Secure Endpoint: Unveiling Latest Key Features!

Filipe Lopes
Technical Leaders Manager, SBG BU
BRKSEC-2544



Webex App

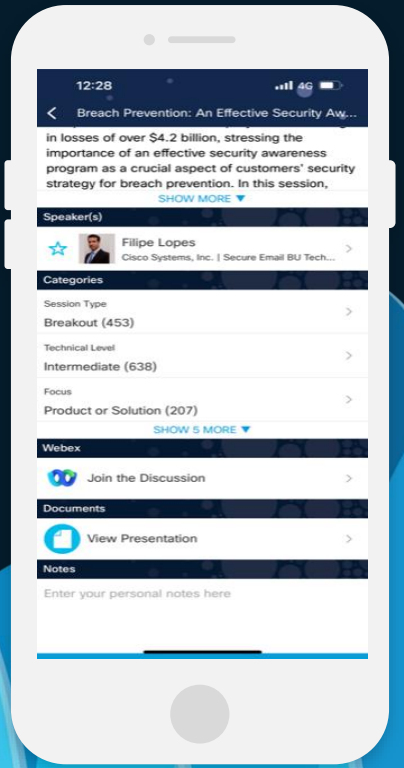
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

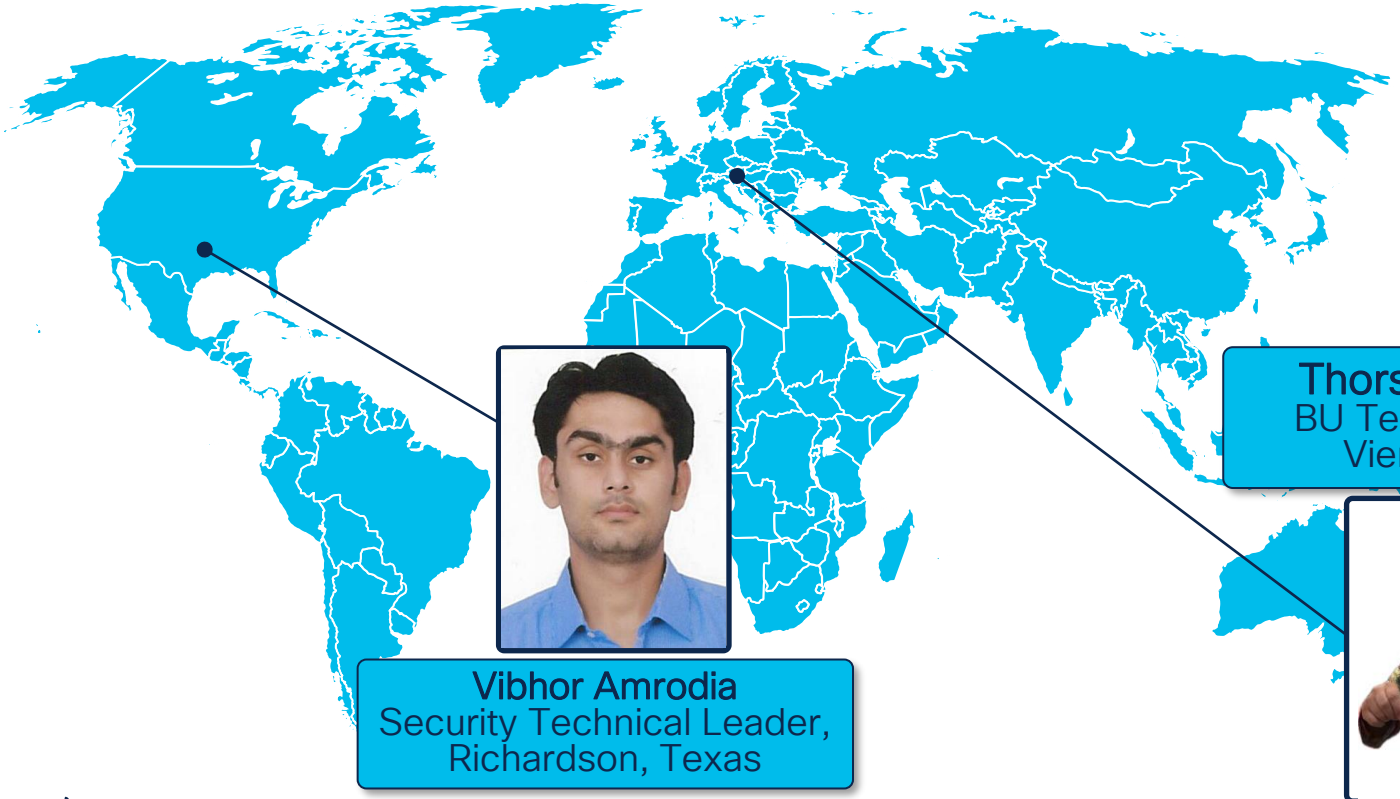
Webex spaces will be moderated by the speaker until February 28, 2025.



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank You,Thorsten & Vibhor!

WebEx Room and Q&A Management



Vibhor Amrodia
Security Technical Leader,
Richardson, Texas

Thorsten Schranz
BU Technical Leader
Vienna, Austria



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

About me...



- 17 years @Cisco
- Worldwide Technical Leaders Manager
- Cisco Live Distinguished Speaker

- Apnea/Scuba Diver
- Outdoor Sports
- World Travelling

- Wanna-be Chef
- Grandpa of a 35Kg Belgium Shepherd Malinois

Happy and Proud father of 13-year-old, Princess Emma!

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Threat Landscape
- Secure Endpoint Vision&Mission (Outcome-driven Security)
- Prevent, Detect, Respond, Protect
- Warning!!! Suspicious Endpoint Activities (Demo)
- Integrations
- Key Takeaways

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

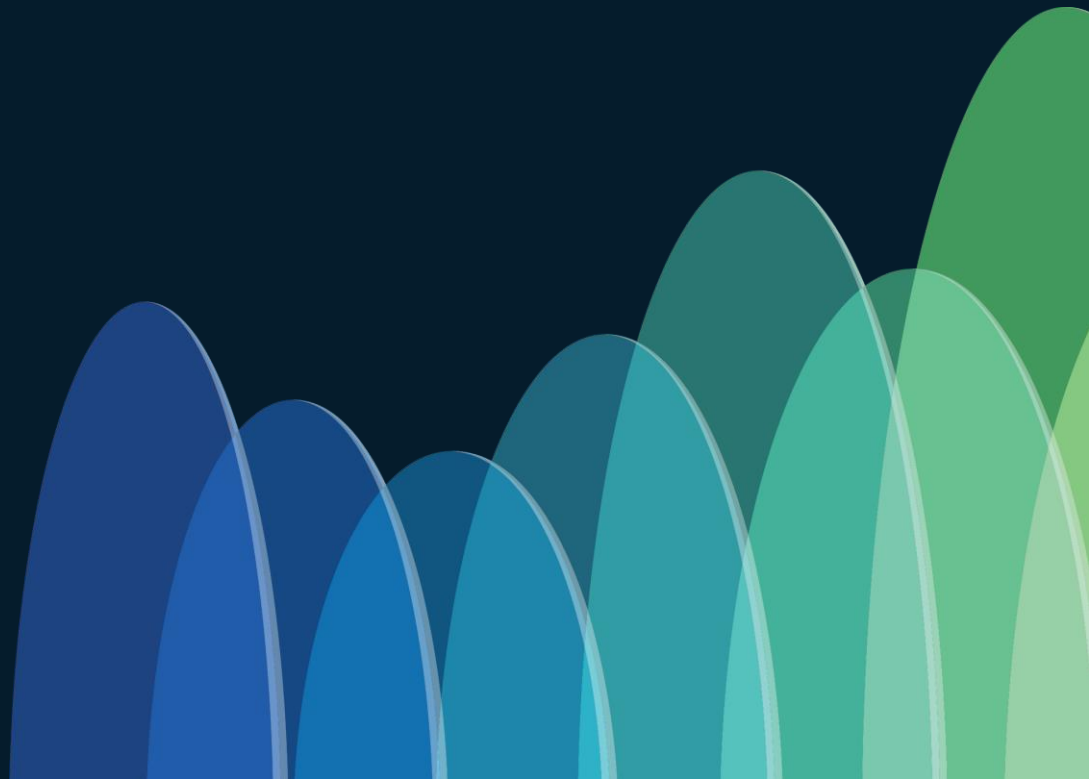
Key Session Objectives

At the end of this session, you will be able to:

- Understand the existing threat landscape and Cisco Secure Endpoint vision and mission
  - Discover key features of Cisco Secure Endpoint (EDR module of Secure Client) that will allow you to Prevent, Detect, Respond, and Protect your organization
  - Implement an effective Outcome-driven Endpoint Security
  - Leverage existing Integrations between multiple products to create a robust, all-around Security Framework

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Landscape



Threat Landscape



Financial T

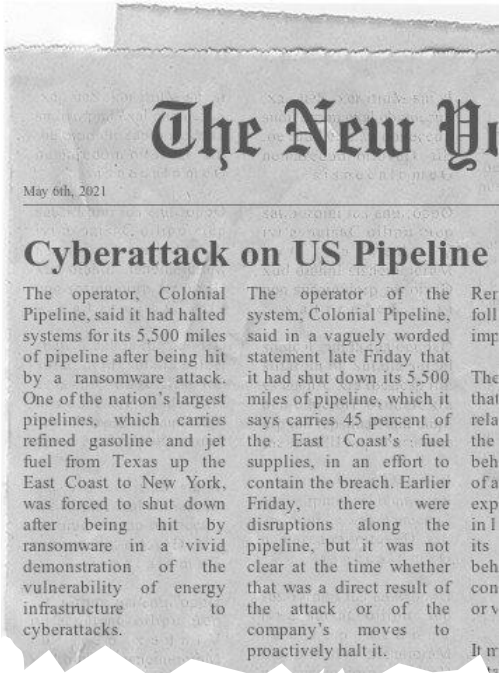
August 27, 2017

Jackpot with a Fish Tank Th

A group of hackers hit a different kind of jackpot in 2017 when they gained access to a casino's database through a smart thermometer. Unexpected doors into the corporate network In the case of the smart fish tank, the casino had configured the tank to use an individual VPN to isolate the tank's communications from the commercial network, but the attacker managed to use this foothold into the company network to scan for vulnerabilities in other

Ultimately, the threat actors managed to transfer 10GB of company data outside the network, to a server in Finland. The data was uploaded to the server via the compromised fish tank.

In the case of the compromised smart drawing pads, unbeknown to the firm, the devices were connected to the office Wi-Fi, while still using the default login credentials that came with the design pad software.



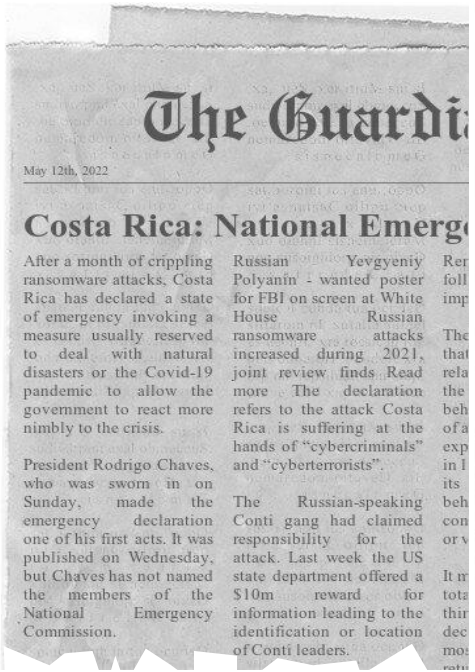
The New Y

May 6th, 2021

Cyberattack on US Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack. One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks.

The operator of the system, Colonial Pipeline, said in a vaguely worded statement late Friday that it had shut down its 5,500 miles of pipeline, which it says carries 45 percent of the East Coast's fuel supplies, in an effort to contain the breach. Earlier Friday, there were disruptions along the pipeline, but it was not clear at the time whether that was a direct result of the attack or of the company's moves to proactively halt it.



The Guardi

May 12th, 2022

Costa Rica: National Emerg

After a month of crippling ransomware attacks, Costa Rica has declared a state of emergency invoking a measure usually reserved to deal with natural disasters or the Covid-19 pandemic to allow the government to react more nimbly to the crisis.

President Rodrigo Chaves, who was sworn in on Sunday, made the emergency declaration one of his first acts. It was published on Wednesday, but Chaves has not named the members of the National Emergency Commission.

Russian Yevgyeniy Polyanin - wanted poster for FBI on screen at White House Russian ransomware attacks increased during 2021, joint review finds Read more The declaration refers to the attack Costa Rica is suffering at the hands of "cybercriminals" and "cyberterrorists".

The Russian-speaking Conti gang had claimed responsibility for the attack. Last week the US state department offered a $10m reward for information leading to the identification or location of Conti leaders.



Le Monde

January 9th, 2025

Ivanti VPN vulnerabilities

U.S. software giant Ivanti has warned that a zero-day vulnerability in its widely used enterprise VPN appliance has been exploited to compromise the networks of its corporate customers.

Ivanti said on Wednesday that the critical-rated vulnerability, tracked as CVE-2025-0282, can be exploited without any authentication to remotely plant malicious code on Ivanti's Connect Secure, Policy Secure, and ZTA Gateways products. Ivanti says its Connect Secure remote-access VPN solution is "the most widely adopted SSL VPN

size, across every major industry."

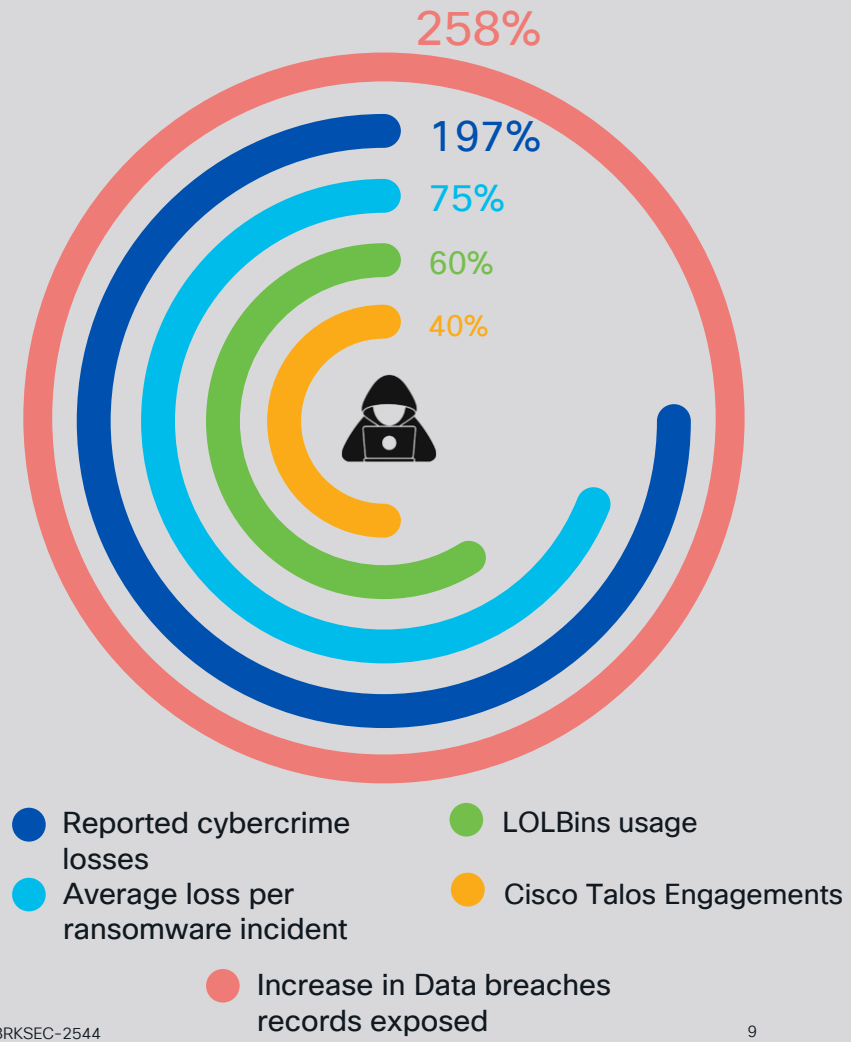
This is the latest exploited security vulnerability to target Ivanti's products in recent years. Last year, the technology maker pledged to overhaul its security processes after hackers targeted vulnerabilities in several of its products to launch mass-hacks against its customers.

The company said it became aware of the latest vulnerability after its Ivanti Integrity Checker Tool (ICT) flagged malicious activity on some customer ap

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Top Cyber Security Threats

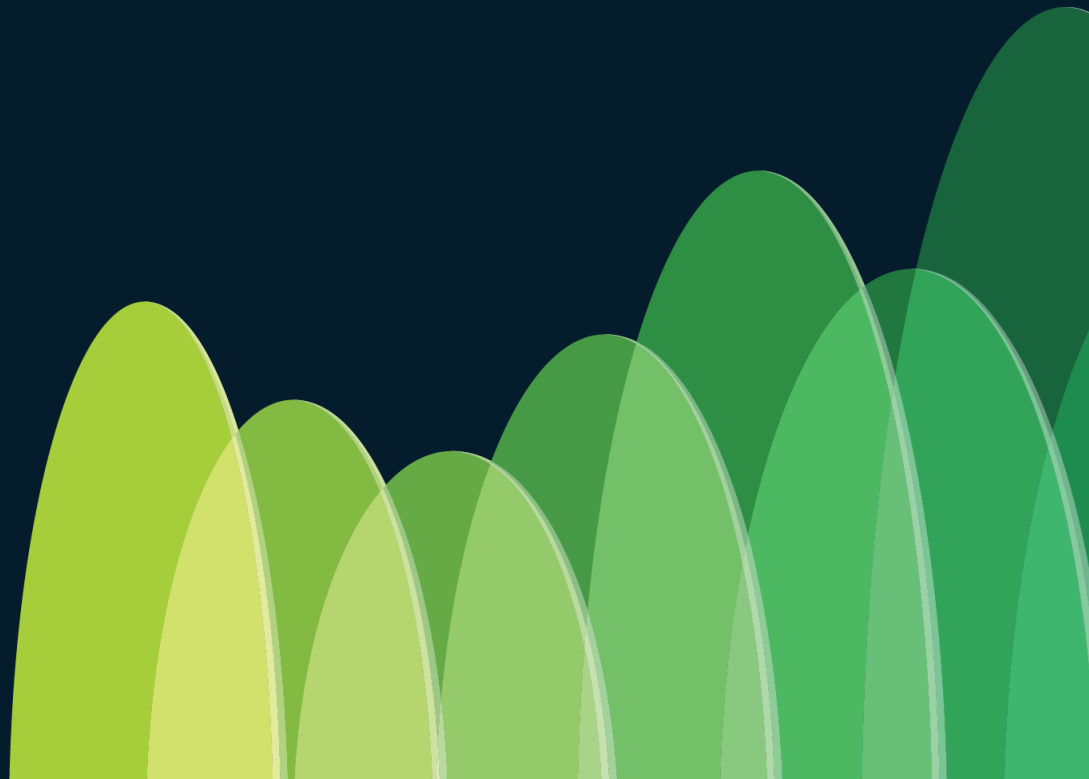
- **Total reported losses** from cybercrime incidents **increased** 197% from 2020 to 2023, growing from $4.2 Billion to **over $12.5 Billion**
- The **average loss per ransomware** incident rose from $12,000 in 2022 to $21,000 in 2023, representing a **75% YoY increase**
- Throughout 2024, **Cisco Talos observed** that **60% of adversaries utilized living-off-the-land binaries** (LoLBins) and open-source tools to execute attacks, highlighting the need for enhanced **monitoring of legitimate applications on endpoints.**
- Nearly **40% of Cisco Talos's engagements** involved **ransomware or data theft extortion**, with new variants emerging, emphasizing the **evolving nature of endpoint threats**
- **Data breaches** exposed 155 million records in 2020 and totalled **more than 400 million records** being exposed in 2023, **representing a 258% increase**



FBI Internet Cybercrime Report (IC3)

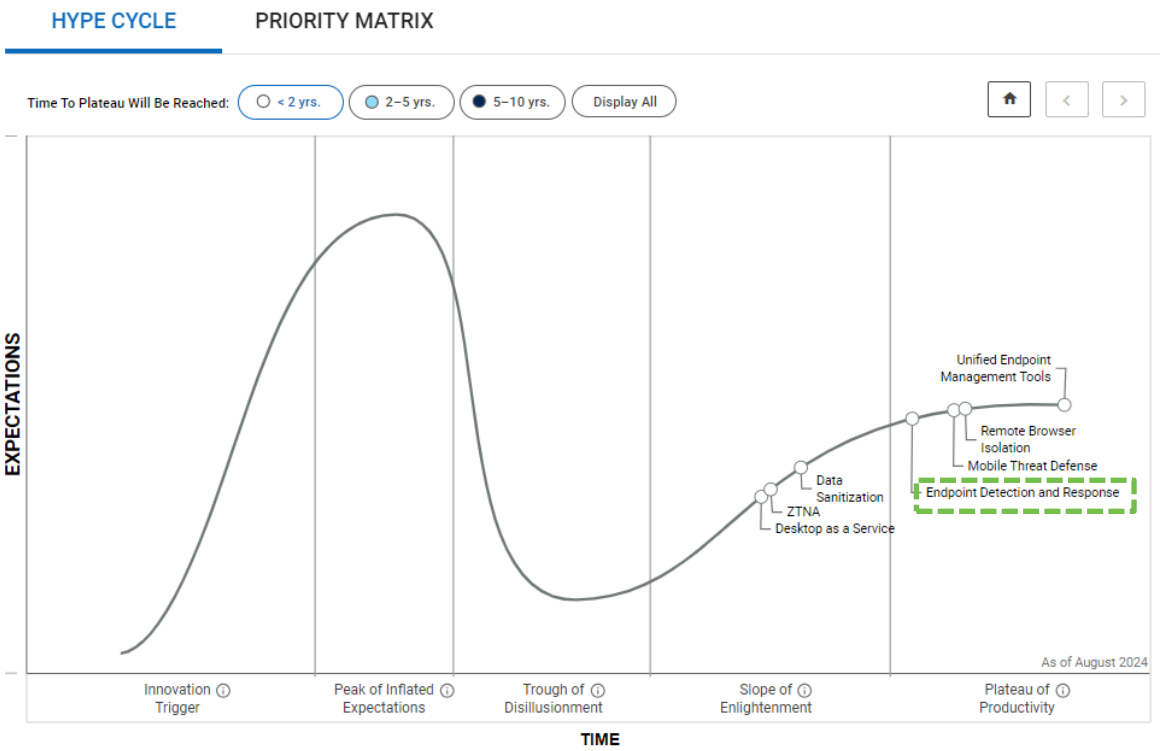
Talos IR trends Q3 2024

Secure Endpoint Vision & Mission



cisco Live!

The State of Endpoint Security

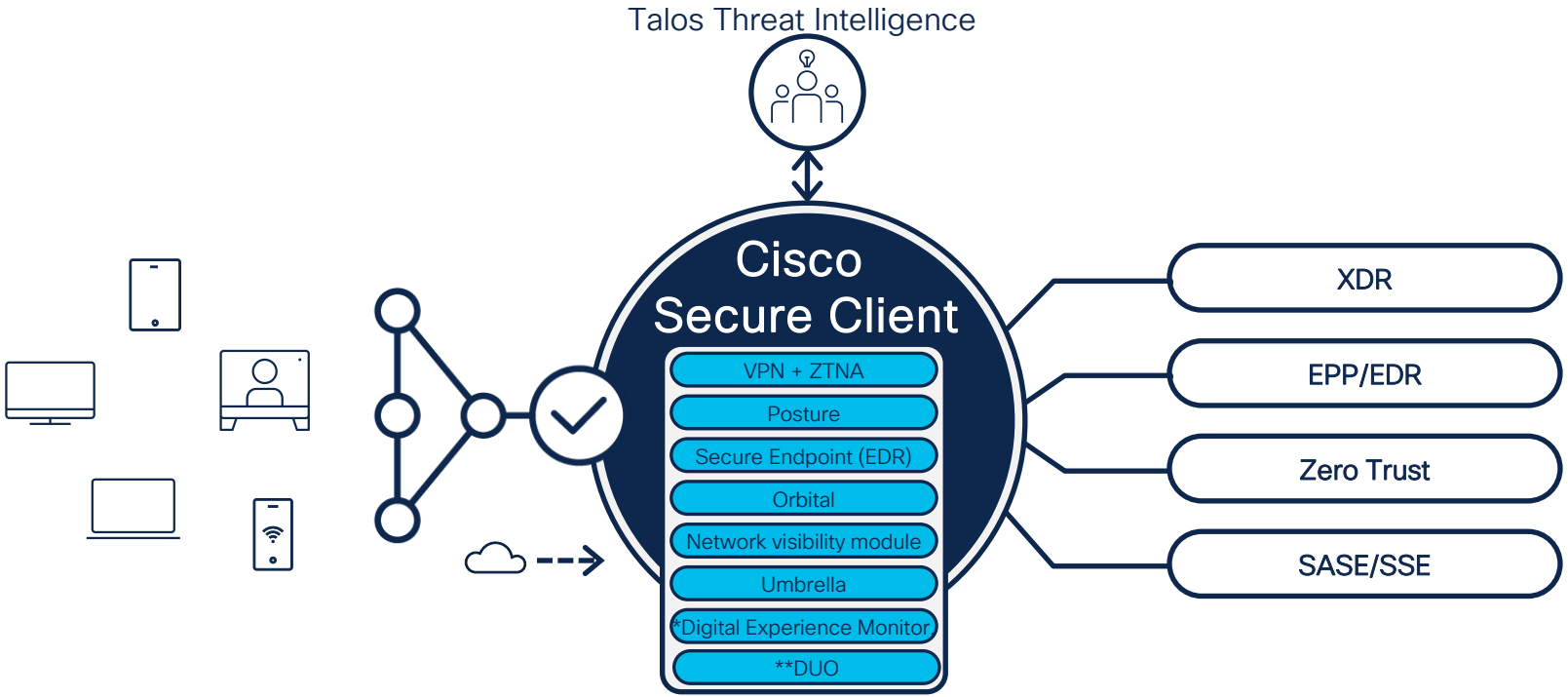


- Gartner Hype cycle: EDR has reached the Plateau of Productivity
- Market Penetration: More than 50% of target audience
- NextGen AV and EDR are now standard – EDR is fully mainstream
- Engines to help combat AI-driven Threats and key integrations with XDR and SASE

Gartner's Hype Cycle 2024

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission

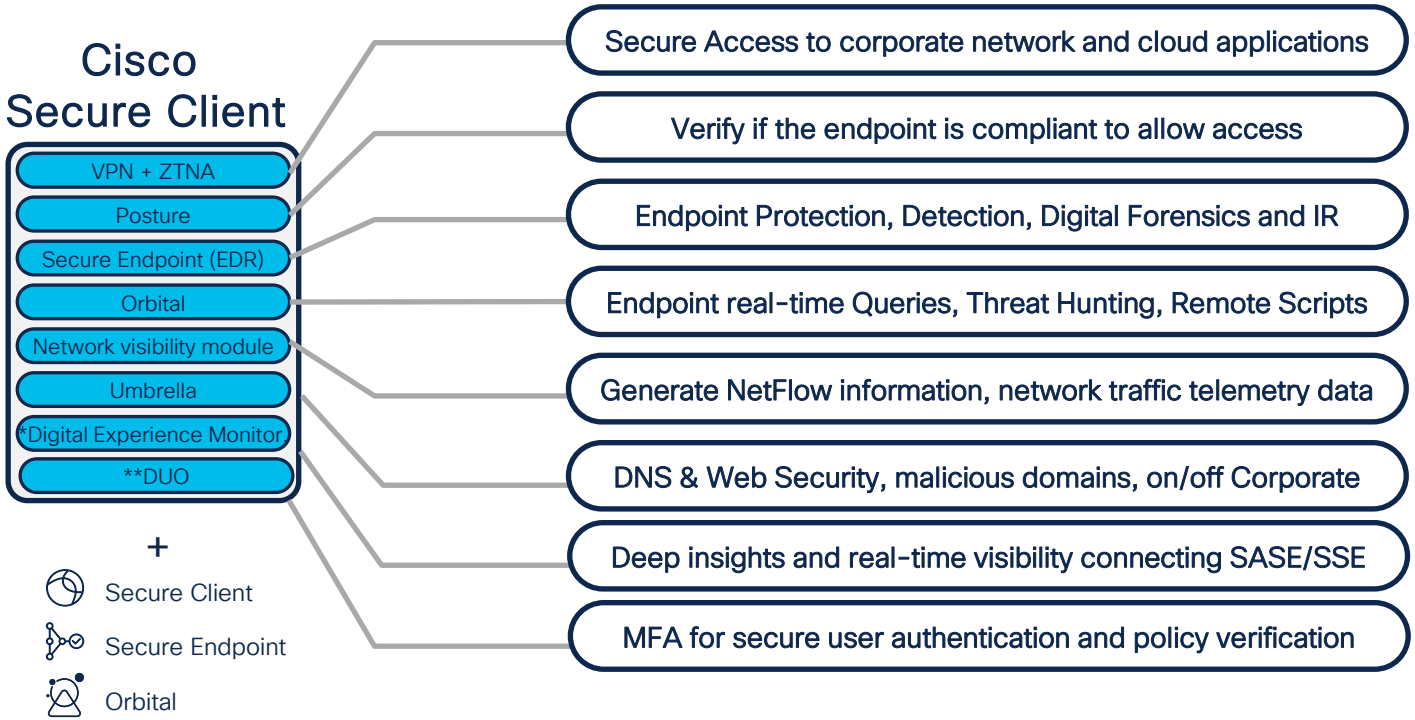


* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission

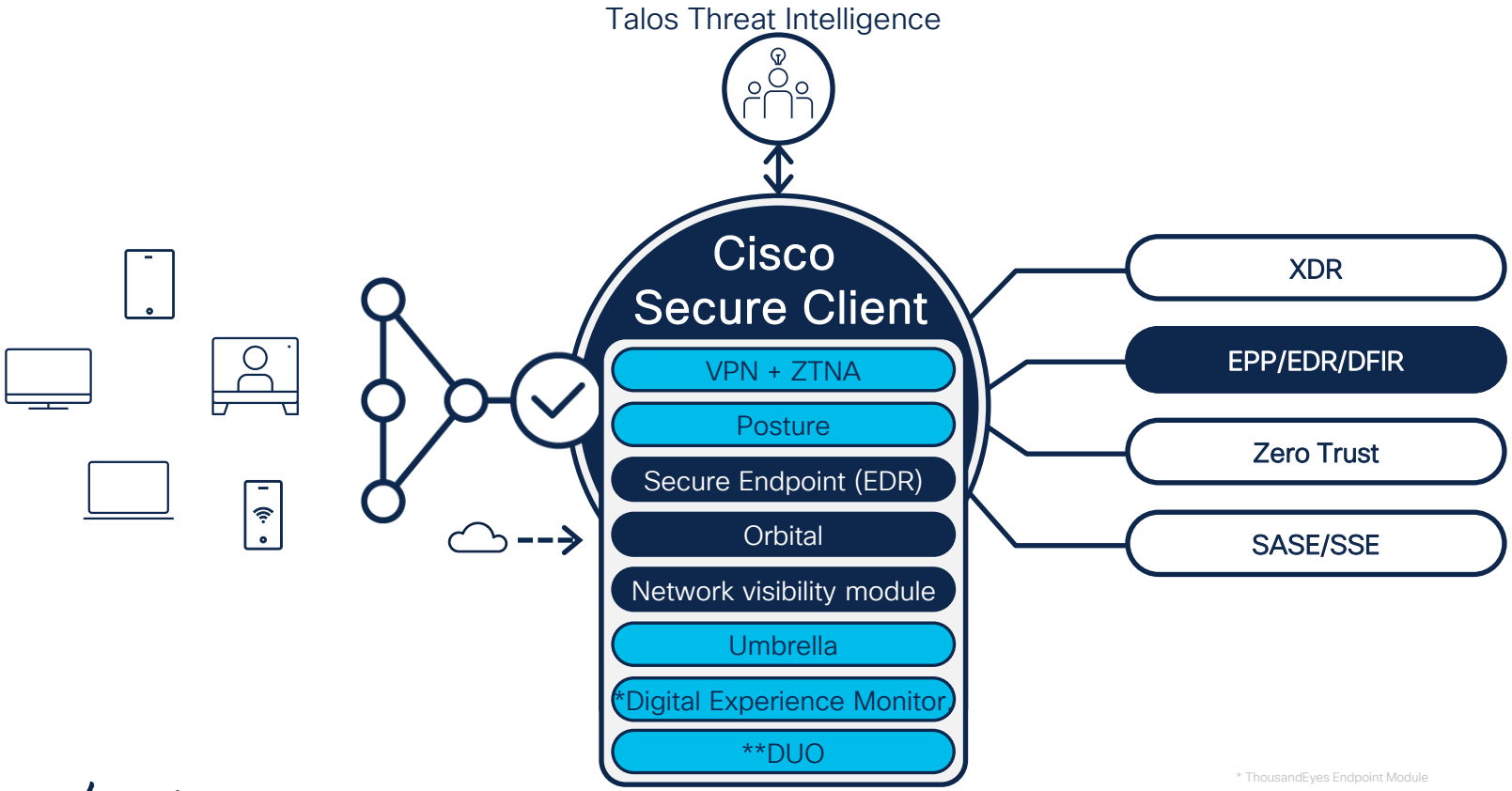


* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission

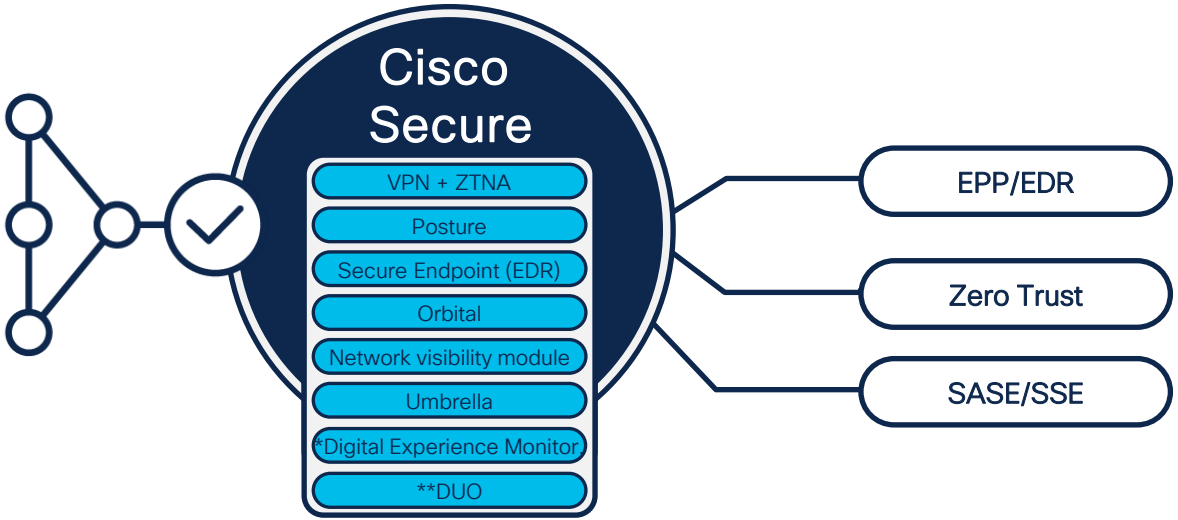


* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission

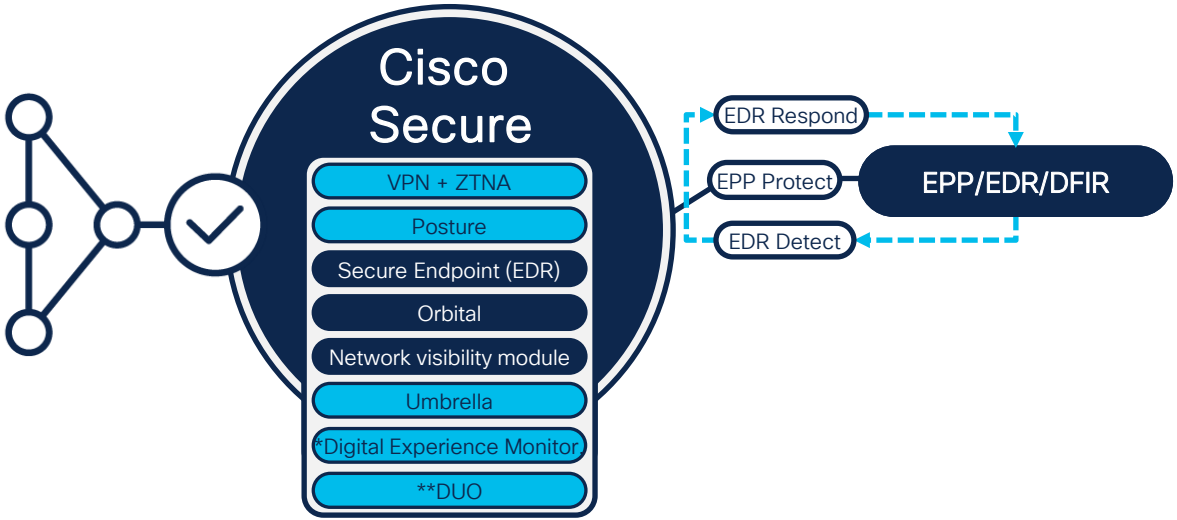


* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission

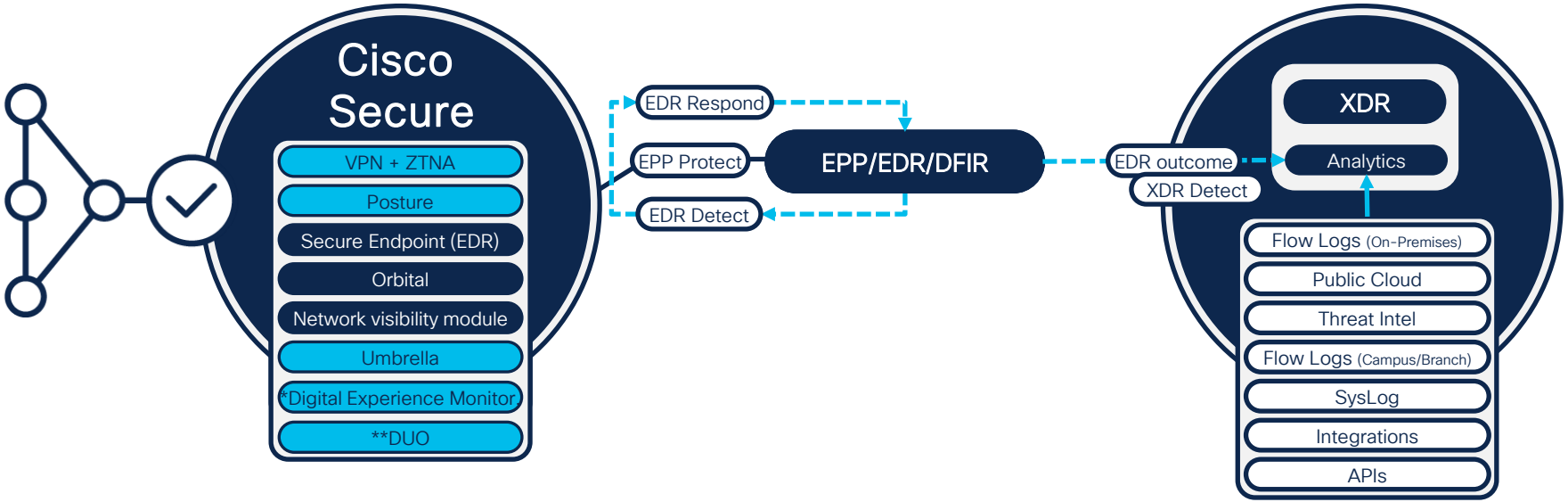


* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission

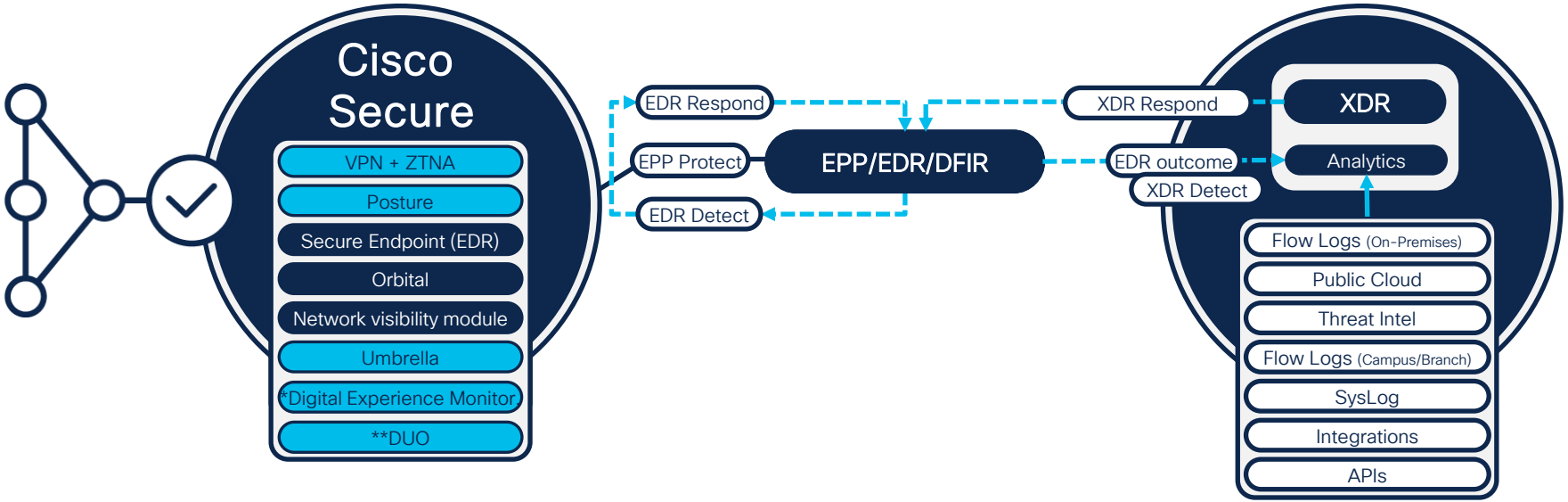


* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Endpoint: Vision & Mission



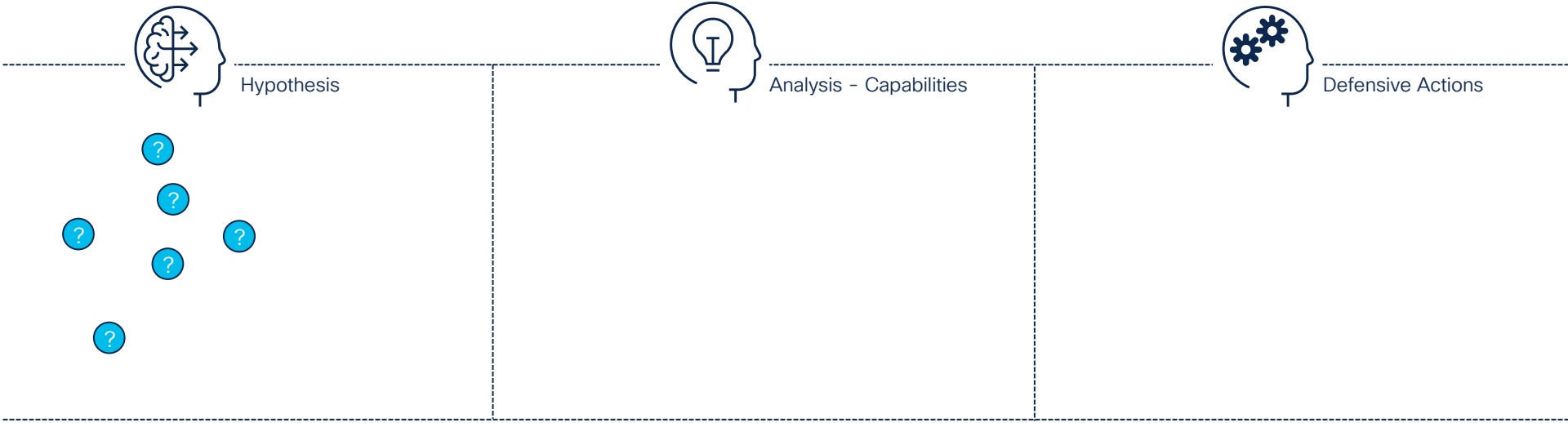
* ThousandEyes Endpoint Module

** Fits in our Vision, technically not yet a module

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Outcome-driven security

Defensive Outcomes Through Risk-Based Cybersecurity

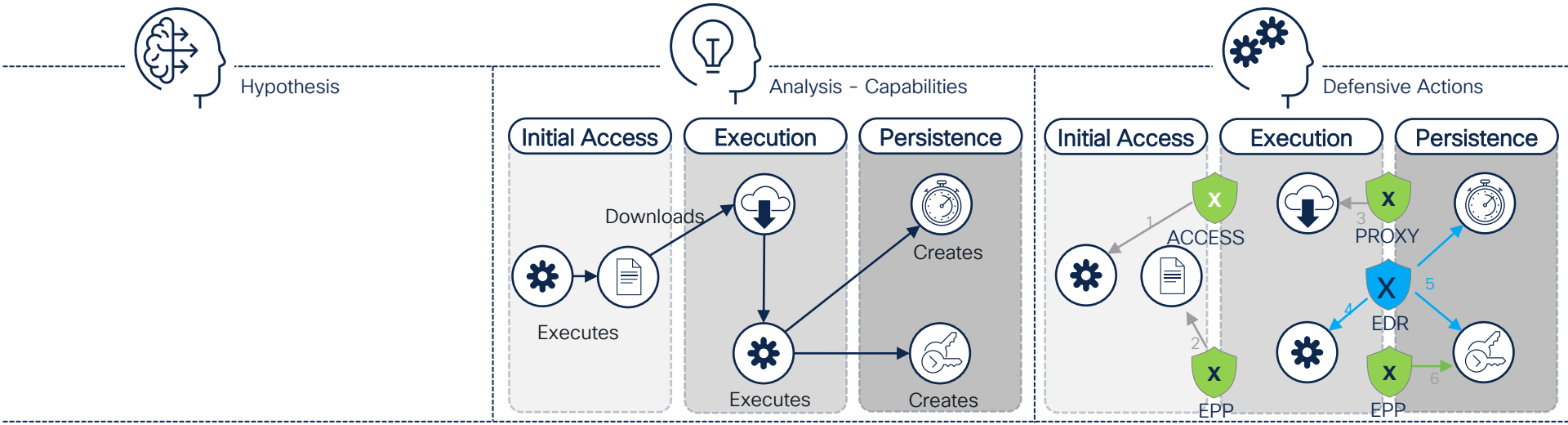


Scenario (Hypothesis)
... Something is showing red in my console.... But what happened??

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Outcome-driven security

Defensive Outcomes Through Risk-Based Cybersecurity



Scenario (Hypothesis)
... Something is showing red in my console.... But what happened??

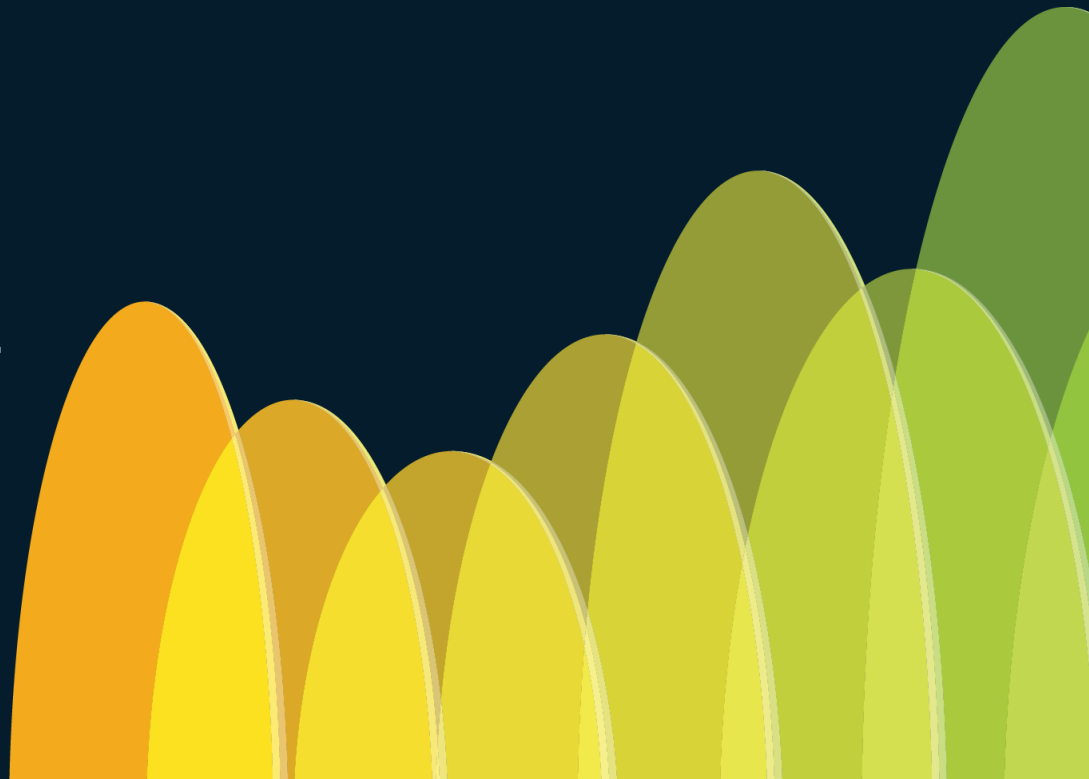
Defenders can
- Characterize the threat
- Express actions against it
- Conduct actions to neutralize it

1. Restrict
2. Block
3. Interrupt
4. Detect
5. Observe
6. Block

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent, Detect

Respond, Protect



Prevent & Detect Capabilities



cisco Live!

Prevention Capabilities

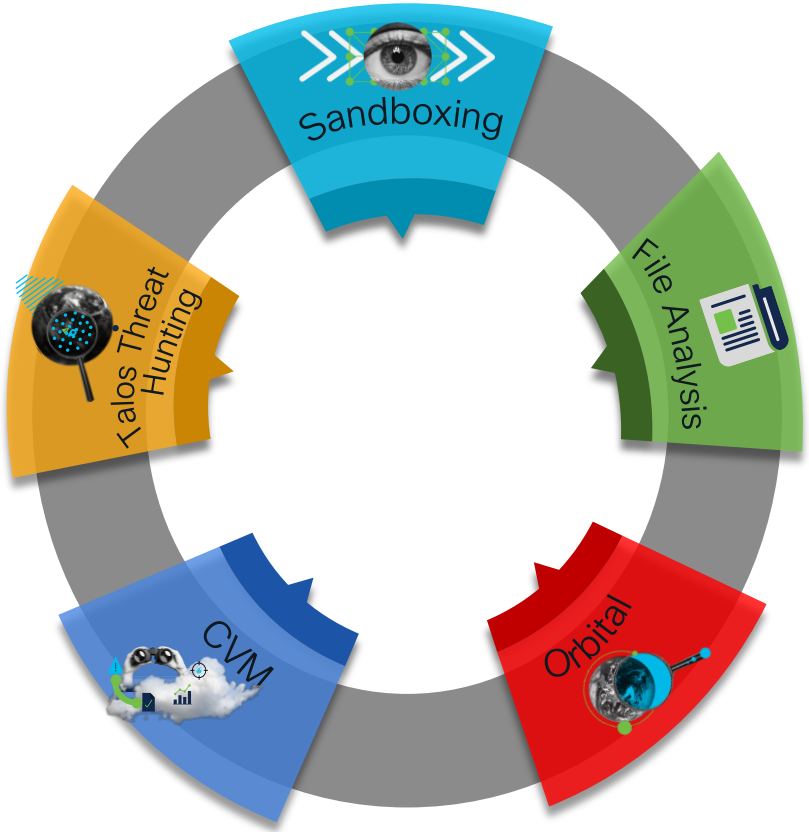


Main Protection Engines/Capabilities

1. **Behaviour Protection Engine** Detects and blocks threats based on abnormal behavior and activity patterns, including fileless malware
2. **Exploit Prevention Engine** Mitigates exploits by targeting vulnerabilities used in ransomware, rootkits, and other attacks
3. **Script-based and Fileless Attacks** Prevents execution of malicious scripts and memory-based, fileless attack techniques
4. **Ransomware** Protects against ransomware by combining behavior analysis, exploit prevention, and dynamic file monitoring
5. **Network Flow correlation** Identifies malicious network activity by analyzing device and network-level behaviors
6. **Signature-based Anti-Virus** Detects known malware based on traditional signature-based methods
7. **Offline Protection** Offers protection without requiring an internet connection by leveraging local engines for behaviour and signature analysis
8. **Cloud-based Reputation lookups** Analyzes file and URL reputations in real-time via Cisco's Cloud for proactive threat prevention

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detection Capabilities

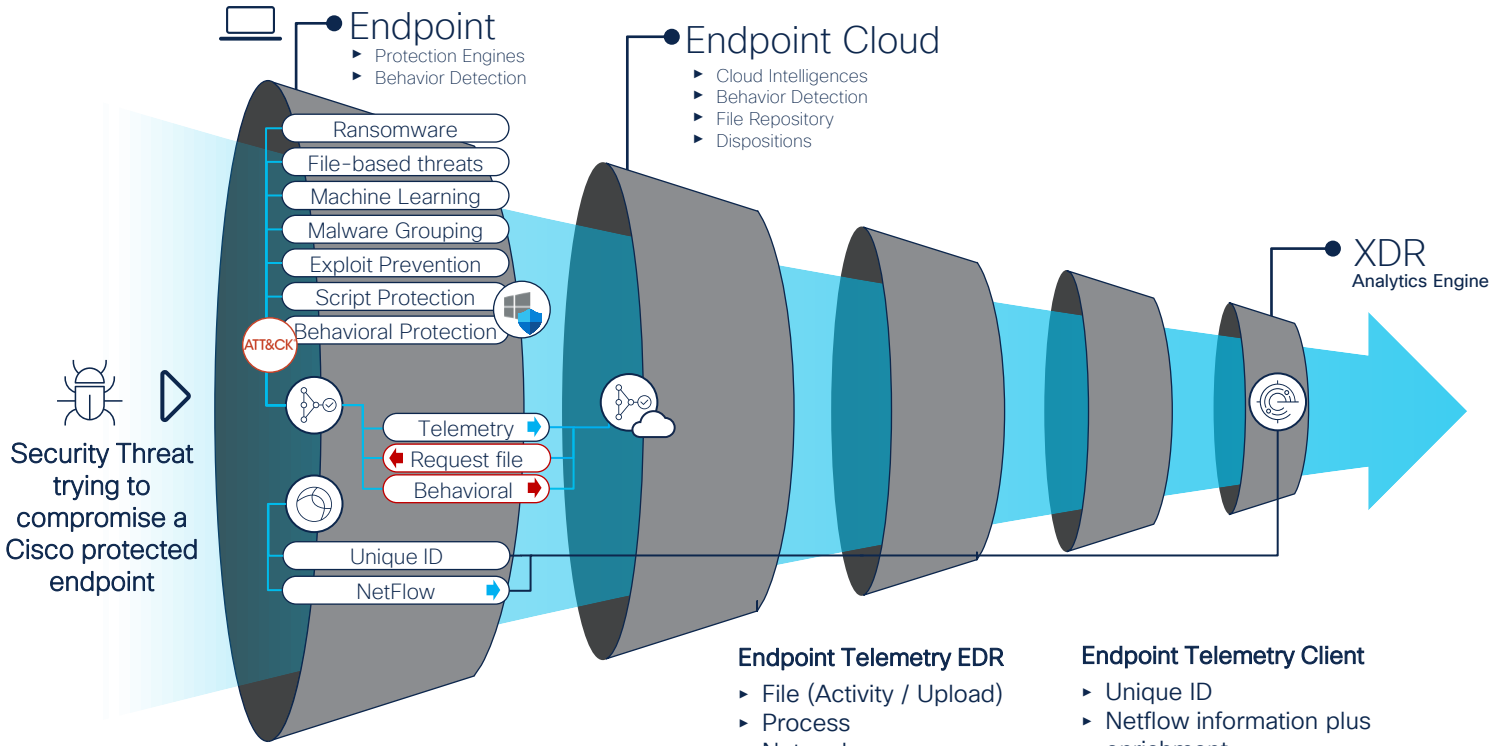


Main Detection Engines/Capabilities

1. **Sandboxing** Dynamically executes suspicious files in an isolated environment to detect malicious behaviours without impacting endpoints
2. **File Analysis** Inspects files in detail using advanced static and dynamic analysis techniques to identify potential threats, by leveraging both cloud-based intelligence and local analysis capabilities and supporting retrospective detection
3. **Orbital Advanced Search** Enables real-time and retrospective endpoint data queries to uncover hidden threats and anomalies. It provides detailed information about file activity, process execution, and registry changes to support forensic analysis
4. **Vulnerability Management** Integrated with CVM, a Risk-Score is provided, enabling organizations to prioritize vulnerabilities based on risk and exposure, enhancing decision-making for remediation efforts
5. **Talos Threat Hunting** Leveraging Cisco Talos Intelligence, this service delivers advanced threat intelligence and proactive hunting capabilities. It combines machine learning with human expertise to identify and mitigate emerging threats

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent & Detect capability layers



Endpoint Telemetry EDR

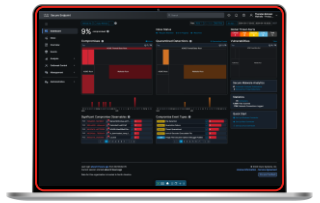
- File (Activity / Upload)
- Process
- Network
- Command Line
- Engine Events
- Endpoint Behavior

Endpoint Telemetry Client

- Unique ID
- Netflow information plus enrichment

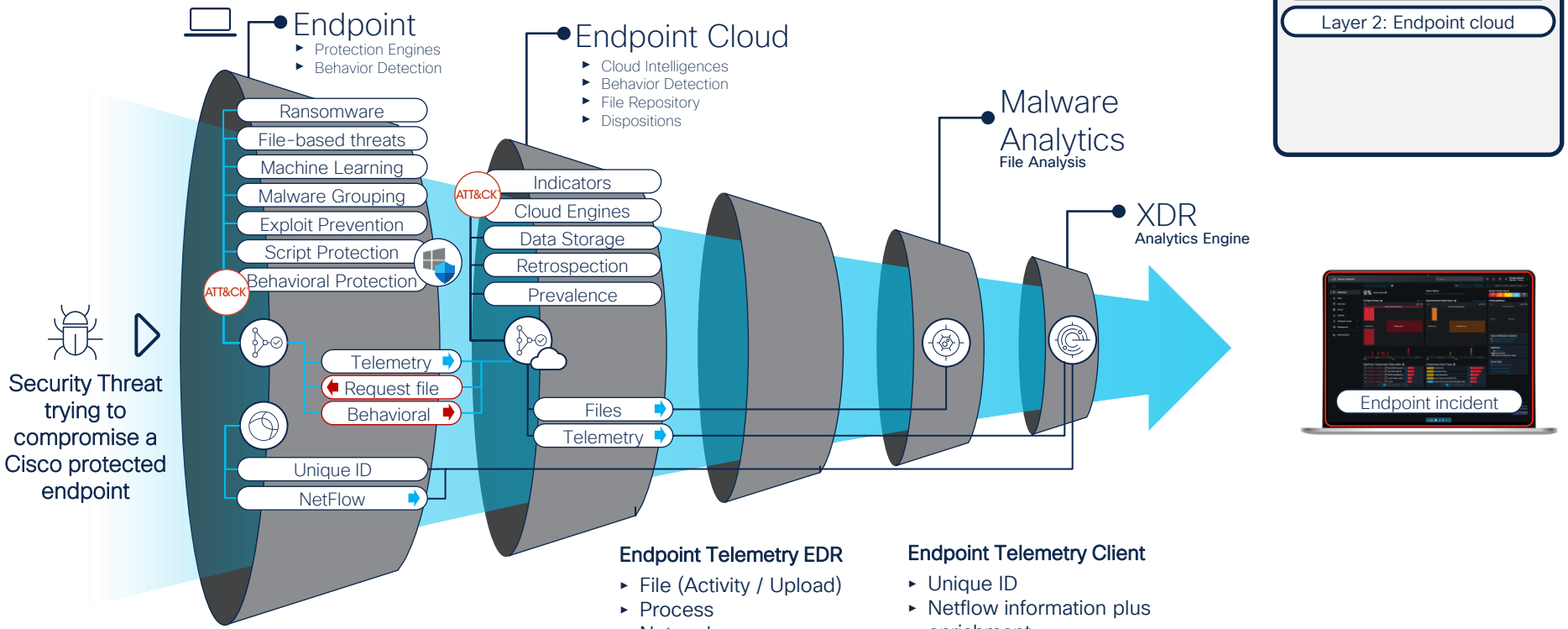
Threat Analysis: Layered Approach

Layer 1: Endpoint connector



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent & Detect capability layers



Endpoint Telemetry EDR

- File (Activity / Upload)
- Process
- Network
- Command Line
- Engine Events
- Endpoint Behavior

Endpoint Telemetry Client

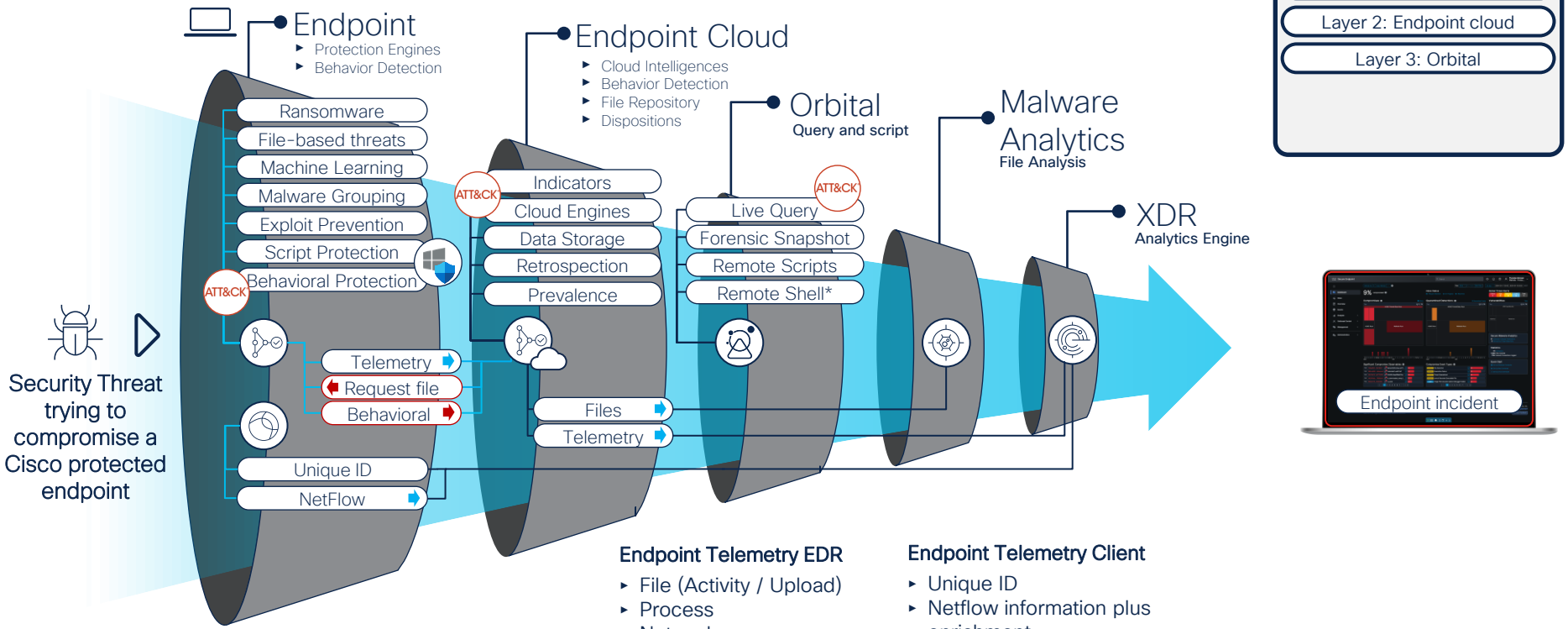
- Unique ID
- Netflow information plus enrichment

Threat Analysis: Layered Approach

- Layer 1: Endpoint connector
- Layer 2: Endpoint cloud

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent & Detect capability layers



Endpoint Telemetry EDR

- File (Activity / Upload)
- Process
- Network
- Command Line
- Engine Events
- Endpoint Behavior

Endpoint Telemetry Client

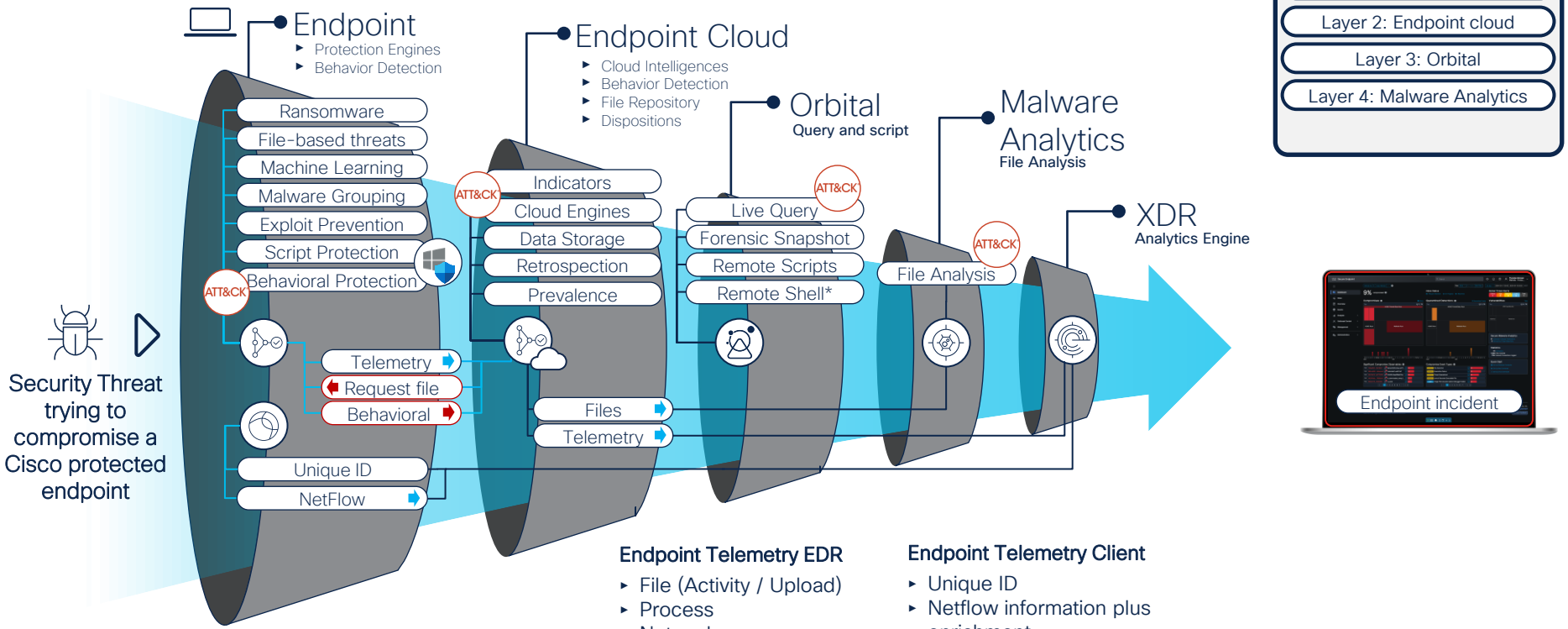
- Unique ID
- Netflow information plus enrichment

Threat Analysis: Layered Approach

- Layer 1: Endpoint connector
- Layer 2: Endpoint cloud
- Layer 3: Orbital

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent & Detect capability layers



Threat Analysis: Layered Approach

- Layer 1: Endpoint connector
- Layer 2: Endpoint cloud
- Layer 3: Orbital
- Layer 4: Malware Analytics

Endpoint Telemetry EDR

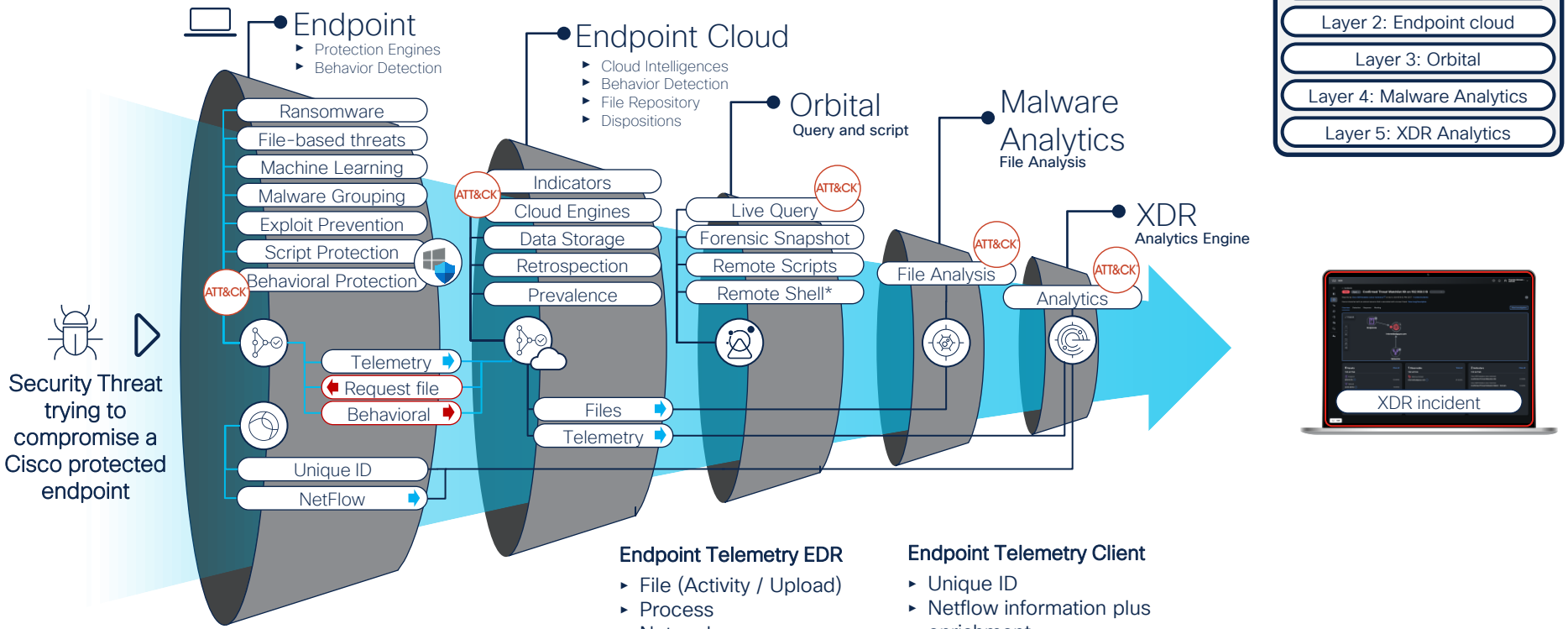
- File (Activity / Upload)
- Process
- Network
- Command Line
- Engine Events
- Endpoint Behavior

Endpoint Telemetry Client

- Unique ID
- Netflow information plus enrichment

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent & Detect capability layers



Threat Analysis: Layered Approach

- Layer 1: Endpoint connector
- Layer 2: Endpoint cloud
- Layer 3: Orbital
- Layer 4: Malware Analytics
- Layer 5: XDR Analytics

Endpoint Telemetry EDR

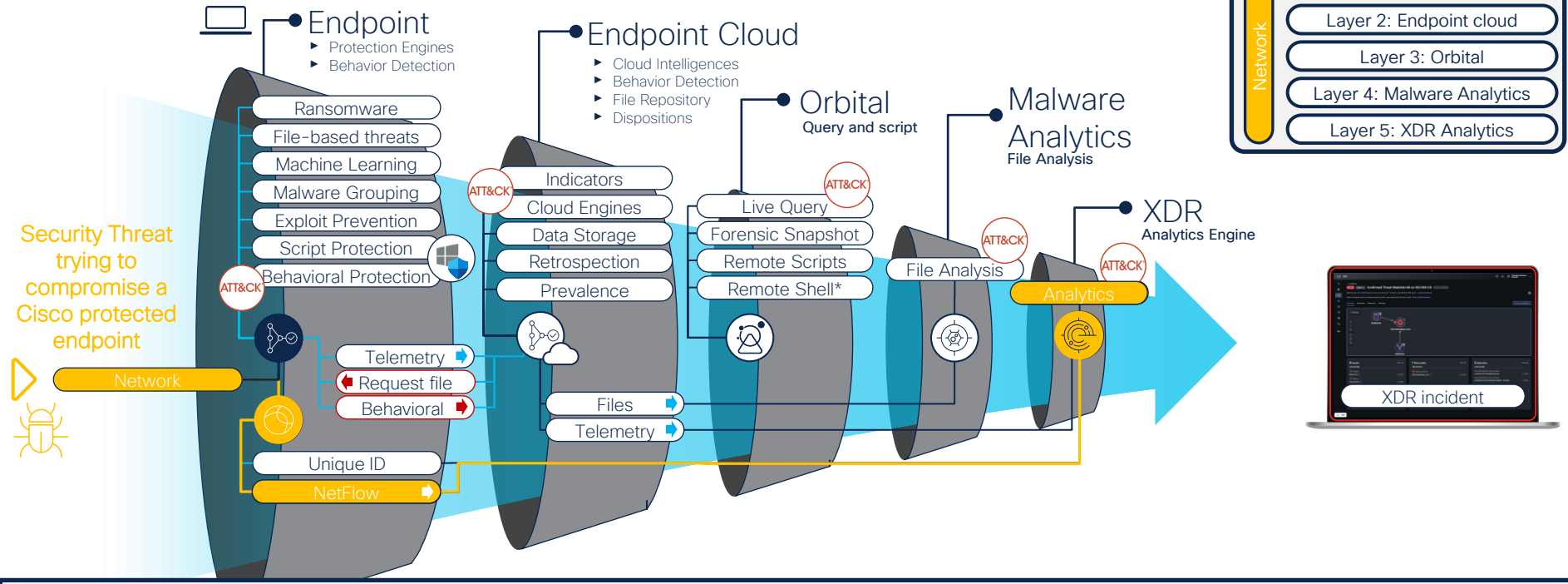
- File (Activity / Upload)
- Process
- Network
- Command Line
- Engine Events
- Endpoint Behavior

Endpoint Telemetry Client

- Unique ID
- Netflow information plus enrichment

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Prevent & Detect capability layers



Threat Analysis: Layered Approach

Network

- Layer 1: Endpoint connector
- Layer 2: Endpoint cloud
- Layer 3: Orbital
- Layer 4: Malware Analytics
- Layer 5: XDR Analytics

Insights into the network behavior are key to detect attacks sooner

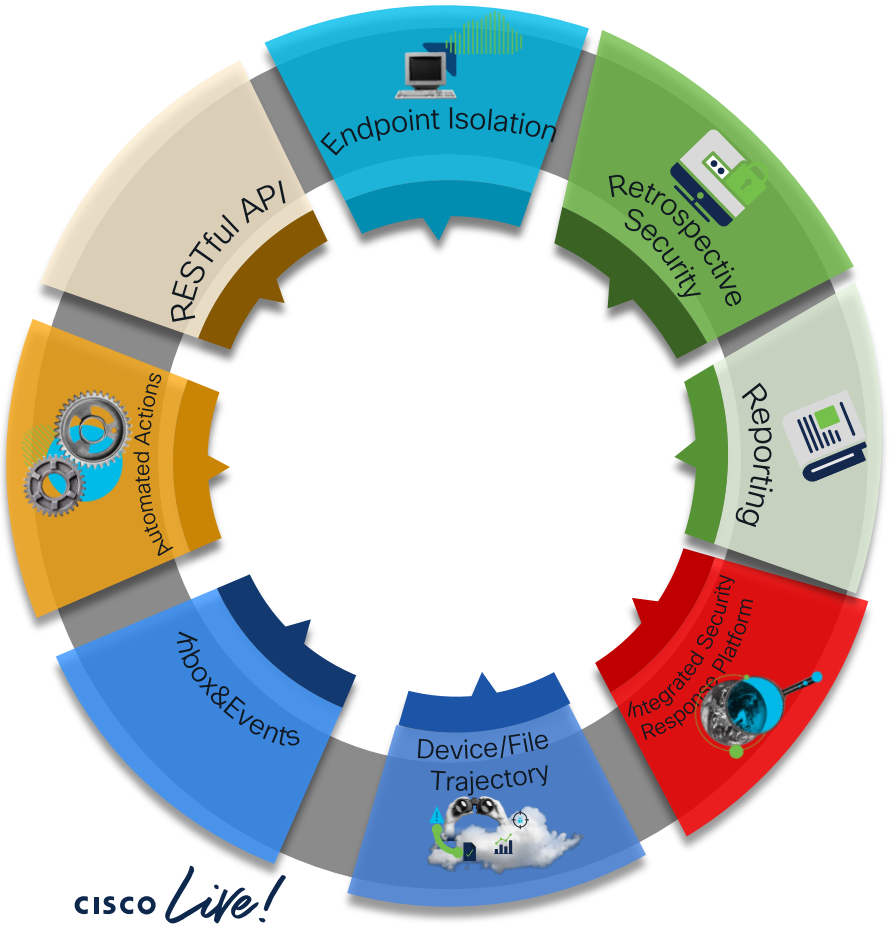
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities



cisco Live!

Response Capabilities



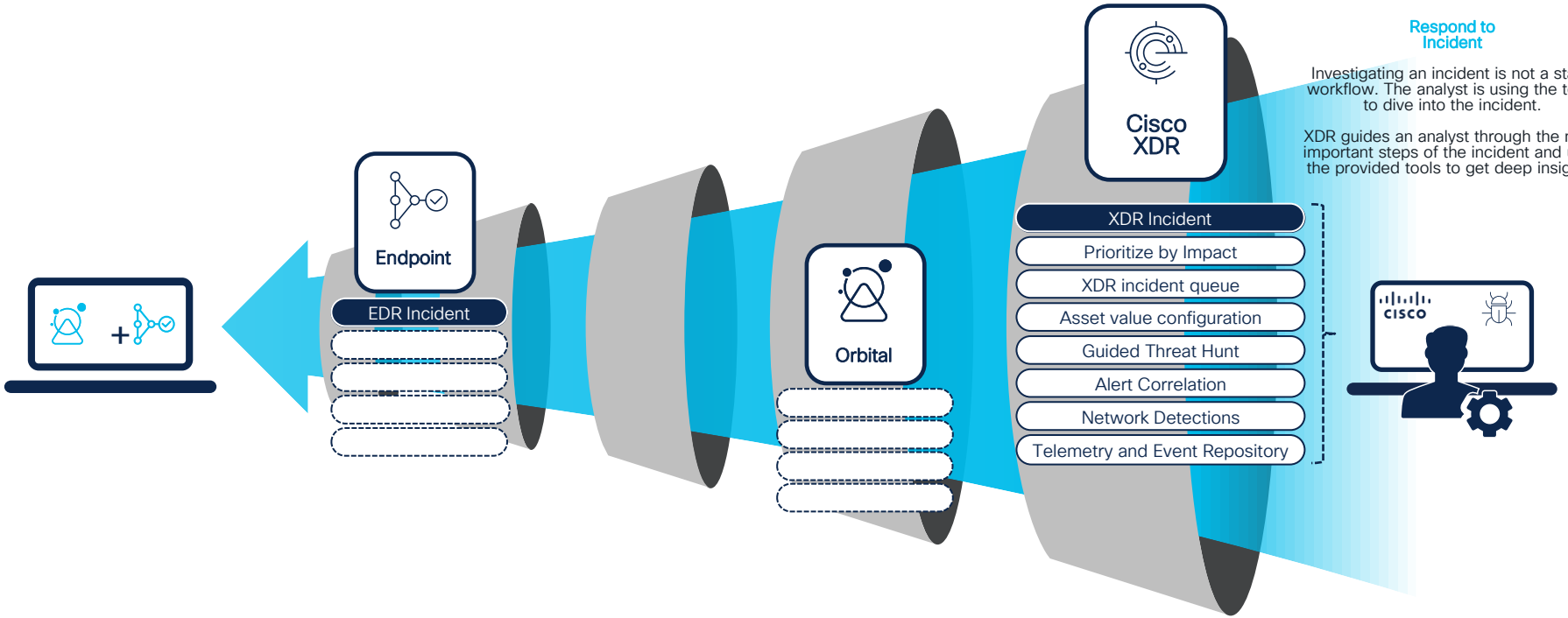
Main Response Engines/Capabilities

1. **Endpoint Isolation** Instantly isolates compromised endpoints from the network to prevent lateral movement and contain threats
2. **Retrospective Security** Evaluate threats in scanned files based on updated threat intelligence and mitigate them retrospectively
3. **Reporting** Customizable dashboards and heatmaps to visualize threats, compromised systems, and quarantine actions
4. **Integrated Security Response Platform** Deep investigations with Orbital Advanced Search to uncover and respond to ongoing or past threats
5. **Device/File Trajectory** Detailed tracking of files and device behaviors to map infection paths and aid in retrospective analysis
6. **Inbox&Events** Centralized threat management with real-time alerts, categorization, and actionable insights for efficient incident handling
7. **Automated Actions** Automatically submit and quarantine potentially malicious files - stop execution and spreading. Isolate an endpoint/move it into a different group automatically
8. **RESTful API** Robust integrations for real-time event streaming, automation, and security ecosystem enhancement

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities

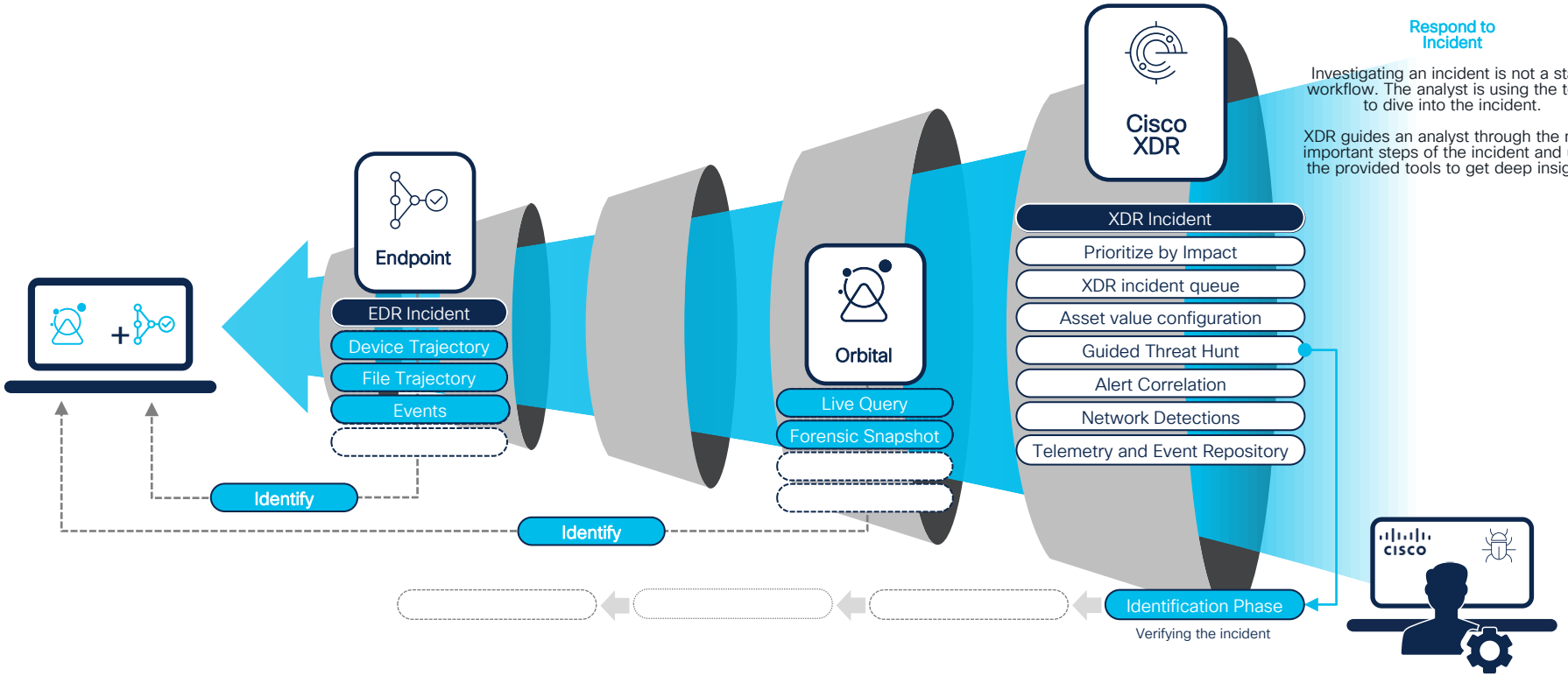
Contain and Eradicate with the endpoint



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities

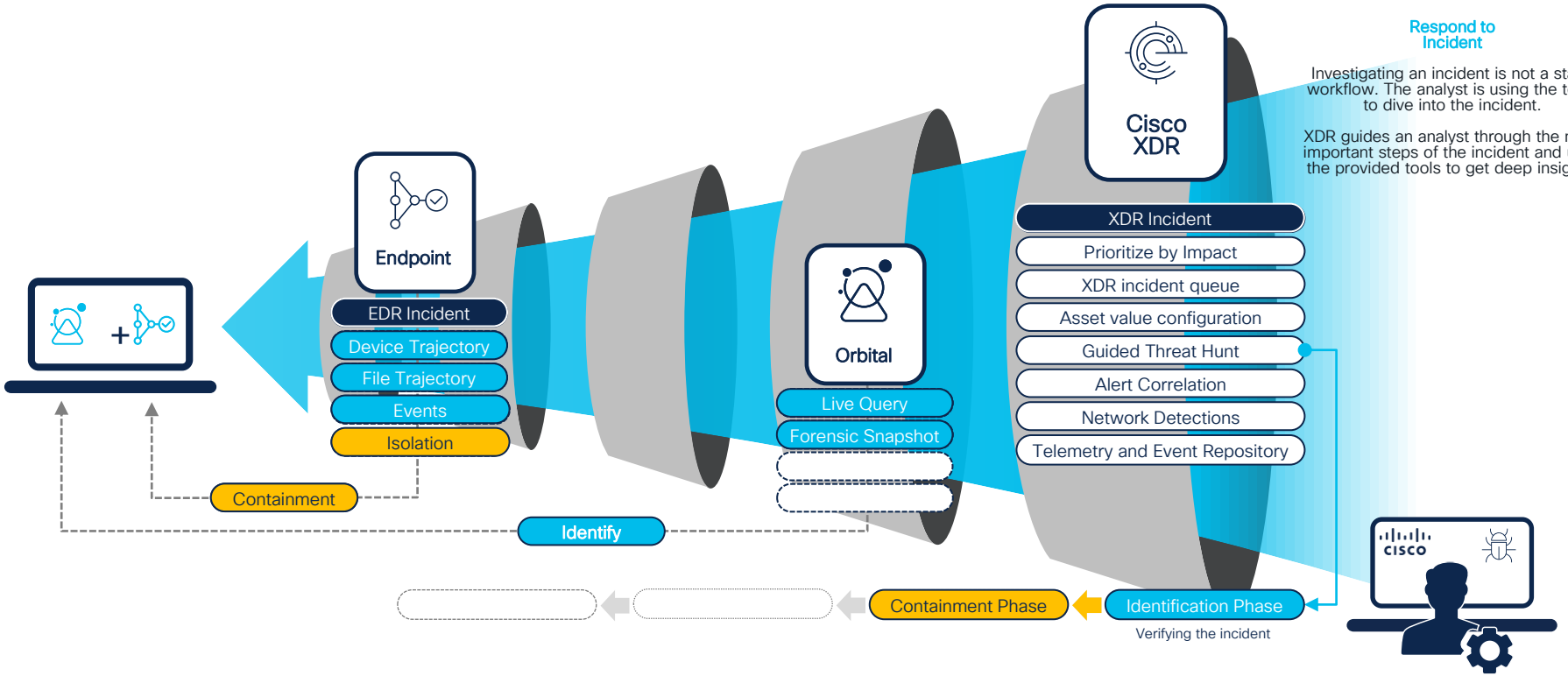
Contain and Eradicate with the endpoint



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities

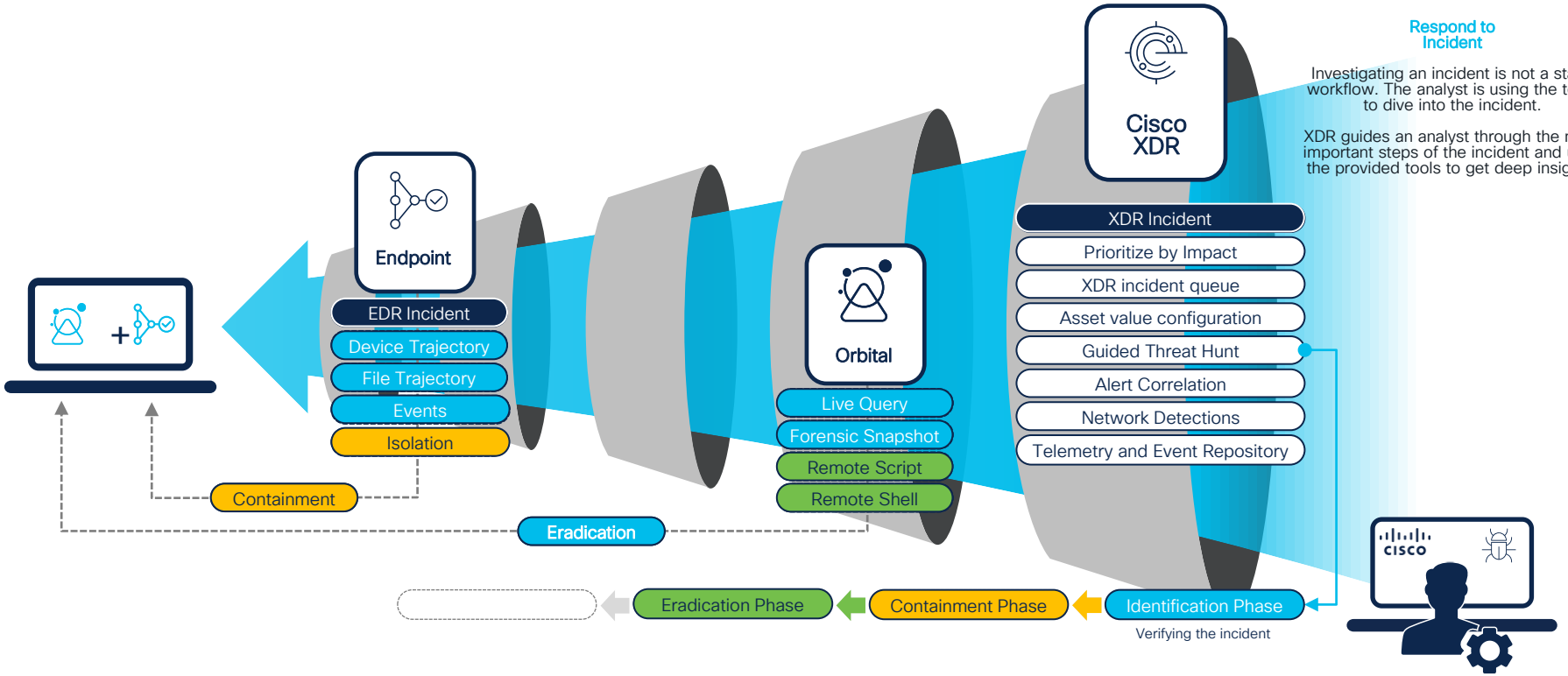
Contain and Eradicate with the endpoint



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities

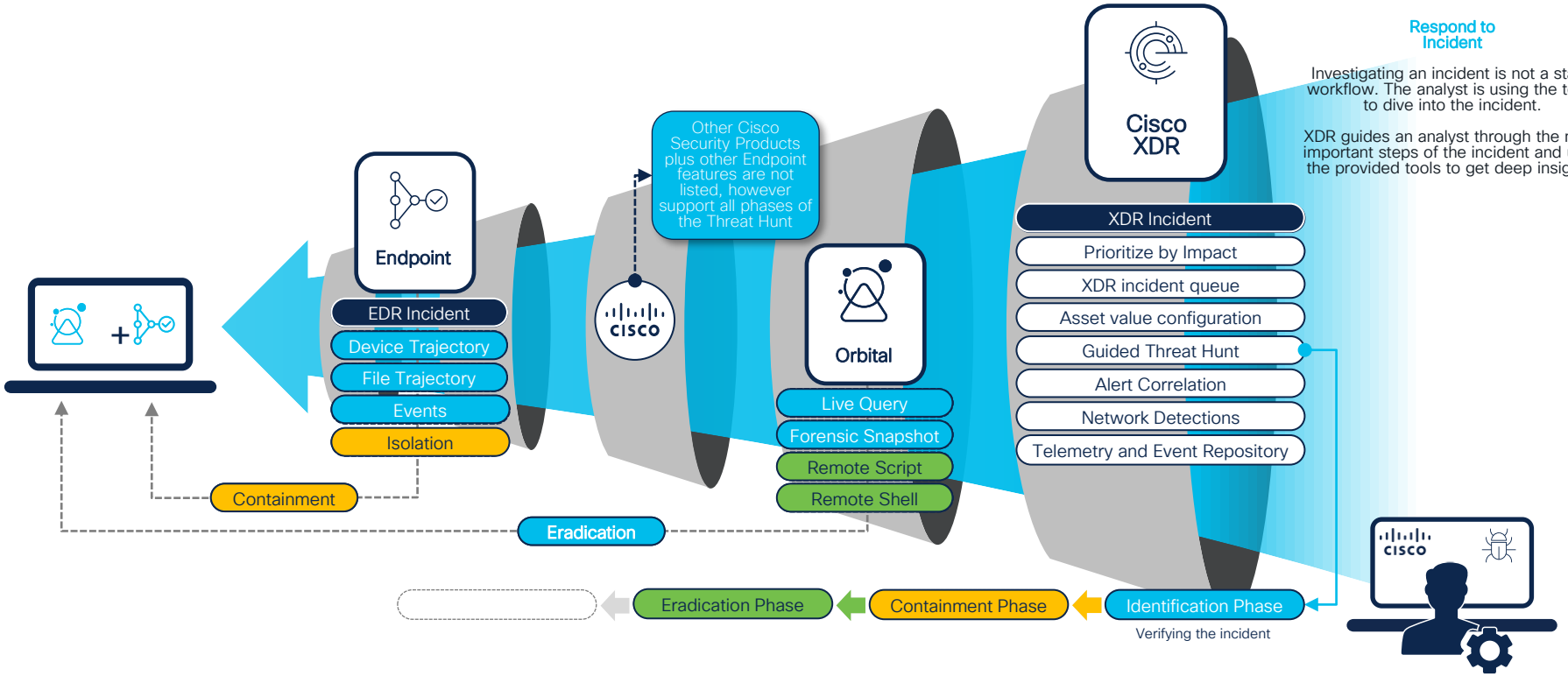
Contain and Eradicate with the endpoint



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities

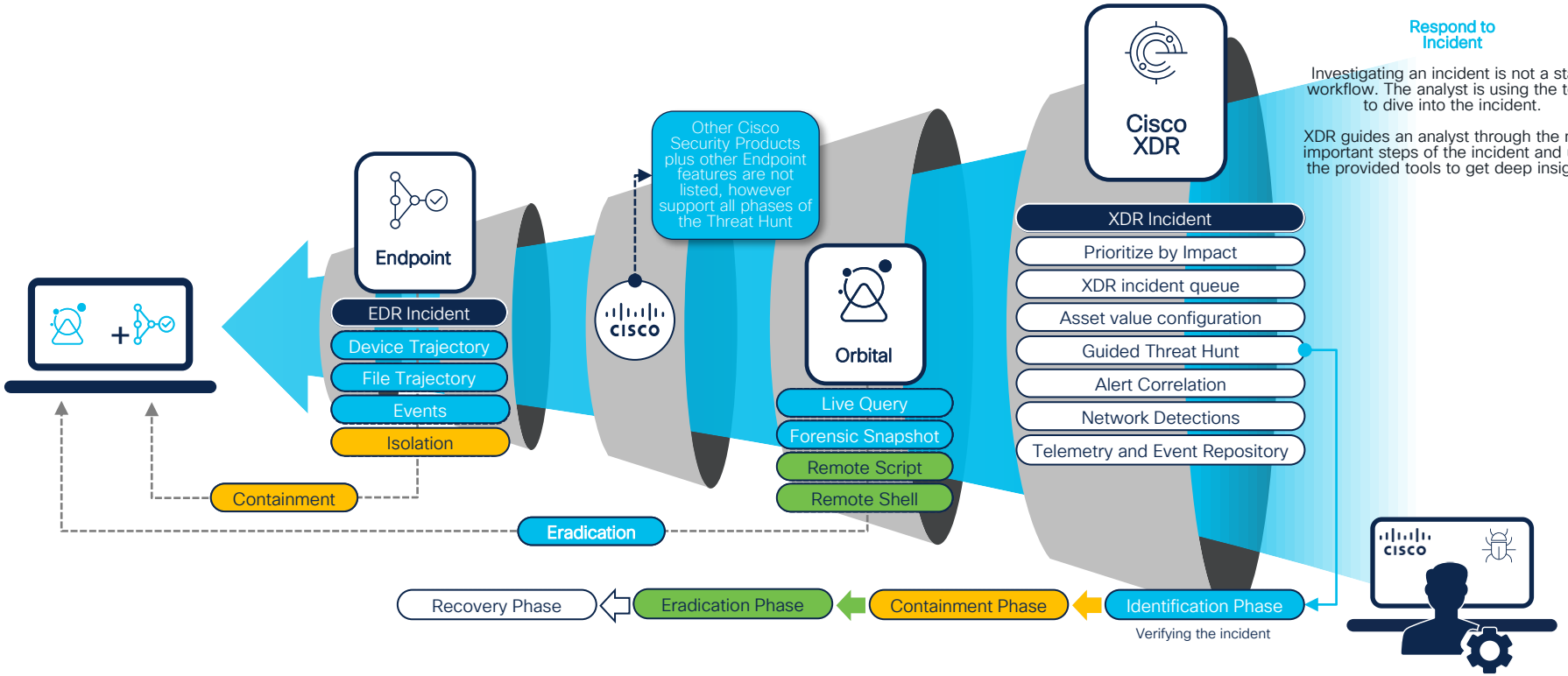
Contain and Eradicate with the endpoint



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Respond & Protect Capabilities

Contain and Eradicate with the endpoint



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary: Prevent, Detect, Respond, Protect

Platform Security Capabilities



PREVENT		DETECT	RESPOND	
Cloud Based Reputation Lookup	Behavior-based protection	Machine Learning	Sandboxing	Continuous activity monitoring	Retrospective Security
Signature-based Antivirus/Offline Protection	Fileless Attacks Protection	Detect&Block complex Attack scenarios	Indications of Compromise	Talos Threat Hunting	Allow List/Block List
	Memory Based Attacks		Vulnerable & Low Prevalence Software Detection	Cisco XDR Integration	Endpoint Isolation & Automated Actions
	Ransomware Protection		Orbital Advanced Search		Integrated Security Response Platform

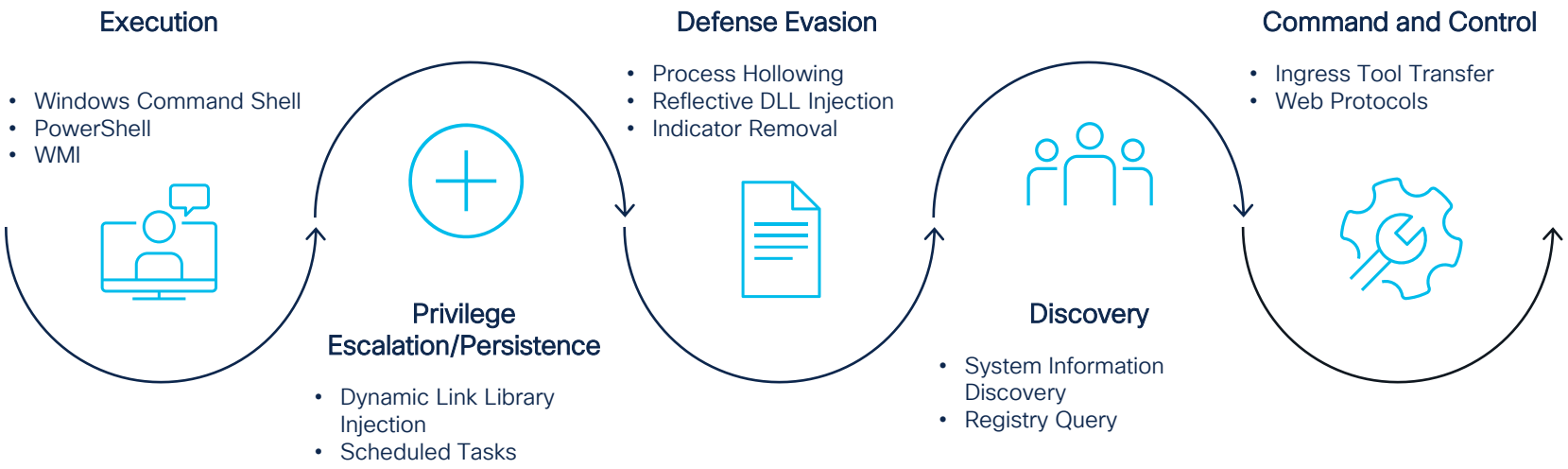
PROTECT

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Warning!!! Suspicious Endpoint Activities

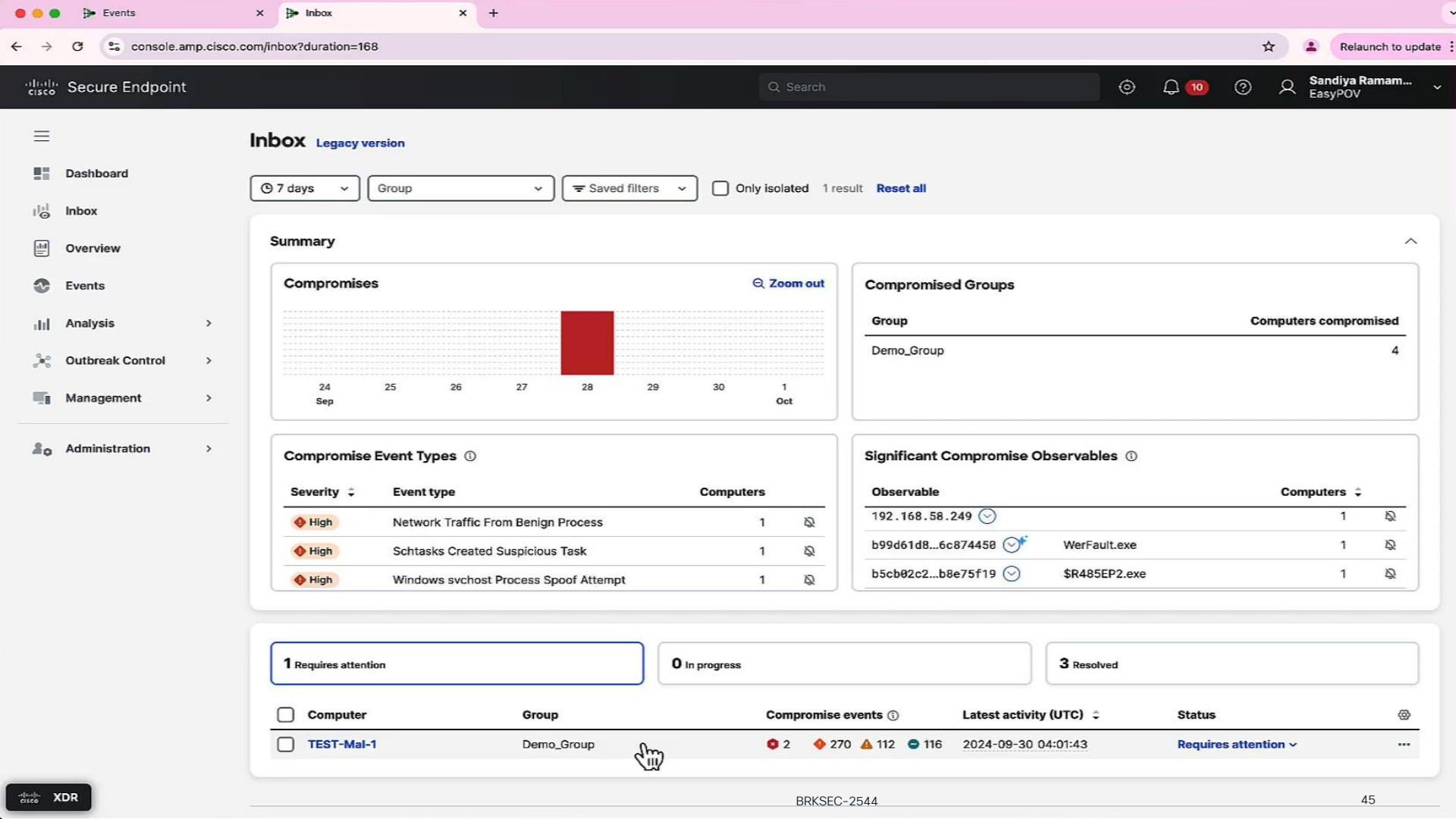


RATNKBA malware



- EDR detected **suspicious outbound traffic** originating from a user's workstation;
- The traffic is accompanied by suspicious modifications to **Windows Scheduled Tasks;**

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public


Events
Inbox
console.amp.cisco.com/inbox?duration=168
Relaunch to update
Secure Endpoint
Search
10
Sandiya Ramam...
EasyPOV
Dashboard
Inbox
Overview
Events
Analysis
Outbreak Control
Management
Administration
Inbox
Legacy version
7 days
Group
Saved filters
Only isolated
1 result
Reset all
Summary
Compromises
Zoom out
24 Sep
25
26
27
28
29
30
1 Oct
Compromised Groups
Group
Computers compromised
Demo_Group
4
Compromise Event Types
Severity
Event type
Computers
High
Network Traffic From Benign Process
1
High
Schtasks Created Suspicious Task
1
High
Windows svchost Process Spoof Attempt
1
Significant Compromise Observables
Observable
Computers
192.168.58.249
1
b99d61d8...6c874458
WerFault.exe
1
b5cb02c2...b8e75f19
$R485EP2.exe
1
1 Requires attention
0 In progress
3 Resolved
Computer
Group
Compromise events
Latest activity (UTC)
Status
TEST-Mal-1
Demo_Group
2
270
112
116
2024-09-30 04:01:43
Requires attention
XDR

Integrations



Key Strategic Integrations

Cisco Secure Client

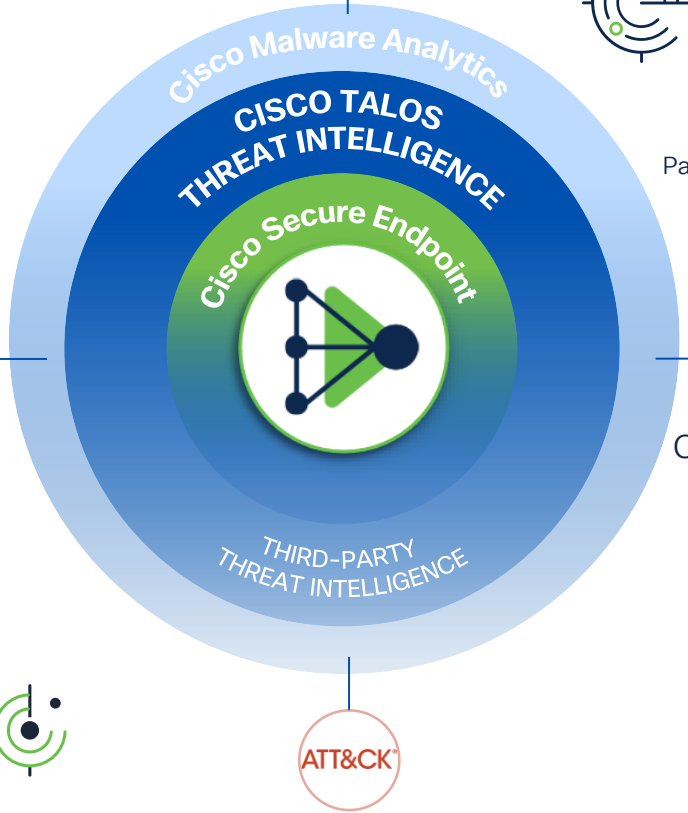
DUO

API

Cisco Malware Analytics
(File Introspection Layer)

Cisco Secure Firewall
Malware Defense

Cisco Vulnerability Management



Cisco XDR / Endpoint Telemetry

Third-Party Endpoint Telemetry supported:

CrowdStrike, Cybereason,
Microsoft Defender for Endpoint,
Palo Alto Networks, SentinelOne, Trend Micro

Cisco Secure Email&Web Telemetry

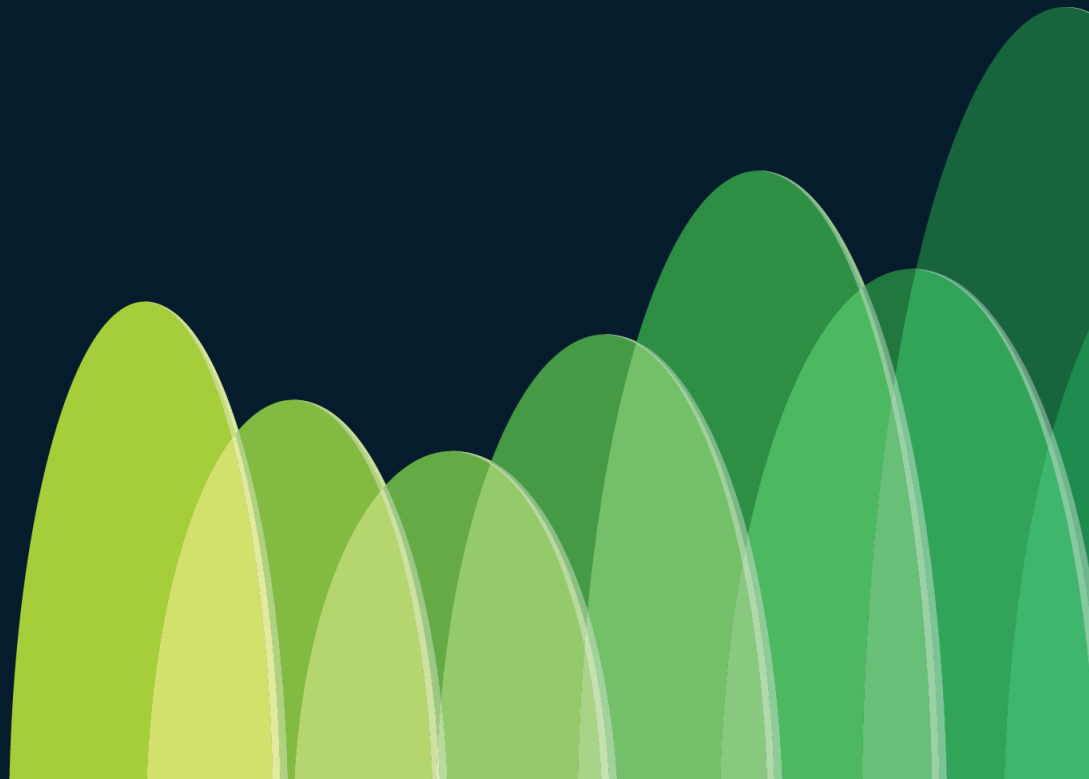
Third-Party Email Telemetry* supported:

Microsoft 365, Proofpoint

* Third-Party integrations leverage Cisco XDR

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaways

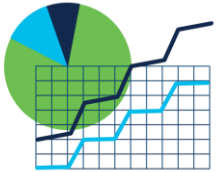


Key Takeaways



Prevent, Detect, Respond, Protect

Security Architecture Framework that will allow you to Prevent, Detect, Respond, and Protect your organization



Outcome-Driven Risk-Based

Transform from a “feature-rich-only” to an “outcome-and-risk-based” Mentality



Key Integrations

Cisco’s native Endpoint telemetry, detections, and response capabilities will bolster Cisco XDR outcomes, coupled with strategic integrations for optimal results



Measure, Analyze, Observe, Improve

Review and compare the impact of incidents and the response process results. Identify improvement areas for future incident response

The Pathway to An Effective Outcome-Driven Endpoint Security!

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex App

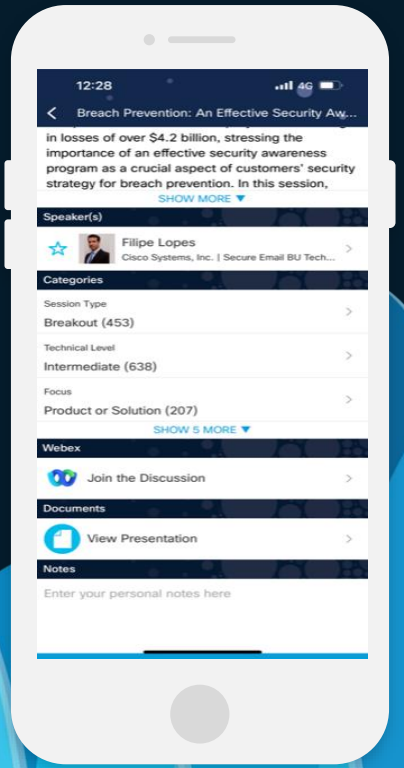
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: flopes@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Review the guided demo for Secure Endpoint and our TDM!
- Try it for free today!
  Register for a Cisco Secure Endpoint 30-day trial
- Download the latest AV comparatives results to learn more about how effective Cisco Secure Endpoint is in malware protection
- Leverage our Best Practices Guide
- Learn more about Cisco Secure Endpoint
- Sign-up for a Threat Hunting Workshop to get hands-on

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security

Breach Protection

Learn about how solutions such as Cisco Secure Client, email and web security can protect your assets. We will also cover how Cisco XDR platform can correlate and make sense of security events, cutting the time and manual effort required for threat hunting and incident response.

START

Tuesday, February 11 | 8:00 a.m.
BRKSEC-2263
Do you Use MS365 for Email? We can Make your Solution Safer!

Tuesday, February 11 | 12:00 p.m.
BRKSEC-2113
Cisco XDR - Making Sense of all the Parts and Pieces

Tuesday, February 11 | 2:30 p.m.
BRKSEC-2248
Design and Deploy Cisco Network Detection and Response with Cisco Breach Suite

Tuesday, February 11 | 4:30 p.m.
BRKSEC-2178
Extended Detection with Cisco XDR: Data, Analytics and Attack Chains

Wednesday, February 12 | 8:00 a.m.
BRKSEC-2143
Do You Know Where Your Data Is? A Deep Dive on Cisco Secure Access CASB and DLP and How to Protect Your Locations, Data and Users

Wednesday, February 12 | 12:30 p.m.
BRKSEC-2502
Incident Response With Cisco XDR: How To Level Up Your SOC Using Both Guided and Automated Response

Wednesday, February 12 | 2:30 p.m.
BRKSEC-1544
Secure Endpoint : Unveiling Latest Key Features!

Wednesday, February 12 | 5:30 p.m.
BRKSEC-3101
Malware Execution As A Service: A Deep Dive into CSMA Advanced File Analysis

Thursday, February 13 | 10:45 a.m.
BRKSEC-2670
Me, My Email and AI

FINISH

Thursday, February 13 | 3:15 p.m.
BRKSEC-3019
Network Detection and Response with Cisco Secure Network Analytics

Join our Security Research Community

Participating in design research gives you a place to share your thoughts and experiences to influence the future of Cisco Security Products.



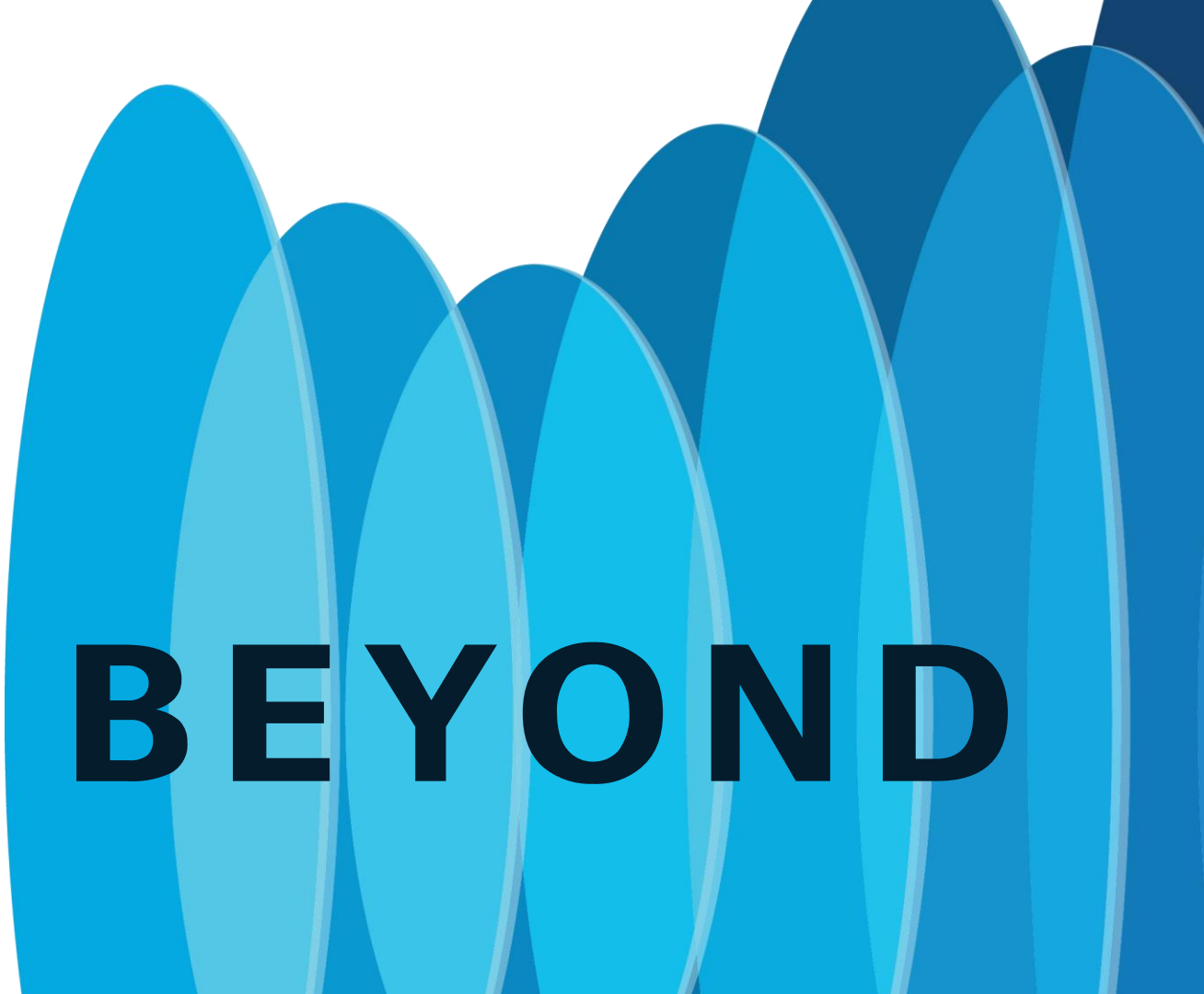
cisco Live!



Thank you

cisco Live!

cisco Live!



GO BEYOND