Cisco XDR

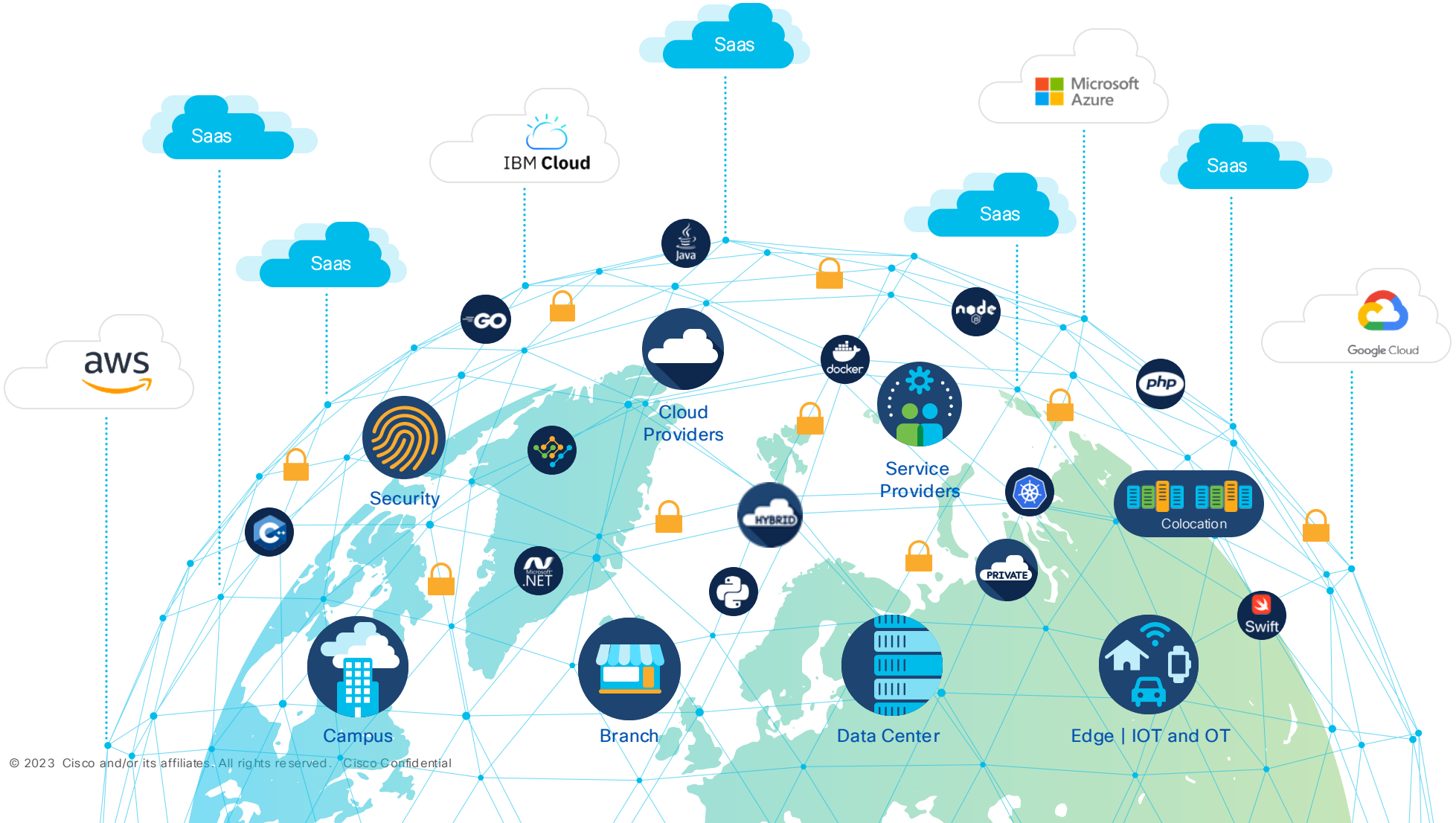
Milan Rášo

Solutions Engineer
Cisco Systems Slovakia

22.05.2025

iDEME Bratislava '25
Informatizácia až po dediny a mestá

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

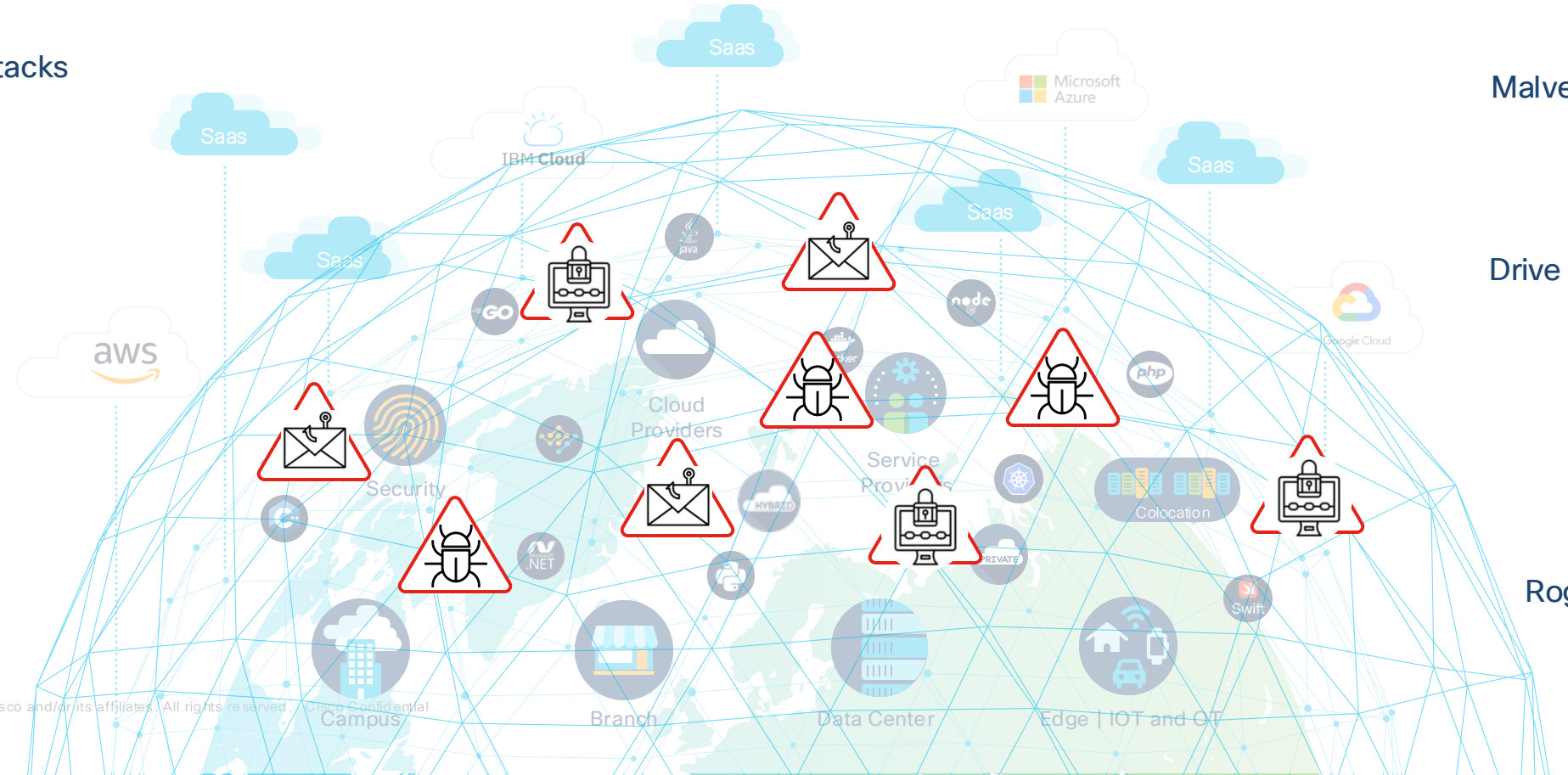
Crypto-mining

Unpatched Software

Data / IP Theft

Wiper Attacks

Malvertising



Phishing

Drive By Downloads

DDoS

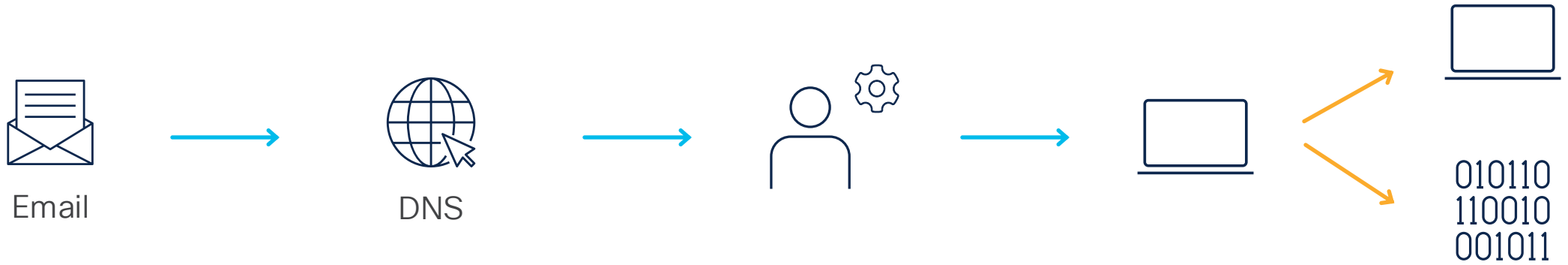
Botnets

Man in the Middle

Rogue Software

Stop advanced threats like ransomware

Most attacks use a sequence like this...



A well-tailored and personalized email causes a user to click...

Which goes to a questionable web site...

Which leads to a strange process being created locally on the user's device...

That process will connect to another machine or directly to their data

T1566: Spear Phishing

T1055: Process Injection

T1189: Drive-by Compromise

T1210: Exploitation of Remote Services

Cisco XDR

Why do we need XDR?

Mandiant Inc

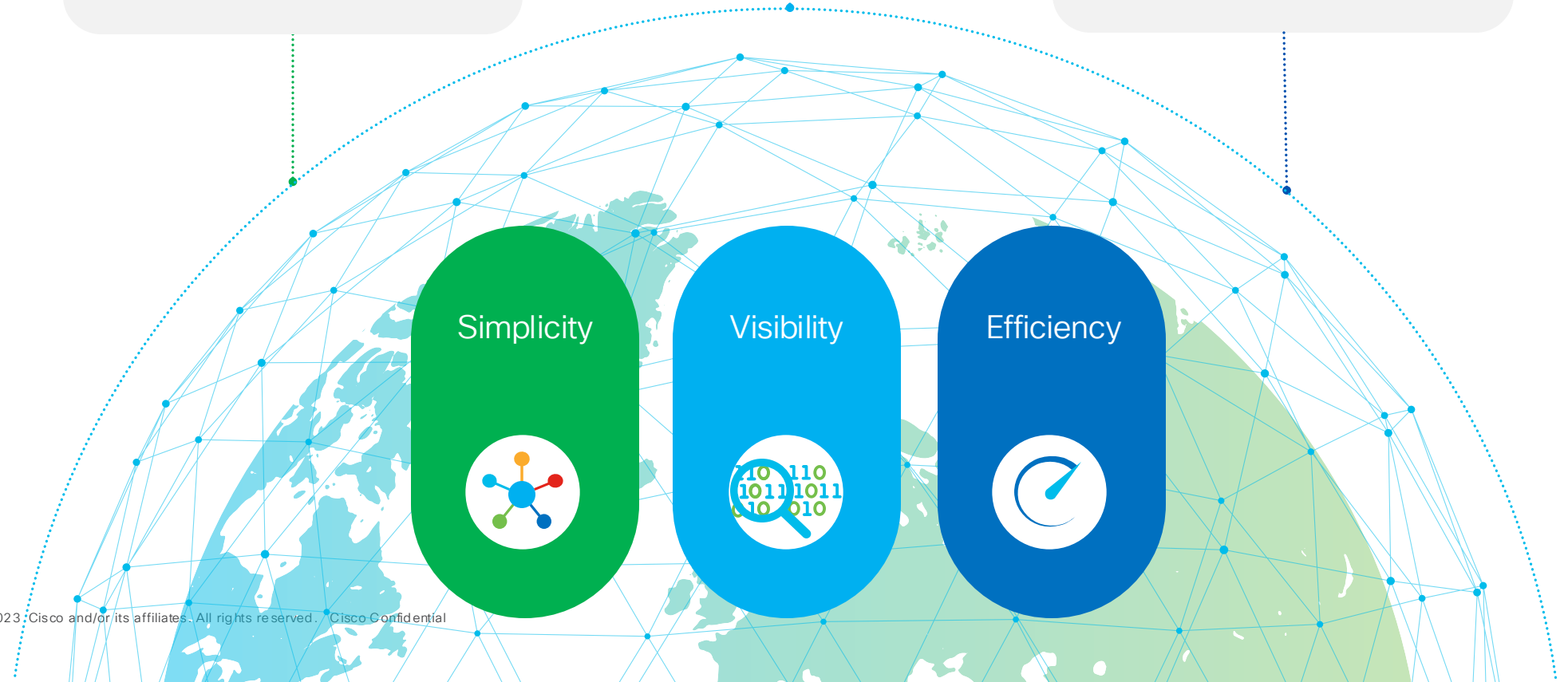
Medium-sized businesses are using 50-60, and large organizations or enterprises are using over **130 tools** on average

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.



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?

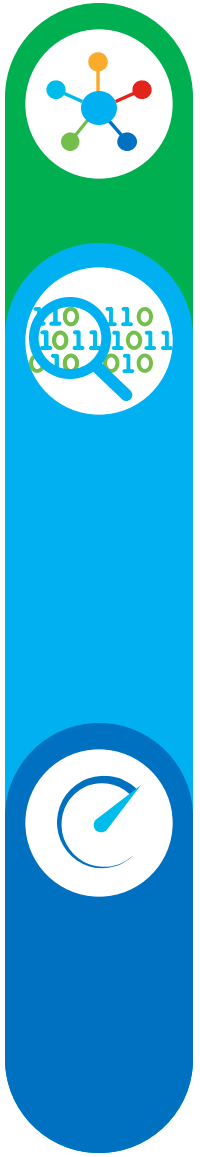
3 Compress Investigation Time

Accelerate Response 4

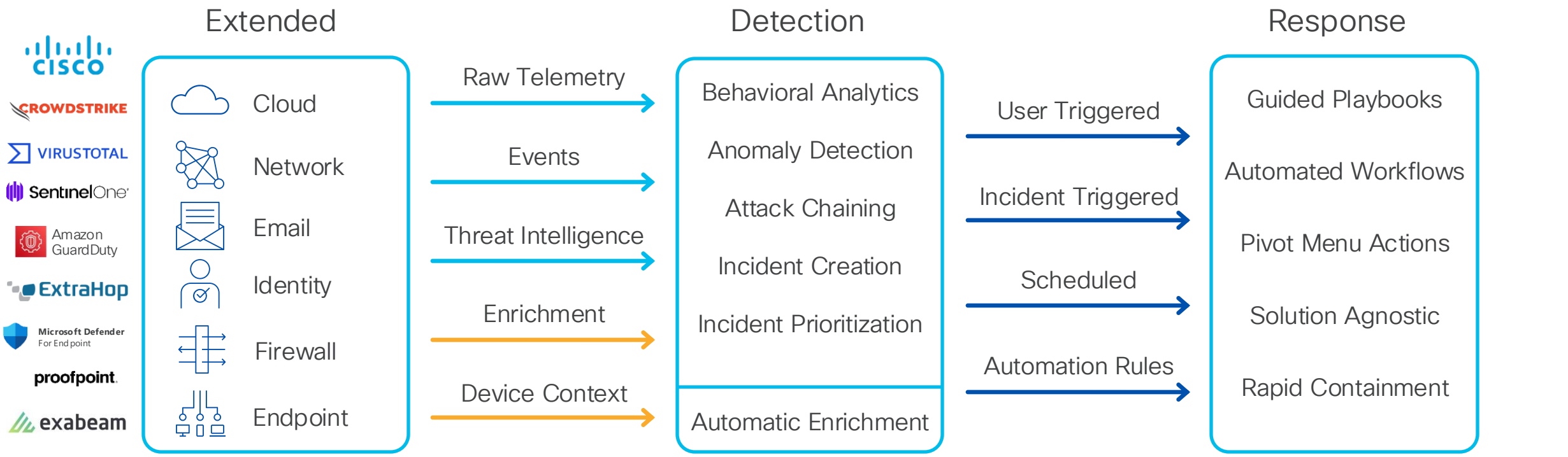
How fast can we confidently respond?
How much can SecOps automate?
Are we improving our time to respond?

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



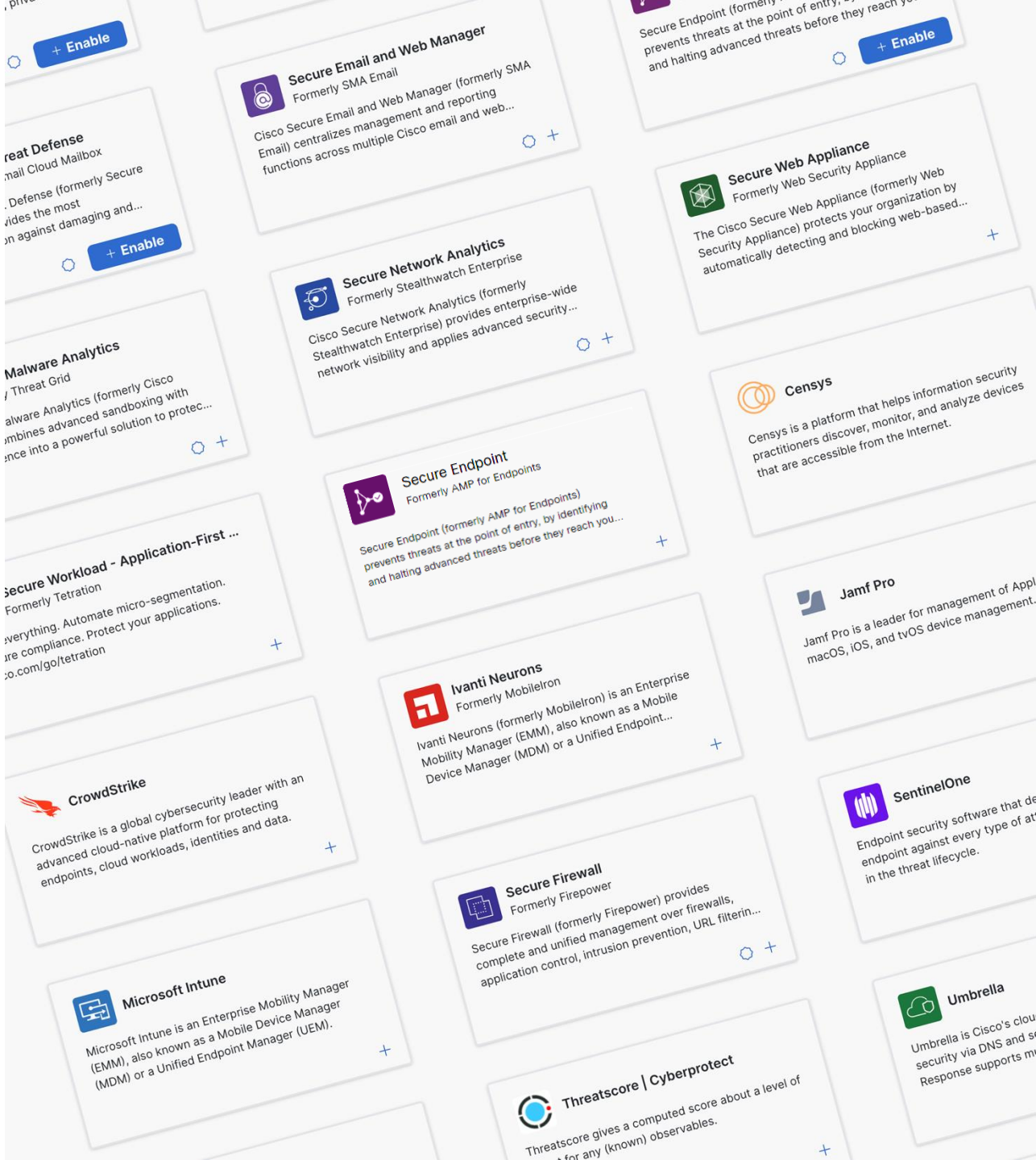
Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

Automated or user triggered responses to block observables using any integrated technology

AI driven at every stage, Detection, Response and Incident Management

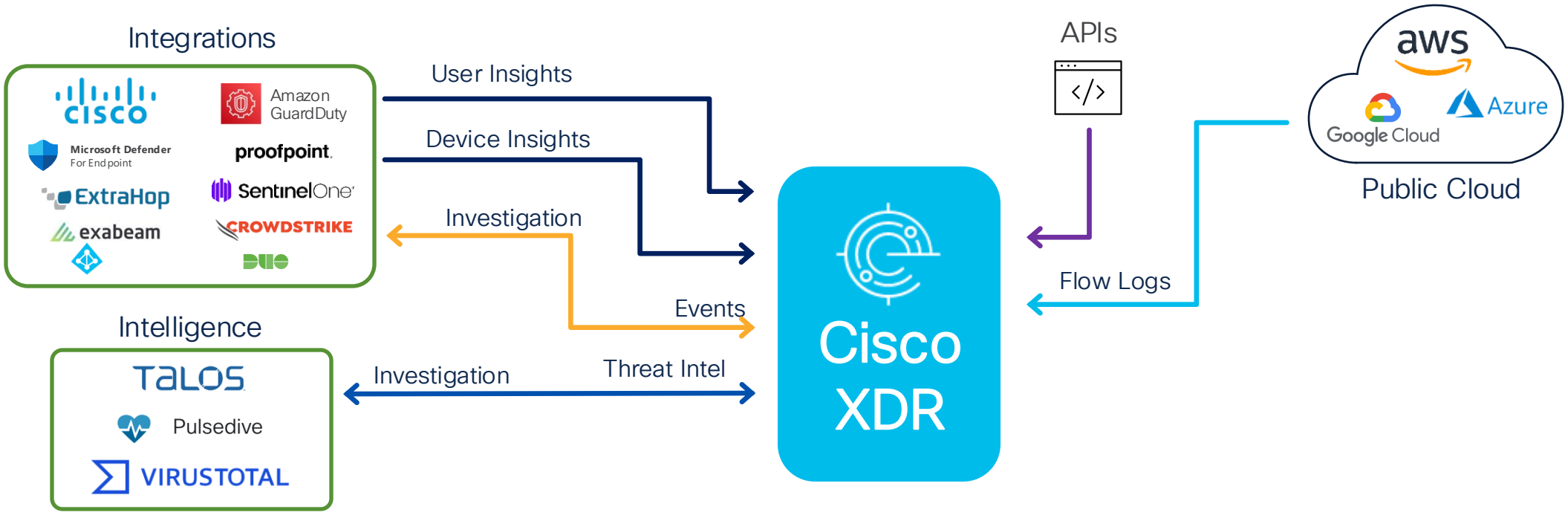
Extended context



Extended context

Telemetry sources for Cisco XDR

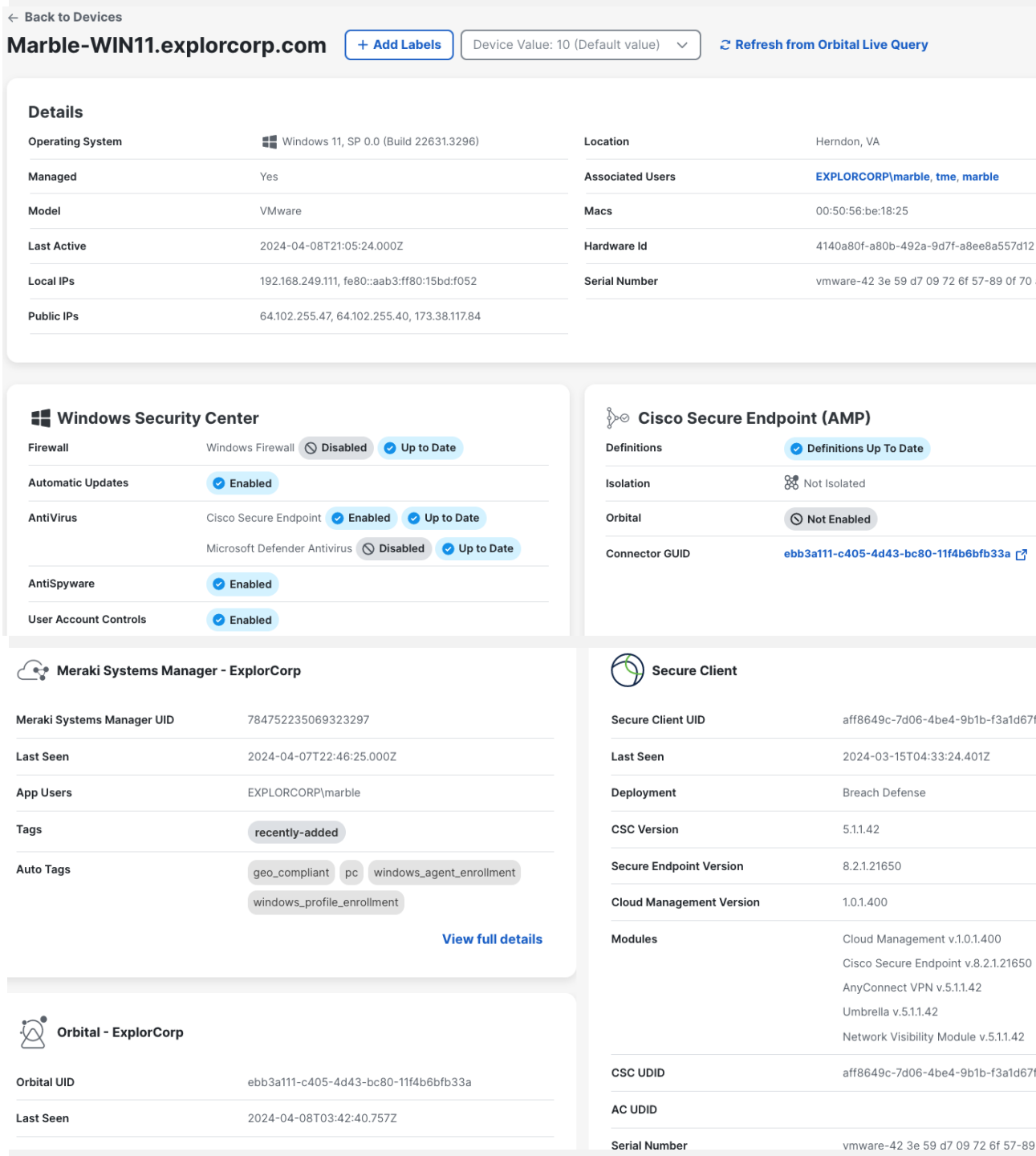
Flexible integration for existing infrastructure



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.

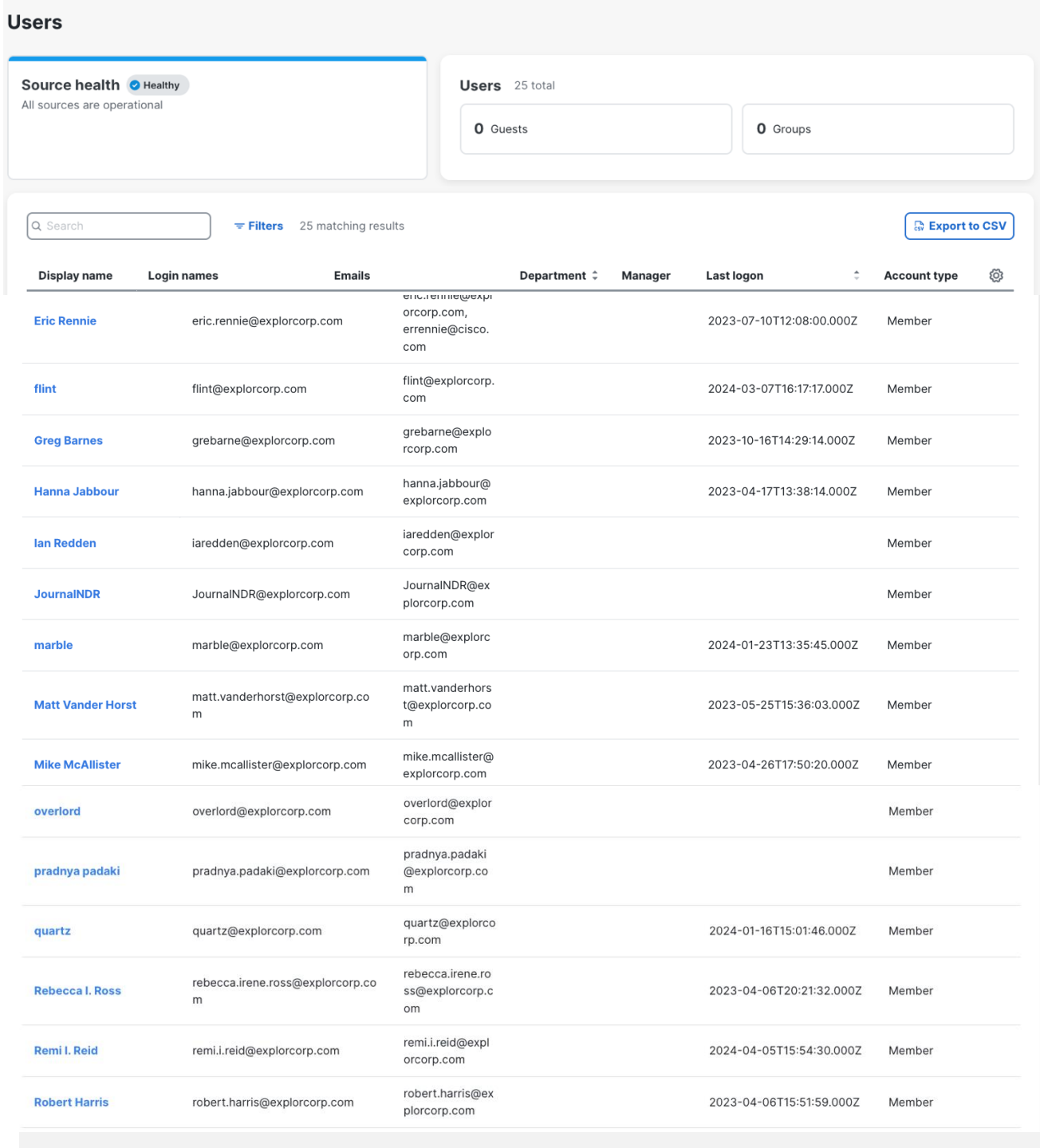


Extended context

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



Extended context

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)

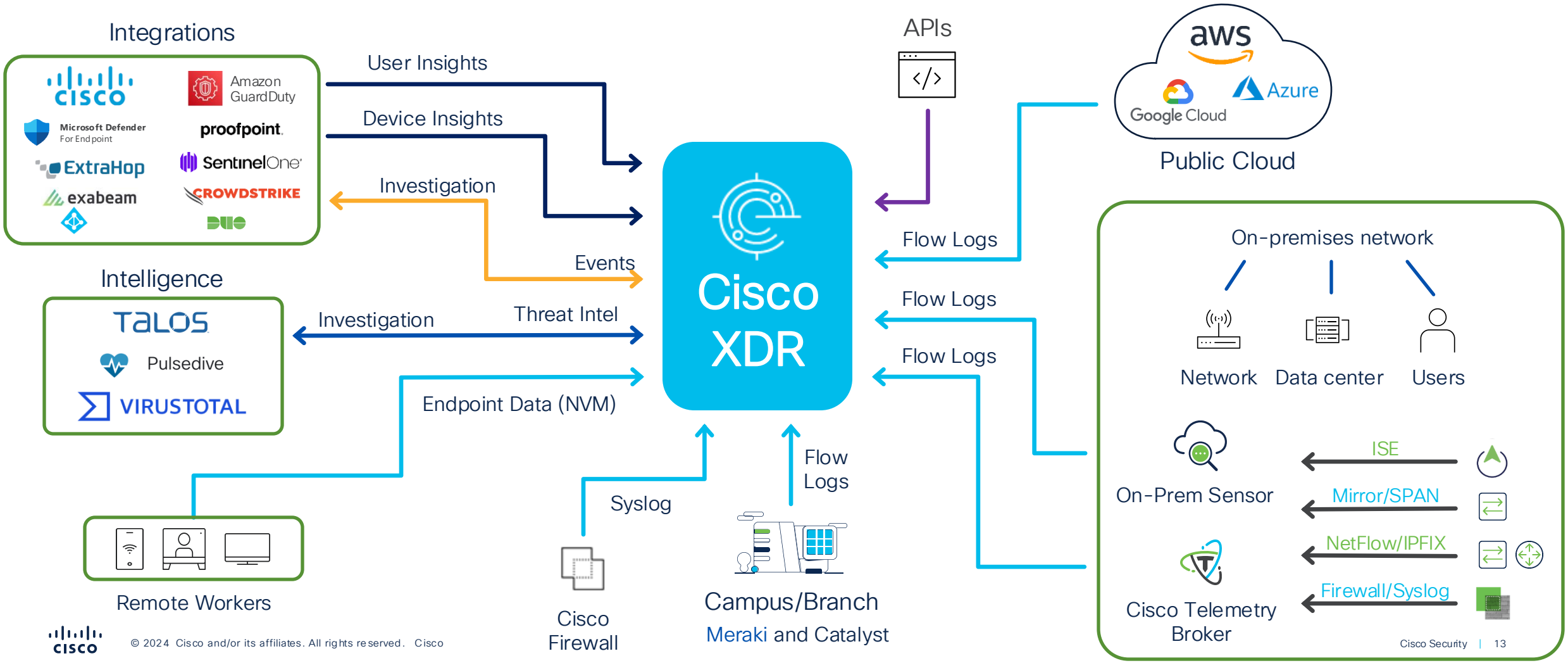
Microsoft Defender
for Endpoint

Microsoft
Azure AD

Extended context

Telemetry sources for Cisco XDR + NDR!!

Flexible integration for existing infrastructure



Network Detection and Response System

XDR

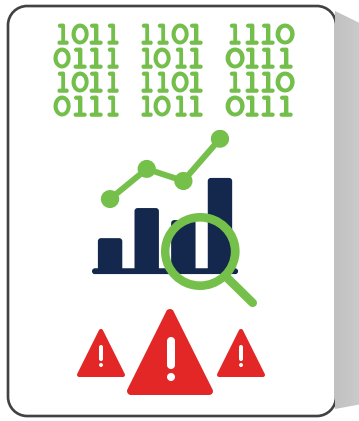
Extended Detection and Response with XDR. Advanced analytics extends local detections with global intelligence and integrations for accelerated response

Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies



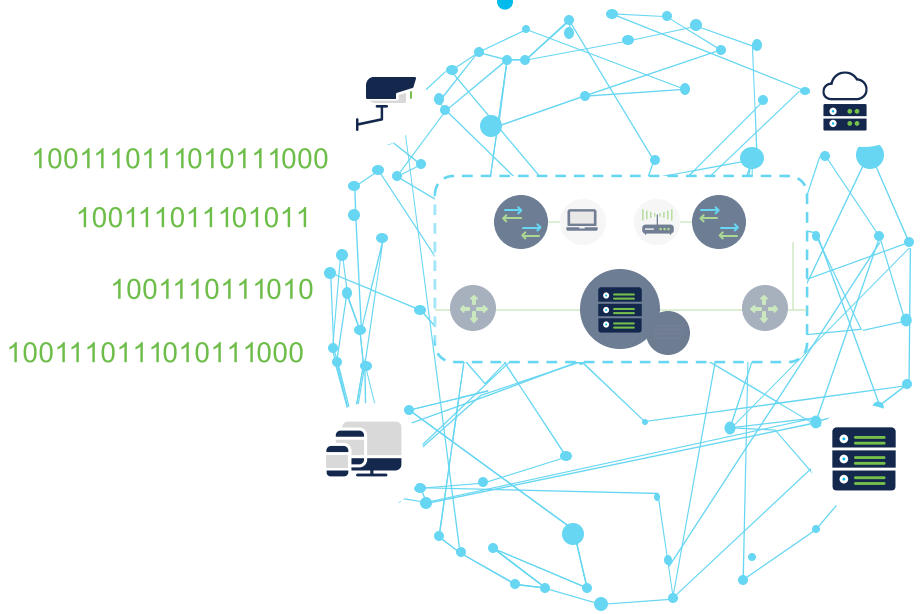
NDR

Endpoint Telemetry

Device and process insight with flow telemetry from Cisco Secure Client

Data collection

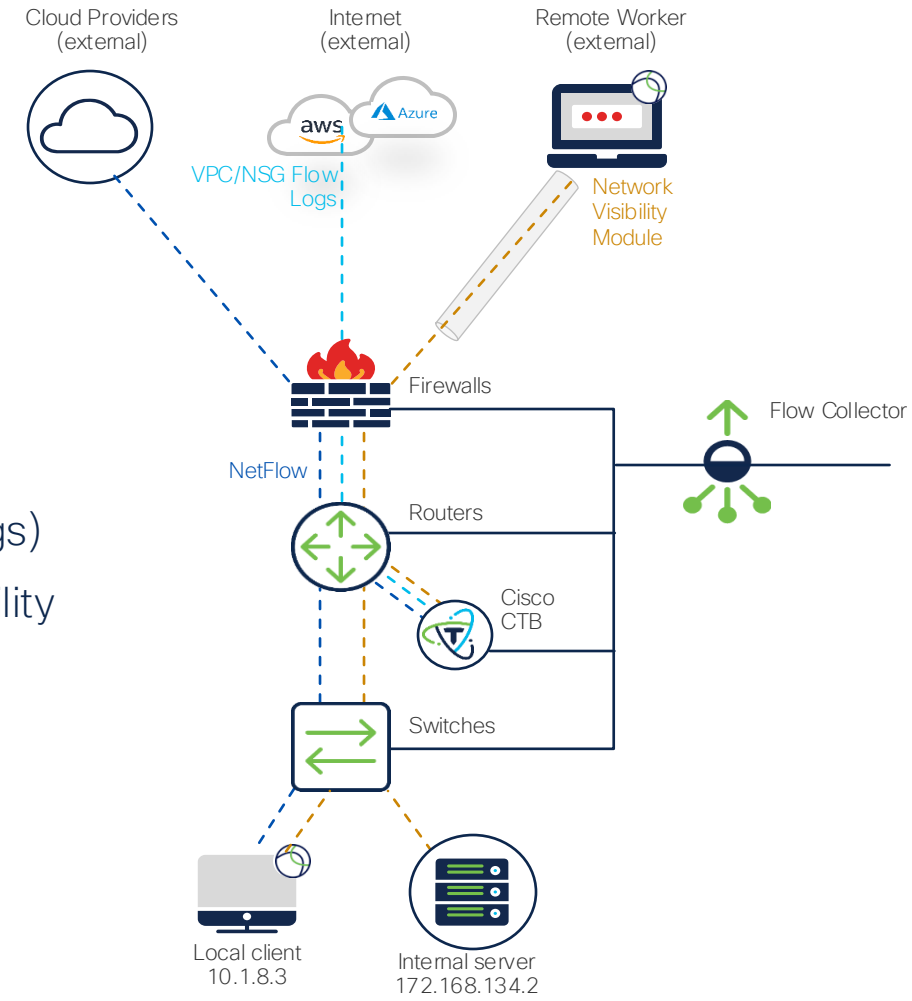
Rich telemetry from the existing network infrastructure including enhanced telemetry for encrypted traffic analytics



The network is the source of truth

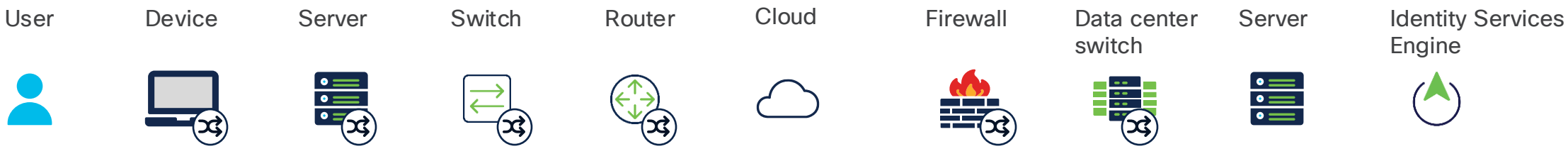
See it ALL!

- 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)

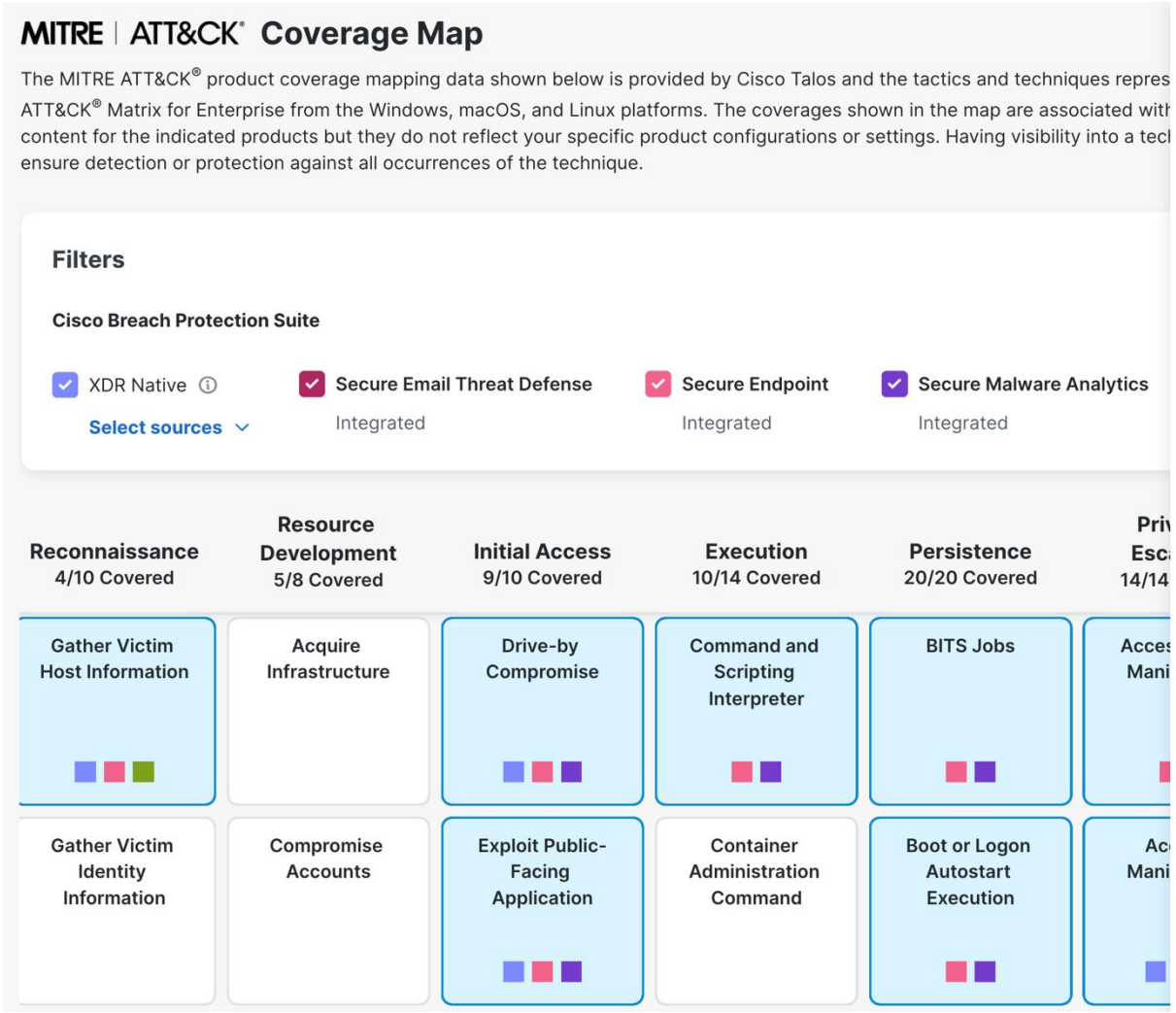
Cloud
AWS
Azure
(Flow Logs via CTB)

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

The above is a non-exhaustive list of Cisco exporters. For individual platform features, reference the Cisco feature navigator: https://cfnng.cisco.com/

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

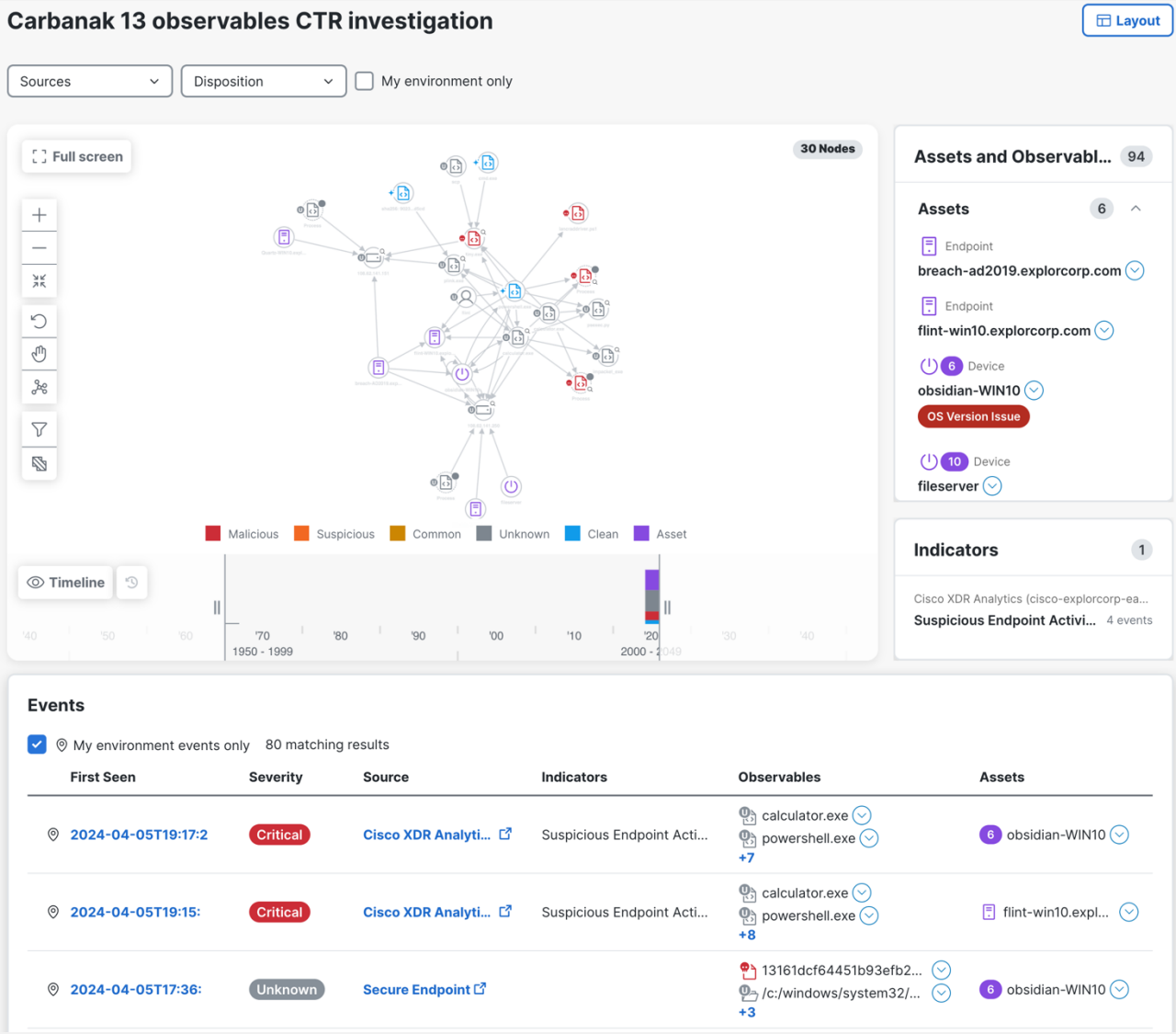


Investigate

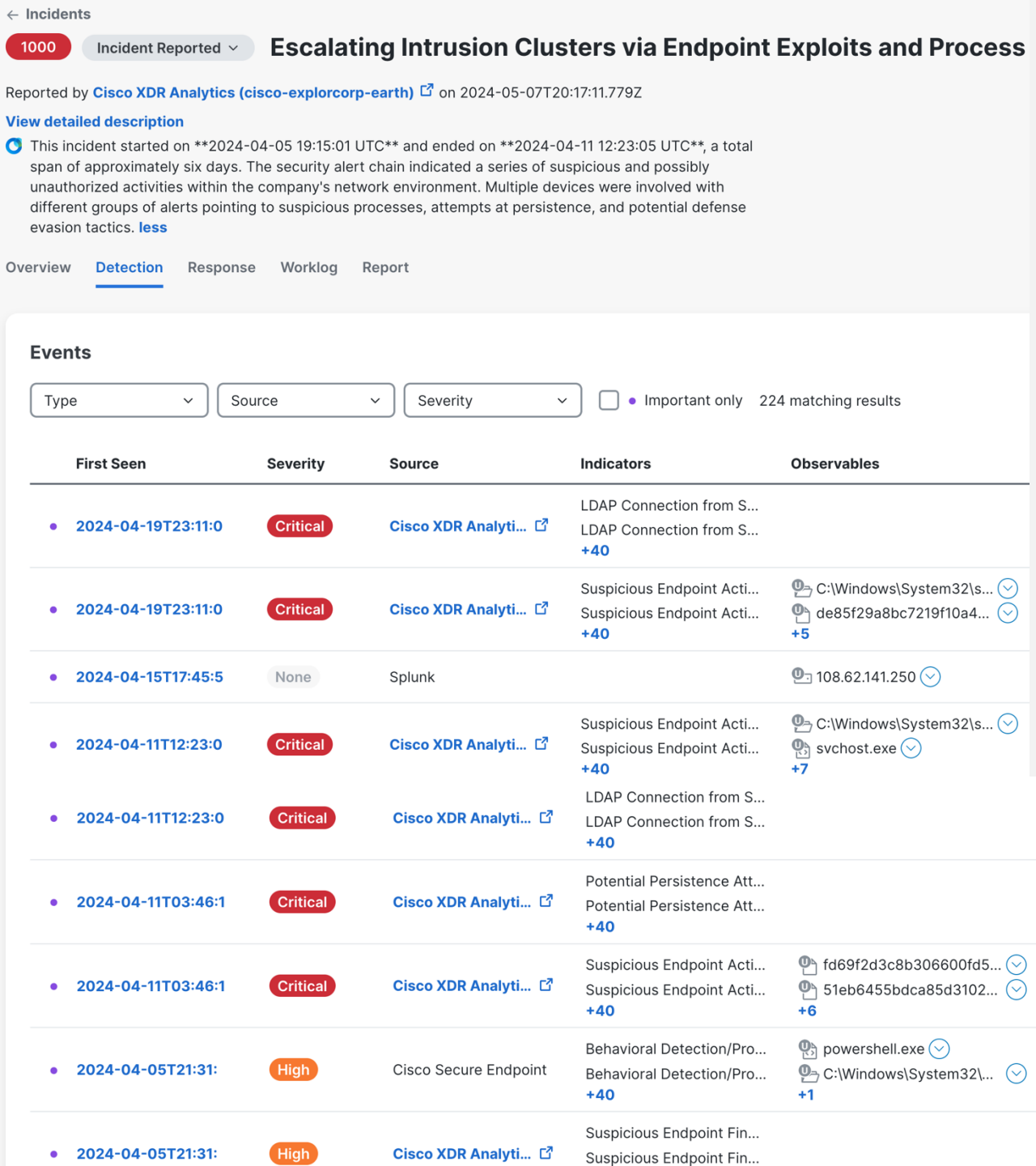
One place to investigate across all your integrated products

- 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.

Example of investigating a previous incident



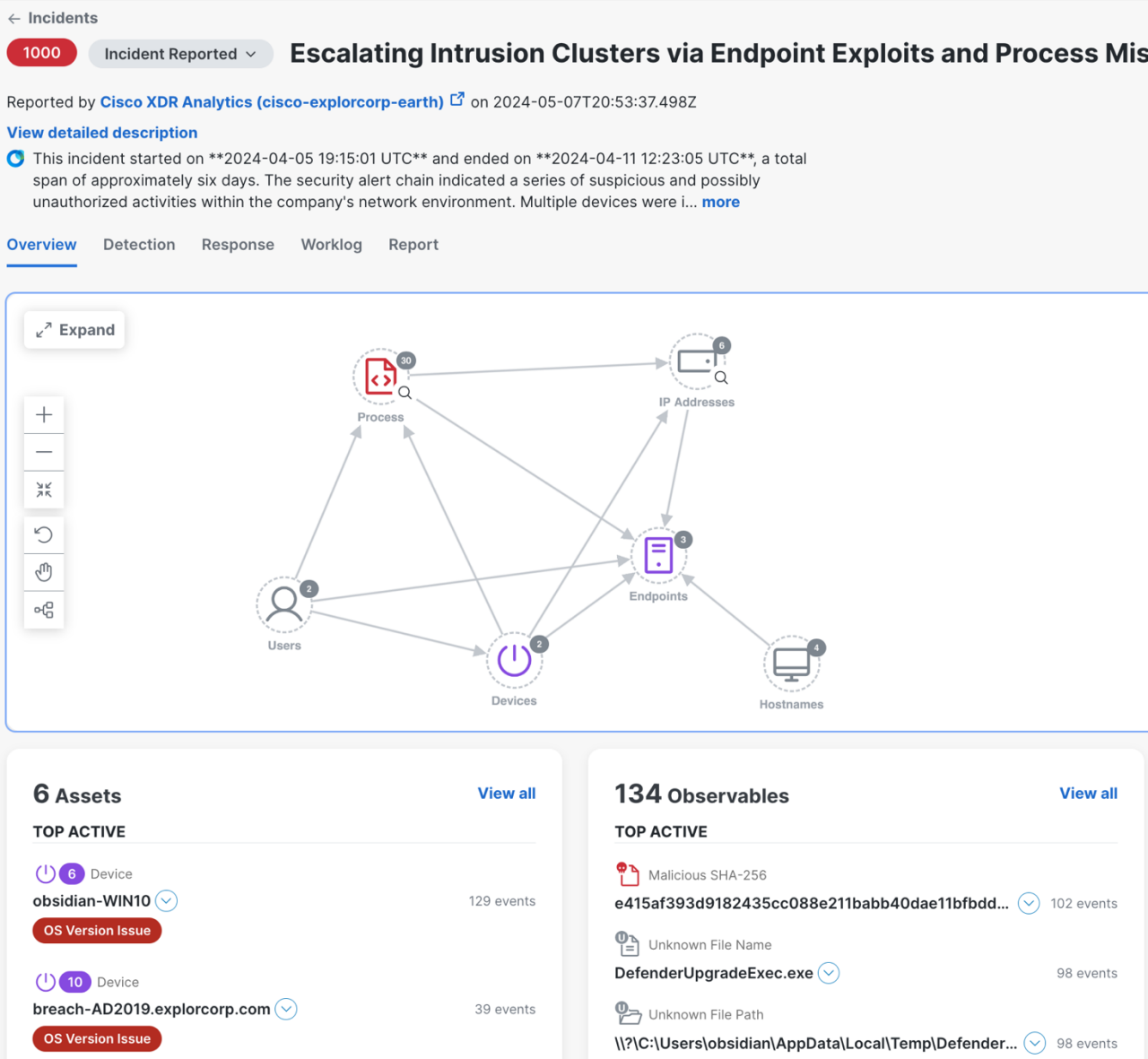
Detections



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

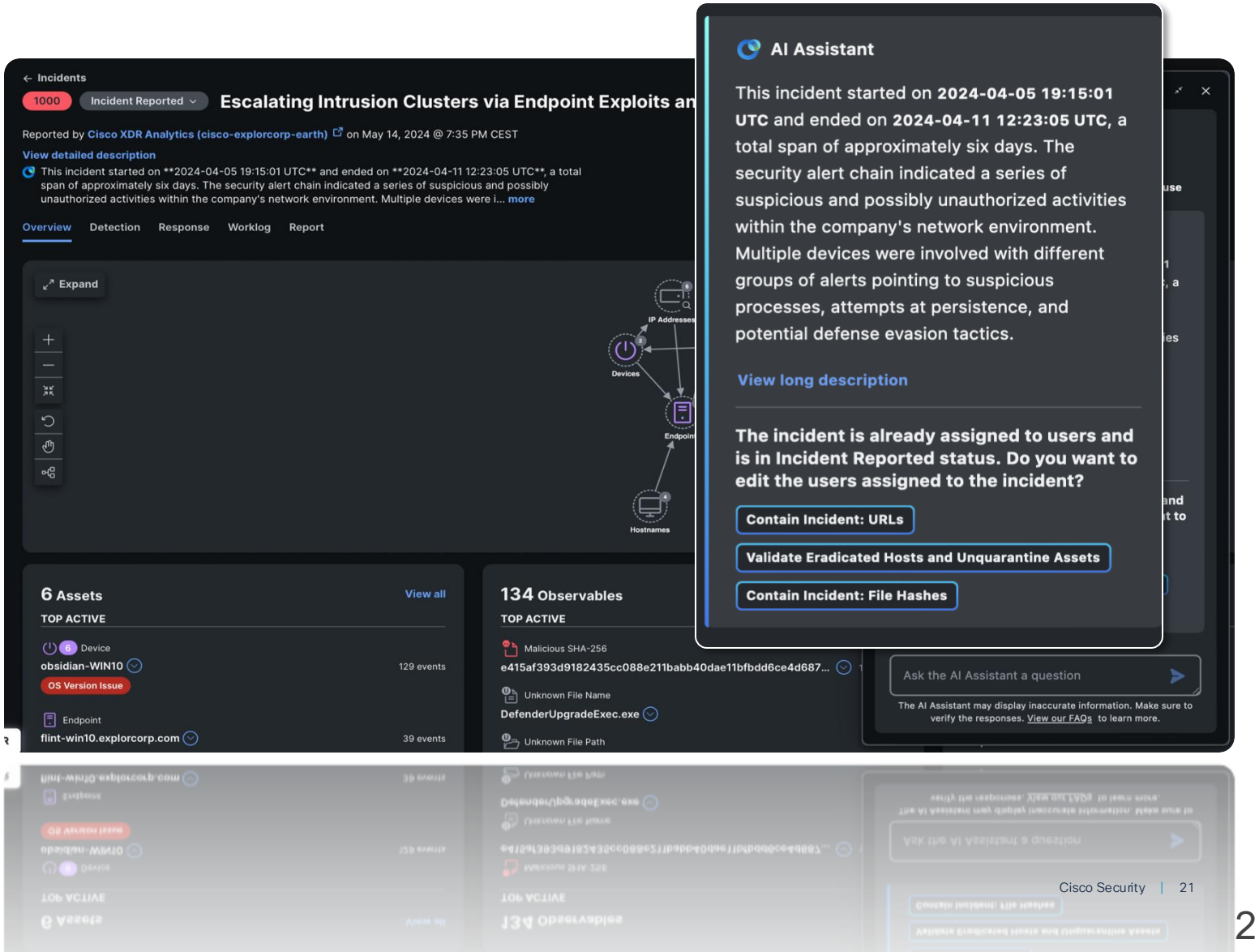
Attach Chain source of incidents



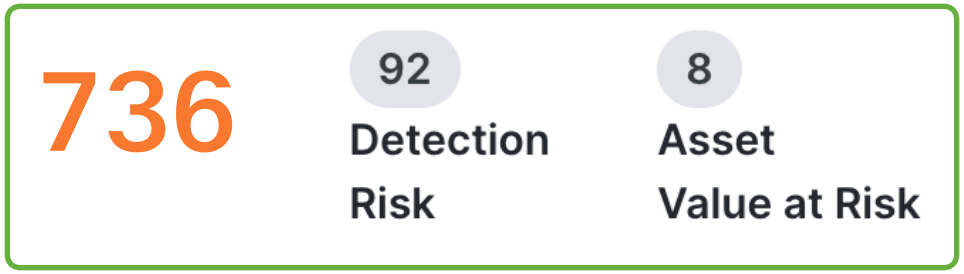
Cisco AI Assistant in XDR quickly guides you through incident response

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



Identify the most impactful incidents based on risk



Priority Score = **Detection Risk** x **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

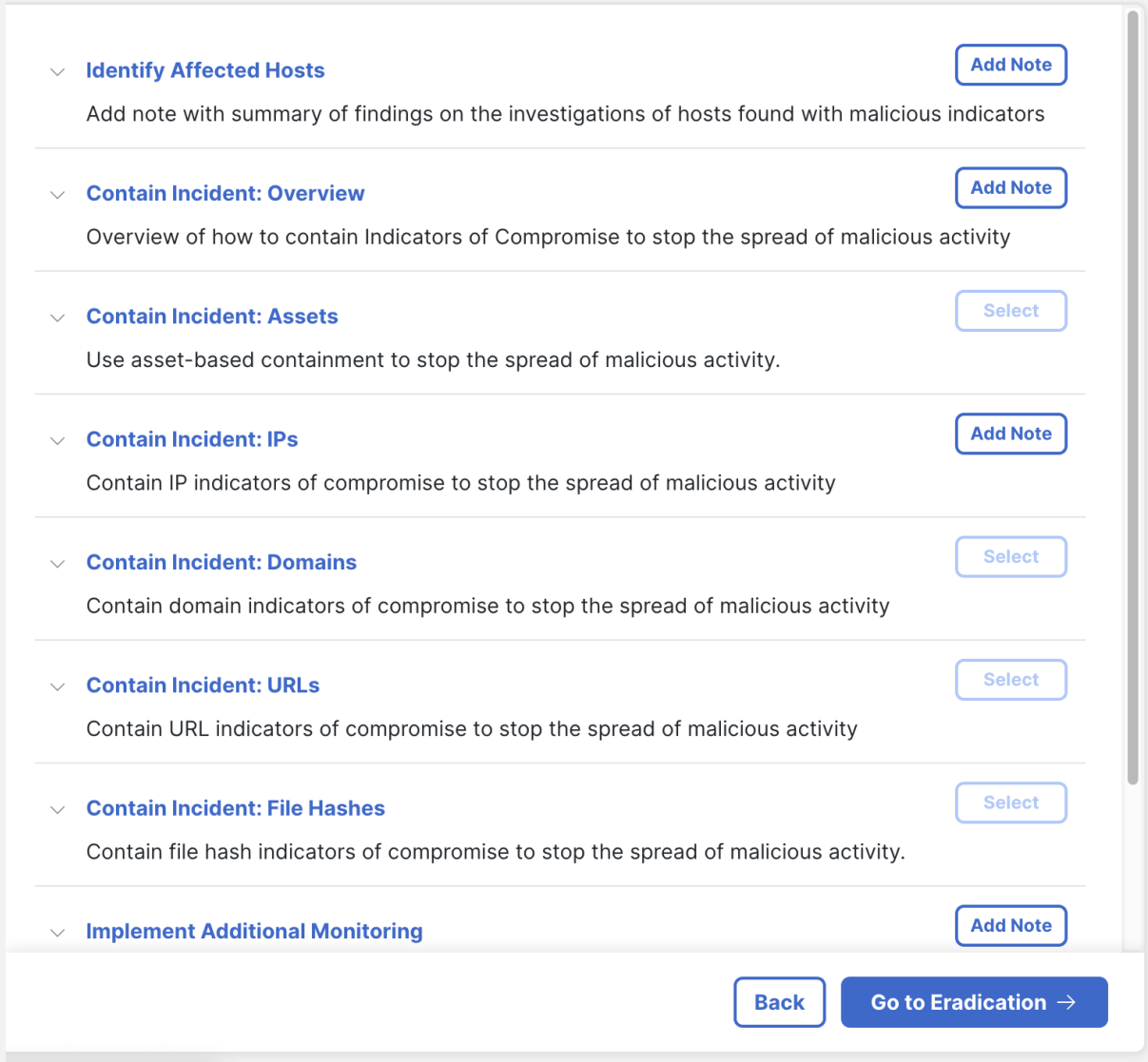
Act on an observable from various places within XDR and other Cisco Secure products

Incident playbooks

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

Automation

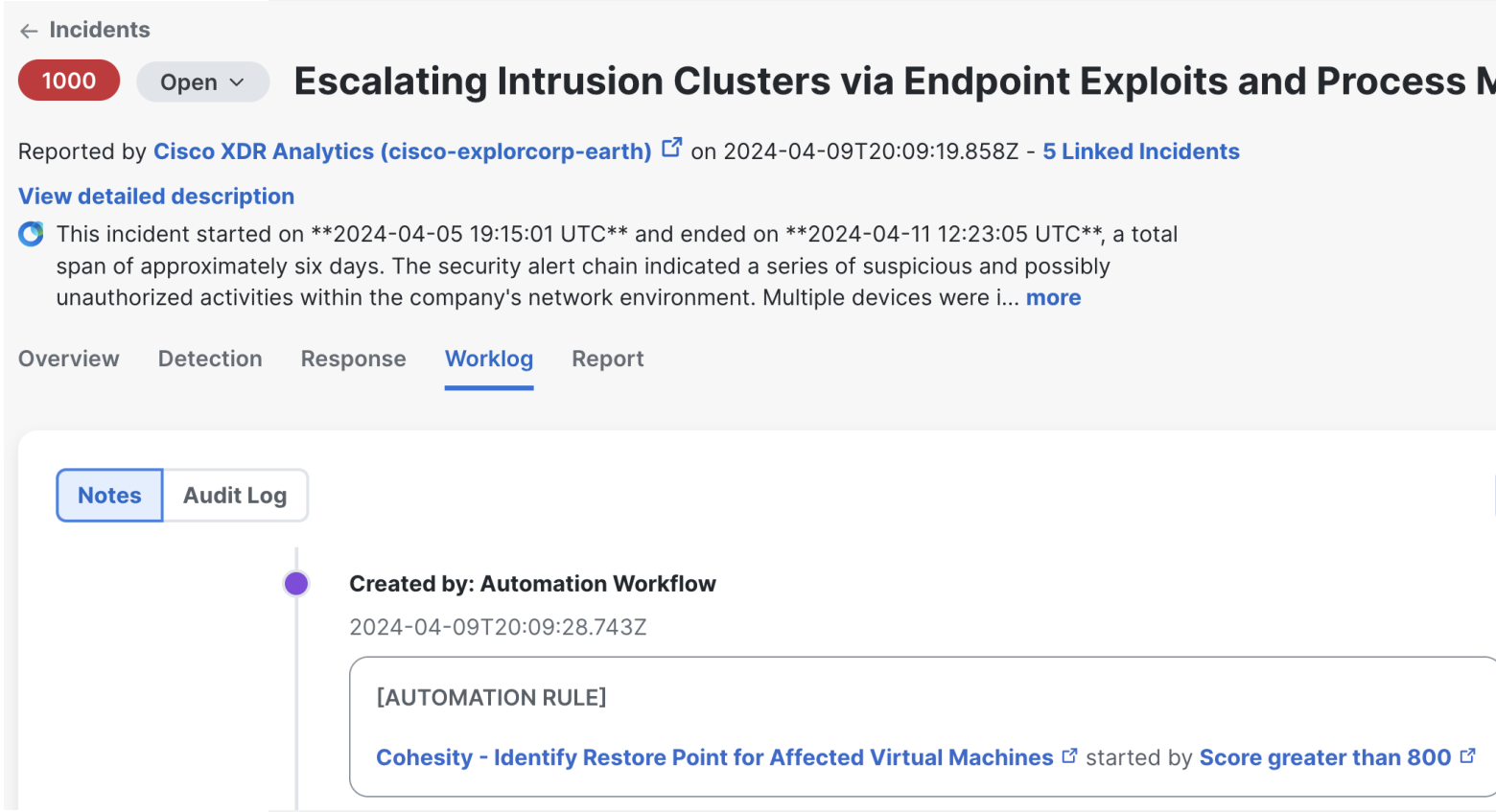
Simple or complex workflows that can investigate and respond at machine speed



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



Solution Overview – Cisco XDR

Experience the Simplicity of Accelerated Threat Detection & Response

Cisco

- Network
- Endpoint
- Email
- Cloud
- Applications
- Identity

Cisco XDR

Built on the Cisco security platform

- Open and extensible
- Clear prioritization
- Automation and response guidance
- Streamlined investigations

Your Infrastructure

- 3rd party tools
- Intelligence
- Others
- SIEM/SOAR

SecOps Analyst CISO Incident responder

Your SOC

The bridge to possible