



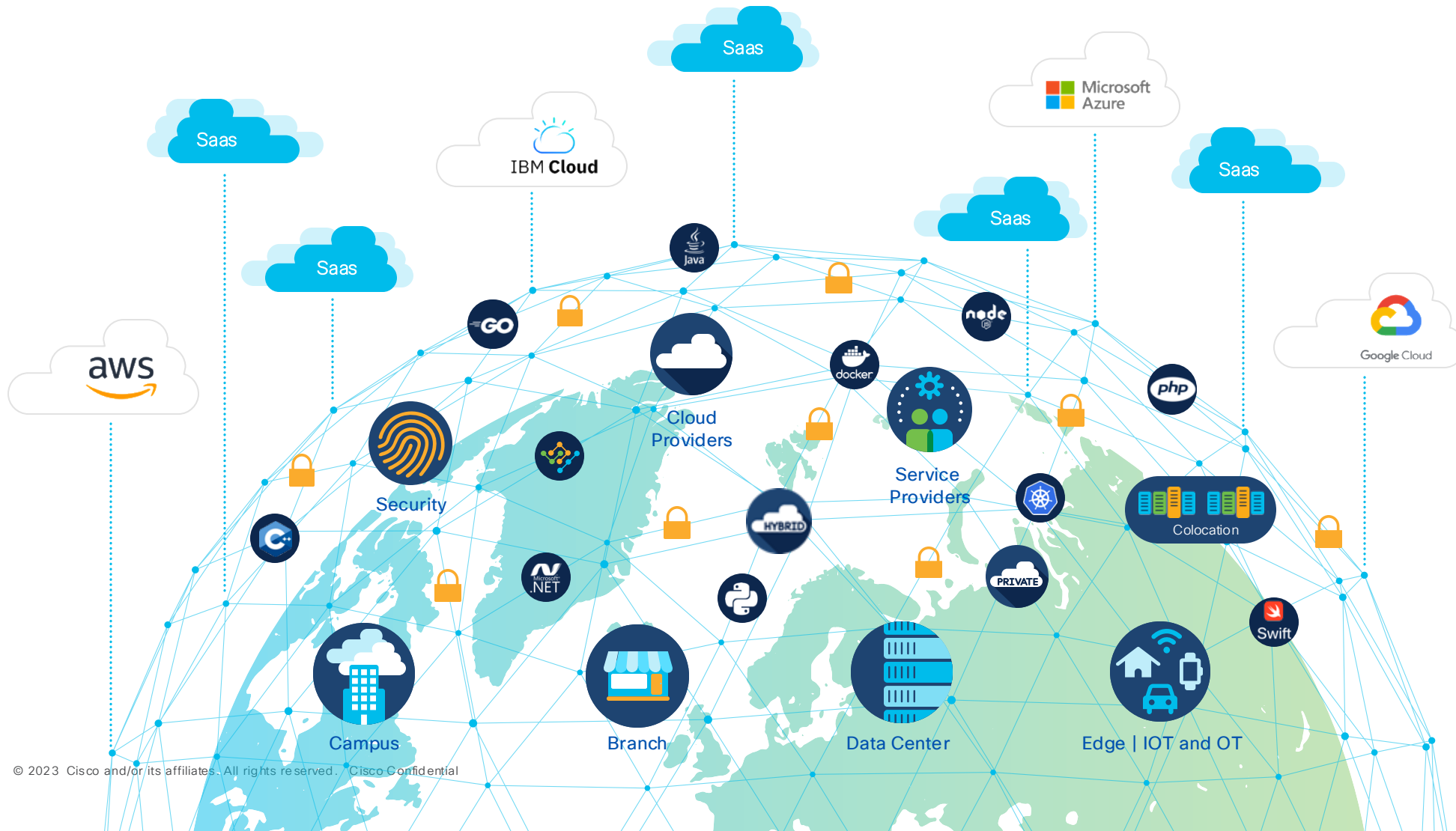
# Cisco XDR

Milan Rášo

Solutions Engineer  
Cisco Systems Slovakia

22.05.2025

# The new normal is a hyper-distributed, extremely diverse IT landscape





Advanced Persistent Threats

Ransomware

Credential compromise

Supply chain attacks

Spyware / Malware

Supply chain attacks

Crypto-mining

Unpatched Software

Data / IP Theft

Wiper Attacks

Malvertising

Phishing

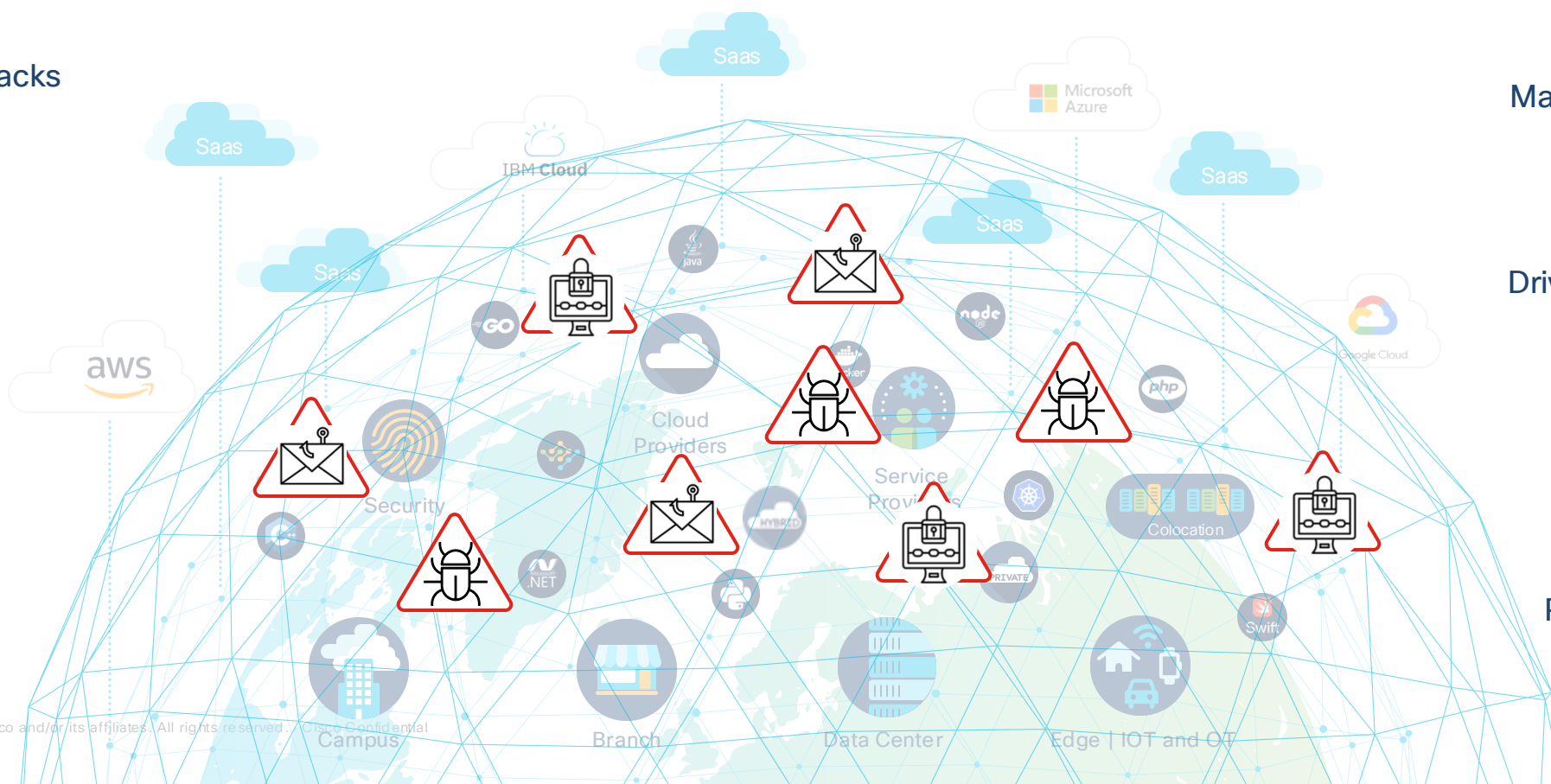
Drive By Downloads

DDoS

Botnets

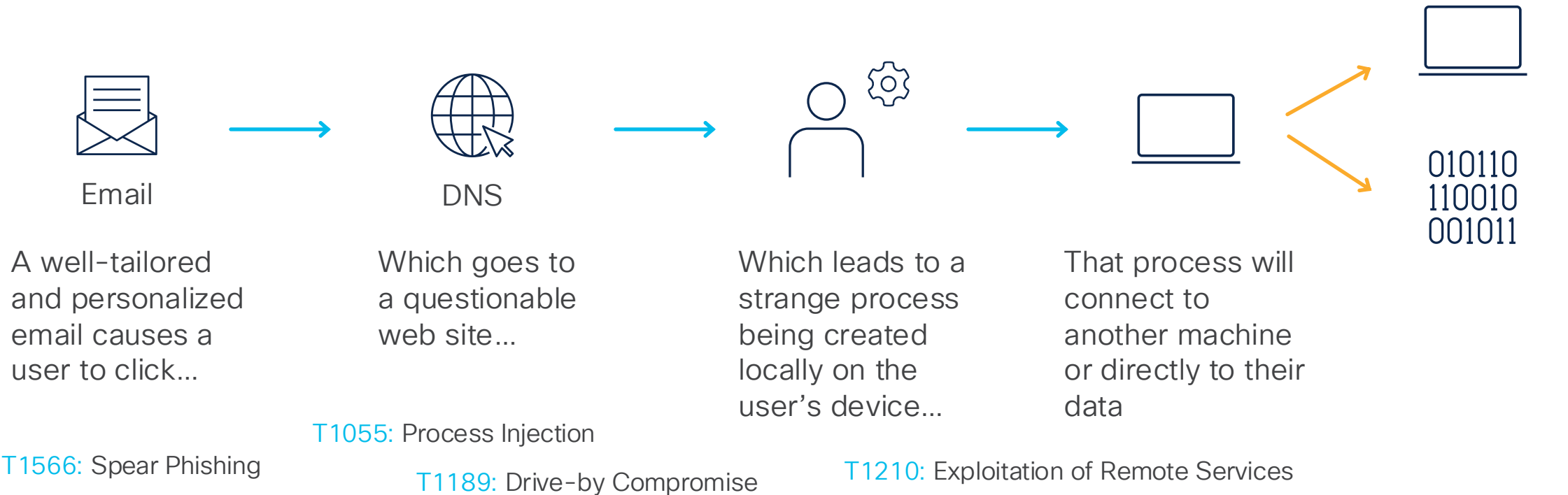
Man in the Middle

Rogue Software



# Stop advanced threats like ransomware

Most attacks use a sequence like this...



# Why do we need XDR?

## Mandiant Inc

Medium-sized businesses are using 50-60, and large organizations or enterprises are using over **130 tools** on average

## ESG reports

**2/3** of security leaders experienced an incident that could have been prevented if security operations were improved.

## ESG reports

**84 %** of organizations claim improving efficacy and efficiency of SecOps is a top 5 priority.

Simplicity



Visibility



Efficiency



# An XDR is as good as its outcomes

Where are we **most exposed** to risk?  
How good are we at detecting attacks **early**?

1

Detect Sooner

Prioritise by Impact

2

Are we **prioritizing the attacks** that represent the largest **material impacts** to our business?

How quickly are we able to understand the **full scope** and **entry vectors** of attacks?

3

Compress Investigation Time

Accelerate Response

4

How fast can we **confidently respond**?  
How much can SecOps **automate**?  
Are we **improving** our time to respond?

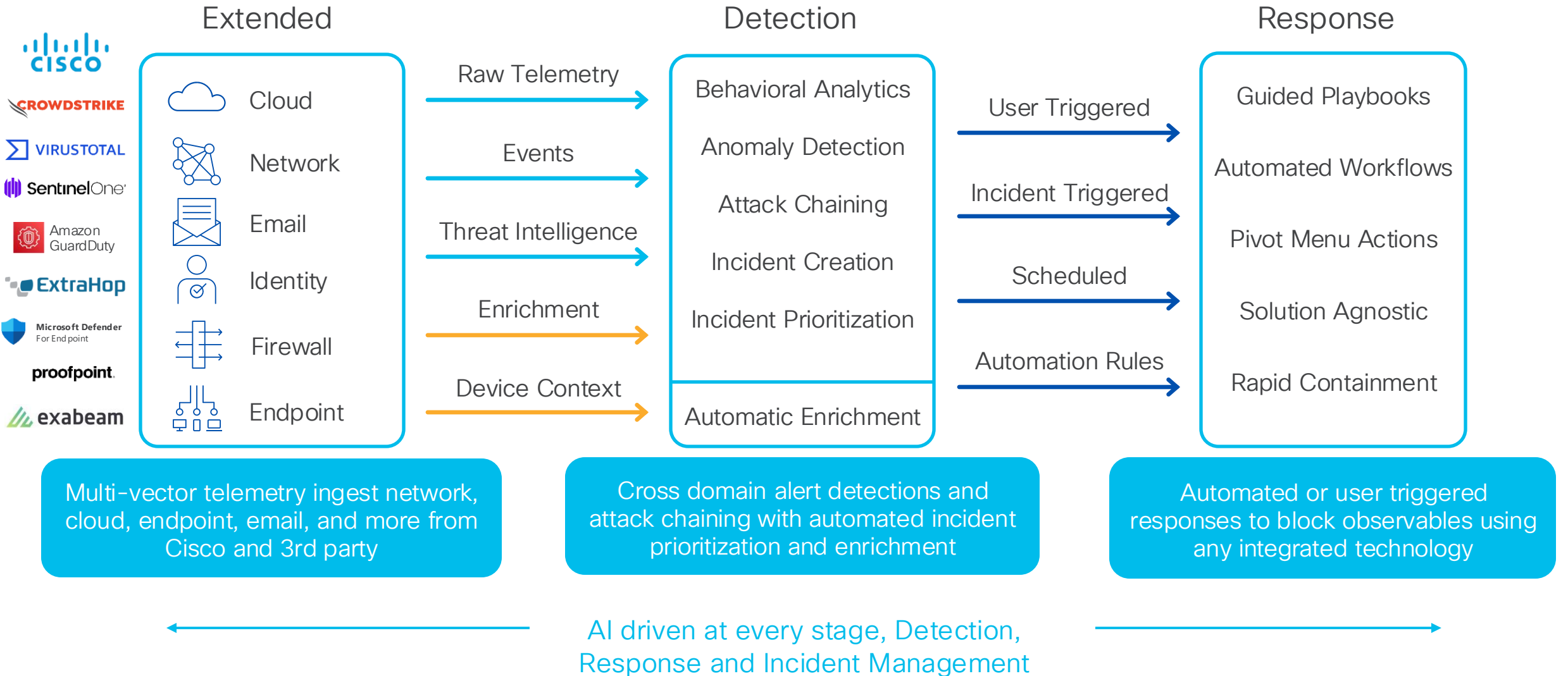
Do we have **full visibility** into all our assets?  
Can we **reliably identify** a device and who uses it?

5

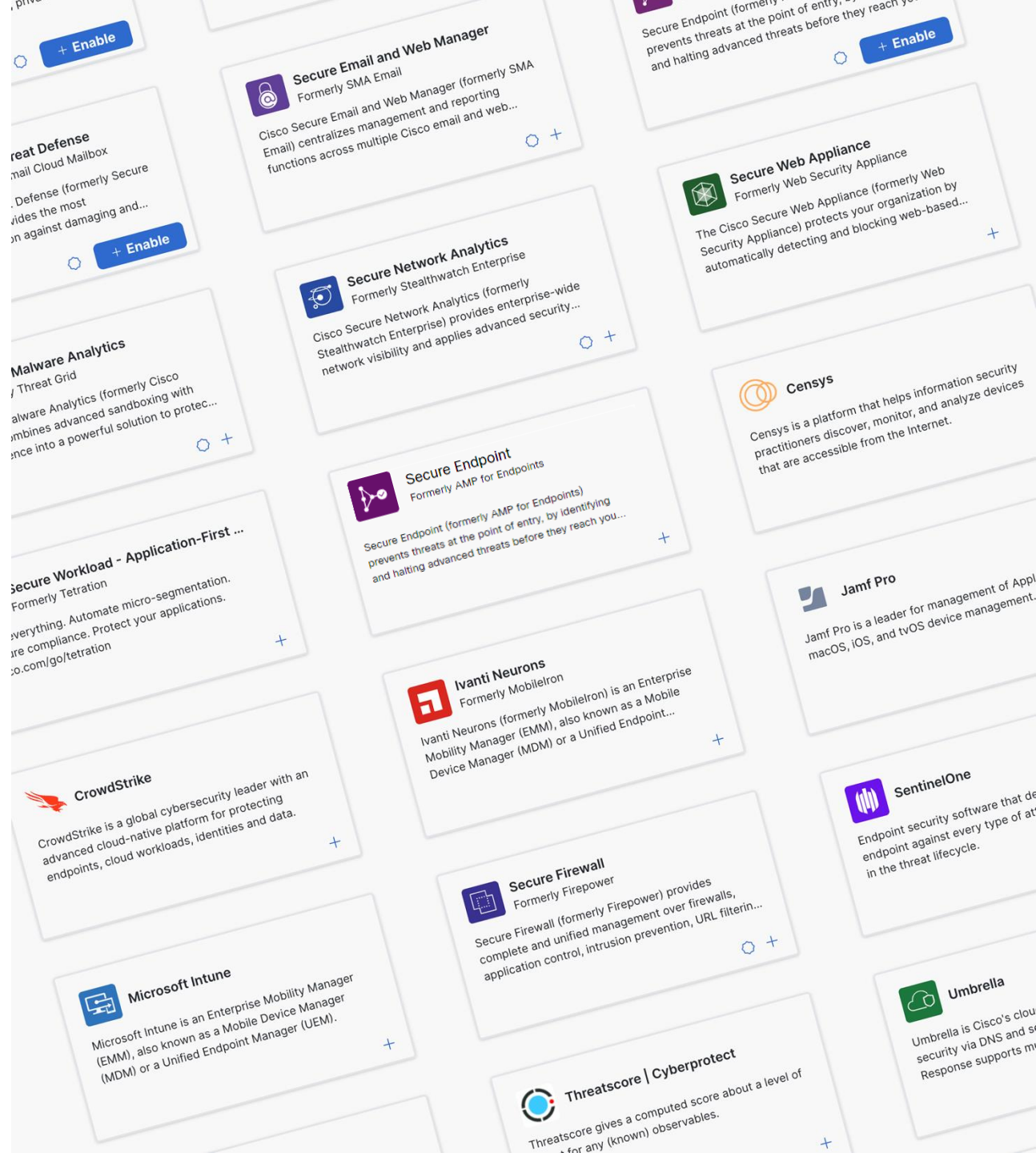
Extend Assets Context



# High level architecture



# Extended context

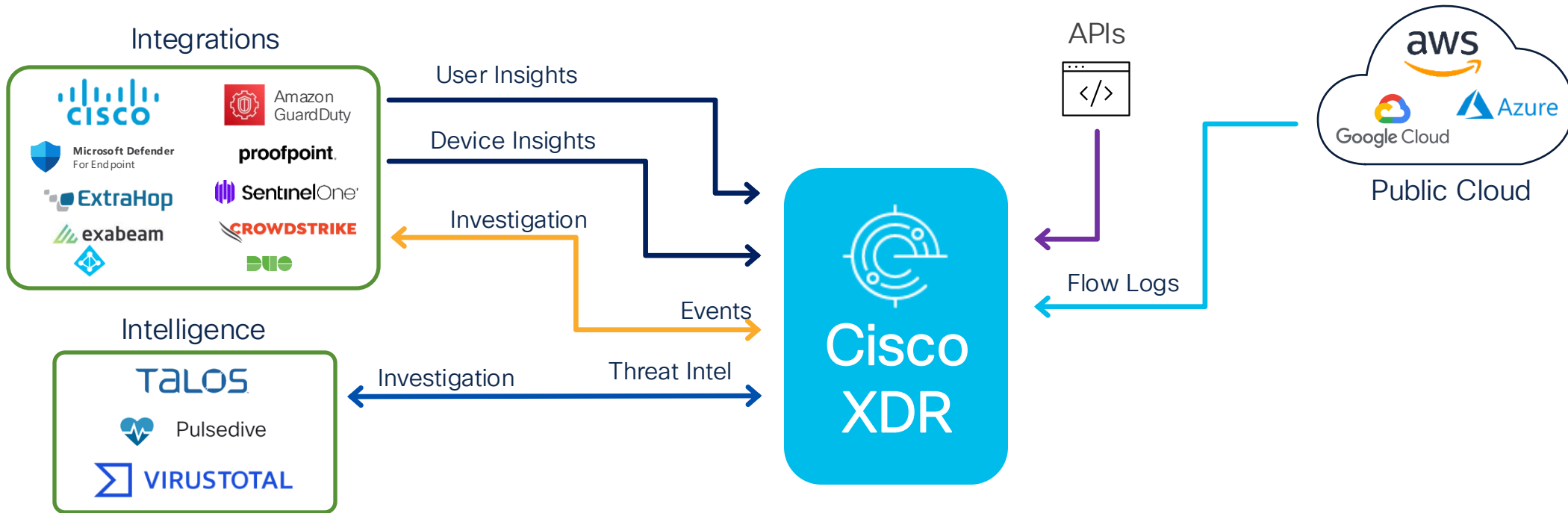




Extended context

# Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Extended context

# Devices

Extends the integration framework to collect data about device inventory and posture.

- Unique combination of data from security products and traditional device managers.
- Results in a unified asset inventory that can be used to provide context to investigations and meaningful reports.
- Each device has a single page of information about it, merged from all sources.
- Allows defining a device's "value" which is used when scoring XDR incidents.

← Back to Devices **Marble-WIN11.explorcorp.com** [+ Add Labels](#) Device Value: 10 (Default value) [Refresh from Orbital Live Query](#)

### Details

Operating System	Windows 11, SP 0.0 (Build 22631.3296)	Location	Herndon, VA
Managed	Yes	Associated Users	EXPLORCORP\marble, tme, marble
Model	VMware	Macs	00:50:56:be:18:25
Last Active	2024-04-08T21:05:24.000Z	Hardware Id	4140a80f-a80b-492a-9d7f-a8ee8a557d12
Local IPs	192.168.249.111, fe80::aab3:ff80:15bd:f052	Serial Number	vmware-42 3e 59 d7 09 72 6f 57-89 of 70
Public IPs	64.102.255.47, 64.102.255.40, 173.38.117.84		

### Windows Security Center

Firewall	Windows Firewall	Disabled	Up to Date
Automatic Updates		Enabled	
AntiVirus	Cisco Secure Endpoint	Enabled	Up to Date
	Microsoft Defender Antivirus	Disabled	Up to Date
AntiSpyware		Enabled	
User Account Controls		Enabled	

### Cisco Secure Endpoint (AMP)

Definitions	Definitions Up To Date
Isolation	Not Isolated
Orbital	Not Enabled
Connector GUID	ebb3a111-c405-4d43-bc80-11f4b6bfb33a

### Meraki Systems Manager - ExplorCorp

Meraki Systems Manager UID	784752235069323297
Last Seen	2024-04-07T22:46:25.000Z
App Users	EXPLORCORP\marble
Tags	recently-added
Auto Tags	geo_compliant pc windows_agent_enrollment windows_profile_enrollment

[View full details](#)

### Orbital - ExplorCorp

Orbital UID	ebb3a111-c405-4d43-bc80-11f4b6bfb33a
Last Seen	2024-04-08T03:42:40.757Z

### Secure Client

Secure Client UID	aff8649c-7d06-4be4-9b1b-f3a1d67f
Last Seen	2024-03-15T04:33:24.401Z
Deployment	Breach Defense
CSC Version	5.1.1.42
Secure Endpoint Version	8.2.1.21650
Cloud Management Version	1.0.1.400
Modules	Cloud Management v.1.0.1.400 Cisco Secure Endpoint v.8.2.1.21650 AnyConnect VPN v.5.1.1.42 Umbrella v.5.1.1.42 Network Visibility Module v.5.1.1.42
CSC UDID	aff8649c-7d06-4be4-9b1b-f3a1d67f
AC UDID	
Serial Number	vmware-42 3e 59 d7 09 72 6f 57-89



Extended context

# Identity

Leverage the integration framework to collect data about user inventory and posture.

- Results in a unified asset inventory that can be used to provide context to investigations and meaningful reports.
- Each user has a single page of information about it, merged from all sources.
- Allow User and Device data association with detections and incidents

The screenshot displays the Cisco Identity Management console for 'Users'. At the top, there is a 'Source health' indicator showing 'Healthy' with a blue checkmark and the text 'All sources are operational'. To the right, a summary box shows 'Users 25 total', '0 Guests', and '0 Groups'. Below this is a search bar with the text 'Search', a 'Filters' button, and '25 matching results'. An 'Export to CSV' button is located in the top right corner of the table area. The table itself has the following columns: 'Display name', 'Login names', 'Emails', 'Department', 'Manager', 'Last logon', and 'Account type'. The table lists 15 users, including Eric Rennie, flint, Greg Barnes, Hanna Jabbour, Ian Redden, JournalNDR, marble, Matt Vander Horst, Mike McAllister, overlord, pradnya padaki, quartz, Rebecca I. Ross, Remi I. Reid, and Robert Harris.

Display name	Login names	Emails	Department	Manager	Last logon	Account type
Eric Rennie	eric.rennie@explorcorp.com	eric.rennie@explorcorp.com, errennie@cisco.com			2023-07-10T12:08:00.000Z	Member
flint	flint@explorcorp.com	flint@explorcorp.com			2024-03-07T16:17:17.000Z	Member
Greg Barnes	grebarne@explorcorp.com	grebarne@explorcorp.com			2023-10-16T14:29:14.000Z	Member
Hanna Jabbour	hanna.jabbour@explorcorp.com	hanna.jabbour@explorcorp.com			2023-04-17T13:38:14.000Z	Member
Ian Redden	iaredden@explorcorp.com	iaredden@explorcorp.com				Member
JournalNDR	JournalNDR@explorcorp.com	JournalNDR@explorcorp.com				Member
marble	marble@explorcorp.com	marble@explorcorp.com			2024-01-23T13:35:45.000Z	Member
Matt Vander Horst	matt.vanderhorst@explorcorp.com	matt.vanderhorst@explorcorp.com			2023-05-25T15:36:03.000Z	Member
Mike McAllister	mike.mcallister@explorcorp.com	mike.mcallister@explorcorp.com			2023-04-26T17:50:20.000Z	Member
overlord	overlord@explorcorp.com	overlord@explorcorp.com				Member
pradnya padaki	pradnya.padaki@explorcorp.com	pradnya.padaki@explorcorp.com				Member
quartz	quartz@explorcorp.com	quartz@explorcorp.com			2024-01-16T15:01:46.000Z	Member
Rebecca I. Ross	rebecca.irene.ross@explorcorp.com	rebecca.irene.ross@explorcorp.com			2023-04-06T20:21:32.000Z	Member
Remi I. Reid	remi.i.reid@explorcorp.com	remi.i.reid@explorcorp.com			2024-04-05T15:54:30.000Z	Member
Robert Harris	robert.harris@explorcorp.com	robert.harris@explorcorp.com			2023-04-06T15:51:59.000Z	Member

# Supported sources for XDR Devices and Identity



Duo Access  
Duo Beyond



Secure Endpoint



Umbrella (DNS)  
Windows / macOS



Meraki SM



Secure Client



Orbital



Duo

---

*Third Party*

---



CrowdStrike



SentinelOne



Microsoft  
Intune



Jamf Pro



Ivanti Neurons  
(formerly MobileIron)



VMware  
Workspace ONE  
(formerly Airwatch)



Microsoft Defender  
for Endpoint



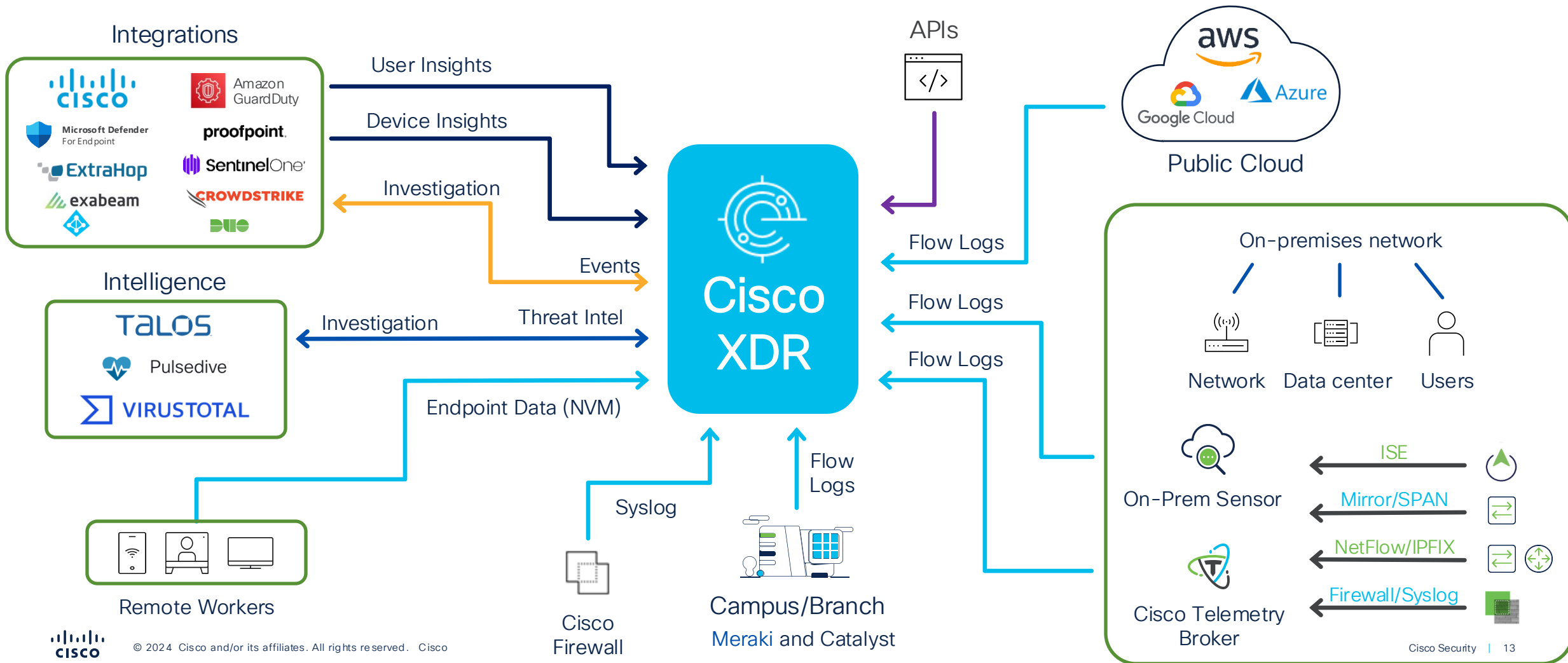
Microsoft  
Azure AD



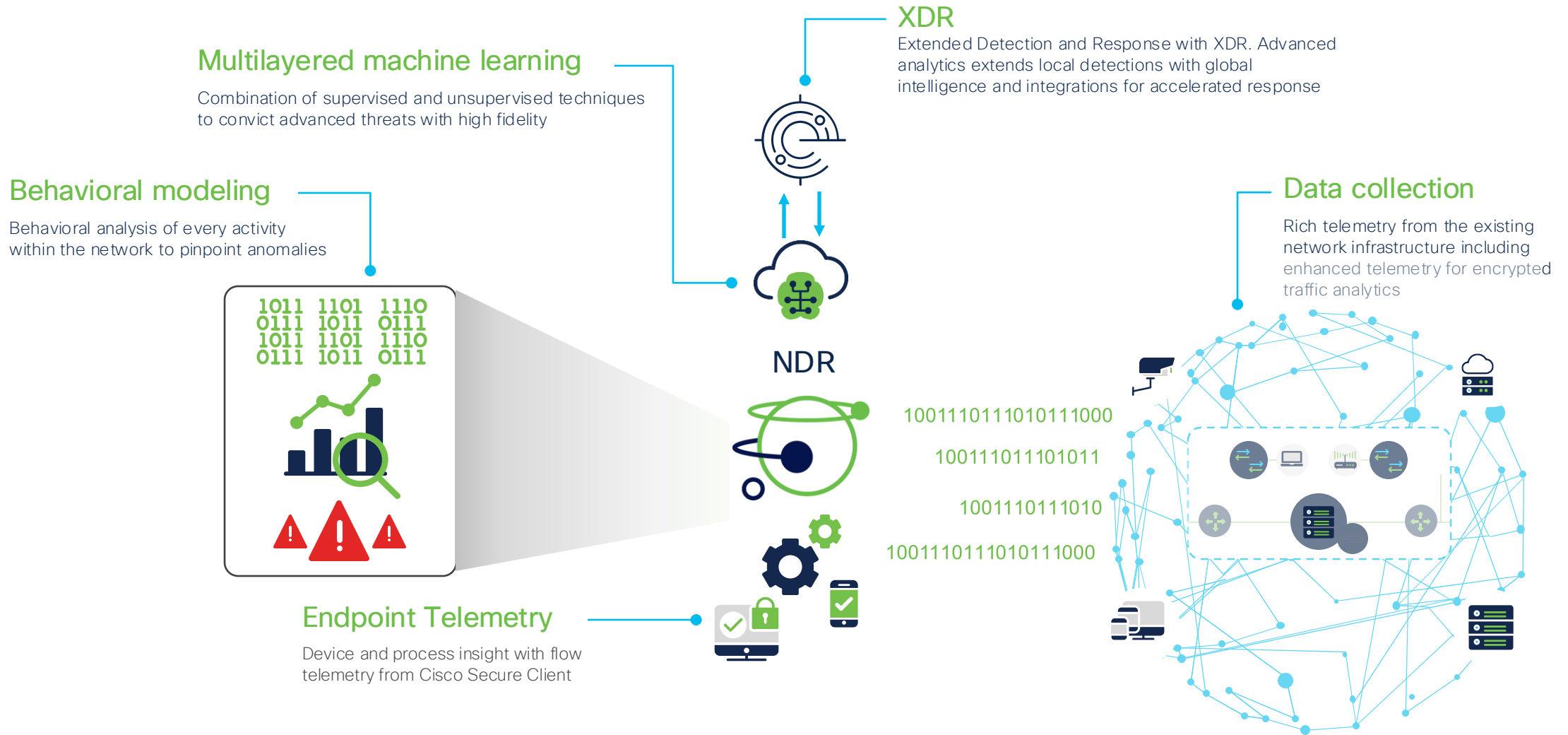
Extended context

# Telemetry sources for Cisco XDR + NDR!!

Flexible integration for existing infrastructure



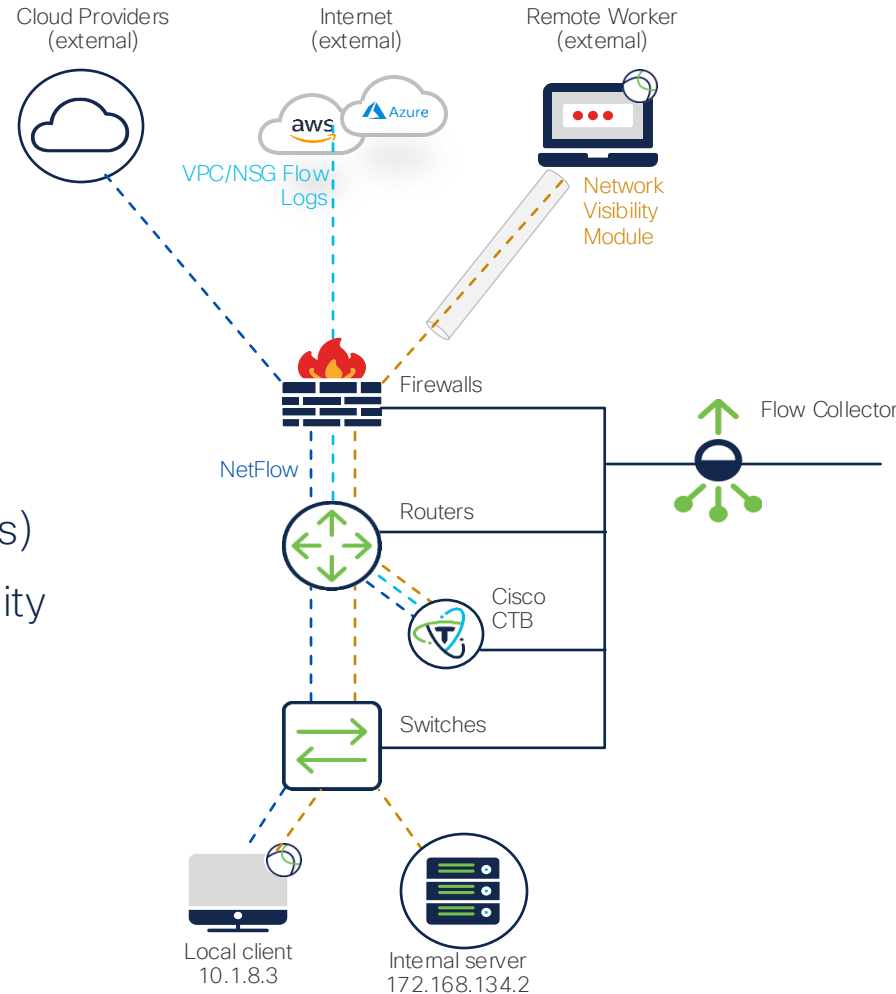
# Network Detection and Response System



# The network is the source of truth

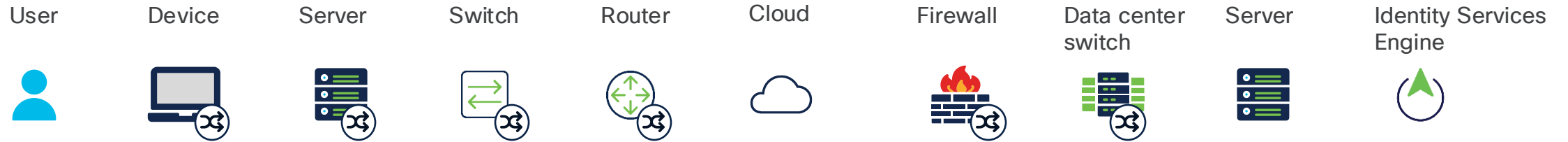
## See it ALL!

- A trace of every conversation
- Agentless information collection
- Remote worker endpoint data collection (NVM)
- Cloud Telemetry ingest (Flow Logs)
- East to west and north south visibility (Cisco FTD logs and NSEL)
- Light meta data collection using the existing infrastructure
- Capture enhanced NetFlow from Cisco ASR, ISR, Catalyst 9000, and Meraki platforms



Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP   SPLT
Application name	NBAR SECURE-HTTP
Process Name	chrome.exe
Process Account User	Acme/john

# End-to-end visibility infrastructure



## NetFlow Export is available across the Cisco portfolio

### Switch

Catalyst 2960-X (v9/IPFIX)  
Catalyst 3650/3850 (v9/IPFIX)  
Catalyst 4500E (v9/IPFIX)  
Catalyst 6500E (v9/IPFIX)  
Catalyst 6800 (v9/IPFIX)  
Catalyst 9200 (v9/IPFIX)  
Catalyst 9300 (v9/IPFIX ETA)  
Catalyst 9400 (v9/IPFIX ETA)  
Catalyst 9500 (v9/IPFIX)  
Catalyst 9600 (v9/IPFIX)  
IE3000 (v9/IPFIX)  
IE4000 (v9/IPFIX)  
IE5000 (v9/IPFIX)

### Router

Cisco ISR 4431 (v9/IPFIX ETA)  
Cisco CSR 1000v (v9/IPFIX ETA)  
Cisco ASR 1000/1001/1002 (v9/IPFIX ETA)  
Cisco ASR 9000 (v9/IPFIX)  
Cisco WLC 5520, 8510, 8540 (v9 Enhanced)  
Catalyst 8000 (v9/IPFIX ETA)  
Catalyst 9800 (v9/IPFIX ETA)

### Meraki

MX/Z (v9 Enhanced v14.5)  
MS390 (IPFIX Enhanced/ETA v15.1)

### Data center switch

Nexus 1000v (v9/IPFIX)  
Nexus 3000 (sFlow)  
Nexus 7000 (M Series - v9/IPFIX)  
Nexus 7000 (F Series- v9/IPFIX sampled)  
Nexus 9000 Series (sFlow)  
Nexus 9000 Series EX/FX (v9)

### Firewall

ASA 5500-X (NSEL,Syslog)  
FTD (NSEL,Syslog)

### Endpoint

Cisco Secure Client (IPFIX)  
AnyConnect (IPFIX)

### Cloud

AWS  
Azure  
(Flow Logs via CTB)

### Servers, software

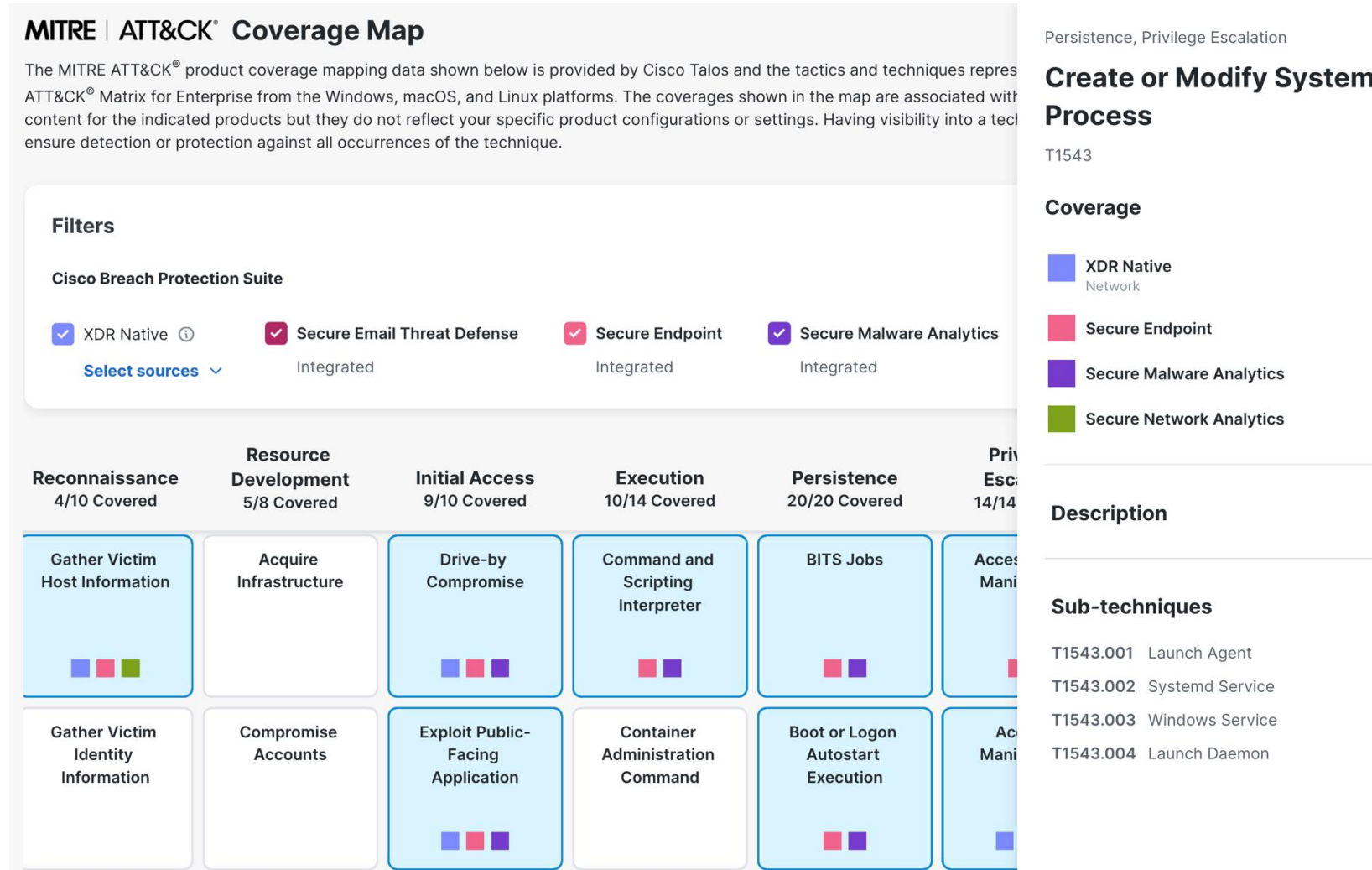
SNA Flow Sensor (v9/IPFIX ETA)  
Cisco UCS VIC (v9/IPFIX)



Extended context

# MITRE Coverage Map

- Mapping to Tactics and Techniques to Cisco Products XDR, Secure Email Threat Defense, Secure Endpoint, Secure Network Analytics and Secure Malware analytics
- Visibility on the coverage provided by each product for each tactic and technique.
- Allow faster identification of gaps and of possible routes to close these gaps
- Non-Cisco product integrations are planned in future updates



# Example of investigating a previous incident

Extended context

## Investigate

One place to investigate across all your integrated products

- Interactive visualization of observables and how they relate to each other.
- Classification of “targets” versus “assets”.
- Built-in response actions via pivot menus.
- Dynamic timeline to filter events by a date/time range.
- Color-coded observables clearly identify dispositions.
- Investigations can be saved to share or to view later.

### Carbanak 13 observables CTR investigation

Sources ▾ Disposition ▾  My environment only

Full screen 30 Nodes

Timeline 2000 - 2049

Assets and Observabl... 94

**Assets** 6

- Endpoint breach-ad2019.explorcorp.com
- Endpoint flint-win10.explorcorp.com
- 6 Device obsidian-WIN10 (OS Version Issue)
- 10 Device fileserver

**Indicators** 1

Cisco XDR Analytics (cisco-explorcorp-ear...)  
Suspicious Endpoint Activi... 4 events

**Events**

My environment events only 80 matching results

First Seen	Severity	Source	Indicators	Observables	Assets
2024-04-05T19:17:2	Critical	Cisco XDR Analyti...	Suspicious Endpoint Acti...	calculator.exe powershell.exe +7	6 obsidian-WIN10
2024-04-05T19:15:	Critical	Cisco XDR Analyti...	Suspicious Endpoint Acti...	calculator.exe powershell.exe +8	flint-win10.expl...
2024-04-05T17:36:	Unknown	Secure Endpoint		13161dcf64451b93efb2... /c:/windows/system32/... +3	6 obsidian-WIN10

# Detections



Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-07T20:17:11.779Z

[View detailed description](#)

This incident started on **2024-04-05 19:15:01 UTC** and ended on **2024-04-11 12:23:05 UTC**, a total span of approximately six days. The security alert chain indicated a series of suspicious and possibly unauthorized activities within the company's network environment. Multiple devices were involved with different groups of alerts pointing to suspicious processes, attempts at persistence, and potential defense evasion tactics. [less](#)

Overview Detection Response Worklog Report

### Events

Type ▾ Source ▾ Severity ▾  Important only 224 matching results

First Seen	Severity	Source	Indicators	Observables
• 2024-04-19T23:11:0	Critical	Cisco XDR Analyti... <a href="#">↗</a>	LDAP Connection from S... LDAP Connection from S... <b>+40</b>	
• 2024-04-19T23:11:0	Critical	Cisco XDR Analyti... <a href="#">↗</a>	Suspicious Endpoint Acti... Suspicious Endpoint Acti... <b>+40</b>	C:\Windows\System32\s... <a href="#">↕</a> de85f29a8bc7219f10a4... <a href="#">↕</a> <b>+5</b>
• 2024-04-15T17:45:5	None	Splunk		108.62.141.250 <a href="#">↕</a>
• 2024-04-11T12:23:0	Critical	Cisco XDR Analyti... <a href="#">↗</a>	Suspicious Endpoint Acti... Suspicious Endpoint Acti... <b>+40</b>	C:\Windows\System32\s... <a href="#">↕</a> svchost.exe <a href="#">↕</a> <b>+7</b>
• 2024-04-11T12:23:0	Critical	Cisco XDR Analyti... <a href="#">↗</a>	LDAP Connection from S... LDAP Connection from S... <b>+40</b>	
• 2024-04-11T03:46:1	Critical	Cisco XDR Analyti... <a href="#">↗</a>	Potential Persistence Att... Potential Persistence Att... <b>+40</b>	
• 2024-04-11T03:46:1	Critical	Cisco XDR Analyti... <a href="#">↗</a>	Suspicious Endpoint Acti... Suspicious Endpoint Acti... <b>+40</b>	fd69f2d3c8b30660fd5... <a href="#">↕</a> 51eb6455bdca85d3102... <a href="#">↕</a> <b>+6</b>
• 2024-04-05T21:31:	High	Cisco Secure Endpoint	Behavioral Detection/Pro... Behavioral Detection/Pro... <b>+40</b>	powershell.exe <a href="#">↕</a> C:\Windows\System32\... <a href="#">↕</a> <b>+1</b>
• 2024-04-05T21:31:	High	Cisco XDR Analyti... <a href="#">↗</a>	Suspicious Endpoint Fin... Suspicious Endpoint Fin...	

# Correlation with attack chaining

- Alerts from XDR and integrated products are correlated prior to becoming XDR incidents.
- Alerts with common indicators are combined into attack chains.
- New alerts are also appended to incidents as they occur over time.
- Analysts can also link incidents together for manual correlation.
- Attack chain are summarized with Gen AI

## Attach Chain source of incidents

← Incidents

1000 Incident Reported ▾ **Escalating Intrusion Clusters via Endpoint Exploits and Process Mis**

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-07T20:53:37.498Z

[View detailed description](#)

This incident started on **2024-04-05 19:15:01 UTC** and ended on **2024-04-11 12:23:05 UTC**, a total span of approximately six days. The security alert chain indicated a series of suspicious and possibly unauthorized activities within the company's network environment. Multiple devices were i... [more](#)

[Overview](#) | [Detection](#) | [Response](#) | [Worklog](#) | [Report](#)

The diagram illustrates an attack chain with the following components and relationships:

- Users (2)** connects to **Process (30)** and **Devices (2)**.
- Process (30)** connects to **IP Addresses (6)** and **Endpoints (3)**.
- Devices (2)** connects to **Process (30)**, **IP Addresses (6)**, and **Endpoints (3)**.
- IP Addresses (6)** connects to **Endpoints (3)**.
- Hostnames (4)** connects to **Endpoints (3)**.

**6 Assets** [View all](#)

**TOP ACTIVE**

- 6 Device: **obsidian-WIN10** (OS Version Issue) 129 events
- 10 Device: **breach-AD2019.explorcorp.com** (OS Version Issue) 39 events

**134 Observables** [View all](#)

**TOP ACTIVE**

- Malicious SHA-256: **e415af393d9182435cc088e211babb40dae11bfbdd...** 102 events
- Unknown File Name: **DefenderUpgradeExec.exe** 98 events
- Unknown File Path: **\\?C:\Users\obsidian\AppData\Local\Temp\Defender...** 98 events



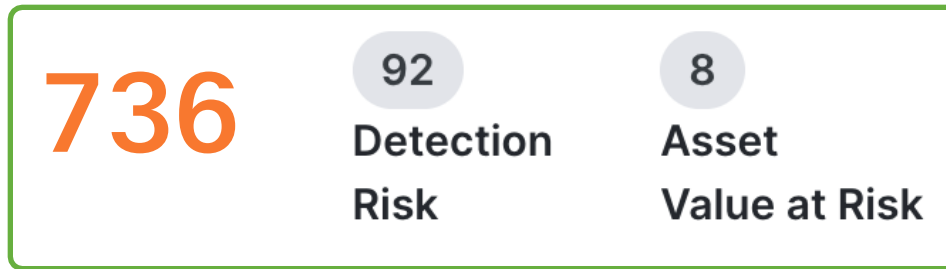
# Cisco AI Assistant in XDR quickly guides you through incident response

Analysts can start a natural language conversation over a security incident to understand:

- Full scope of the incident
- Affected users and devices
- Key artifacts and indicators
- Next recommended steps

The screenshot displays the Cisco XDR 'Incidents' page for an incident titled 'Escalating Intrusion Clusters via Endpoint Exploits and Persistence'. The incident is reported by Cisco XDR Analytics (cisco-explorcorp-earth) on May 14, 2024, at 7:35 PM CEST. The status is 'Incident Reported' with 1000 events. The AI Assistant overlay provides a summary of the incident, including the start and end times (2024-04-05 19:15:01 UTC to 2024-04-11 12:23:05 UTC) and a description of suspicious activities. It offers a 'View long description' link and a confirmation prompt: 'The incident is already assigned to users and is in Incident Reported status. Do you want to edit the users assigned to the incident?'. Below the prompt are three action buttons: 'Contain Incident: URLs', 'Validate Eradicated Hosts and Unquarantine Assets', and 'Contain Incident: File Hashes'. At the bottom of the AI Assistant window, there is a text input field 'Ask the AI Assistant a question' and a disclaimer: 'The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.'

# Identify the most impactful incidents based on risk



$$\text{Priority Score} = \text{Detection Risk} \times \text{Asset Value}$$

0-1000                      0-100                      0-10

The Incident total priority score used to prioritize incidents

Detection Risk composed of multiple values:

- MITRE TTP Financial Risk
- Number of MITRE TTPs
- Source Severity

User Defined Asset Value represent the value of the asset involved in the incident

# Robust native response options



## Pivot menus

Act on an observable from various places within XDR and other Cisco Secure products



## Incident playbooks

Built in Guided, four stage process for incident response, Bring your own playbook and apply it when needed



## Automation

Simple or complex workflows that can investigate and respond at machine speed

The screenshot displays a list of incident response options, each with a dropdown arrow, a title, a description, and an action button:

- Identify Affected Hosts** (Add Note): Add note with summary of findings on the investigations of hosts found with malicious indicators
- Contain Incident: Overview** (Add Note): Overview of how to contain Indicators of Compromise to stop the spread of malicious activity
- Contain Incident: Assets** (Select): Use asset-based containment to stop the spread of malicious activity.
- Contain Incident: IPs** (Add Note): Contain IP indicators of compromise to stop the spread of malicious activity
- Contain Incident: Domains** (Select): Contain domain indicators of compromise to stop the spread of malicious activity
- Contain Incident: URLs** (Select): Contain URL indicators of compromise to stop the spread of malicious activity
- Contain Incident: File Hashes** (Select): Contain file hash indicators of compromise to stop the spread of malicious activity.
- Implement Additional Monitoring** (Add Note)

At the bottom right, there are two buttons: **Back** and **Go to Eradication →**.

Response

# Ransomware Recovery

Achieve automated ransomware recovery leveraging XDR automation, rule-based triggering and Cohesity integration.

- Restore a device to its previous known good state before infection.
- Automate snapshot taking and recovery for devices to their known good state.
- Reduce downtimes and time for recovery with end-to-end automation

← Incidents

1000 Open ▾ Escalating Intrusion Clusters via Endpoint Exploits and Process M

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-04-09T20:09:19.858Z - [5 Linked Incidents](#)

[View detailed description](#)

This incident started on **\*\*2024-04-05 19:15:01 UTC\*\*** and ended on **\*\*2024-04-11 12:23:05 UTC\*\***, a total span of approximately six days. The security alert chain indicated a series of suspicious and possibly unauthorized activities within the company's network environment. Multiple devices were i... [more](#)

Overview Detection Response Worklog Report

Notes Audit Log

Created by: **Automation Workflow**  
2024-04-09T20:09:28.743Z

[AUTOMATION RULE]

[Cohesity - Identify Restore Point for Affected Virtual Machines](#) started by [Score greater than 800](#)

# Solution Overview – Cisco XDR

Experience the Simplicity of Accelerated Threat Detection & Response





The bridge to possible