

CISCO  
SECURE

# 思科協助SASE+XDR， 開啟安全雲化之路

Fan

2022



# Agenda

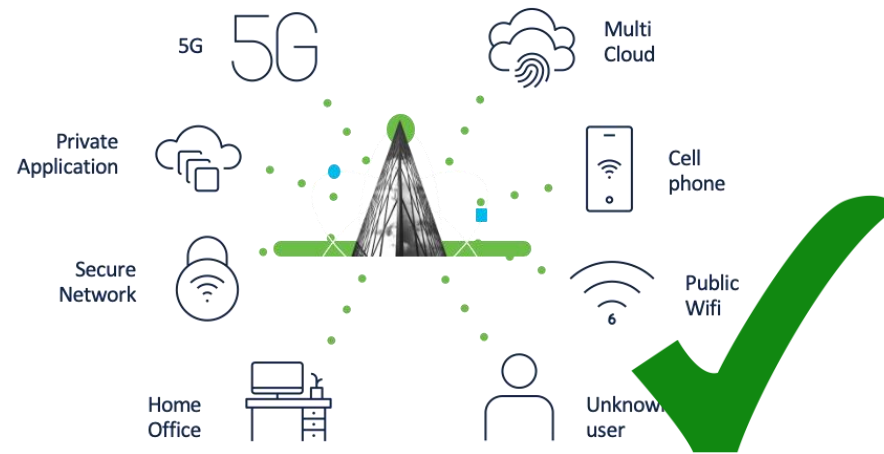
1 背景介紹

2 SASE

3 XDR

# 為什麼我們需要XDR和SASE?

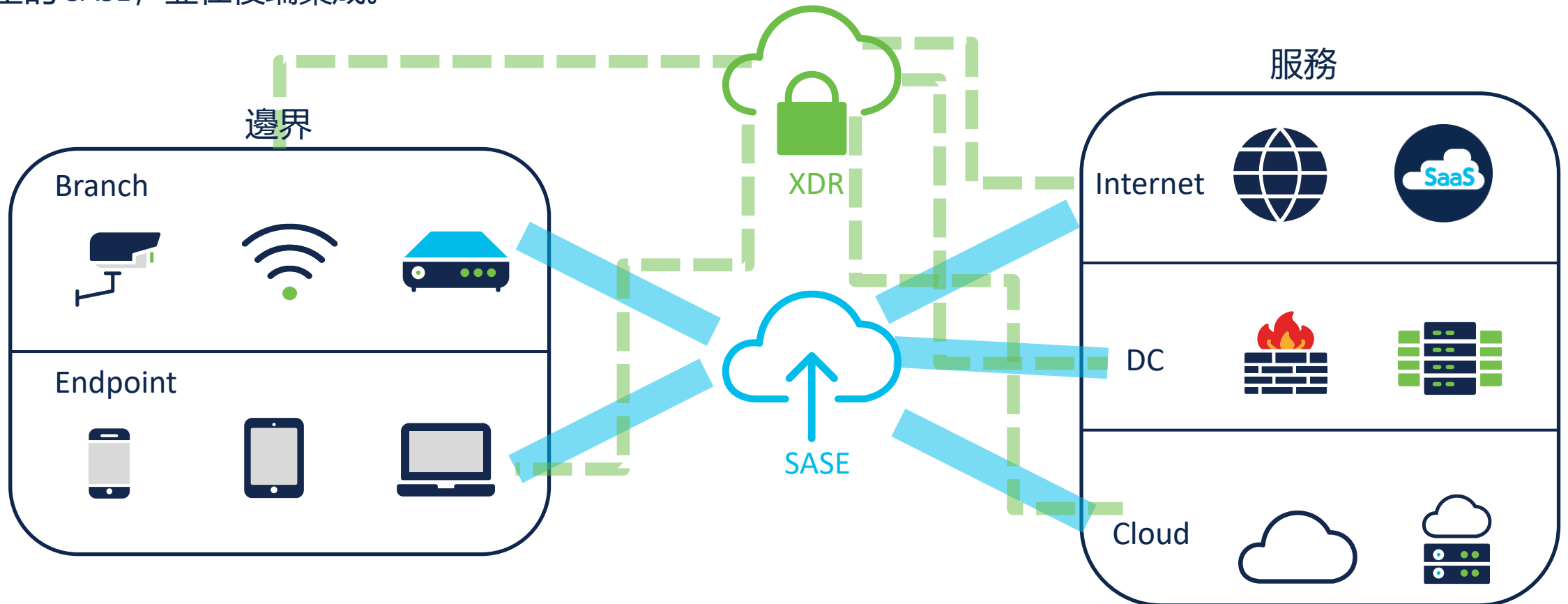
Gartner, Inc. 最近的一項調查發現，到 2022 年，75% 的組織正在尋求安全供應商整合，高於 2020 年的 29%。



<https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022>

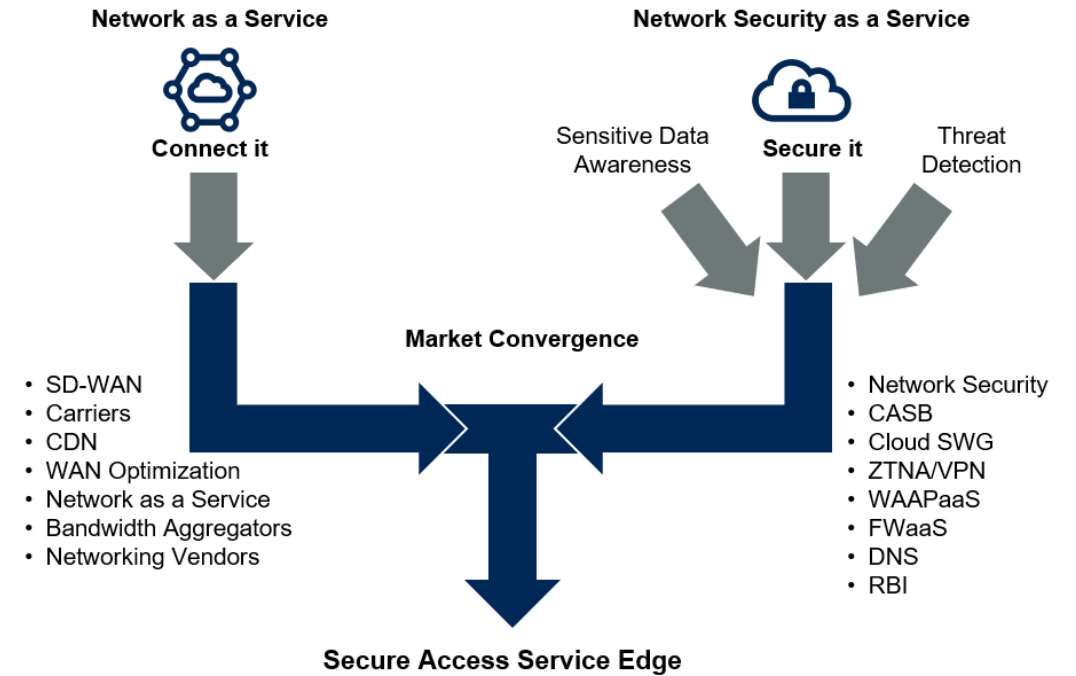
# 為什麼我們需要XDR和SASE?

冗長的採購流程，碎片功能迫使資安廠商進行整合，例如用於端點的 XDR 和用於邊緣連接和安全的 SASE，並在後端集成。



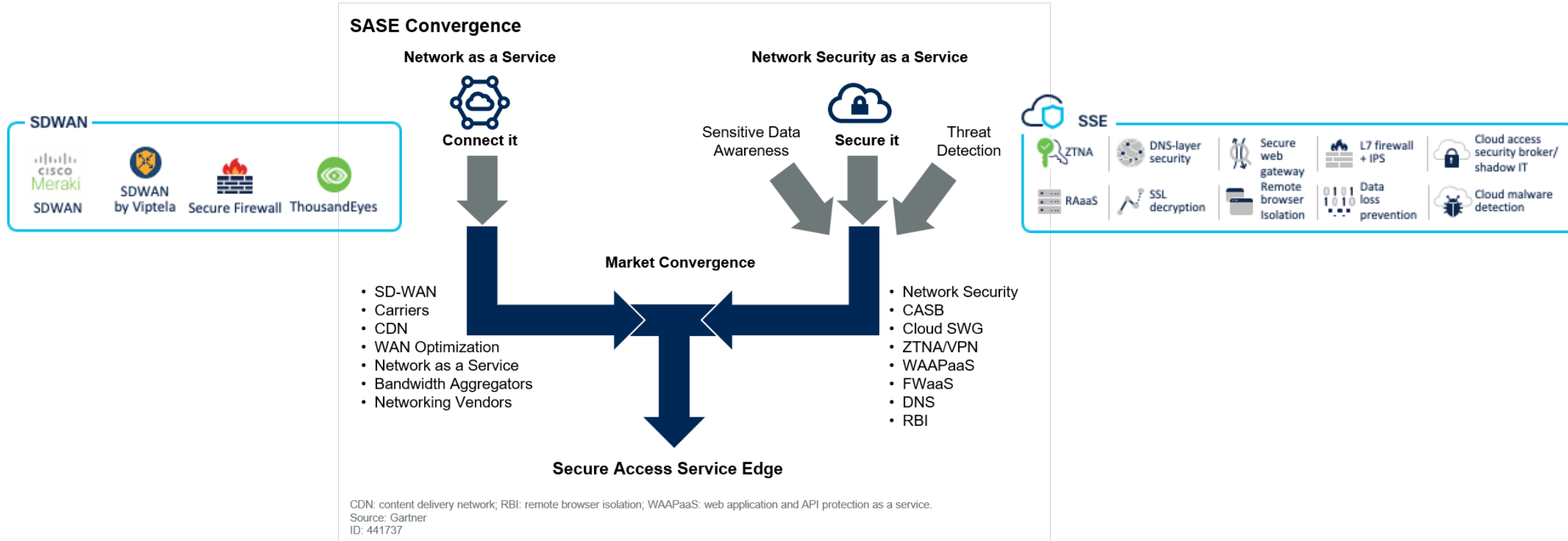
# SASE

## SASE Convergence

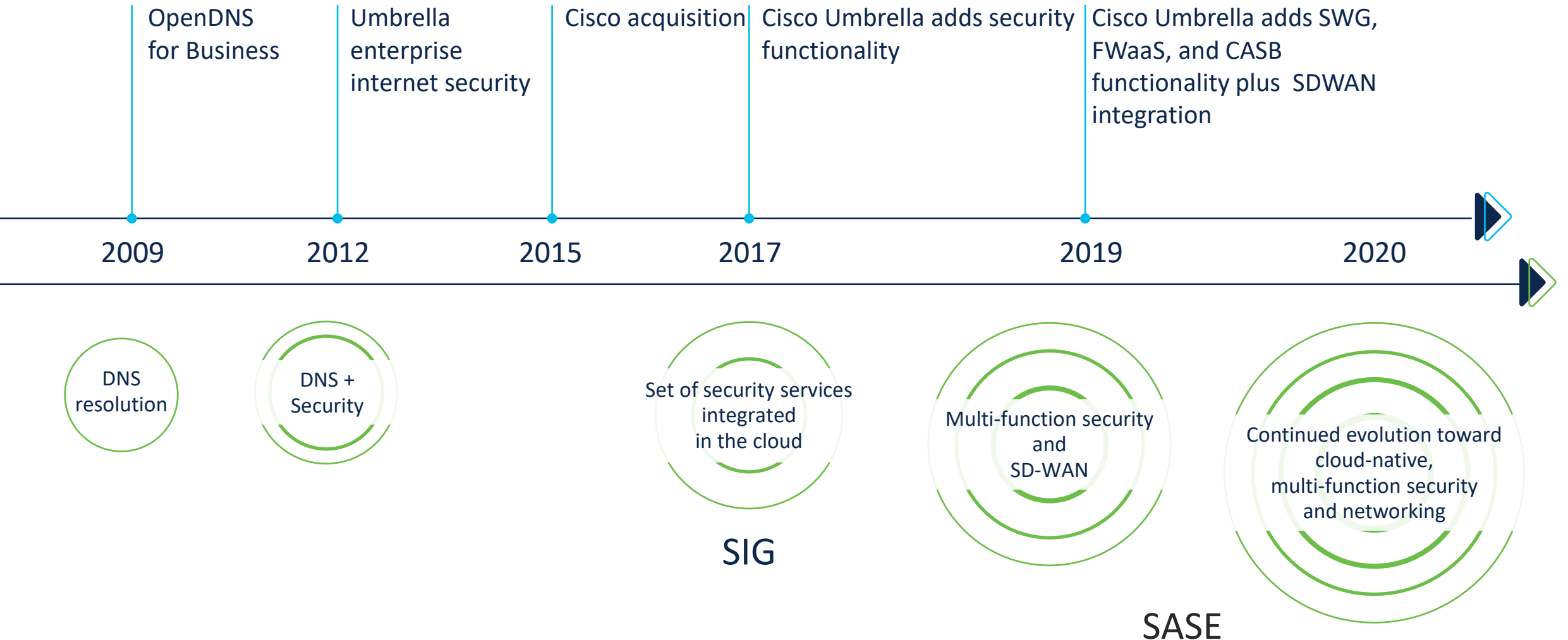


CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a service.  
Source: Gartner  
ID: 441737

# The Architecture of SASE



# Cisco Umbrella evolution



# Cisco Umbrella key capabilities

## Secure access to the internet & usage of cloud applications



### Visibility

- On & off corporate network
- All internet and web traffic
- All apps
- All devices
- SSL decryption
- Shadow IT
- Sensitive data transmitted

### Protection

- DNS-layer security
- Web inspection
- File inspection & sandboxing
- Data loss prevention
- Non-web traffic inspection
- Intrusion prevention system
- Remote browser isolation
- Data at rest cloud malware scanning



### Control

- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls

Built-in extended detection and response (XDR) platform with Cisco SecureX



SECURE

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



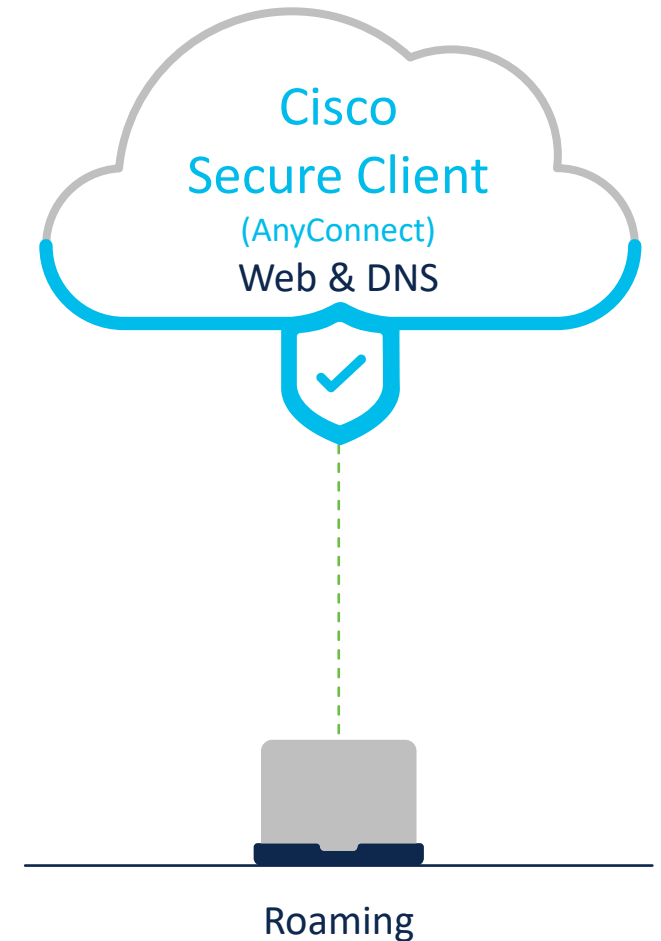
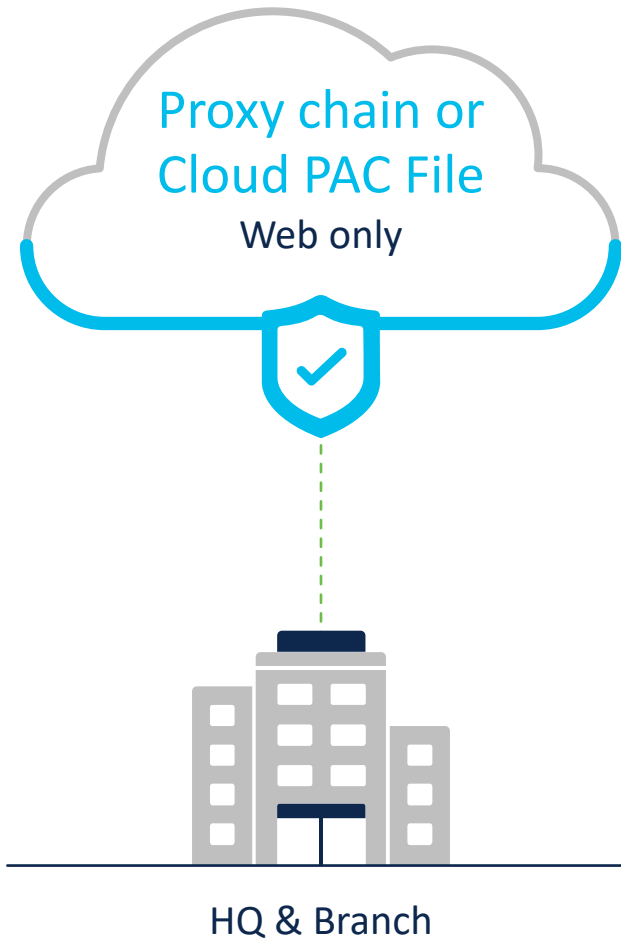
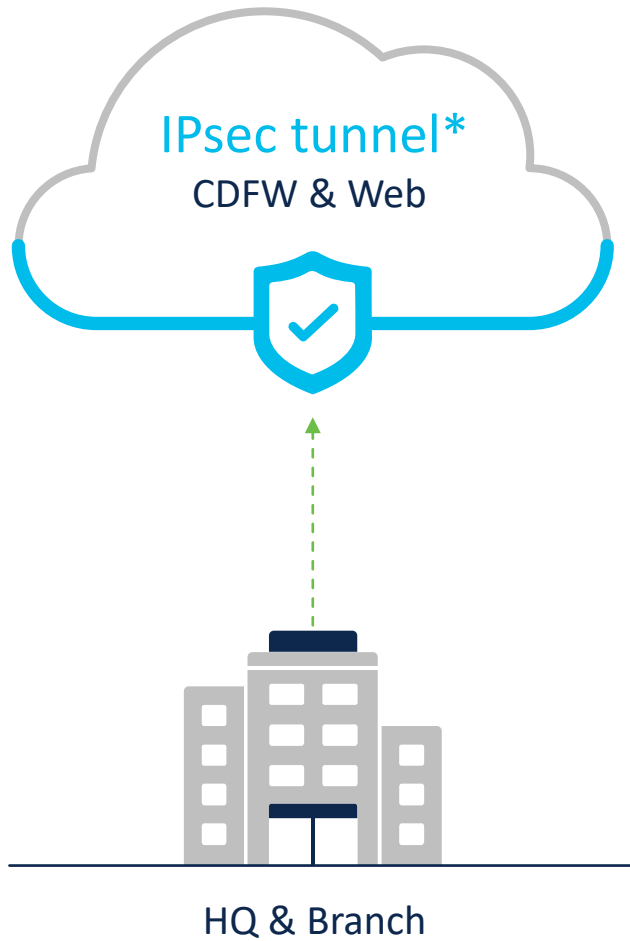
# Lightning-fast performance

## Reduce latency and speed performance

- 1,000+ peering partnerships with ISPs, CDNs and SaaS platforms - fastest route
- 6,000 peering sessions to create shortcuts to major ISPs - decrease hop count
- Carrier neutral: locate data centers based purely on best and diverse connections and services



# Flexible connection methods



\*Optional customer hosted PAC file

# Global Datacenters

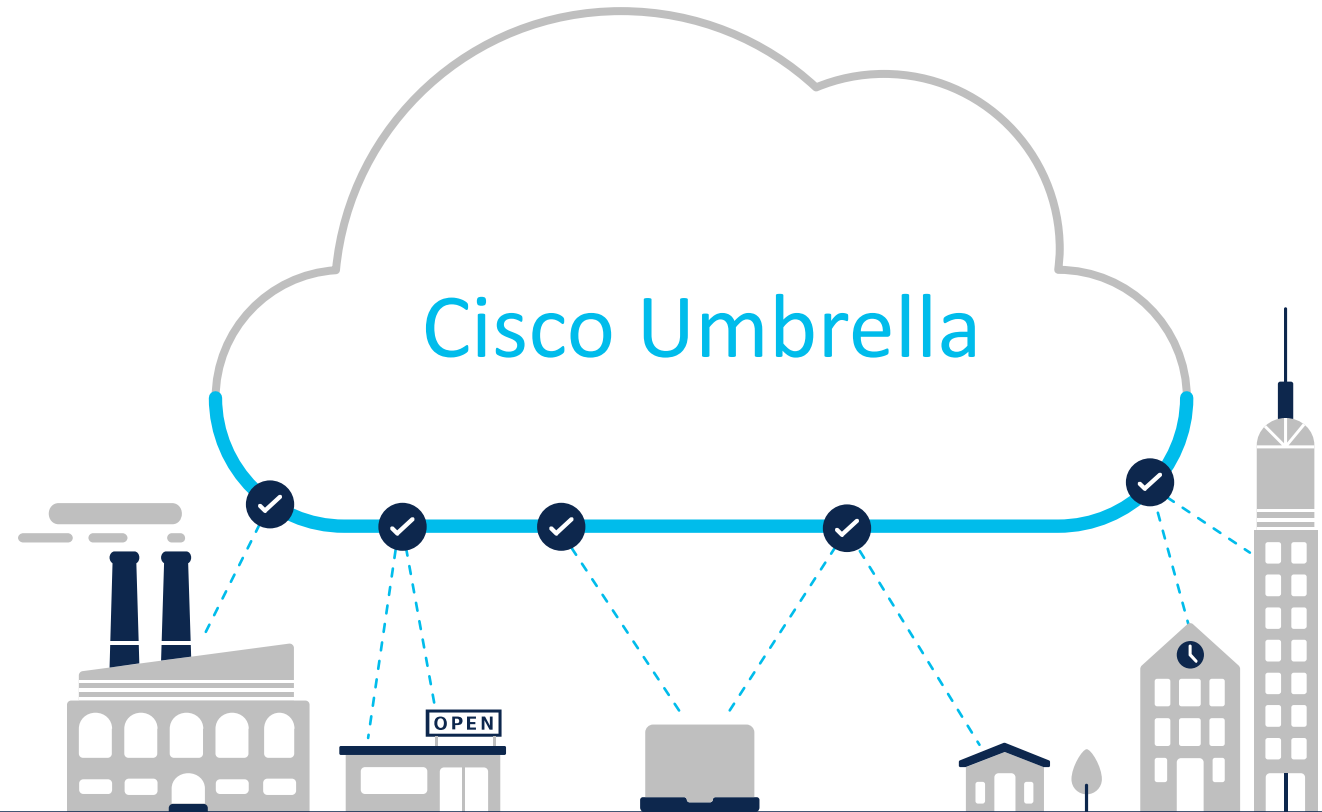
Americas	Europe	Asia	Africa	Australia
Atlanta, GA, US	<b>Amsterdam, NL</b>	<b>Dubai, AE</b>	Cape Town, ZA	Melbourne, AU
Ashburn, VA, US	Copenhagen, DK	Hong Kong, CN	Johannesburg, ZA	Sydney, AU
<b>Chicago, IL, US</b>	Frankfurt, DE	Mumbai, IN		
<b>Dallas, TX, US</b>	London, UK	<b>Osaka, JP</b>		
<b>Denver, CO, US</b>	Madrid, ES	Singapore, SG		
Los Angeles, CA, US	<b>Marseille, FR</b>	Tokyo, JP		
Miami, FL, US	Milan, IT			
New York, NY, US	Paris, FR			
Querétaro, MX	Prague, CZ			
Rio de Janeiro, BR	Stockholm, SE			
<b>Reston, VA</b>				
Santa Clara, CA, US				
Sao Paulo, BR				
Toronto, ON, CA				
Vancouver, BC, CA				

雖然大多數 Umbrella 數據中心都支持 SWG 和 CDFW，但那些以粗體顯示的數據中心僅支持 SWG

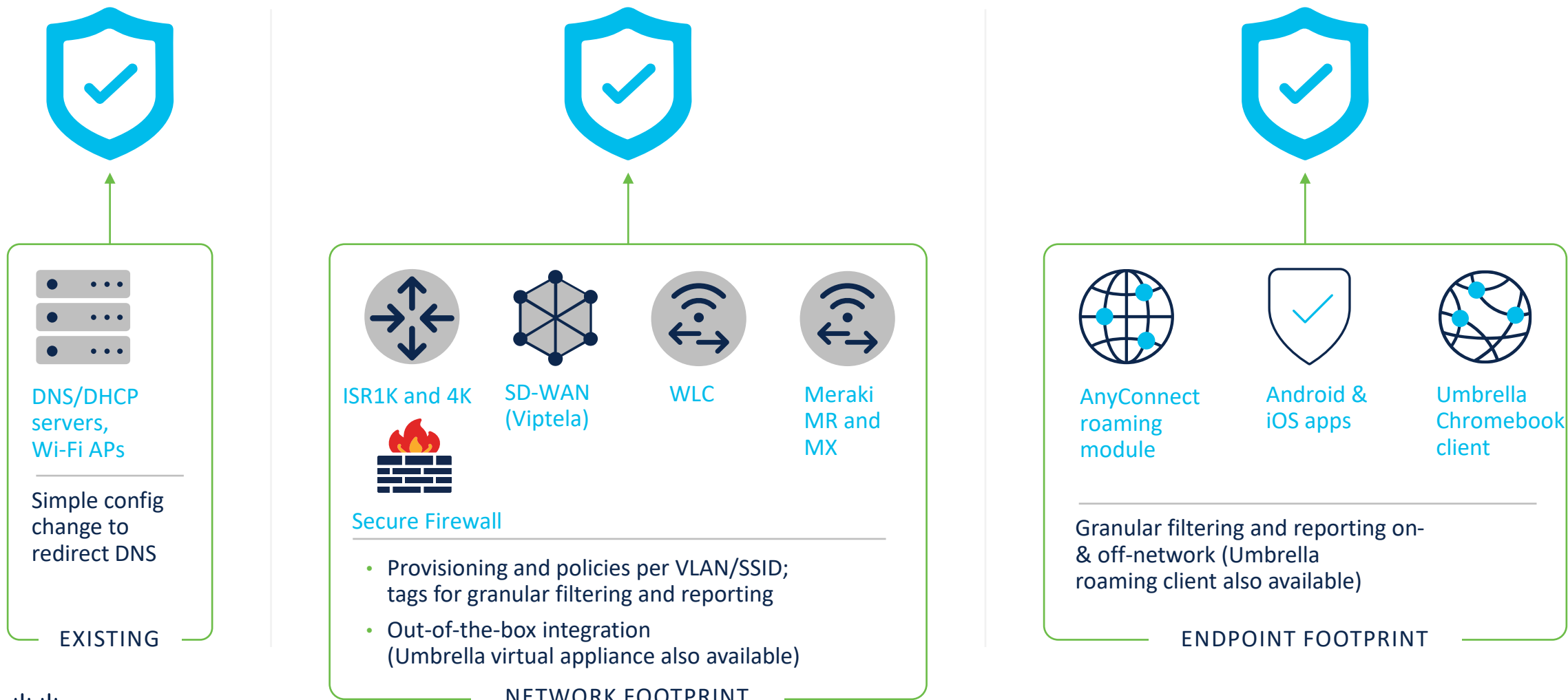
# Umbrella DNS-layer security

Visibility and protection for all activity, anywhere

- See all internet traffic
- Block attacks earlier
- Contain malware if already inside
- Easily enforce content web filtering
- Discover, manage or block cloud apps
- Gain context for faster investigation



# Enterprise-wide deployment in minutes



# Content Categories

- Apply policy to a large number of sites
  - Content categories are used for “acceptable use policies”
  - Security categories are used for security policies
- Umbrella SWG uses Talos categories for both content and security
- Over 100+ categories
- Dynamic Cloud updates (full dataset)

## Add New Content Setting

### Setting Name

### This content list is applied to:

### Copy From Existing

### Categories [SELECT ALL](#)

<input type="checkbox"/> Academic Fraud	<input type="checkbox"/> Mobile Phones
<input type="checkbox"/> Adult	<input type="checkbox"/> Nature
<input type="checkbox"/> Advertisements	<input type="checkbox"/> News / Media
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Non-Profits
<input type="checkbox"/> Arts	<input type="checkbox"/> Nudity
<input type="checkbox"/> Astrology	<input type="checkbox"/> Online Communities
<input type="checkbox"/> Auctions	<input type="checkbox"/> Online Meetings
<input type="checkbox"/> Automotive	<input type="checkbox"/> Online Trading

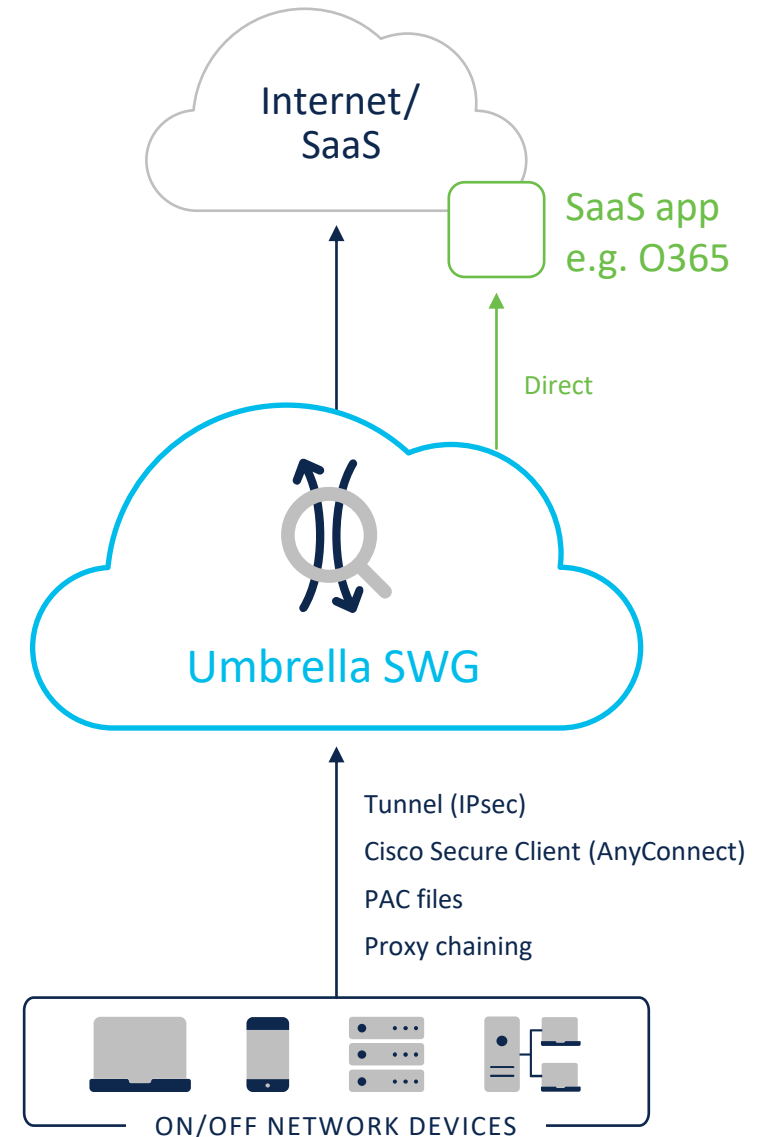
CANCEL

SAVE

# Umbrella SWG

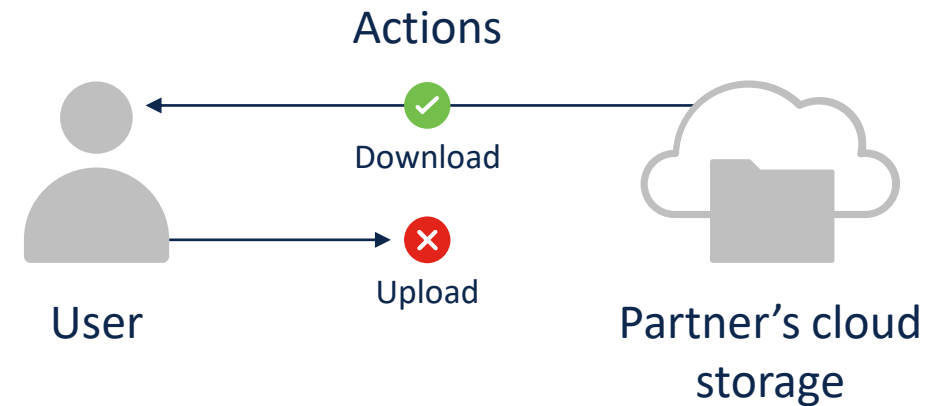
## Multiple functions and aggregated reporting in one cloud console

- Malware scanning includes two anti-virus engines and Secure Endpoint (AMP) lookup
- File type controls
- Full or selective SSL decryption
- Category or URL filtering for content control
- Secure Malware Analytics (Threat Grid) file sandboxing
- App visibility and granular controls
- Full URL level reporting



# Granular controls for over 40 popular SaaS apps

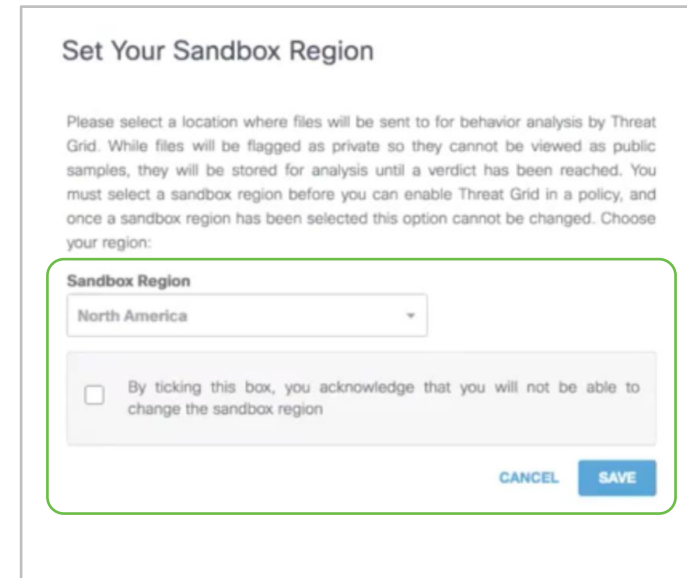
- Block posts/shares to social media apps
- Block attachments to webmail apps
- Block uploads to cloud storage, collaboration, office productivity, content management, and media apps





# Cisco Secure Malware Analytics (Threat Grid) sandboxing

- Ability to detect hidden threats in files that are being downloaded
- A set of new or higher risk files are placed in a sandbox environment and checked for malicious activity/content
  - Alerts posted on files that do show bad activity
  - Umbrella threat intelligence is updated for that file



Regions:  
Europe  
or North  
America

SIG Essentials: Cisco Secure Malware Analytics limit of 500 files per day

SIG Advantage: Includes unlimited submissions and access to the full sandbox console for 3 users

# Most Secured SSE

Secure Web Gateway Test Results

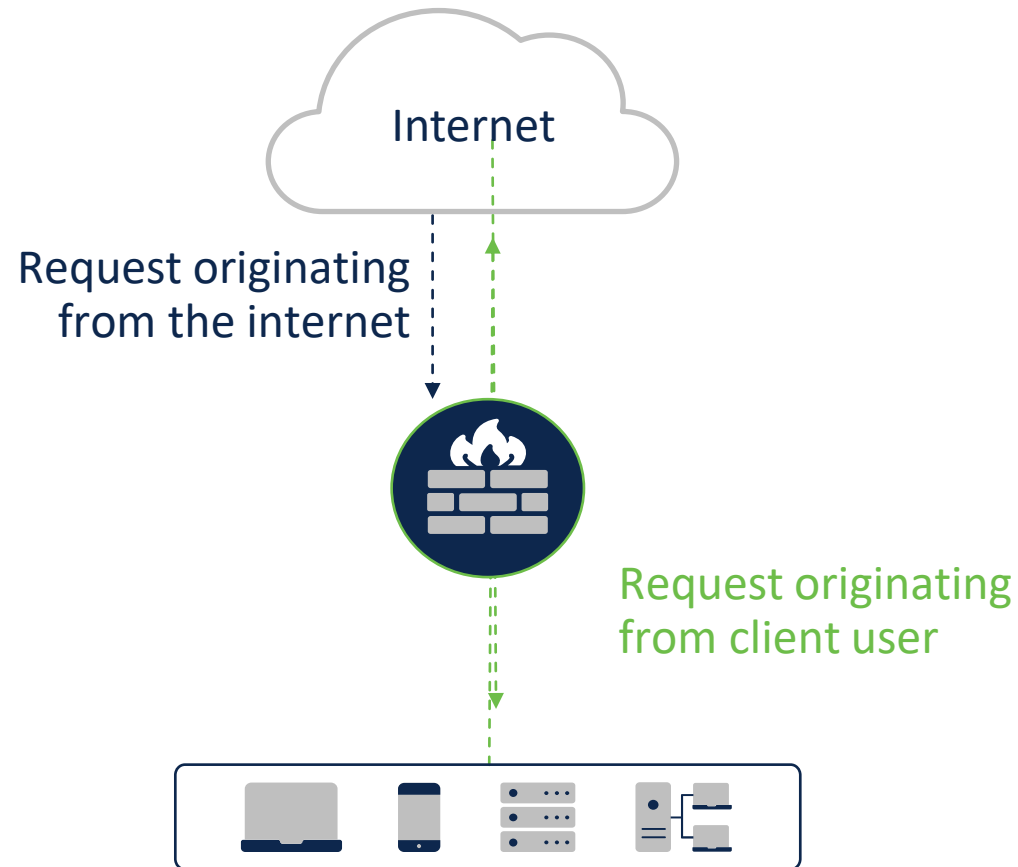
Vendor	Package	Detection rate	False positive rate
Number of test cases		3,682	2,984
Cisco Umbrella	SIG Advantage	90.41%	1.44%
Netskope	Secure Web Gateway	80.12%	0.57%
Zscaler	Internet Access Transformation	79.60%	0.44%
Palo Alto Networks	Prisma Access for Mobile Users	79.33%	3.42%
Skyhigh Security	Secure Web Gateway	63.96%	0.60%
Iboss	Zero Trust Edge	44.60%	0.20%

DNS Tunneling Test Result

Vendor	Package	Protection Against:		
		DNSCat2	DNSExfiltrator	Iodine
Cisco Umbrella	DNS Security Advantage	50%	100%	100%
Cloudflare	Secure Web Gateway	0%	50%	100%
DNSFilter	DNSFilter	100%	0%	100%
Infoblox	BloxOne Advanced	0%	0%	100%



# Umbrella firewall protects traffic from requests originating from a client user



Firewall use cases that protect traffic from requests **originating from a client user** are **essential to securing access** to the internet and controlling cloud app usage



Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view [Manage Firewall](#).

**FILTERS**

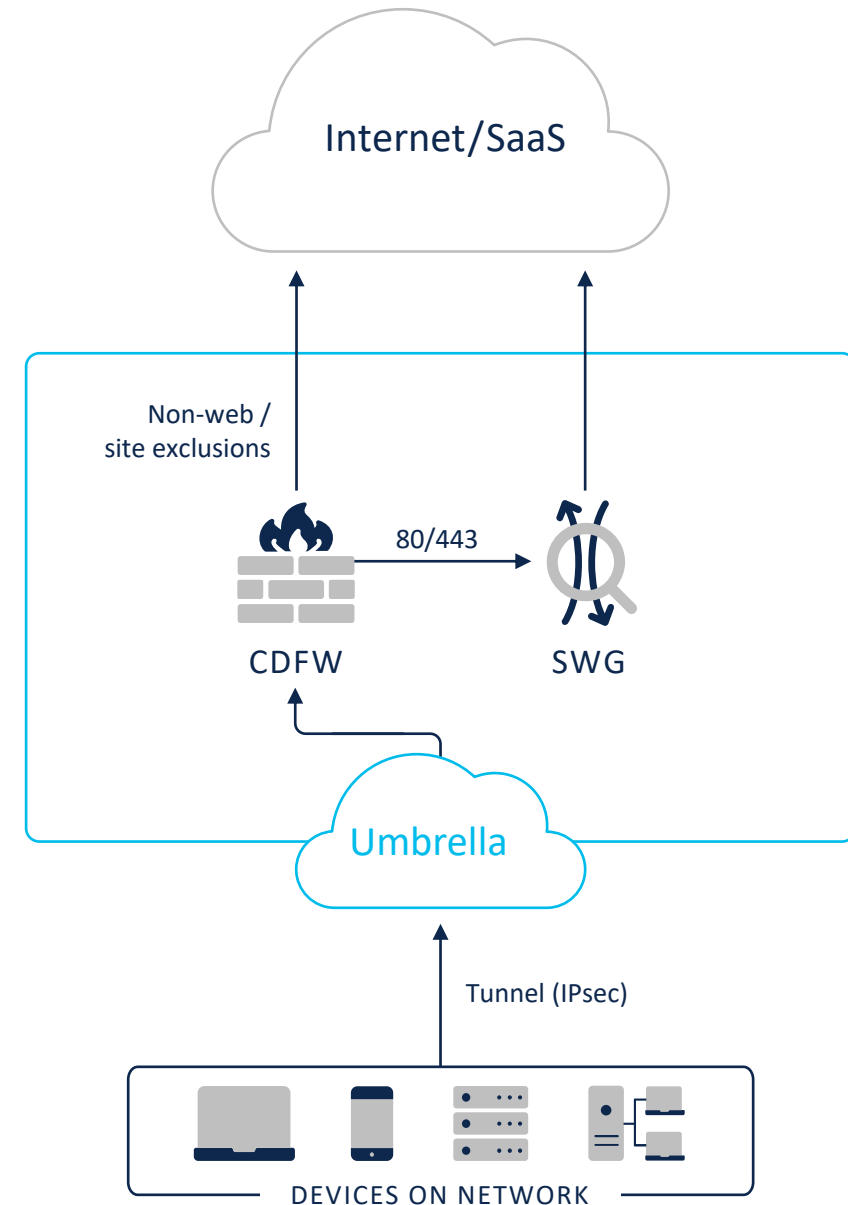
🔍 Search Firewall Rule names or descriptions

3 Total

<input type="checkbox"/>	Priority	Name	Status	Action	Applications	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit	
<input type="checkbox"/>	1	Block SSH	<span style="color: green;">●</span> Enabled	<span style="color: red;">⊖</span> Block	ssh	Any	Any IPs Any Ports	Any IPs 1 Port	<span style="background-color: black; color: white; border-radius: 10px; padding: 2px 5px;">▲ 0/24hrs</span>	▲ No Hits	...
<input type="checkbox"/>	2	p2p rule	<span style="color: green;">●</span> Enabled	<span style="color: red;">⊖</span> Block	Any P2P ftp	Any	Any IPs Any Ports	Any IPs Any Ports	<span style="border: 1px solid gray; border-radius: 10px; padding: 2px 5px;">25.0 /24hrs</span>	Aug 24, 2020 - 09:33am	...
<input type="checkbox"/>	3	Default Rule	<span style="color: green;">●</span> Enabled	<span style="color: green;">✓</span> Allow	Any Application	Any	Any IPs Any Ports	Any IPs Any Ports	<span style="border: 1px solid gray; border-radius: 10px; padding: 2px 5px;">69.1 k/24hrs</span>	Aug 24, 2020 - 03:15pm	...

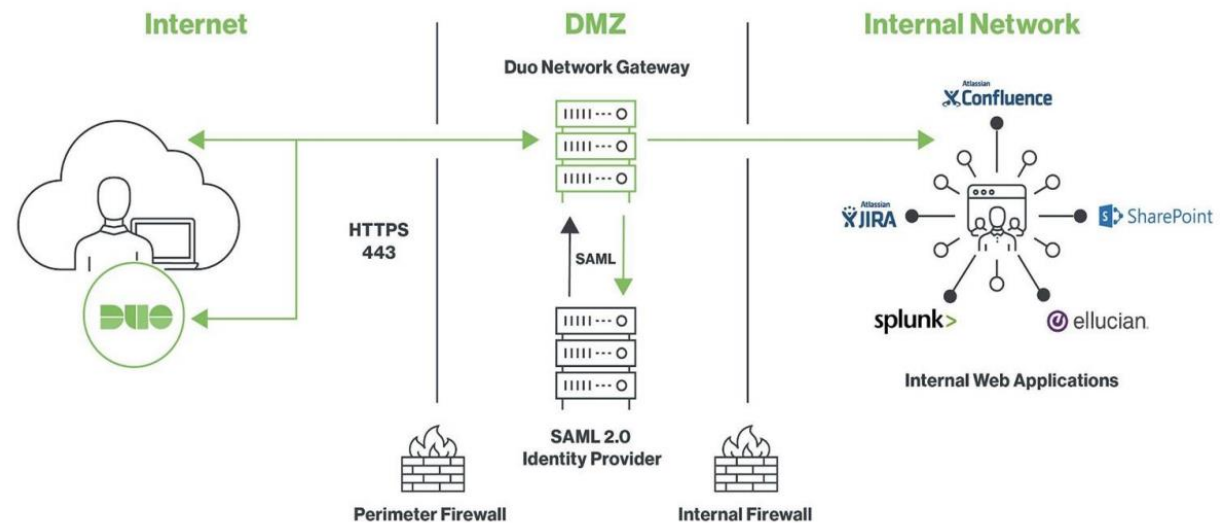
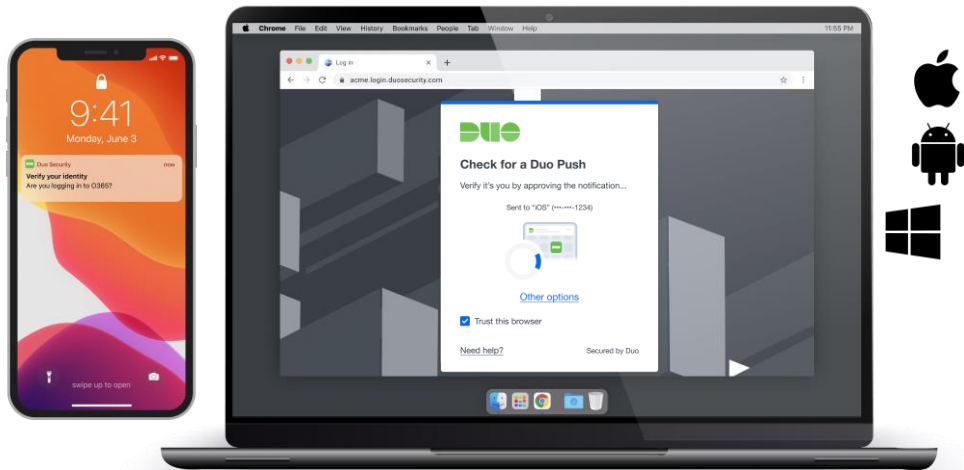
# Layer 7 application visibility and control

- Tunnel all client-driven traffic to Umbrella
- Block high risk applications and protocols (layer 7 application visibility & control)
- Centrally manage IP, port, protocol and application rules (layer 3, 4 and 7 with IPS)
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination required



# DUO for ZTNA

Remote user trying to access a cloud app from their device





# SASE Adoption Hurdles

Exciting times... but not always easy to figure out the transition path to SASE !







# SASE Adoption Plan


Leading the way

## From “Try” to “Scale”

 “Try” new solutions in a real production environment



 “Scaled” deployment across Cisco production

 We are here !

## The pathway to SASE ...



### CZ SASE HUB

Modernized  
On-Prem “SASE-like” platform




### Supplement & Replace

Integrate  
On-Prem + Cisco SASE



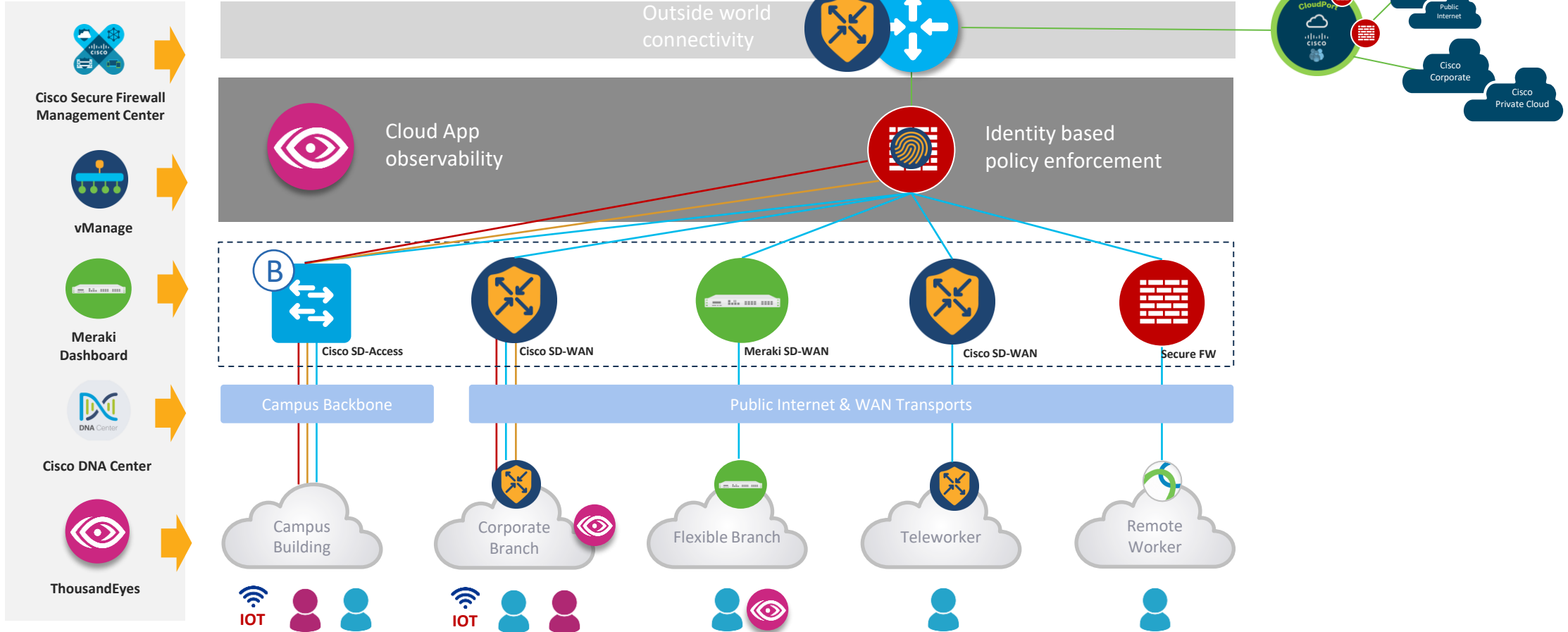
### Standalone SASE

Aspiration to replace On-Prem  
with 100 % Cisco SASE

 We are here !

# CZ "SASE" HUB

SJC, RTP, London and Sydney



# CZ Teleworker

## Objectives

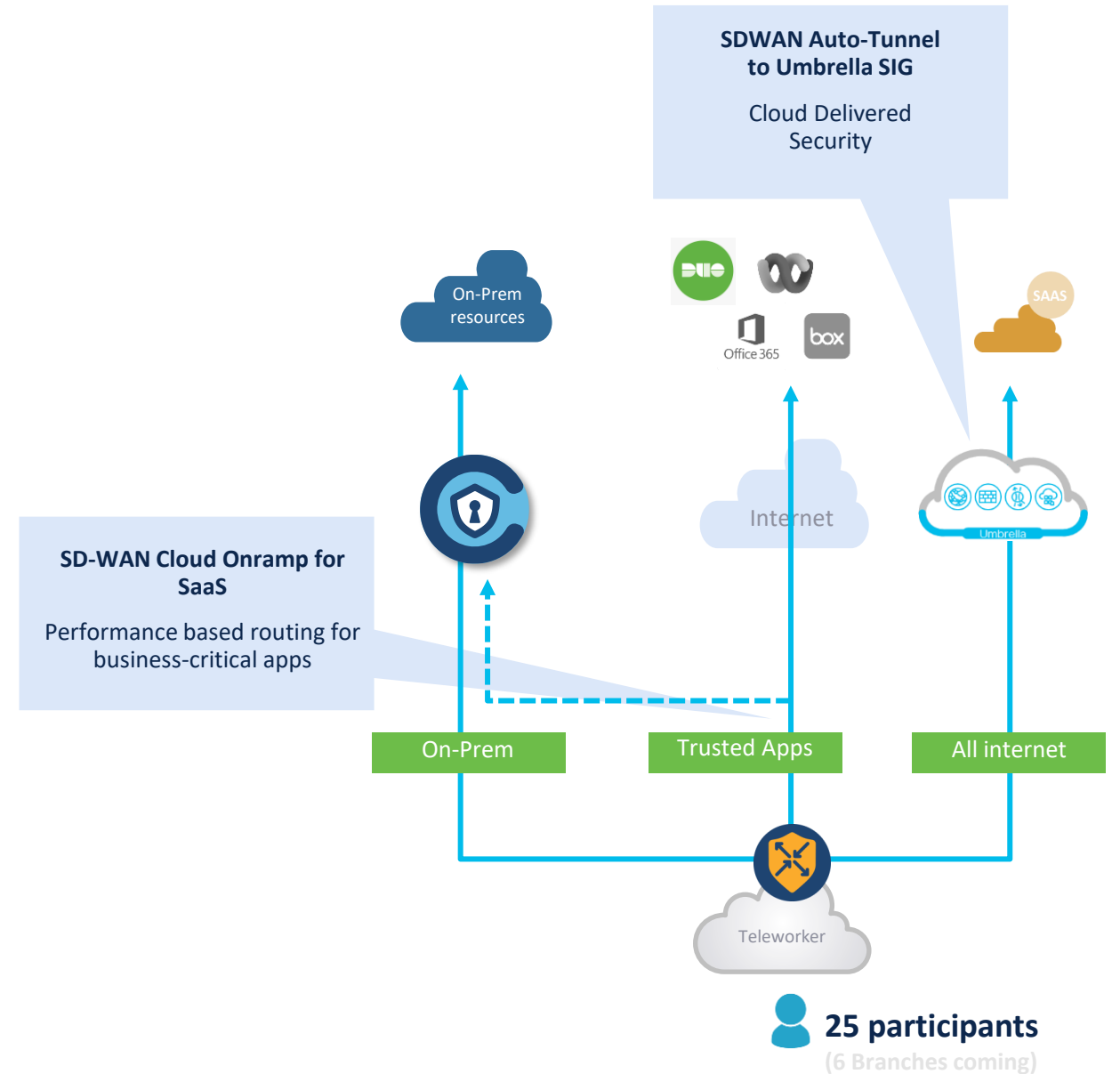
- Redefining the network edge - bring applications closer to the users for a better client experience
- Reduce dependency on high cost on-prem infrastructure & telco circuits

## Solution

- Hardware based offering (ISR1K) for selective group of users that need it
- Intelligent & performance-based traffic routing via Cisco SD-WAN
- Umbrella Cloud delivered security for all-internet based traffic

## Success stories

- Easy to enable – works as expected
- Successfully mitigated internet issues
- Offloaded a significant amount of traffic



# CZ Remote Worker

## Objectives

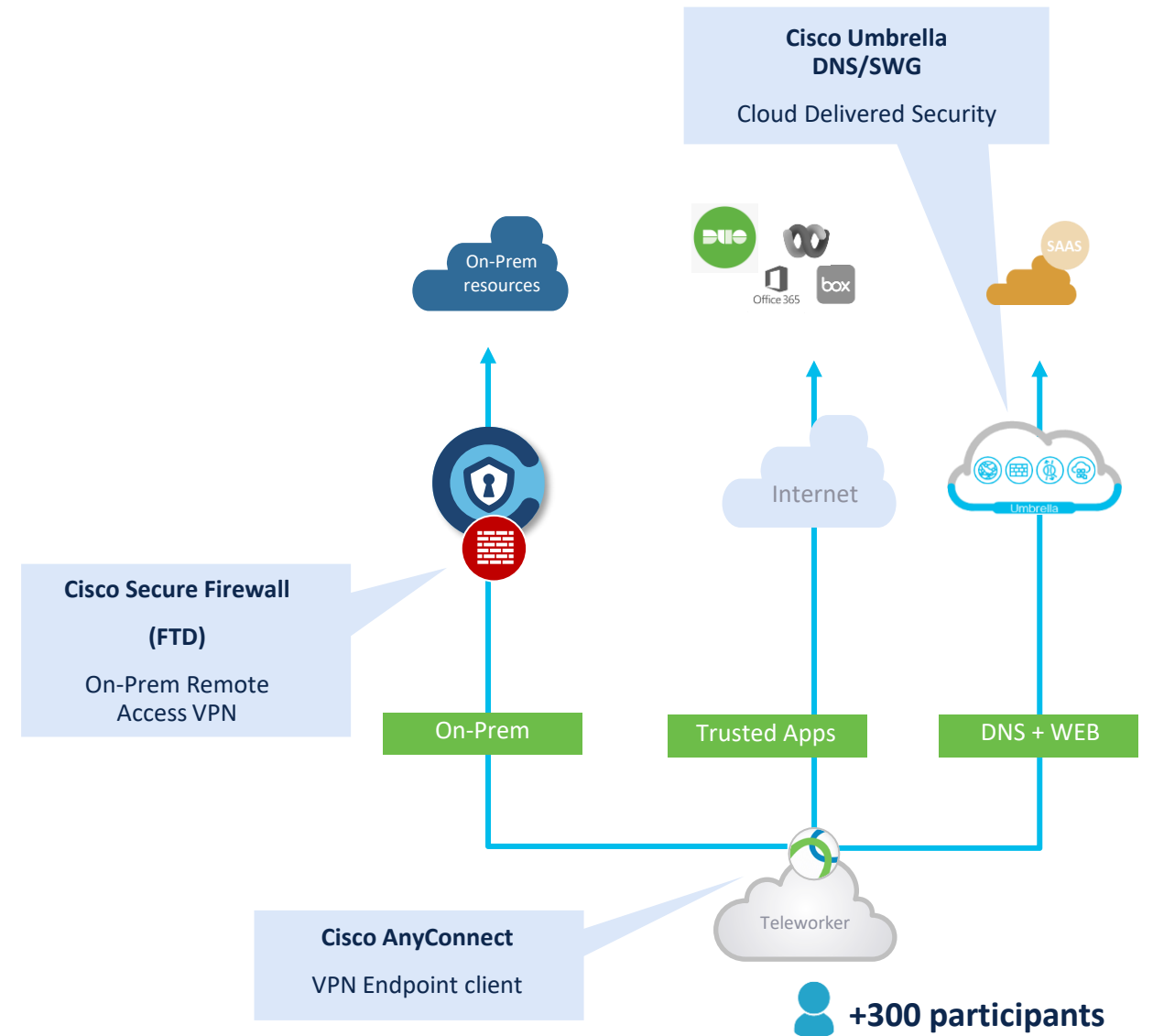
- Redefining the network edge - bring applications closer to the users for a better client experience
- Reduce dependency on high cost on-prem infrastructure & telco circuits

## Solution

- Software based offering (AnyConnect) for selective 300+ remote workers
- AnyConnect IP/Domain based split-tunneling for trusted & zero trust enabled applications
- Redirection of all other Web traffic to Umbrella Secure Web Gateway (SWG) & DNS Security

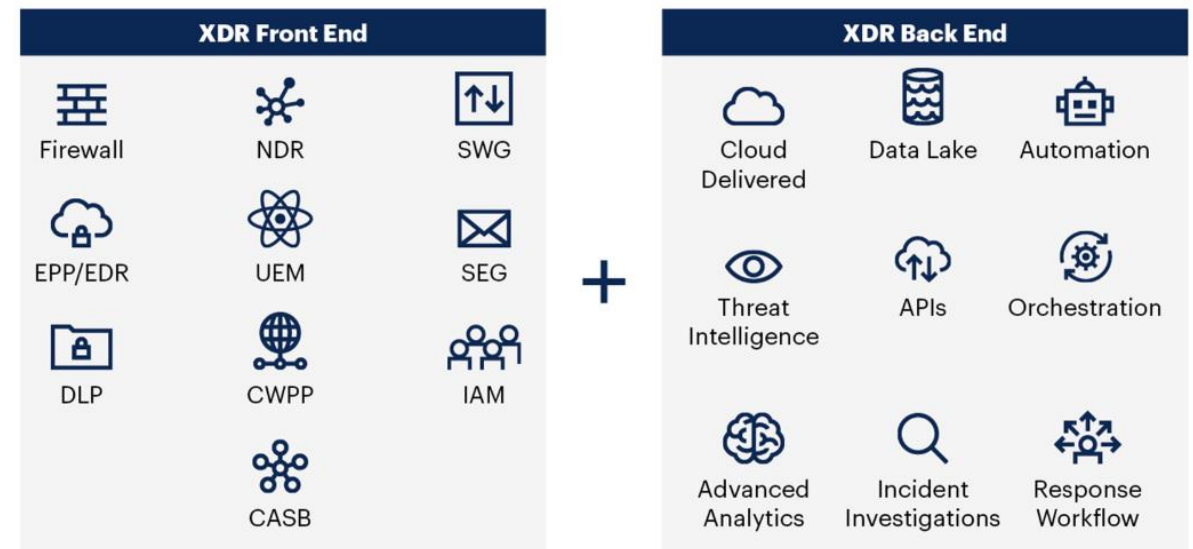
## Success stories

- Improved visibility into Web traffic
- Better security (malware, app visibility controls ,... )
- Ease of policy creation
- DNS Security protection



# XDR

## XDR Overview

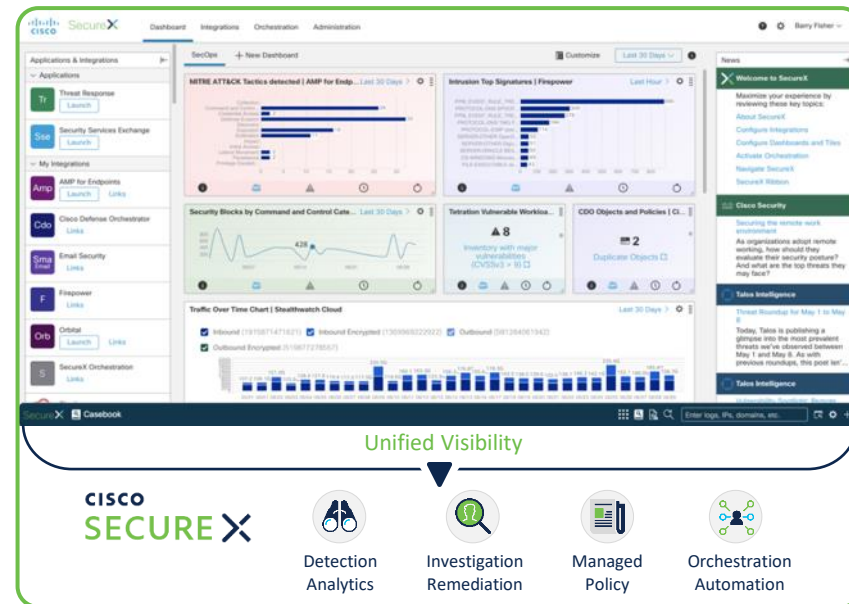


Source: Gartner

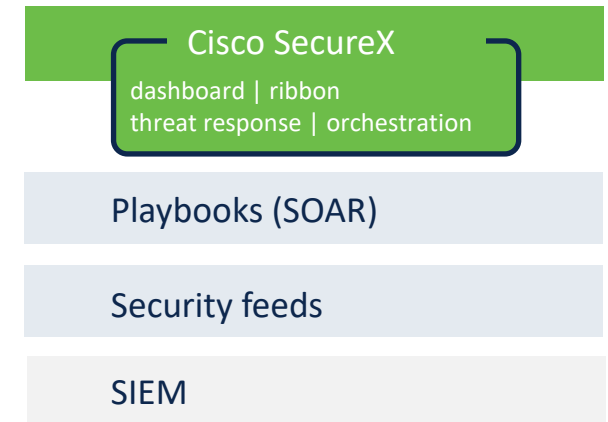
# The Architecture of XDR



# The Architecture of XDR

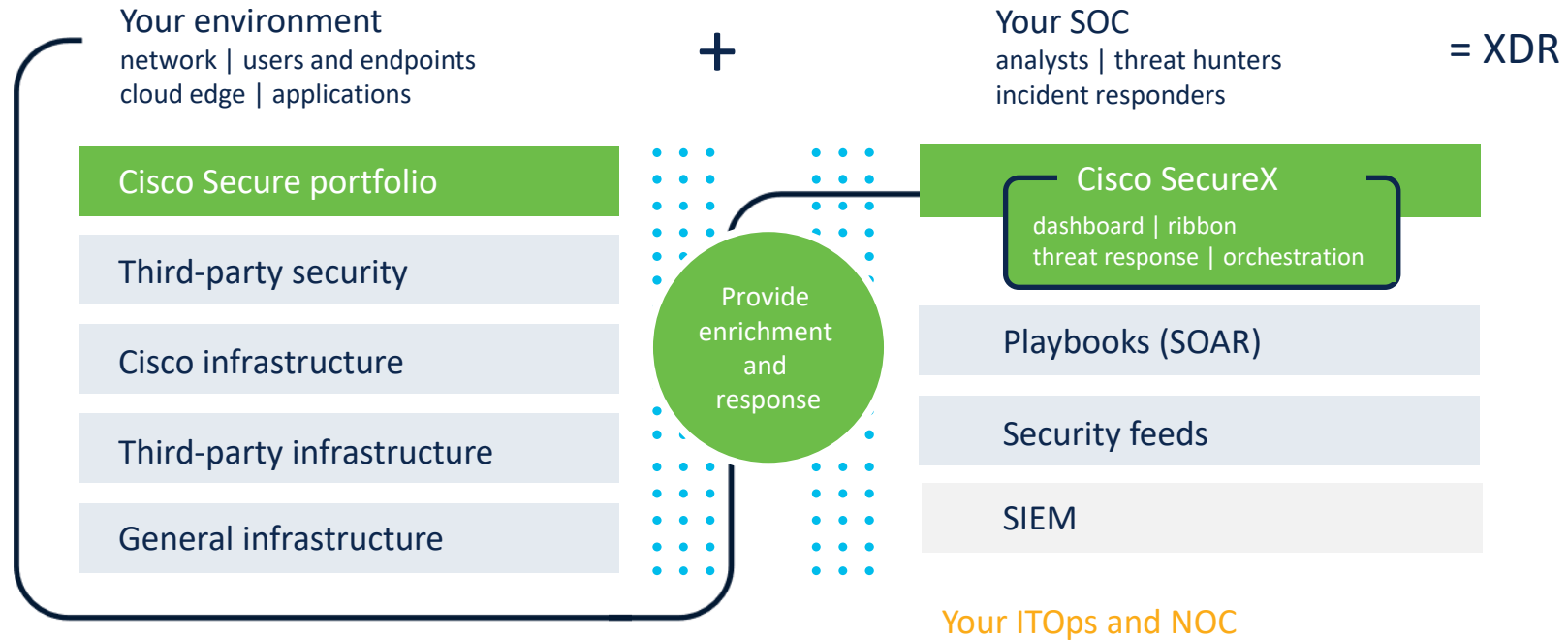


Your SOC analysts | threat hunters incident responders



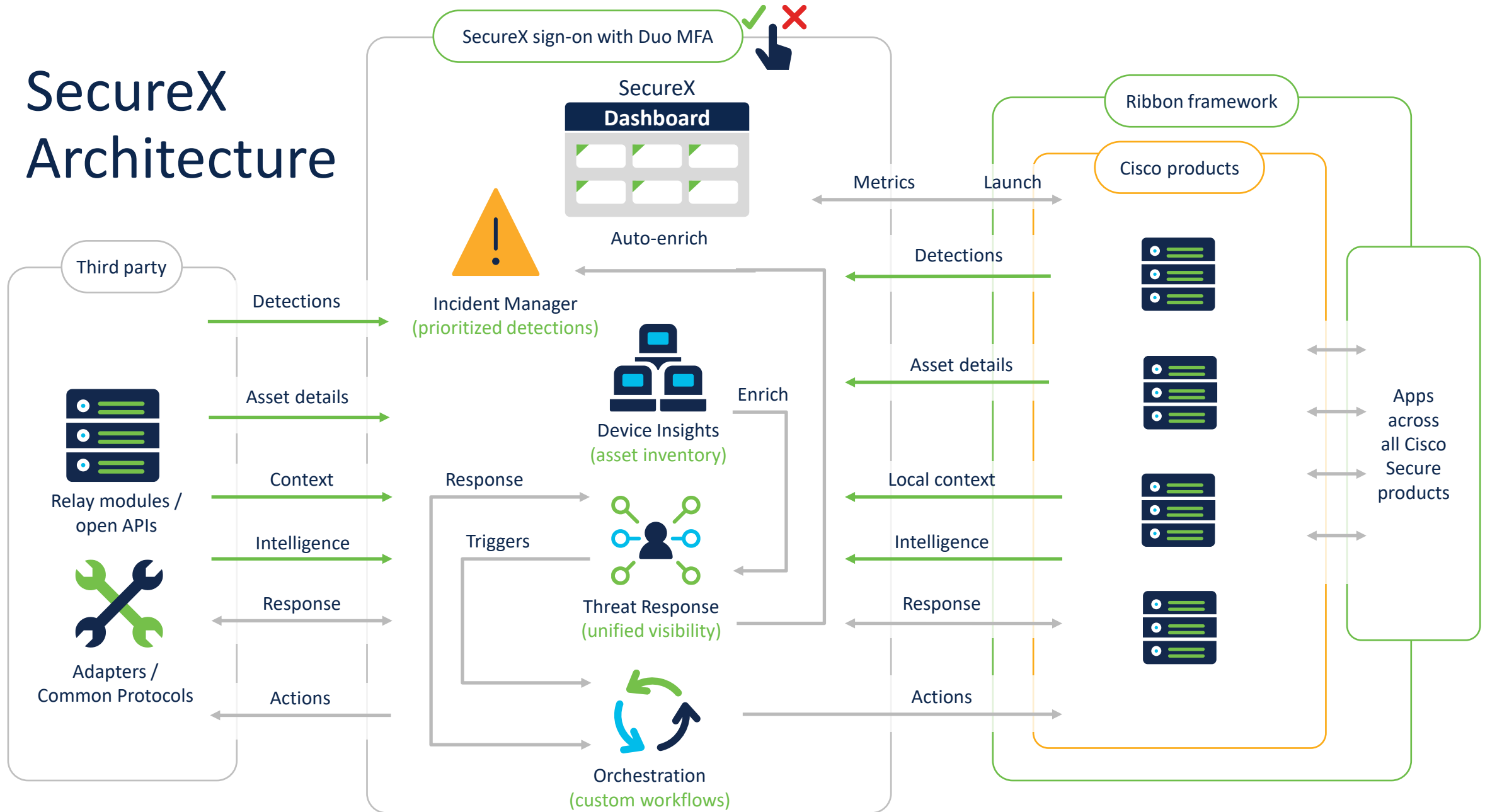
Your ITOps and NOC

# The Architecture of XDR

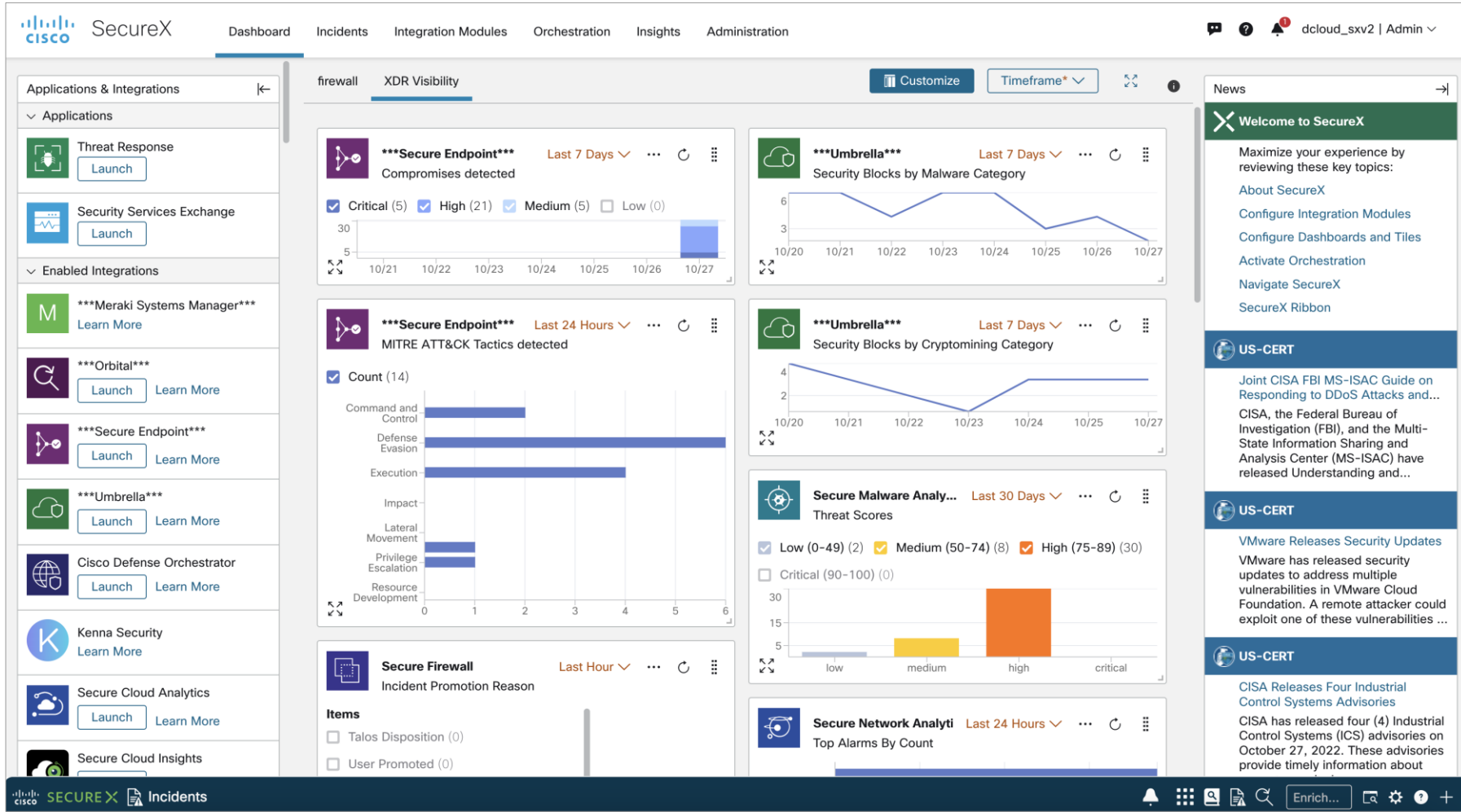




# SecureX Architecture



# A new level of visibility with SecureX dashboard



- Applications (left)  
View, launch or trial the integrated products
- Tiles (middle)  
Presents metrics and operational measures from the integrated products
- News (right)  
Product updates, industry news, and blog posts

# Never lose context with SecureX Ribbon



The screenshot displays the Cisco SecureX Incidents interface. The top navigation bar includes the Cisco logo, 'SECUREX Incidents', and various utility icons. The main content area is divided into a left sidebar with a search bar and incident filters, a central incident detail view, and a right sidebar with 'Info', 'ASSIGNEES', and 'KEY PROPERTIES'.

**Incident List (Left Sidebar):**

Incident ID	Service	Date
High Impact 41		
Other 757,013		
Intrusion event 1-50714	NGFW Event Service	Sep 20, 2022
Intrusion event 1-33906	NGFW Event Service	Sep 20, 2022
Intrusion event 1-33905	NGFW Event Service	Sep 20, 2022
Intrusion event 1-50125	NGFW Event Service	Sep 20, 2022
Intrusion event 1-42841	NGFW Event Service	Sep 20, 2022
Intrusion event 1-57893	NGFW Event Service	Sep 20, 2022
Intrusion event 1-39686	NGFW Event Service	Sep 20, 2022

**Incident Detail View (Center):**

**Security Intelligence event - URL\_SI\_Category:dcloud-SI-URL**

**Investigate Incident** | Status | Manage Incident | Link

Security Intelligence event - URL\_SI\_Category dcloud-SI-URL /

**New** · Created By NGFW Event Service on 2022-09-19 07:58:24 UTC

Summary | Events | **Observables** | Timeline | Linked References (0)

**Targets (1)** · Investigate these Targets

- 192.168.249.115
- Endpoint** · Targeted by 1 unique observable, 1 time in the last day
- IP Address · 192.168.249.115
- First: 2022-09-19T07:48:01.000Z · Last: 2022-09-19T07:48:01.000Z

**Observables (3)** · Investigate these Observables

- http://drinkfoodapp.com/AdminDF/assets/img/app/settings.doc
- Suspicious URL** · 1 Target · 1 Sighting · 0 Snapshots
- First: 2022-09-19T07:48:01.000Z · Last: 2022-09-19T07:48:01.000Z

- 108.62.141.250
- IP Address · 1 Target · 1 Sighting · 0 Snapshots
- First: 2022-09-19T07:48:01.000Z · Last: 2022-09-19T07:48:01.000Z

Threat Grid [Submit Sample](#) Dashboard

Basic Search

Query:

Match By:

Date Range:

Scope:  My Organization My Samples

Access:  Private Public

[Search](#)



Download Help Query Feedback

... will return samples that match on the instance's geo-...  
... as shown above, rather than the leading element.) You

... search by targeting specific database indices.

... types that exhibit the behavioral indicator. For example

... components, a search for `alice.com` will return results

User Name	Access	Status
cdm-locked...	Secure& Orchestrator	
gffm3_secure...	Jeff Smith	

让我们转到Incident Manager

SECURE X Casebook

Search:

Overview

Details

File: [Secure& Academy /](#)

Created: [Mar 27, 2021, 6:18:25 PM](#)

Owner: [Ben Greenbaum](#)

Summary: [Domains up to no good /](#)

Observables (2)

Enter logs, IPs, domains, etc.

2 Domains

- [cdm.chattodh.net](#)
- [p-entomle.com](#)

Notes

is.hafnium?

Owned By Me (3)

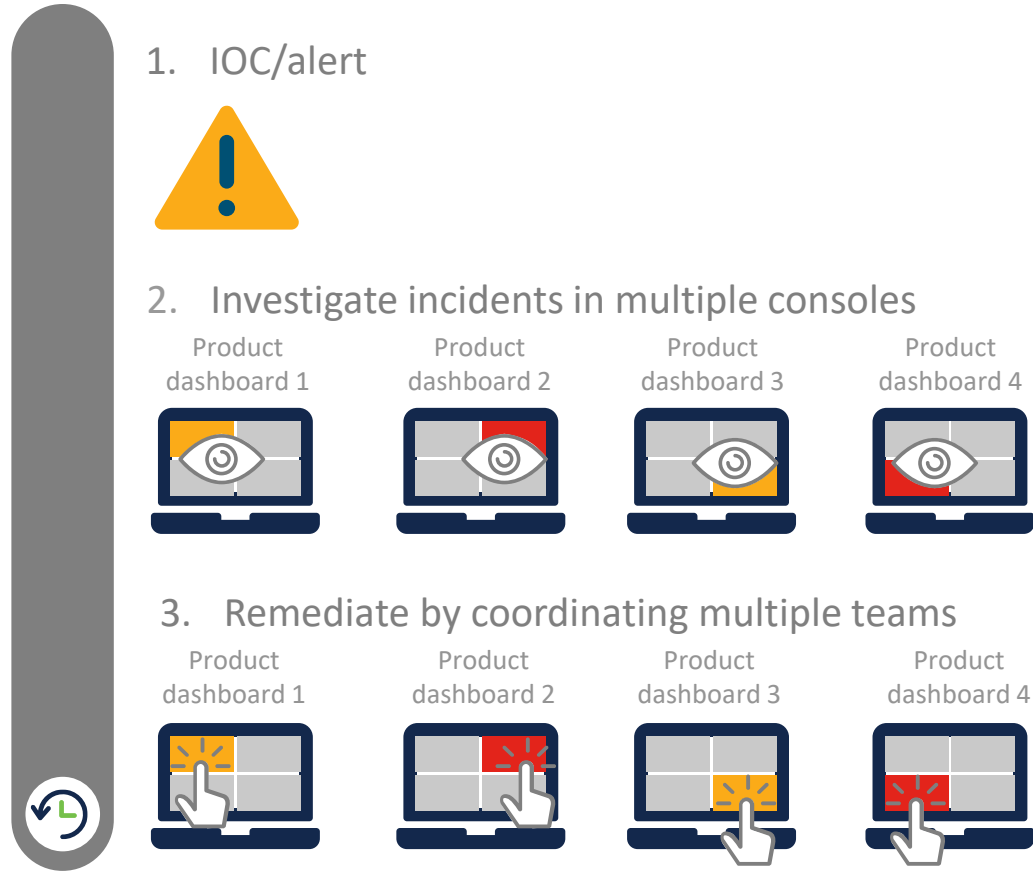
- [Talos Intelligence domains](#) (21 Observables)
- [stony & new](#) (3 Observables)
- [Secure& Academy](#) (2 Observables)

Owned By Others (1,005)

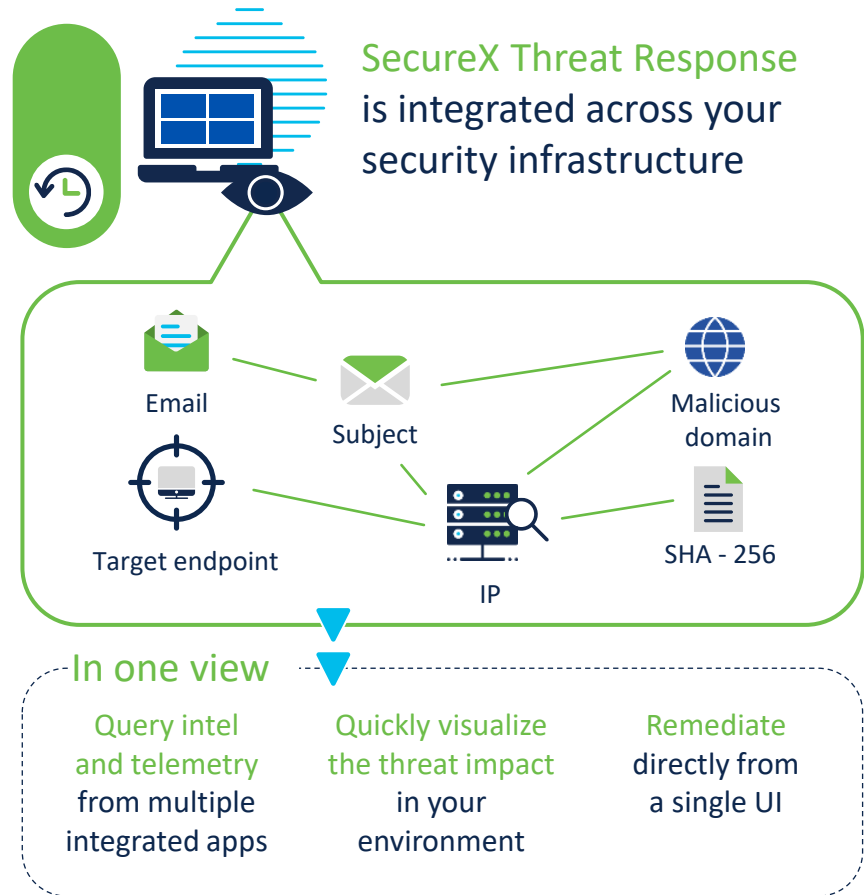
- [Intrusion event 1 25276.3](#) (2 Observables)
- [Dfns Received](#) (2 Observables)

# Threat Response for true simplicity

Before: 32 minutes



After: five minutes



Add to Investigation

New Investigation

Snapshots

2 of 2 enrichments complete

Fit to Screen 3 Panel Layout

4 Targets

2 Investigated

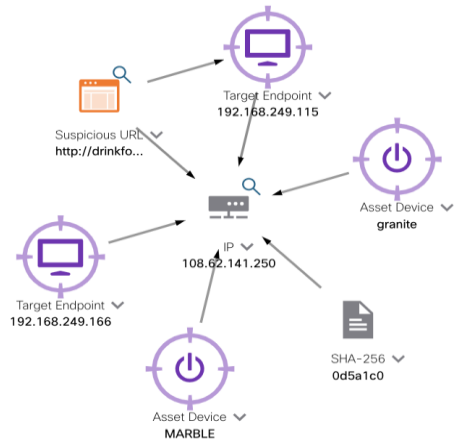
1 Omitted

4 Related

5 Indicators

8 Modules

Graph Filters: Show All, Expanded Showing 7 nodes



Results

Details Threat Context

- Endpoint
- 2 ASSETS
  - MARBLE Device
  - granite Device
- 2 INVESTIGATED
- 1 OMITTED
- 4 RELATED

### MARBLE

Asset Device  
[View in Device Insights](#)

Overview Sightings (6)

#### Unified Observables

AMP GUID: 0d13fc67-c5a7-421e-b5fe-dd5f1e5201c4

Hostname: marble

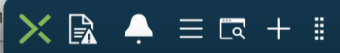
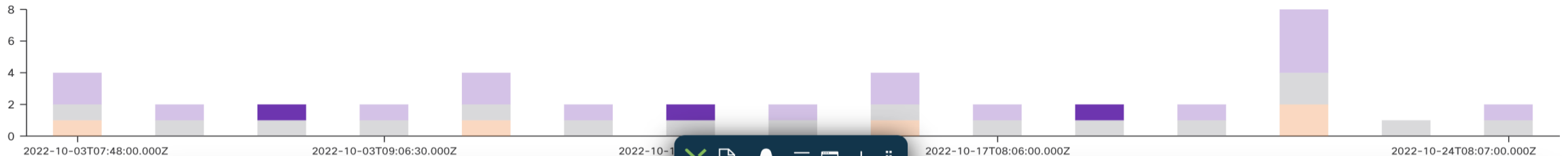
IP Address: 192.168.249.111

Sightings

My Environment (21) Global (22)

2022-10-03T07:48:00.000Z - 2022-10-24T08:07:00.000Z

Malicious Suspicious Common Unknown Clean Targets



# Simplifying SOC Operations

## SecureX Threat Response

### Threat Hunting

The screenshot displays the Cisco Threat Response interface for Threat Hunting. It features a navigation bar with 'Investigate', 'Snapshots', 'Incidents', and 'Intelligence'. Below the navigation bar, there are filters for '9 Targets', '4 Observables', '76 Indicators', '2 Domains', '1 File Hash', '1 IP Address', '0 URLs', and '8 Modules'. The main content area is divided into several sections: 'Investigation' showing search criteria for 'office360.com', 'Relations Graph' showing a network diagram, 'Sightings Timeline' showing a graph of sightings for 'Office360.com', and 'Observables' showing details for 'Office360.com' and '100.62.141.247'.

### Incident Response

Title	Status	Confidence	Description	Source	Modified	Actions
Intrusion event 1:100000...	New	Medium	MALWARE CNC SIGNAL ...	ngfw_ips_event_service	Dec 18, 2019	...
Data Exfiltration	New	Low	Tracks inside and outsid...	Cisco Stealthwatch Enterprise	Dec 18, 2019	...
Security Intelligence eve...	New	High	Security Intelligence eve...	ngfw_event_service	Dec 17, 2019	...
Security Intelligence eve...	New	High	Security Intelligence eve...	ngfw_event_service	Dec 17, 2019	...

Protect your organization against

- Ransomware
- Server-based attacks
- File-less malware
- Cryptomining
- Phishing attacks
- Corporate espionage
- IoT attacks
- Data breaches

# Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).



SecOps

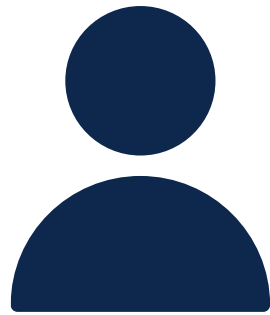


Query SecureX

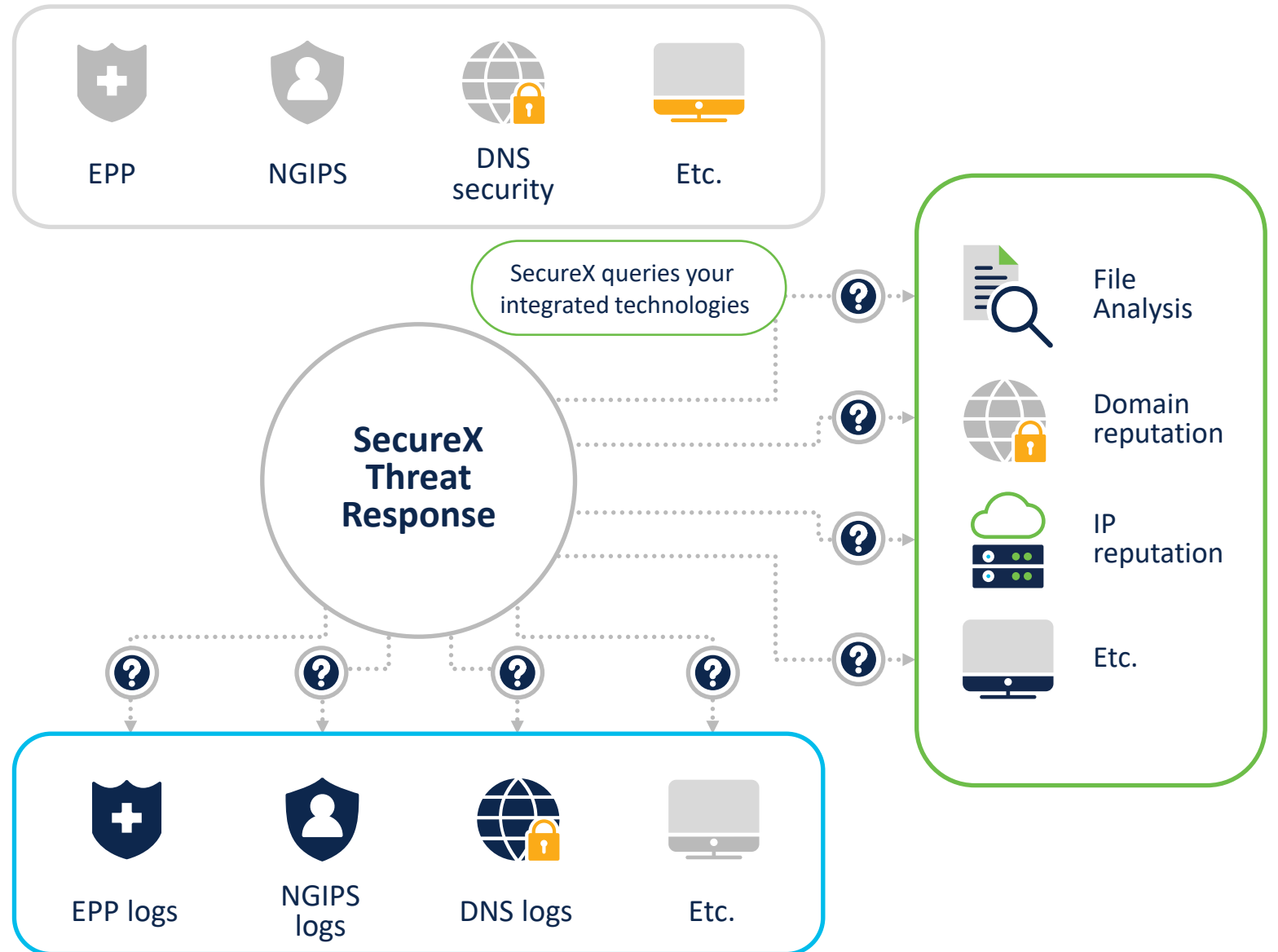




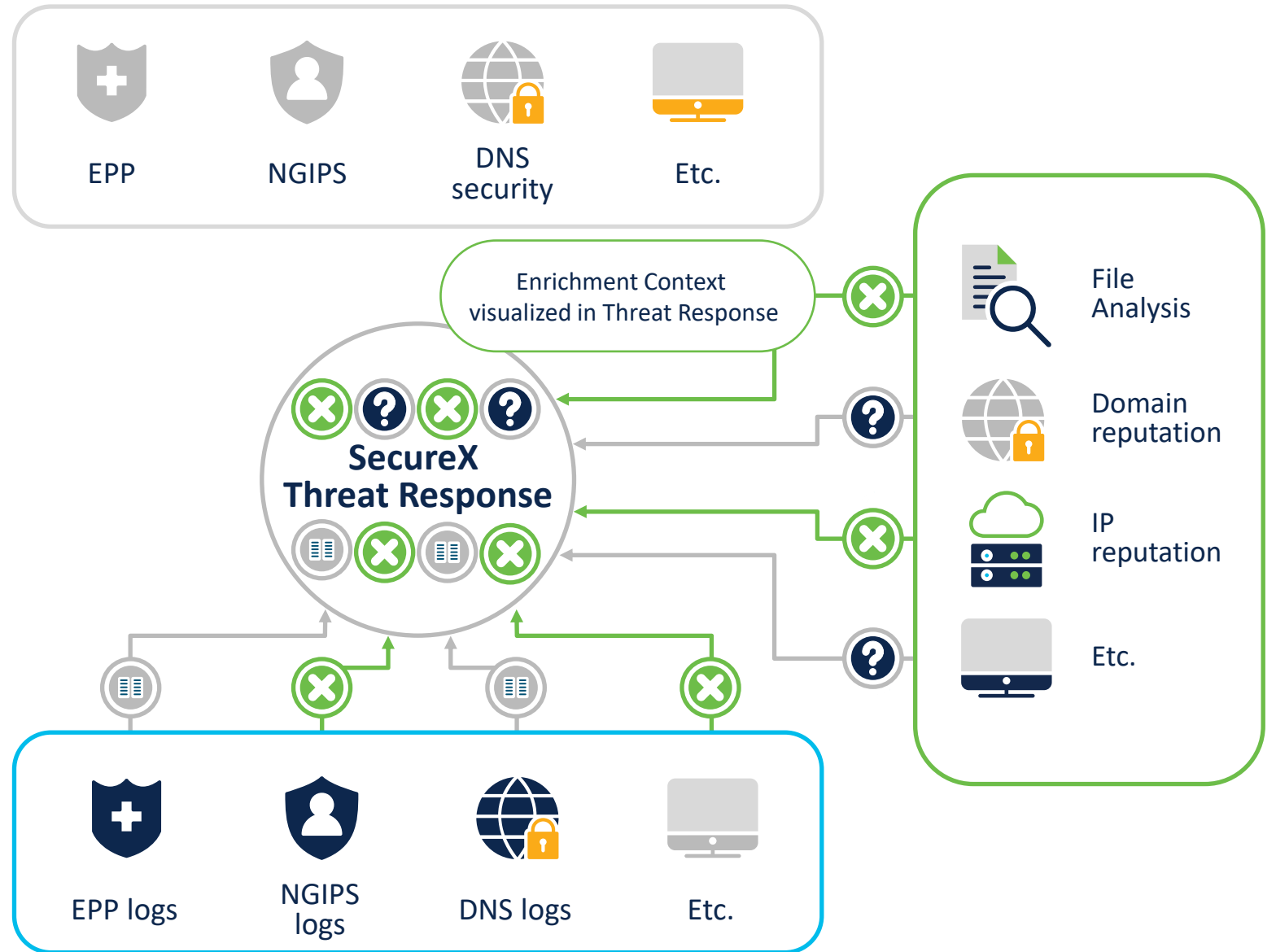
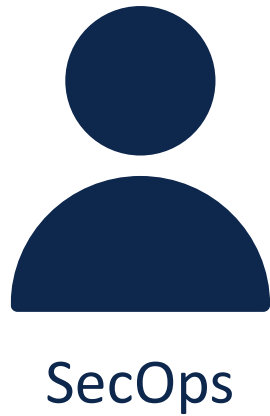
# Enrichment



SecOps



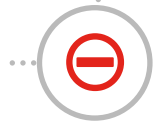
# Enrichment



The process of leveraging the capabilities of SecureX enabled technologies to mitigate threats by acting on observables or targets.



SecOps



# Response



SecOps



# SecureX Orchestration for Efficiency

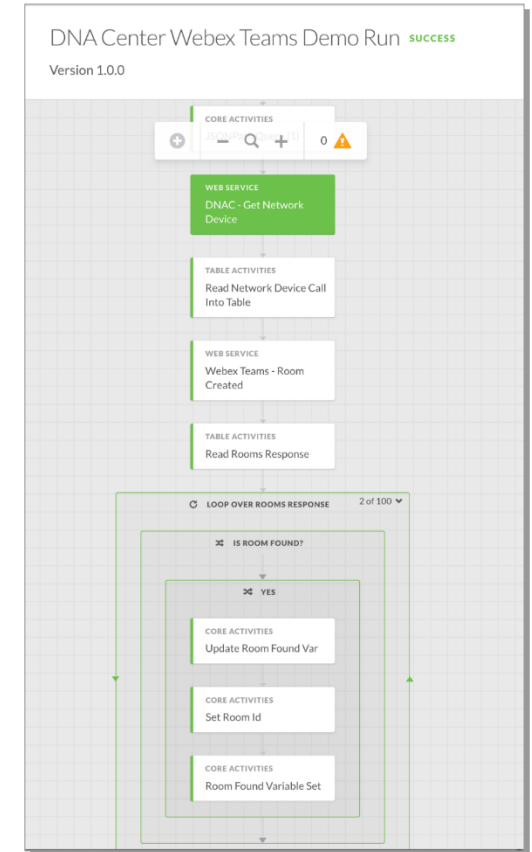
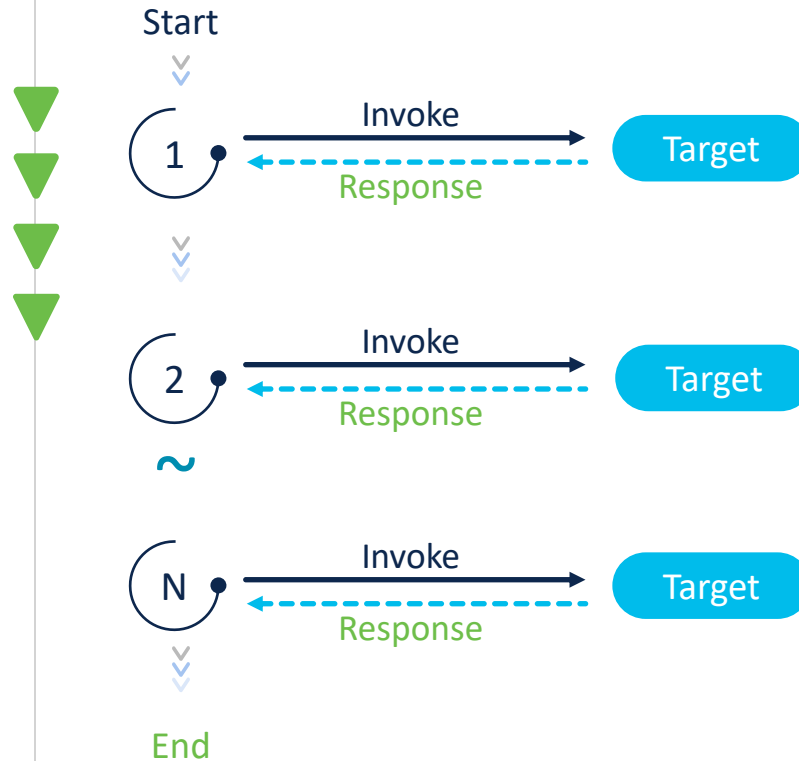
## Cloud-Native, microservice architecture

- Highly Performant, Scalable and Secure
- Reusable and Embeddable

## Intuitive drag-drop UI with visual workflows

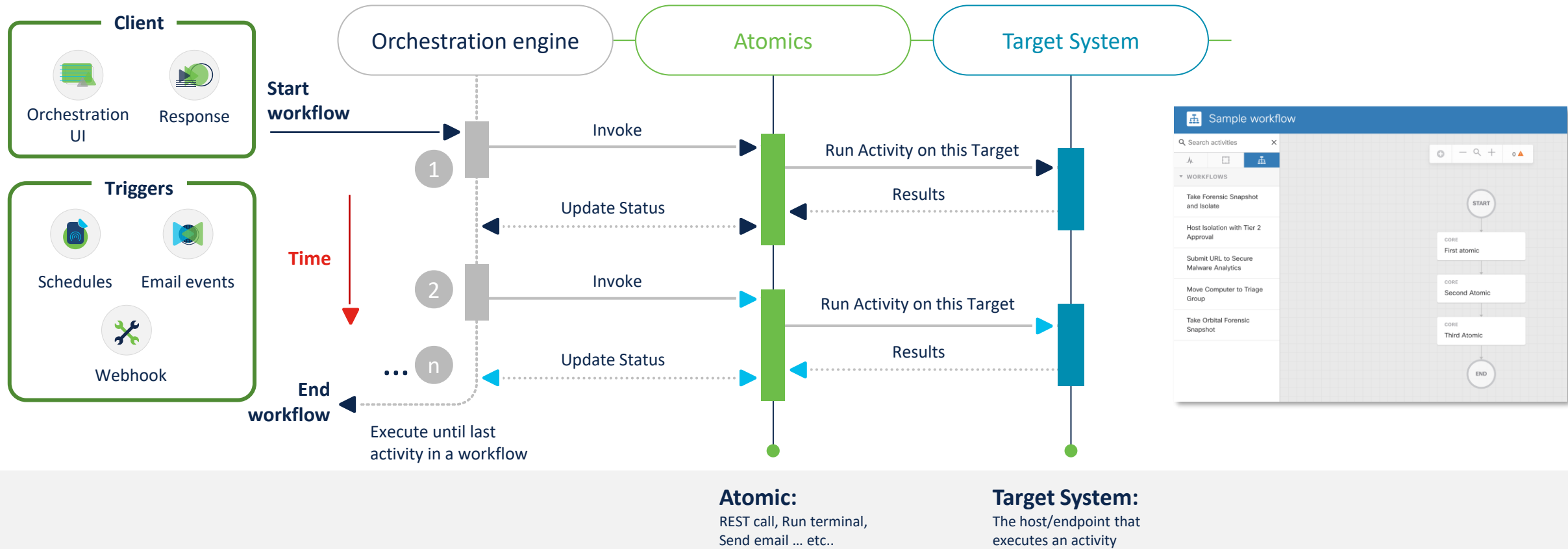
## Combine flexible out of the box atomics and workflows to create new integrations

- Automate tasks according to schedules or external events such as email events



# SecureX Orchestration workflow sequence

The orchestration engine runs **workflows** to execute **atomics** on the **target systems**, which returns results and **status**, then the next step in the workflow begins.



# SecureX Orchestration canvas overview

**0010 - Phishing Investigation** Modified: April 30, 2021 at 10:42:50 AM VALIDATED COMMIT VIEW RUNS RUN ⌵ ✕

**Search activities**

- CORE
- AWS SERVICE
- APPD
- CISCO ACI
- CISCO AMP FOR ENDPOINTS
- CISCO DNA CENTER
- CISCO DEFENSE ORCHESTRATOR
- CISCO DUO SECURITY
- CISCO FMC
- CISCO ISE
  - ISE Create ANC Policy
  - ISE List ANC Policy
  - ISE Quarantine Endpoint
  - ISE UnQuarantine Endpoint
- CISCO ORBITAL
- CISCO PROCESS ORCHESTRATOR
- CISCO STEALTHWATCH CLOUD
- CISCO STEALTHWATCH ENTERPRISE
- CISCO TETRATION
- CISCO THREAT RESPONSE

**Drag n' Drop UI**

**Activity Group**

**Atomic Action (Activity)**

**Stacked Activities" indicates Atomic Action**

**Logical Constructs**

**Creates Atomic Action**

**Tags Workflow**

**Variables**

**Details Pane**

**Validate & Save Run & Audit**

**PROPERTIES**  
0010 - PHISHING INVESTIGATION

**OWNER**  
adisanka+ctr-dcloud@cisco.com

**DESCRIPTION**  
This workflow monitors a mailbox for incoming phishing reports. When an email is received, the workflow investigates its attachments and attempts to determine if anything in the email (or its attachments) was suspicious or malicious. If anything suspicious or malicious is found, the user is told to delete the email, create an incident, and create a Threat Response...

DELETE WORKFLOW INSTANCE AFTER SUCCESSFUL EXECUTION

IS ATOMIC WORKFLOW

**GROUP NAME**  
Select

**CATEGORY**  
Select

NAME	TYPE	SCOPE	VALUE
Consolidated Headers	String	Local	
Has Email Attachment	Boolean	Local	false
Notification Email Addresses	String	Local	bromide@cisco.com
Number of Clean Observables	Integer	Local	0

# References to continue learning

- [cisco.com/go/securex](https://cisco.com/go/securex)
- [cs.co/SecureX\\_videos](https://cs.co/SecureX_videos)
- SecureX session at CiscoLive  
on-demand: [cs.co/SecureX\\_CiscoLive](https://cs.co/SecureX_CiscoLive)
- SecureX Academy:  
<https://learnsecurex.cisco.com>



# Resources

## Integration documentation

[cs.co/SecureX\\_integration\\_workflows](https://cs.co/SecureX_integration_workflows)

The screenshot shows the Cisco SecureX Integration Workflows documentation page. The left sidebar contains a navigation menu with sections for 'THREAT RESPONSE' (Getting Started, Pivot into threat response, Queries, Refer "Pivot" Actions, Response Actions, Relay API) and 'ORCHESTRATION' (Getting Started, Workflows, Engic, Events, Schedules, Import/Export, API Documentation). The main content area is titled 'Cisco SecureX Integration Workflows' and 'threat response'. It lists several sections: 1. Getting Started (Global API Endpoint URLs, Create API Client in Threat Response UI, Scopes, Using API Client Credentials to Get Access Token, Authentication, Rate Limits, API Endpoints); 2. Pivot into threat response (Launch Investigation From URL, Launch Investigation From a Newly Created Casebook, Launch Investigation From an Existing Casebook); 3. Queries (Get Verdicts for an Observable, Contextualize an Observable); 4. Refer "Pivot" Actions (Extract Observables, Refer Observables, Use Cases); 5. Response Actions (Extract Observables, Respond Observable); 6. Relay API (Requirements, Good Practices When Possible); and 7. Orchestration (Workflows, Burs).

## UI docs and proto tools

[github.com/threatgrid/ctim/tree/master/doc](https://github.com/threatgrid/ctim/tree/master/doc)

The screenshot shows the Cisco SecureX UI documentation page. It features a 'Parameters' section with a 'Cancel' button, an 'Observable' section with a 'Cancel' button, and a 'Response' section with a 'Cancel' button. The 'Observable' section contains a code block with the following content: 

```
{ "hostname": "192.168.1.1", "ip": "192.168.1.1", "type": "ip" }
```

## GitHub

[github.com/CiscoSecurity](https://github.com/CiscoSecurity)

The screenshot shows the Cisco Security GitHub repository page. It features a search bar, a 'Find a repository...' input, and a list of repositories. The first repository is 'tr-05-gigamon-threatinsight', which is a Threat Response Serverless Relay for Gigamon ThreatINSIGHT. It is written in Python and has 0 stars and 0 forks. The second repository is 'tr-05-serverless-farsight-dnsdb', which is a Threat Response Serverless Relay for Farsight DNSDB. It is written in Python and has 0 stars and 0 forks. The third repository is 'tr-05-serverless-shodan', which is a Threat Response Serverless Relay for Shodan. It is written in Python and has 0 stars and 0 forks.

# SecureX Threat Response resources

## DevNet

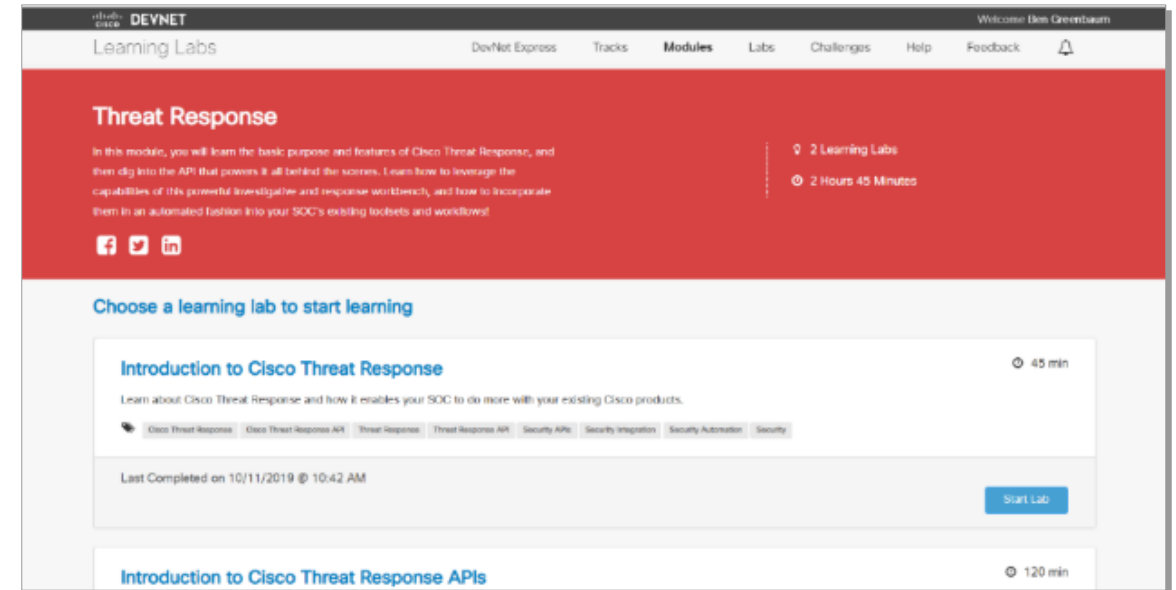
- [developer.cisco.com/threat-response/](https://developer.cisco.com/threat-response/)
- [cs.co/SecureX\\_integration\\_workflows](https://cs.co/SecureX_integration_workflows)



The screenshot shows the DevNet page for SecureX threat response. The header includes the DevNet logo and navigation links like Discover, Technologies, Community, Support, Events, and New Announcement. The main content area features a large heading "SecureX threat response" and a sub-heading "Cisco's SecureX threat response is built upon a collection of APIs which, can be used to integrate your Cisco and third-party security products, automate the incident response process, and manage threat intelligence and security context data in a single location." Below this is a "Read the docs" button. At the bottom, there are three blog cards: "Harvesting Threat Intelligence with the SecureX Threat...", "SecureX Threat Response Ecosystem", and "Introduction to SecureX". A footer question asks "What can you do with SecureX threat response APIs?"

## DevNet learning labs

- [cs.co/CTR-API-labs](https://cs.co/CTR-API-labs)

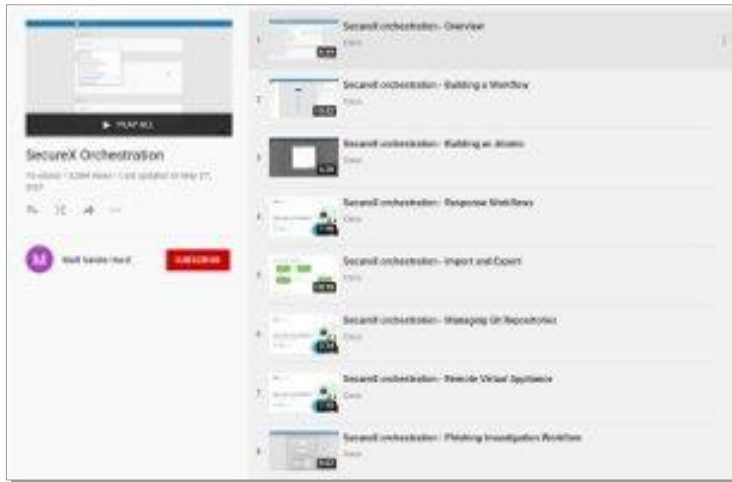


The screenshot shows the DevNet Learning Labs page for Threat Response. The header includes the DevNet logo and navigation links like DevNet Express, Tracks, Modules, Labs, Challenges, Help, Feedback, and a welcome message for Ben Greenbaum. The main content area features a large heading "Threat Response" and a sub-heading "In this module, you will learn the basic purpose and features of Cisco Threat Response, and then dig into the API that powers it all behind the scenes. Learn how to leverage the capabilities of this powerful investigative and response workflow, and how to incorporate them in an automated fashion into your SOC's existing tickets and workflows!" Below this is a "Choose a learning lab to start learning" section with two lab cards: "Introduction to Cisco Threat Response" (45 min) and "Introduction to Cisco Threat Response APIs" (120 min). The first lab card also shows a "Start Lab" button and a "Last Completed" timestamp of 10/11/2019 @ 10:42 AM.

# SecureX Orchestration resources

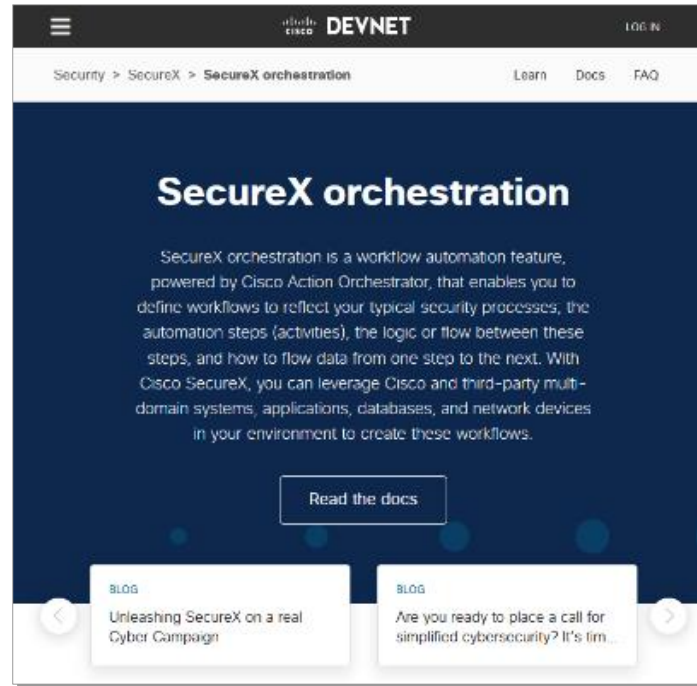
## Videos

[cs.co/SXO\\_videos](https://cs.co/SXO_videos)



## DevNet

[developer.cisco.com/securex/orchestration](https://developer.cisco.com/securex/orchestration)



## GitHub

[cs.co/SXO\\_docs](https://cs.co/SXO_docs)

