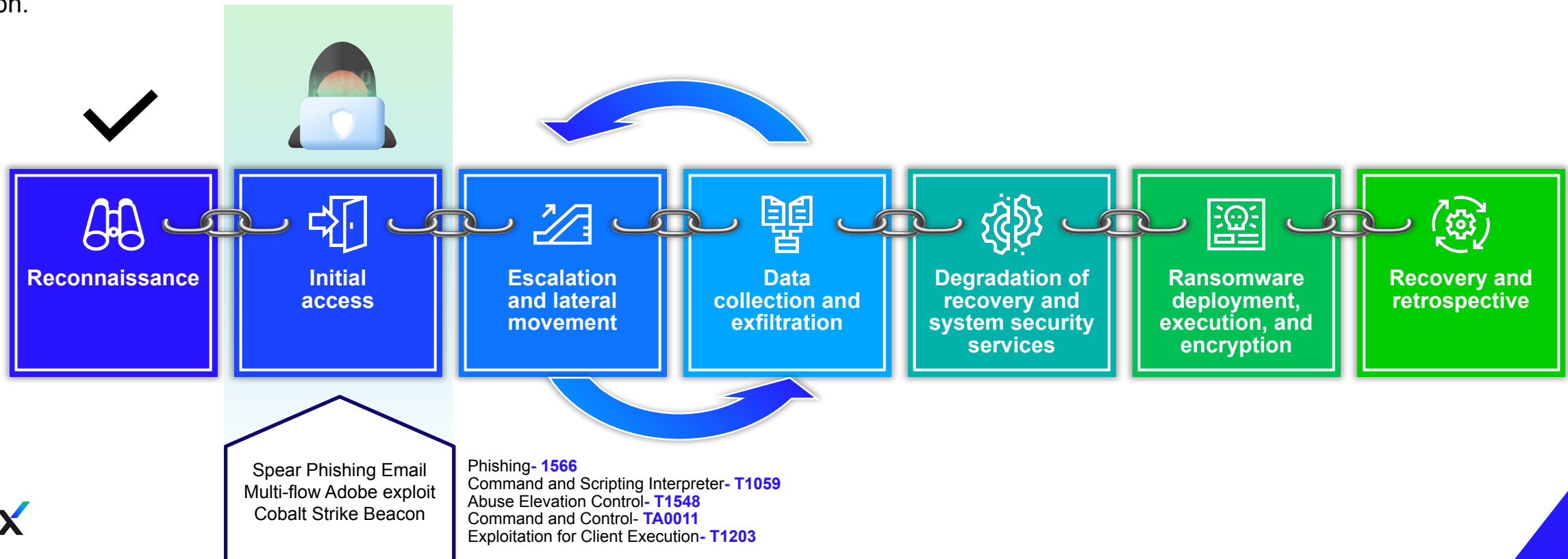




# One misguided click and they are in...

## Getting In

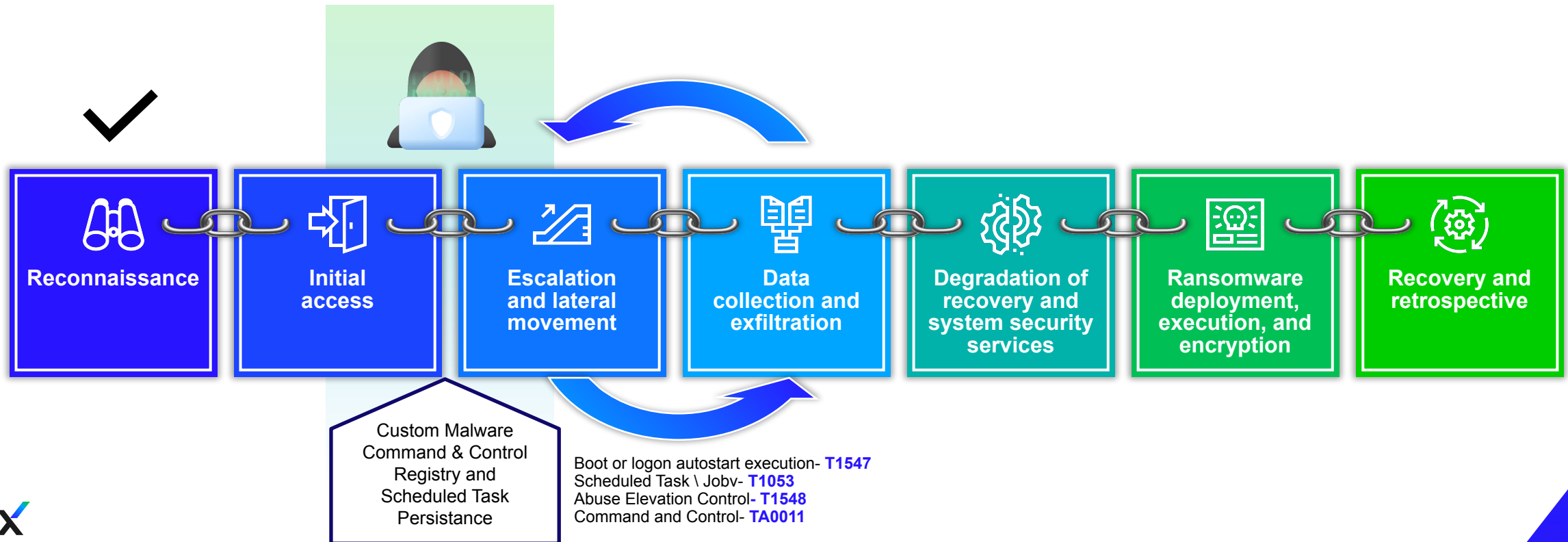
Email is still a common entry point for initial compromise, phishing emails trick recipients into clicking malicious links or downloading infected attachments. These emails often impersonate trusted entities to lower the guard of the targets. An arbitrary code execution vulnerability identified in Adobe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



# Then they establish themselves...

## Establishing Foothold

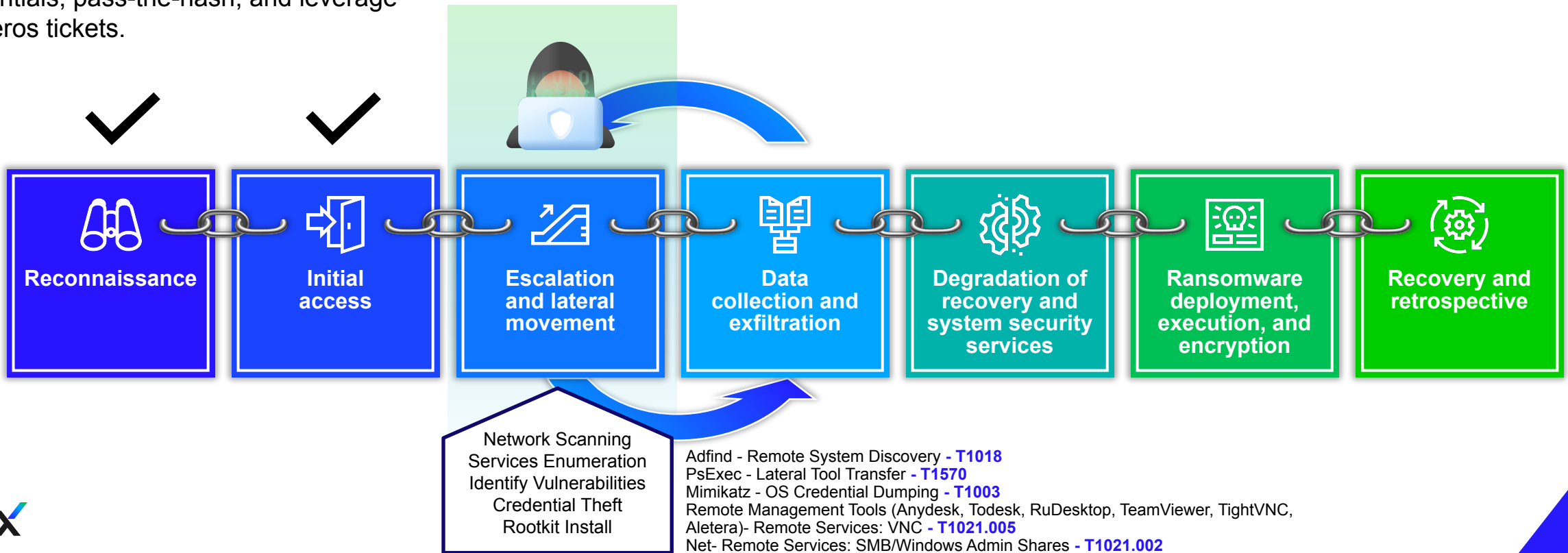
The infected endpoint will connect back to the Attacker's command and control infrastructure. Additional Payload is downloaded on the target machine. Registry and scheduled tasks to help maintain access



# 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.

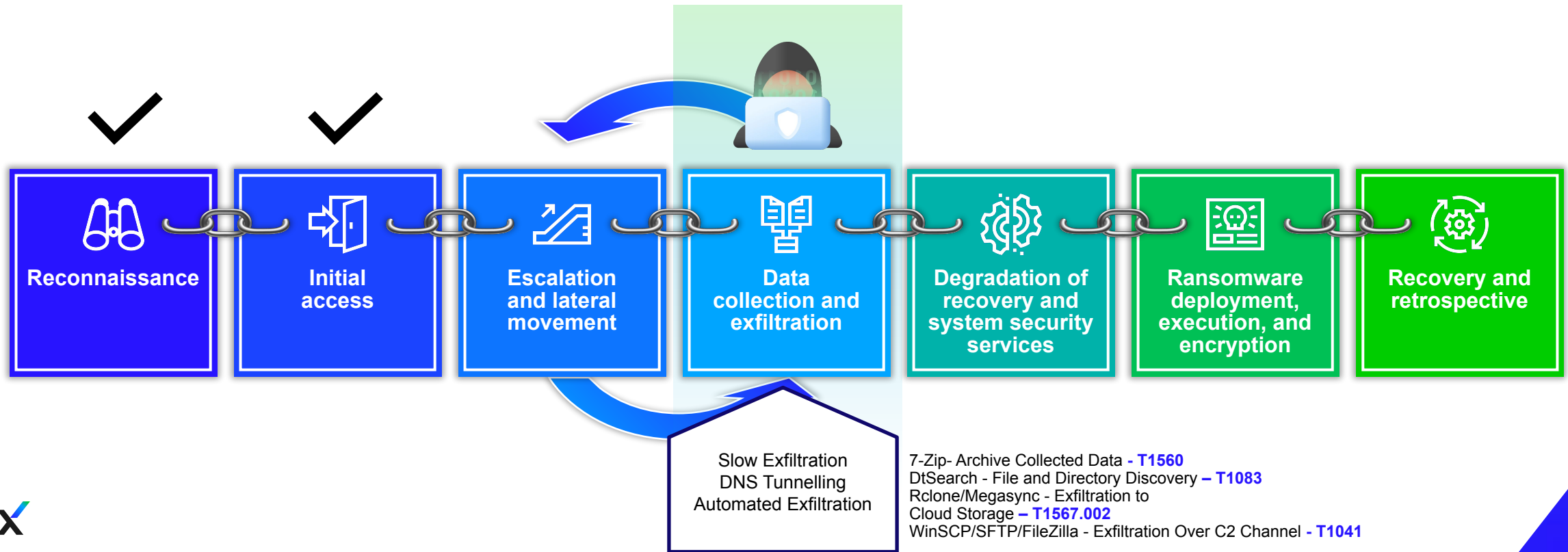




# Exfiltrating organization's data..

## 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

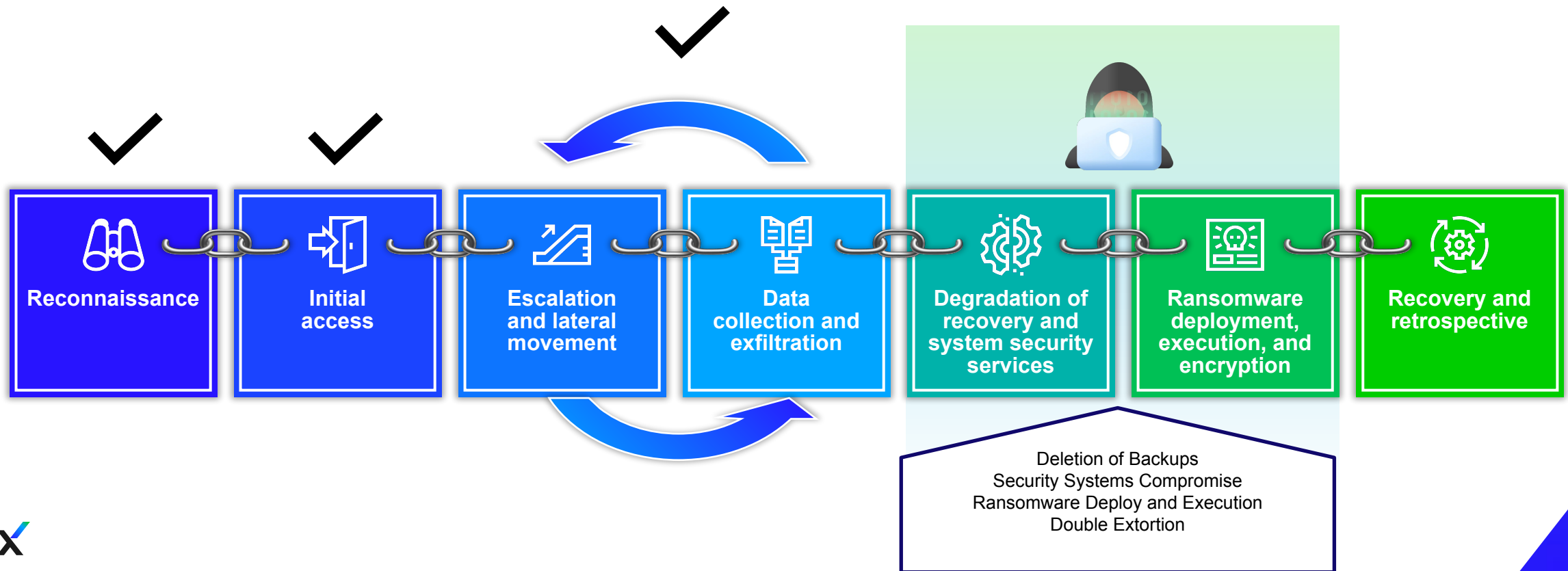


# Until they reach the goal..

## 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.



# 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**



### Assets

Show: Last 7 days

Devices Users

## 75272 Active Devices

- Mail Server 15
- NTP Server 176
- Web Server 338
- Other 74346
- PC 393
- Database 4

Asset Type: Mail Server, Web Server, NTP Server

Show 10 entries

Search:

IP Address	Asset Name	Asset type	OS	Total Events	Last Active
198.186.190.61	Not Available	Mail Server	Linux 2.6.x	1116	2024-03-11T13:24:48
10.14.1.148	Not Available	Mail Server	Not Available	85	2024-03-11T05:25:23
10.14.1.152	Not Available	Mail Server	Not Available	89	2024-03-11T05:25:23
10.14.1.68	Not Available	Mail Server	Not Available	108	2024-03-11T05:25:23
198.186.182.203	Not Available	Mail Server	Not Available	166	2024-03-11T13:25:33
198.97.35.104	Not Available	Mail Server	Not Available	166	2024-03-11T13:21:48
198.97.197.191	Not Available	Mail Server	Not Available	166	2024-03-11T09:24:48
198.97.197.23	Not Available	Mail Server	Not Available	43	2024-03-11T13:23:00
216.8.179.25	Not Available	Mail Server	Not Available	47	2024-03-11T13:23:45
217.12.11.66	Not Available	Mail Server	Not Available	267	2024-03-11T13:21:10

# NDR Asset Discovery

# 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

- 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

## Traffic Analysis

“User anomaly detection”

Identifying unlikely  
behaviors

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

## Signature-based Detection

“Find known bad”

High speed  
analysis  
at scale

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

# 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

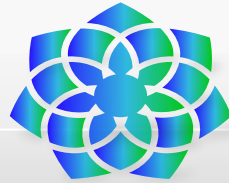
- ML exfil module detects unusual file transfers
- Signature-based exfil detection

Leveraging multiple detection and AI approaches



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



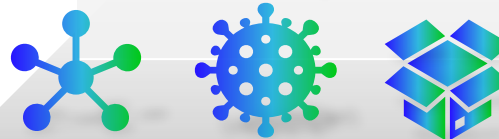
Network Investigator

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 Network Portfolio



## Trellix Intrusion Prevention System (IPS)

### Primary Function

**Server / Datacenter workloads**  
**High-throughput traffic**

### Scalability

100 Gbps (200 Gbps planned)

### Security Capability

**Deep packet inspection:**  
Exploit protection / virtual patching, adv. Malware engines, DoS/ DDoS, deep file inspection, C&C, reputation, L7 visibility

Integration with IVX

**Zero-Day Suspicious File Detonation**

**Deployment Options**



## Trellix Network Security (NX)

**User Devices,**  
**Web and SMB traffic**

20 Gbps

**Advanced Threat Detection:**  
Lateral movement, web infections, callbacks, beaconing, data exfiltration, basic IPS, L7 visibility

On-box or  
via IVX for clustering

Physical, Virtual, Public and Private Cloud, Integrations with AWS Load Balancer



## Trellix Packet Capture (PX)

**Visibility for Forensics, Compliance**

40 Gbps

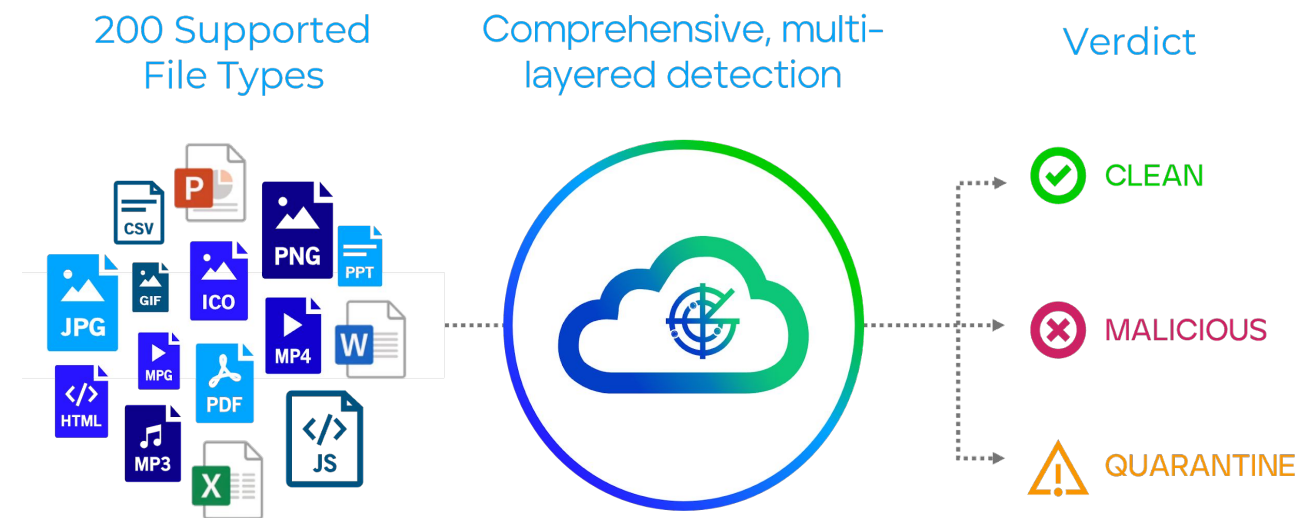
**Full packet capture:**  
Lossless packet capture, Session decoder, indexing and fast search

Integration with IVX

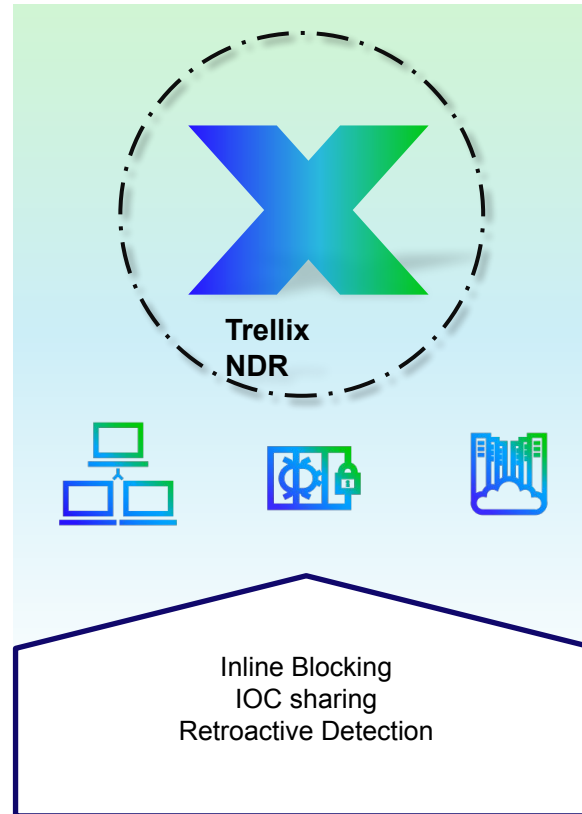
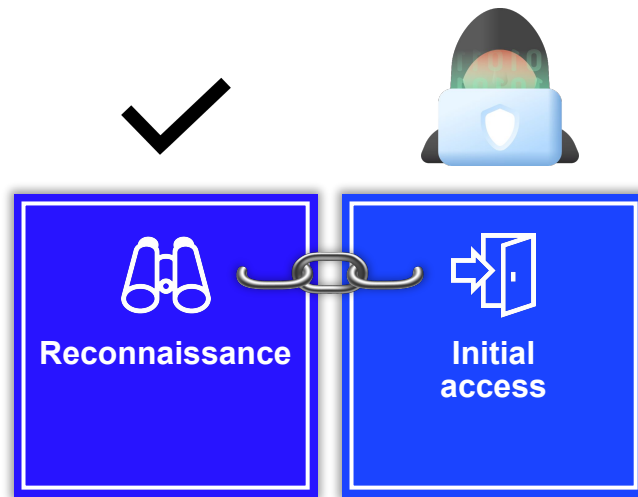
# For that zero-day evasive attack

## 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



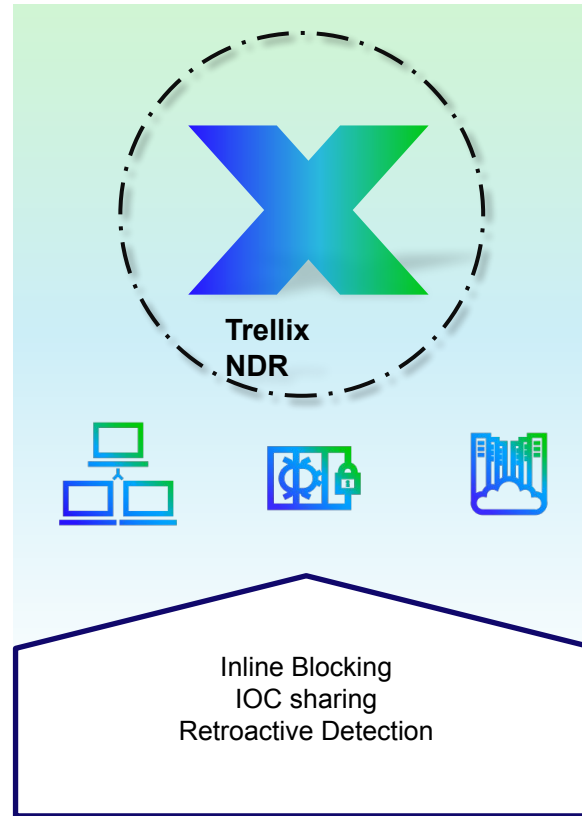
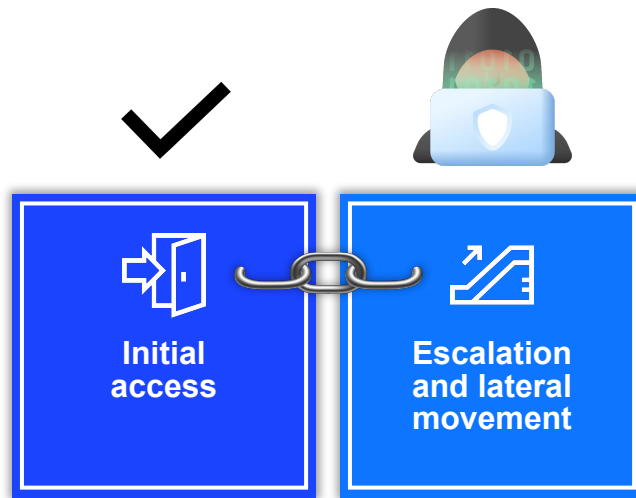
# NDR disrupts initial access



- ✓ Full protocol analysis
  - ✓ Domain/URL Blocking
  - ✓ Phishing Detection
  - ✓ Signature based intrusion prevention
  - ✓ Dynamic Analysis
  - ✓ C2 Detection
- 
- ✓ Telemetry and L7 Metadata sent to NDR

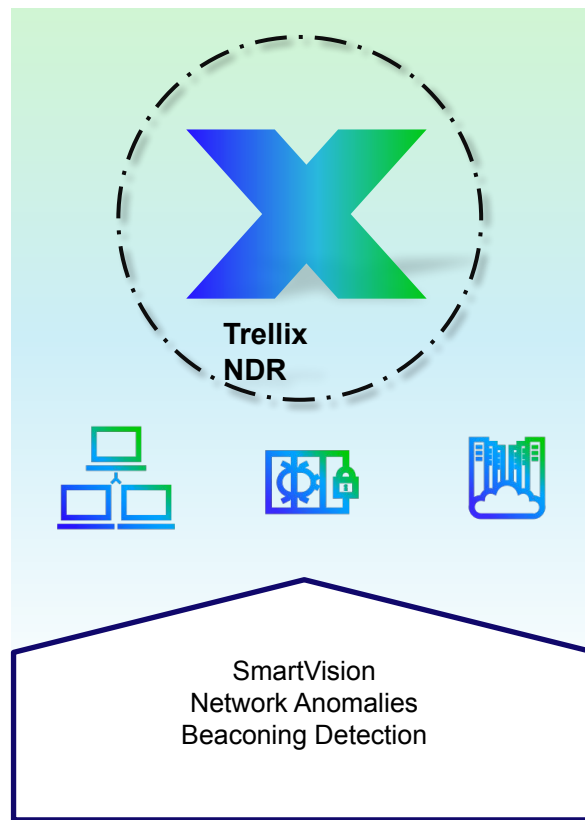
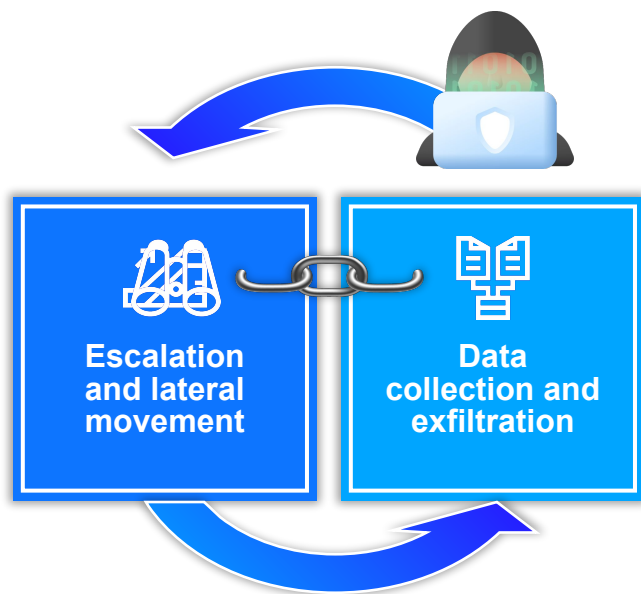


# NDR detects lateral movement and escalation



- ✓ Pass the Hash
  - ✓ Credential Dumping
  - ✓ Fileless Malware Detection
  - ✓ Host Enumeration
  - ✓ User Enumeration
  - ✓ Network Mapping
- 
- ✓ Telemetry and L7 Metadata sent to NDR

# 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

### Dashboard

Show: Last 24 hours

Detection Visibility

#### Top Threats

Threats: All Status: All

Severity and Threat Name	Status	Time Detected (UTC)	Assets
MINOR ICMP: Unsolicited Echo Reply	<b>3564 Alerts</b> 3564 New   0 Open   0 Closed	2024-03-11T10:01:50 (2 minutes ago)	22
MINOR DNS: ISC BIND RPZ Rule Processing Vul...	<b>1267 Alerts</b> 1267 New   0 Open   0 Closed	2024-03-11T09:56:56 (7 minutes ago)	51
MINOR SSL: TLSv1.x Session Detected	<b>99 Alerts</b> 99 New   0 Open   0 Closed	2024-03-11T09:24:50 (39 minutes ago)	14
MINOR DNS: Invalid Field Value Detected	<b>82 Alerts</b> 82 New   0 Open   0 Closed	2024-03-11T09:09:39 (an hour ago)	2

#### Threat Types



- CRITICAL 1
- MAJOR 130
- MINOR 5514

#### MITRE ATT&CK MATRIX

Focused View

# NDR Threat Reporting

- Resource Development (1)
- Defense Evasion (1)
- Discovery (1)
- Command and Control (3)
- Impact (2)

8 Tactics

- Resource Development 1
- Defense Evasion 1
- Discovery 1
- Command and Control 3
- Impact 2

# Accelerate investigation and response

## Advanced Threat Detection

Advanced signatures, ML/AI and behavioral analysis detect emerging threats

## Scoping

Multi sensor correlation and integrations deep visibility for forensics and root cause analysis

## Investigation

Automated enrichment with threat intel, MITRE techniques, and analytics speeds investigations

## Hunting

Full PCAP, L7 metadata, and flow data visibility for adv. hunting

## Containment & Remediation

Expedite responses with XDR, SOAR playbooks and ticketing system integrations

**Provides visibility and alert priority to respond quickly**



# 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

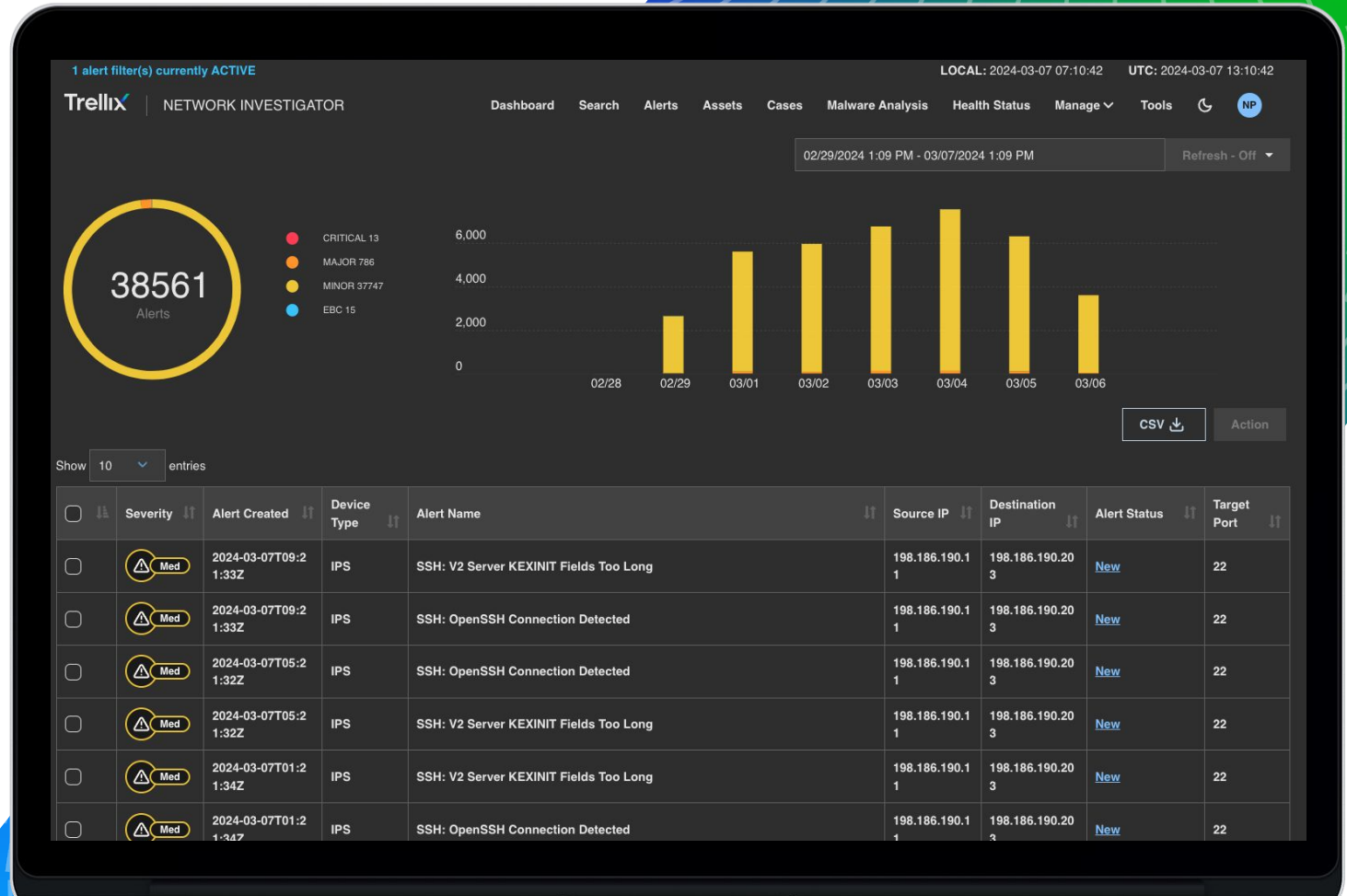
- NDR lets you turn on all sources, NDR will correlate

## 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



← 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?

19

MINOR 19

# NDR Investigation Workflow

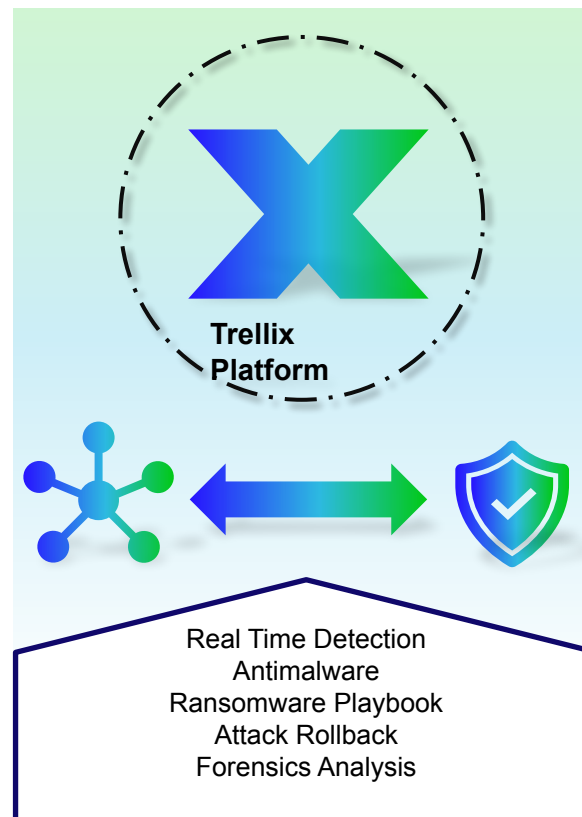
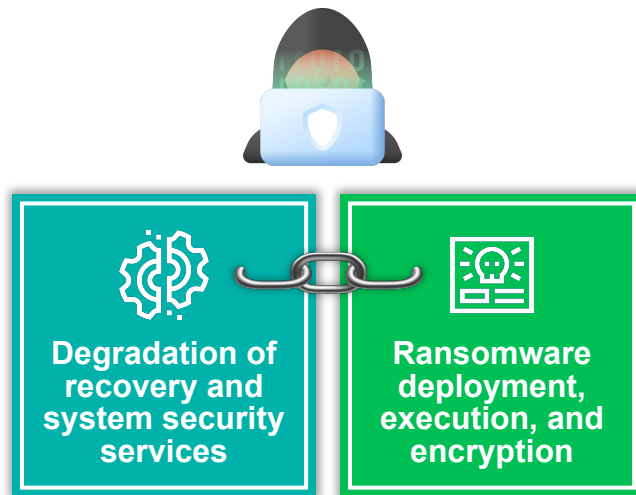
Traffic Distribution Over Time

By Traffic Volume  By Network Flows

# 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 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**





# 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



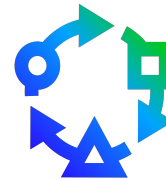
### Analytics & Correlation

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



### Detection Dashboards

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



### Enrichment & Prioritization

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



### Asset Discovery

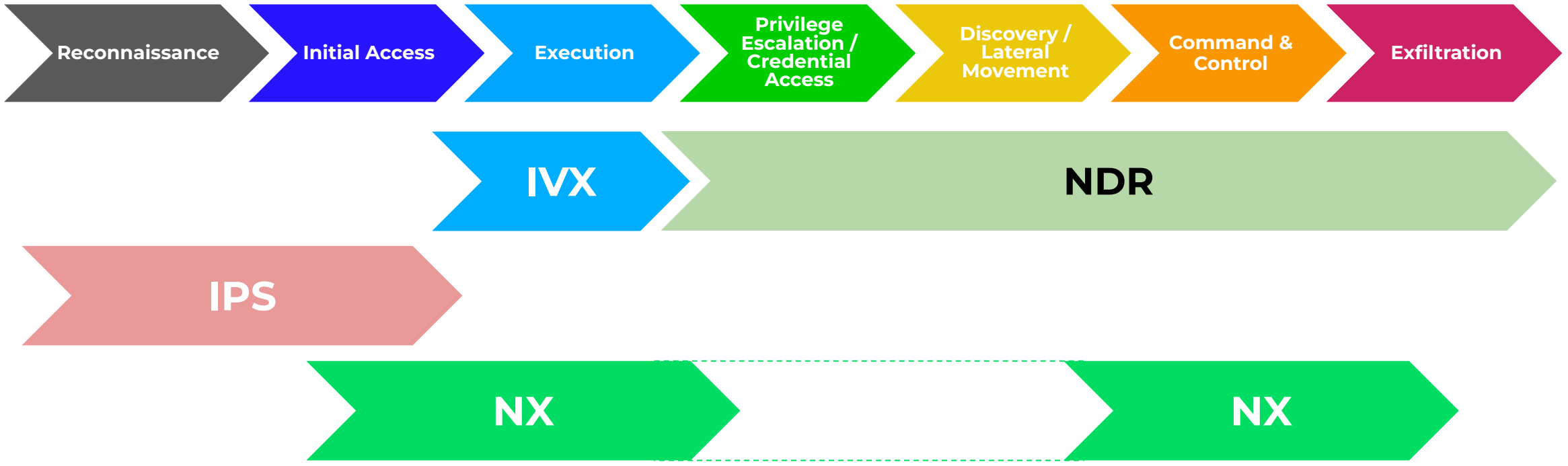
Extend visibility and automatically map discovered assets to device type, including new devices. Additional correlation with sensor telemetry



### Investigative Workflow

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

# For existing customers



**NDR provides post-compromise detection**

# Leverage Existing Your Investment

