

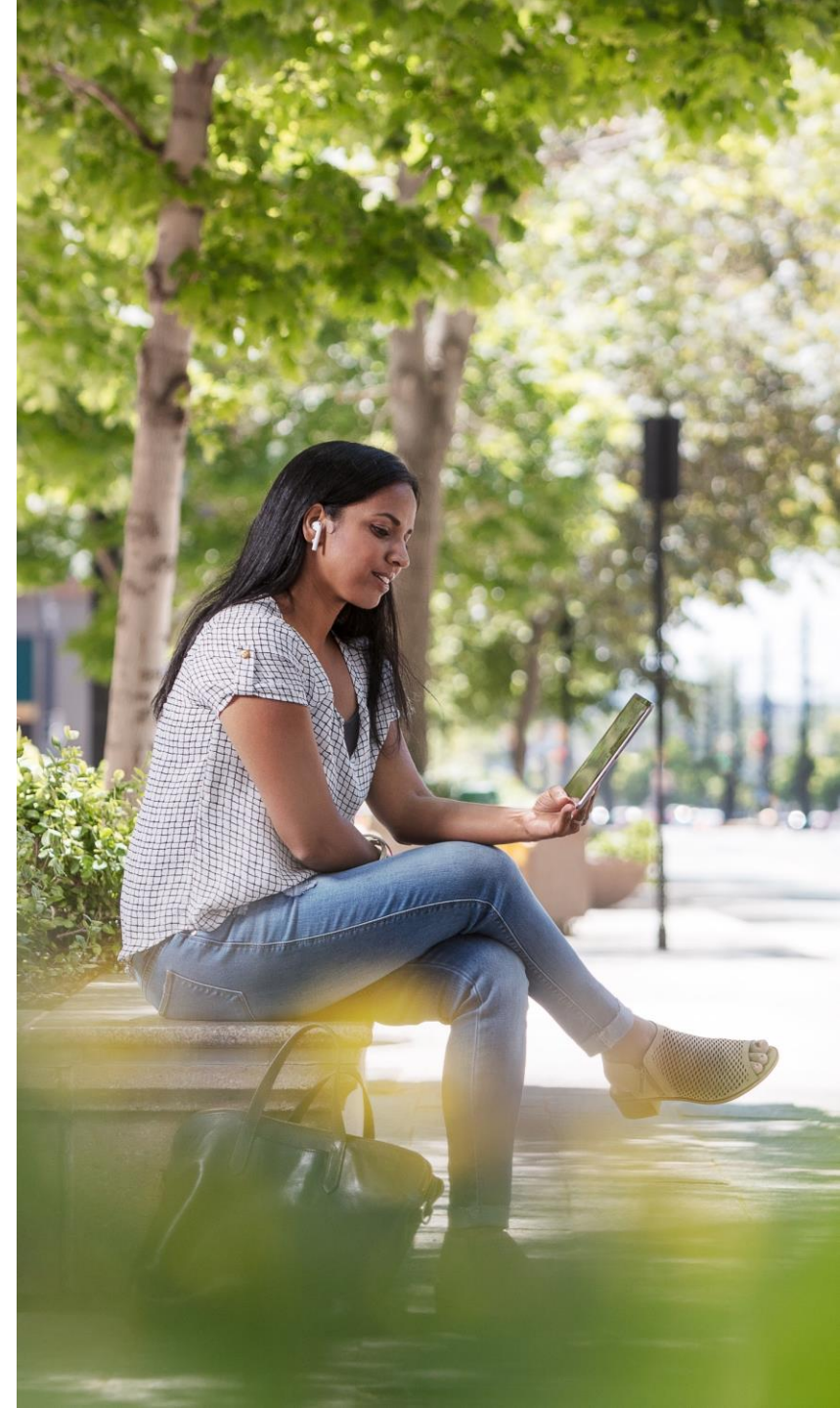



# Cisco Talos & XDR

TEMS Security Day 2023

David Emamjomeh, CSS

September 2023





You cannot be in the connection business  
without being in the protection business.

## Cisco Security Suites

### Cisco Breach Protection

Extended Detection & Response

### Cisco User Protection

Posture & Auth Management

Endpoint Security

Email Security

Experience Insights

Remote Browser Isolation

Network Access Control

Security Service Edge

### Cisco Cloud Protection

Workload Security

Application Security

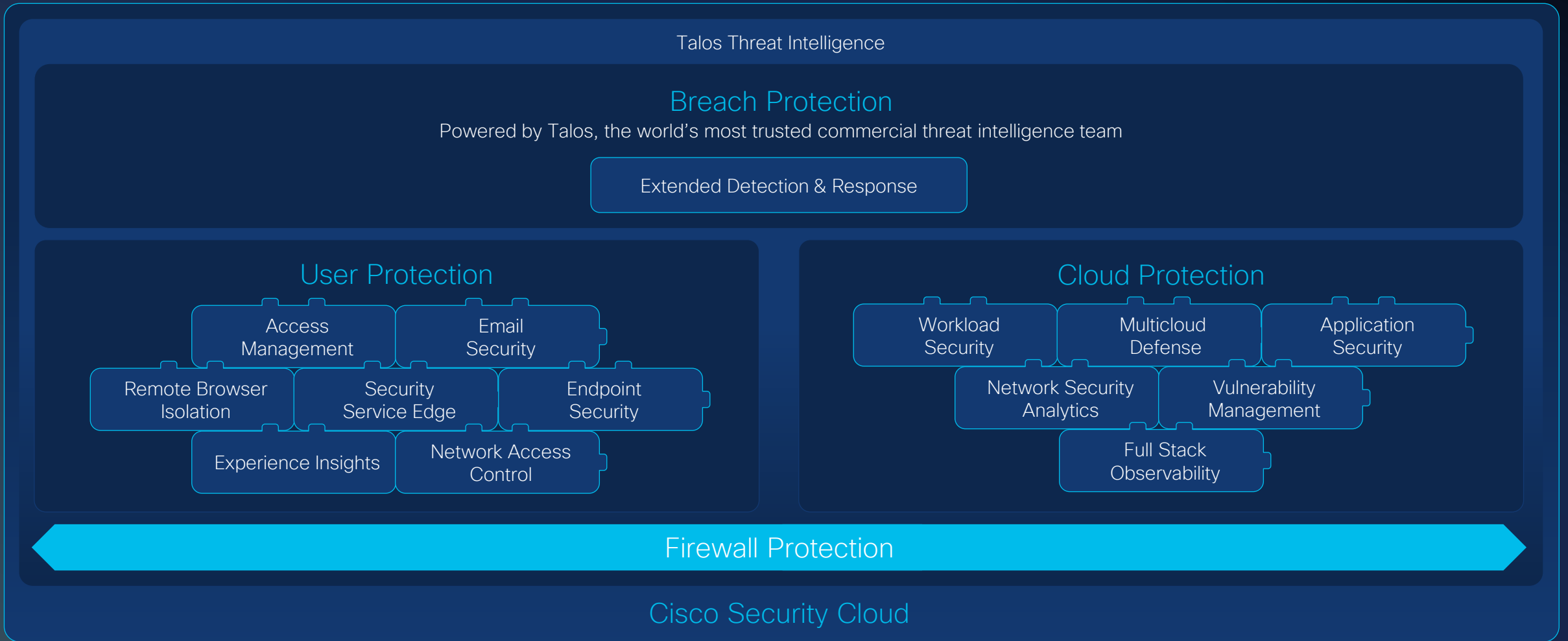
Vulnerability Management

Full Stack Observability

Multicloud Defense

← Firewall Protection →

# Security that only Cisco can deliver for you



TALOS

1) Talos

Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Threat Visibility & Hunting

Security, O

Device Insights

2) XDR = Extended Detection and Response

Incident Response and Remediation Services

Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adapt | Passwordless | Trust

Secure Access | Secure Email

3) Identity

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

4) Secure Client

Query



ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access | Managed Remote Access

Umbrella/Duo



ZTNA



DNS-layer security



RAaaS



SSL decryption



Remote browser isolation



Prevention



Access broker

5) Umbrella

SDWAN



SDWAN

SDWAN by Viptela



SandEyes

5) SD Wan

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Security

Network Edge



SDWAN by Viptela



ThousandEyes

6) Network Edge

IoT/OT SECURITY

Secure C | Unified IT and OT



Industrial Router



Industrial Firewall



Industrial Switch/AP



Vision



ISE TrustSec

9) IOT

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Security Analytics and Log



Secure DDoS

Full Stack



Secure Analytics

Secure Appliance



Secure Appliance

7) Zero Trust Workplace

DuoCloud SSO+IDP



Network Gateway



Cisco IANA Center



Application Security

ZERO TRUST WORKLOAD

Policy | API Security | Application Segmentation | Run-time Application Security

Application Security Stack



Cloud Native Security



APIC

8) Application Security

App Visibility | Detection



Hybrid Private



Public Cloud\*



Secure Cloud Analytics



Secure Firewall



ThousandEyes





# Talos powers the Cisco portfolio with intelligence

## TALOS



# 500

threat researchers



# AI

powered algorithms



# 550B

security events observed daily

# Global Threat Intelligence and Research Overview



Over 100 Threat Intelligence Partners



3-5 minutes Updates to all security devices



1.6 MILLION Telemetry Agents



600+ Full Time Threat Intel Researchers

# Incident Response Retainer – Proaktiv & Reaktiv

Reaktiv

Proaktiv



Ich benötige  
jetzt Hilfe!  
(24x7x365)

**Emergency  
Incident  
Response**



Ich benötige  
einen Plan für  
wenn es passiert.

**IR Plans  
& Playbooks**



Bin ich im  
Krisenfall gut  
aufgestellt?

**IR Readiness  
Assessments**



Ich möchte  
Gewissheit,  
dass wir richtig  
reagieren.

**Tabletop  
Exercises**



Bin ich aktuell  
kompromittiert?  
(Breites Bild)

**Compromise  
Assessments**



Bin ich aktuell  
kompromittiert?  
(Fokussiert)

**Threat  
Hunting**



Ich möchte Wissen  
aufbauen, um mich  
zu verteidigen

**Cyber  
Range  
Training**



Wo sind die  
Schwachstellen &  
Einfallstore in  
meiner  
Infrastruktur?

**Network  
Security  
Architecture  
Assessment**



## Penetration Testing

Ich möchte spezielle Anwendungen, Systeme (IT, OT, IoT) oder Infrastruktur Komponenten auf Schwachstellen überprüfen.



## Red Teaming

Ich möchte ein realistisches Angriffsszenario simulieren, welches *Advanced Persistent Threat (APT)* Taktiken verwendet.

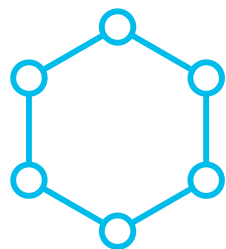


## Purple Teaming

Ich möchte meine Fähigkeiten auf der Verteidigungs-Seite (Blue-Team) verbessern, mittels Durchführung & Analyse von *Threat Actor Tactics, Techniques and Procedures (TTPs)*.



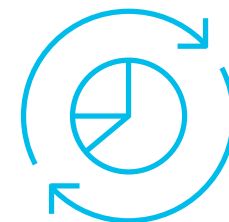
# What is eXtended Detection and Response?



Collection of detections and raw telemetry from multiple sensor technologies across your environment



Application of advanced analytics to the collected and normalized evidence to produce correlated and prioritized detections of malicious activity



Guided responses across multiple control planes to quickly and effectively contain, mitigate, and eradicate the threat.

# The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience



Detect  
the most  
sophisticated threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments



Act on  
what truly matters,  
faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations



Elevate productivity

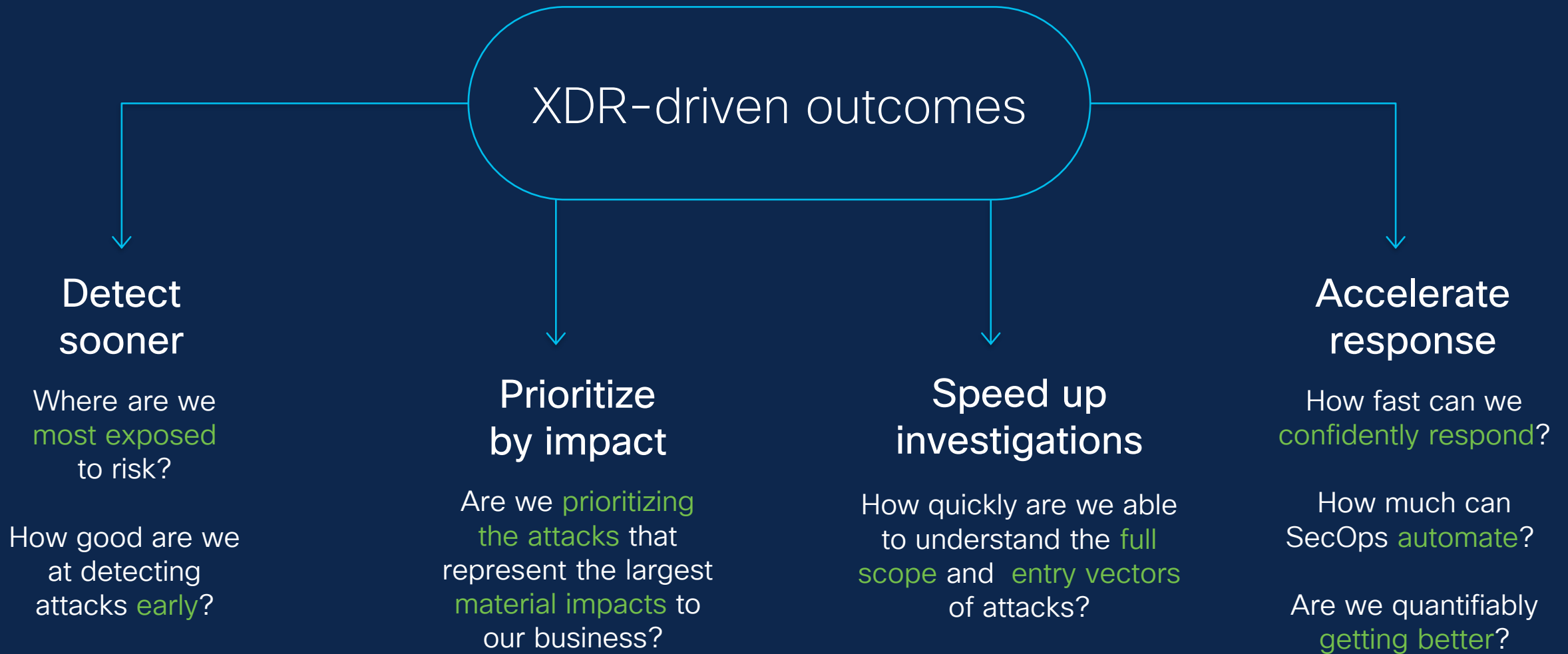
- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks



Build  
resilience

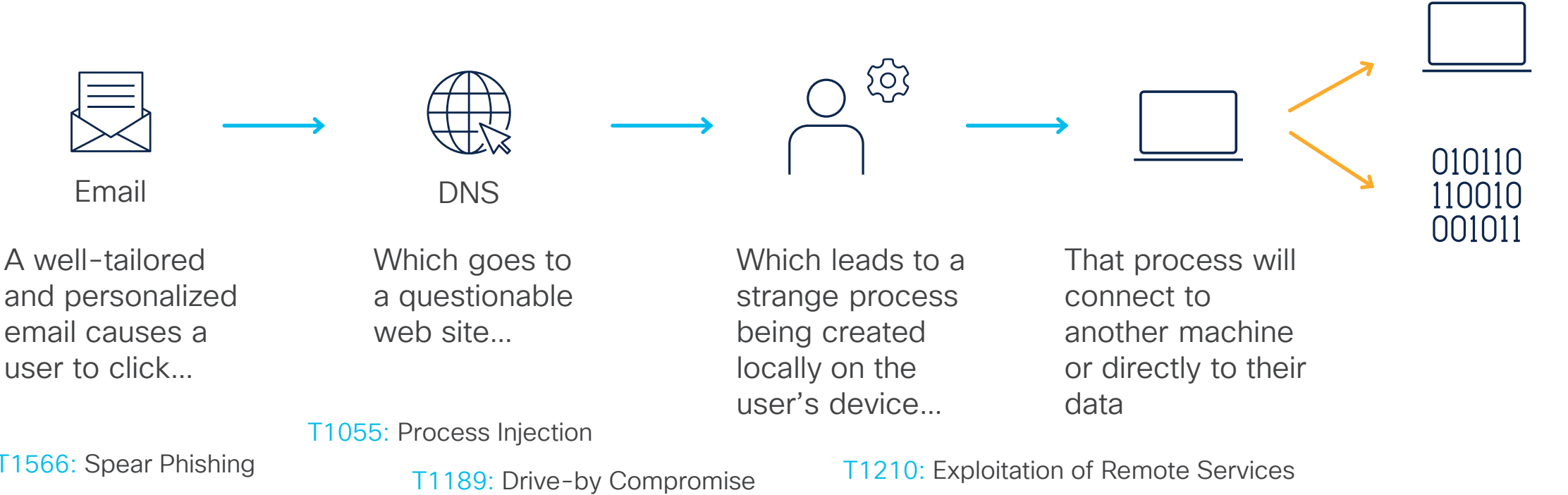
- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

# Shift the focus to outcomes



# Stop advanced threats like ransomware

Most attacks use a sequence like this...



 **Cisco XDR**



# An XDR is as good as its outcomes

How good are we at detecting attacks **early**?

1 Detect Sooner

Extend Asset Context

2

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

Where are we **most exposed** to risk? Are we **prioritizing the attacks** that represent the largest **material impacts** to our business?

3 Prioritize by Impact

Reduce Investigation Time

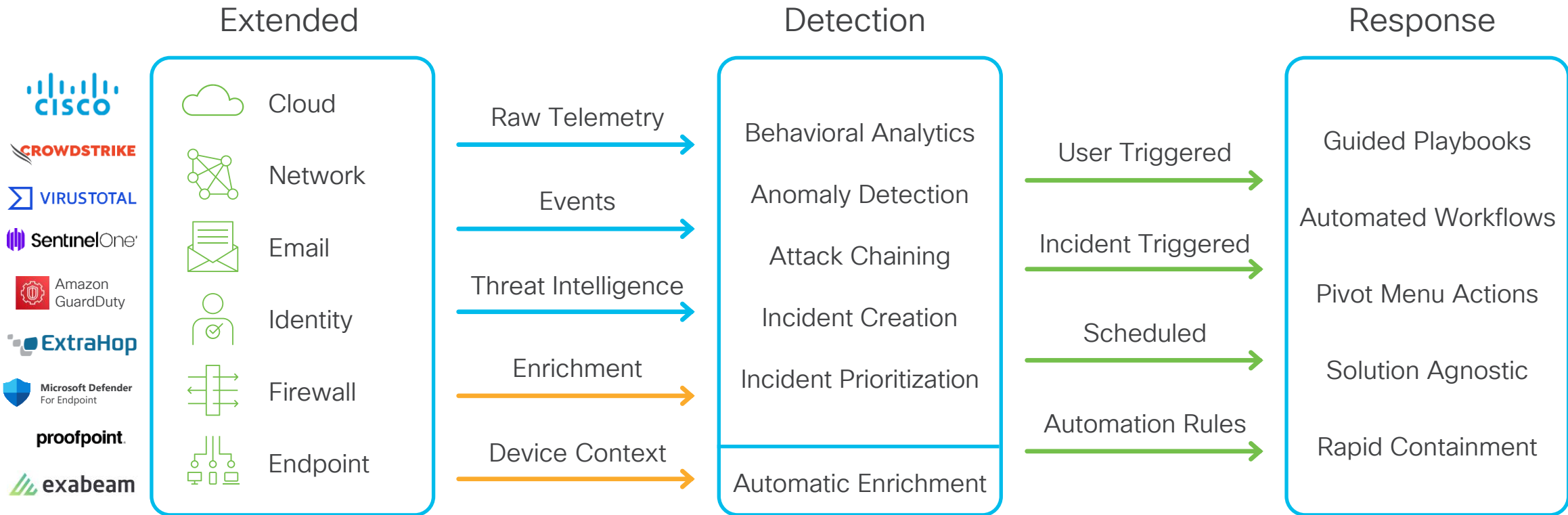
4

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

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

5 Accelerate Response

# High level architecture



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

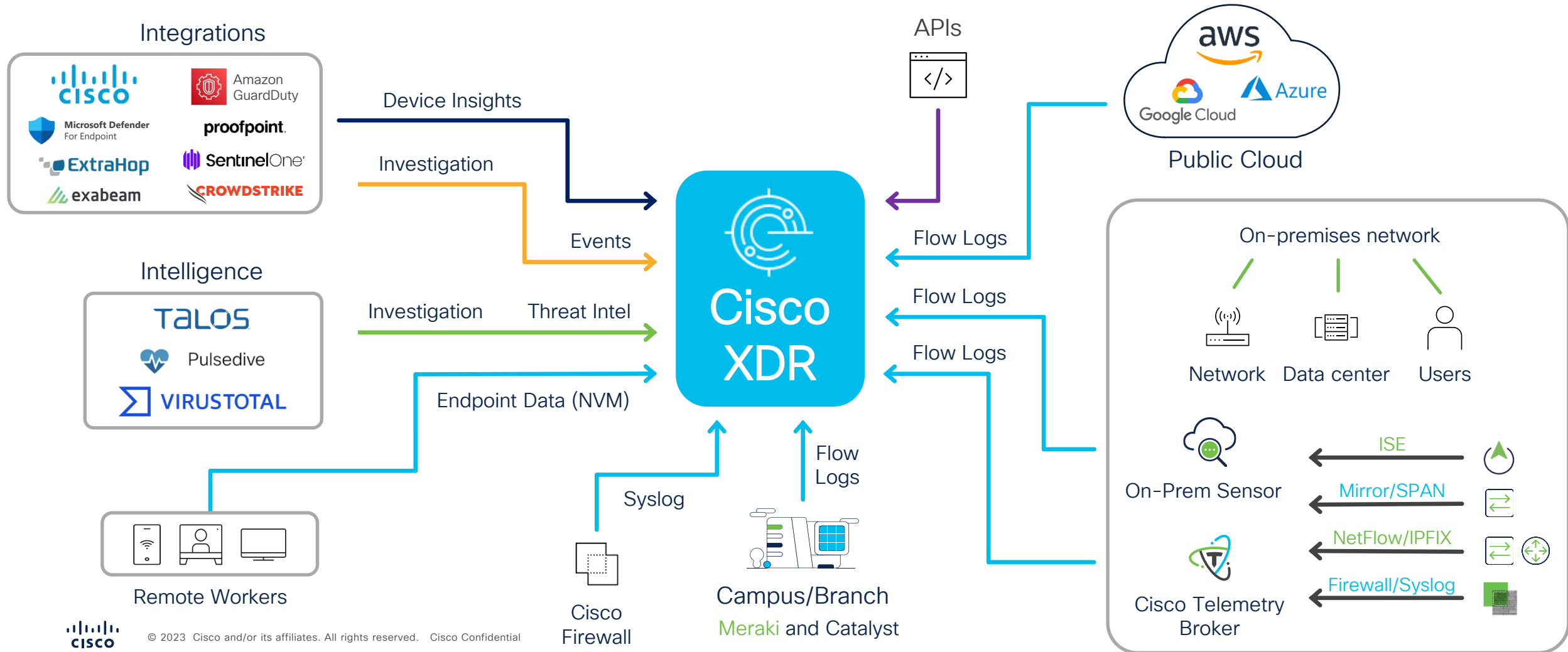
Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

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

Extended context

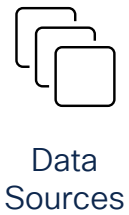
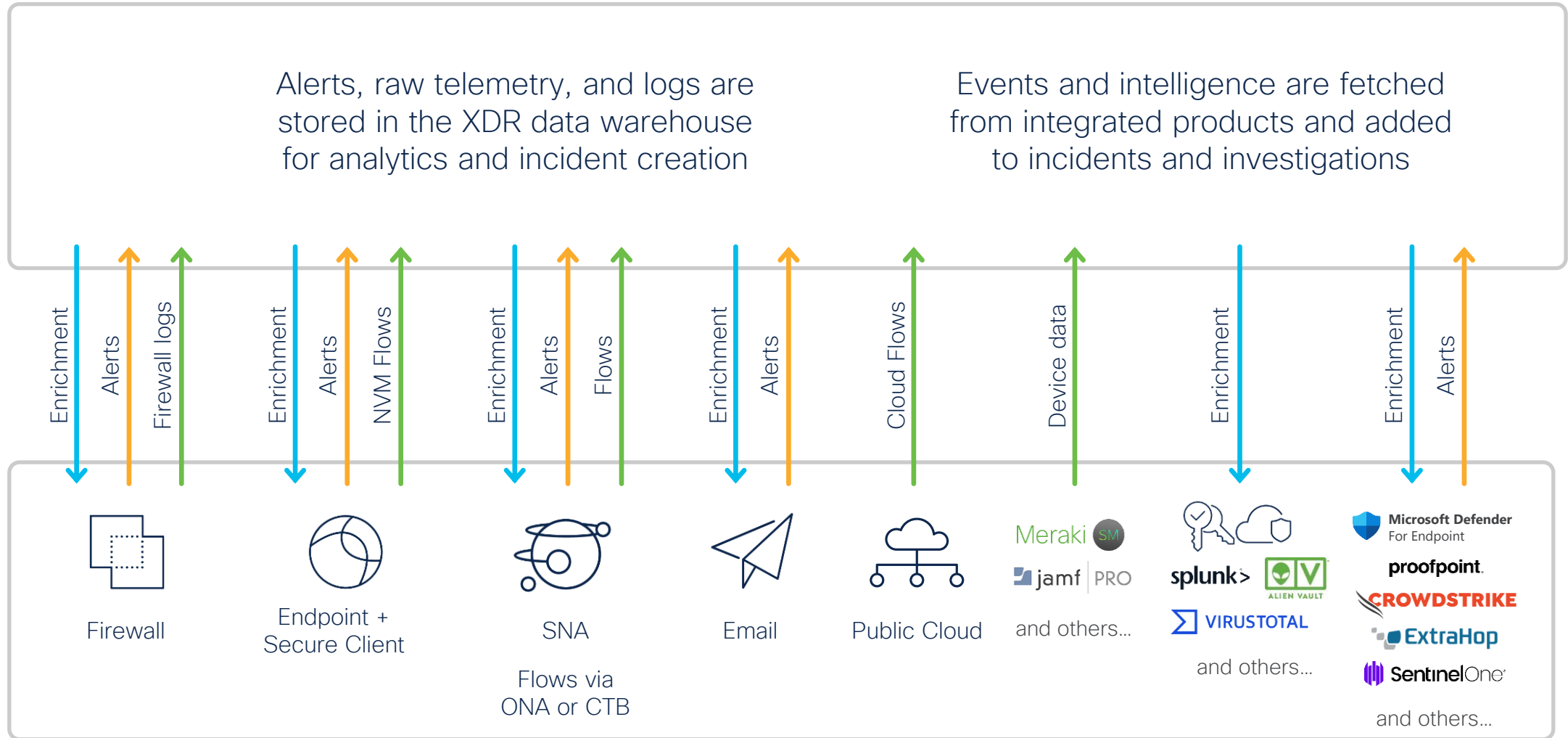
# Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Extended context

# Telemetry and enrichment



Data Sources





Extended context

# Integrations

XDR is as powerful as its integrations, and Cisco XDR has over 80+ integrations with a wide variety of products.

- Open platform with more third-party integrations than Cisco integrations.
- Mix of security products, intelligence sources, device managers, and more.
- Easy to enable and configure.
- API-based communication with other products.



## Integrations

[Filters](#)

### My Integrations

Integration Name	Name	Status
<a href="#">Orbital</a>	Orbital	✓ Connected
<a href="#">XDR Analytics</a>	Secure Cloud Analytics	✓ Connected
<a href="#">Email Security</a>	Secure Email and Web Manager	✓ Connected
<a href="#">Secure Endpoint</a>	Secure Endpoint	✓ Connected
<a href="#">Secure Firewall</a>	Secure Firewall	✓ Connected
<a href="#">Secure Network Analytics</a>	Secure Network Analytics	✓ Connected
<a href="#">Umbrella</a>	Umbrella	✓ Connected
<a href="#">AlienVault Open Threat Exchange</a>	AlienVault Open Threat Exchange	✓ Connected
<a href="#">CrowdStrike</a>	CrowdStrike	✓ Connected
<a href="#">CyberCrime Tracker</a>	CyberCrime Tracker	✗ Error

Extended context

# Supported sources for XDR Devices



Duo Access  
Duo Beyond



Secure Endpoint



Umbrella (DNS)  
Windows / macOS



Meraki SM



Secure Client



Orbital

---

*Third Party*

---



CrowdStrike



SentinelOne



Microsoft Intune



Jamf Pro



Ivanti Neurons  
(formerly MobileIron)



VMware  
Workspace ONE  
(formerly Airwatch)

# Summary

# Why Cisco XDR?



## Faster detections

Detect threats sooner with advanced analytics and a unique attack chaining capability that provides end-to-end attack correlation with automated incident prioritization based on risk and threat risk.



## Simplified investigation

Simplified investigation using automated incident enrichment and event correlation. Empowering the SOC to quickly identify the source of a threat, its impact, and relevant resources like assets across integrated products.



## Rapid containment

Contain threats with robust, automated response actions while keeping track of who did what right within the incident. Various places to initiate a response from an investigation, incident, or the XDR Ribbon.



# Cisco XDR correlating and prioritizing security threats

Telemetry from native and third-party control points



Endpoint



Network



Email



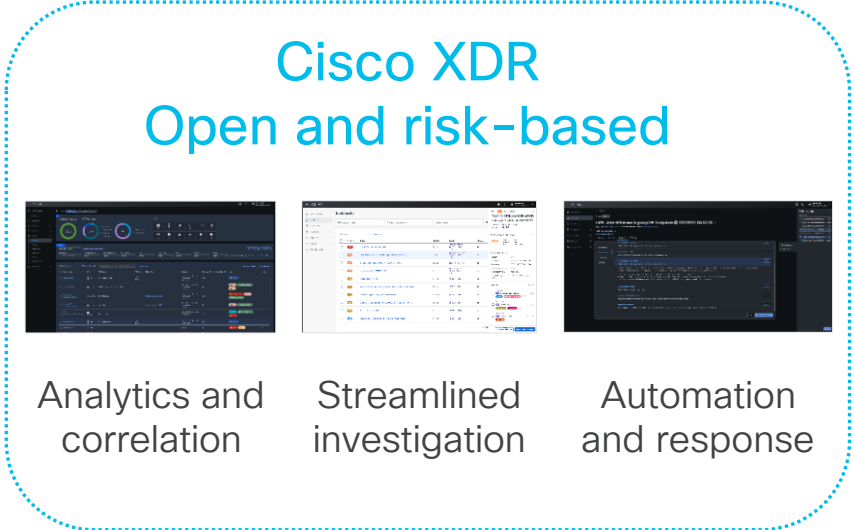
Cloud



Identity



Firewall



Threat intel

Asset & user context

MITRE



Streamlined investigations, shortening time from detection to response



Prioritized alerts, focusing SOC efforts on threats that pose the most harm



Automated response actions, meaning threats are mitigated rapidly, and proactive measures taken

Simplify security operations to elevate productivity and stay resilient against the most sophisticated threats



# Resources



# Getting started

Where can you learn more about Cisco XDR?

- [Cisco XDR At a Glance](#)
- [An XDR Primer: The Promise of Simplifying Security Operations Position Paper](#)
- [Cisco XDR: Security Operations Simplified eBook](#)
- [Five Ways to Experience XDR eBook](#)
- [Cisco XDR Overview Video](#)
- [XDR Instant Demo](#)
- [Threat Hunting Workshop](#)

[Cisco XDR on Cisco.com](#)





The bridge to possible