



# 雲端世代的資安新思維: Cisco Umbrella

鄭炤仁博士

華電聯網副總經理

September 27, 2019

# 思科是全球最大的資安廠商

**Top 5 Vendors, Worldwide Security Appliance Revenue, Market Share, and Growth, Second Quarter of 2018** (revenue in US\$ millions)

Vendor	2Q18 Revenue	2Q18 Market Share	2Q17 Revenue	2Q17 Market Share	2Q18/2Q17 Growth
1. Cisco	\$560.5	15.5%	\$450.2	14.6%	24.5%
2. Palo Alto Networks	\$521.5	14.4%	\$421.9	13.7%	23.6%
3. Fortinet*	\$388.3	10.7%	\$320.1	10.4%	21.3%
3. Check Point*	\$387.9	10.7%	\$381.1	12.3%	1.8%
5. Symantec	\$154.3	4.3%	\$157.4	5.1%	-2.0%
Other	\$1,601.2	44.3%	\$1,356.6	43.9%	18.0%
<b>Total</b>	<b>\$3,613.7</b>	<b>100.0%</b>	<b>\$3,087.4</b>	<b>100.0%</b>	<b>17.0%</b>

Source: IDC Worldwide Quarterly Security Appliance Tracker Q2 2018, September 11, 2018


# 思科是唯一獲Gartner評鑑同時在NGFW & NGIPS中居領導地位的資安廠商

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems



Source: Gartner (January 2018)

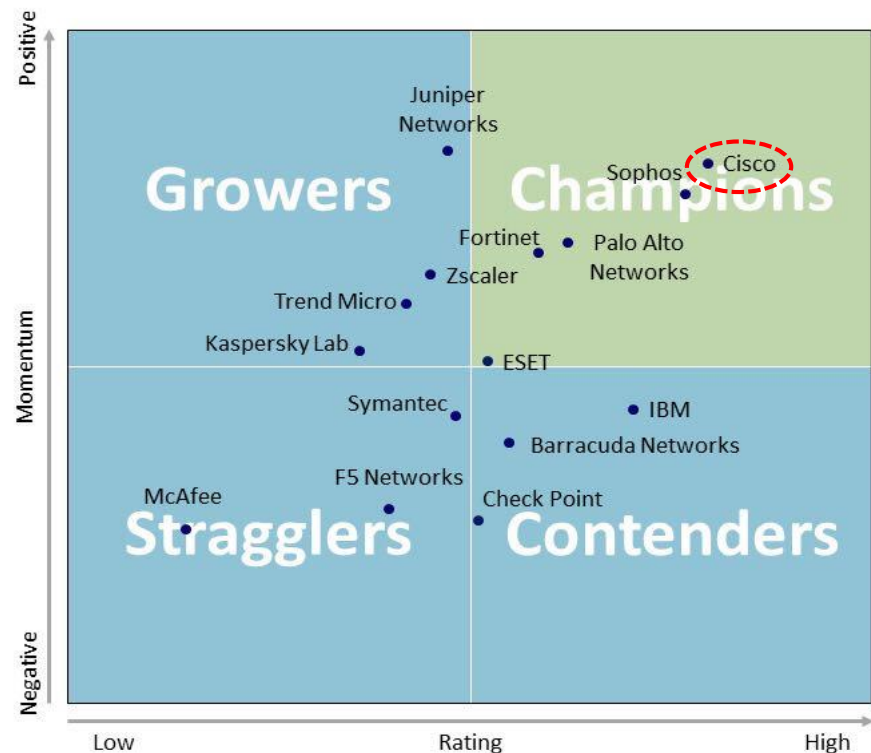
# IDC 報告 - 2019年台灣ICT市場十大趨勢預測

1. AI as the new UI
  2. 群體智慧 (Federated AI) 生態圈 = 個人智慧 + 集體反饋 + 機器學習
  3. 微服務架構與敏捷創新驅動 Service Mesh 需求崛起
  4. 雲端原生資訊技術 (Cloud Native IT) 全方位轉化
  5. Digital Twin 創造企業核心價值
  6. 新世代資安防禦思維, 「威脅生命週期管理 (Threat Life-Cycle Management)」實現主動防護
  7. FoW (Future of Work) 加速創新
  8. 列印加值服務 (Print-as-a-service) 將加速企業在工作流程中數位轉型
  9. 從人工智能到環境智能
  10. 5G時代來臨, 垂直市場新應用為電信業者未來佈局重點
- 

企業面臨更嚴苛的資料保護挑戰, 在資安防禦心態上, 從被動轉為主動, 從資安事件發生前、後, 包括進階資安測試、威脅情報、事件回應演練、網路安全訓練等「威脅生命週期管理 (Threat Life-Cycle Management)」服務, 將是新世代資安防禦的思維。

# Canalys: Five “Champion” vendors lead the Cybersecurity Leadership Matrix 2019

Global Cybersecurity Leadership Matrix – May 2019

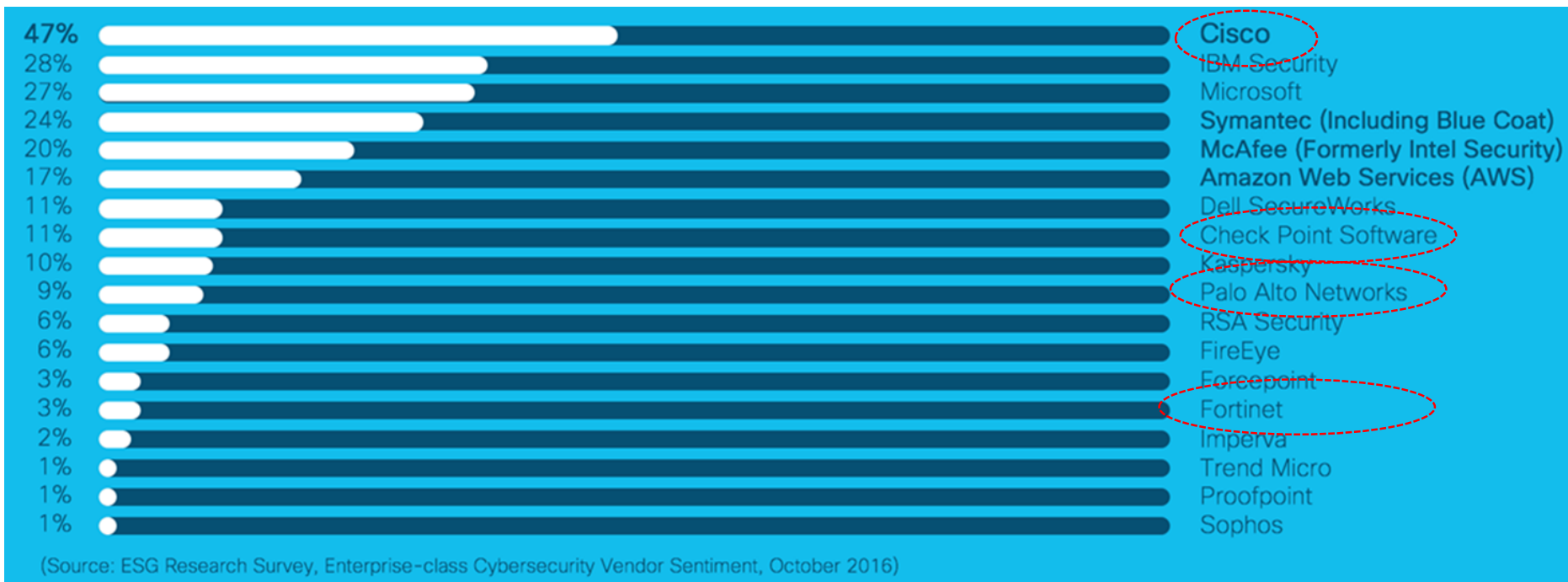


- Canalys的分析側重於五個安全領域：端點安全，網絡安全，數據安全，漏洞和安全分析以及Web和電子郵件安全。
- 思科提供了自動化執行策略，威脅檢測和威脅回應的能力而為客戶帶來更大的價值...
- 沒有一家安全公司能夠像思科那樣提供廣泛安全解決方案需要強大的解決方案涵蓋先前所提的客戶關注的五個安全領域的範圍的安全產品組合。
- 這15家中我們選出五家為領導廠商，然而我們很高興地宣布思科被公認為評選冠軍的廠商...

<https://www.canalys.com/newsroom/canalys-five-champion-vendors-lead-the-cybersecurity-leadership-matrix-2019>

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# ESG Research – Enterprise class CyberSecurity – 威脅情資資料庫排名



# 思科安全威脅資料中心-Talos

## TALOS

### 威脅情報

1.5 million 每天惡意擋樣本量

600 billion 每天郵件消息

16 billion 每天web請求

100 billion 每天DNS請求

### 安全覆蓋面



終端

WWW

Web



網路



入侵防禦



設備

### 研究回應中心



250+  
研究員



24 x 7 x 365  
運行

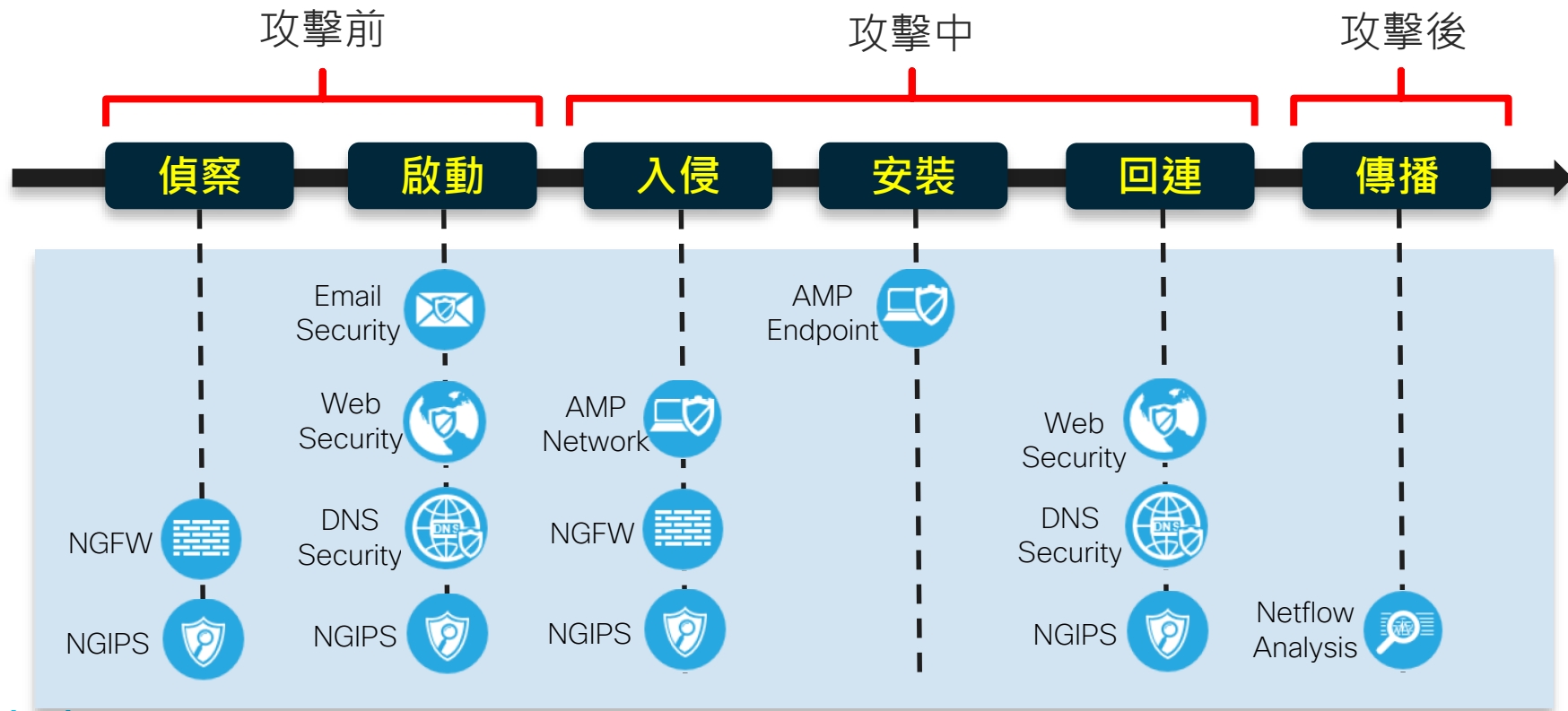
標識高級威脅

獲得威脅資訊

捕捉隱含威脅

即時威脅更新防禦

# 思科是唯一在攻擊前中後三個面向都能有效防治的資安供應商

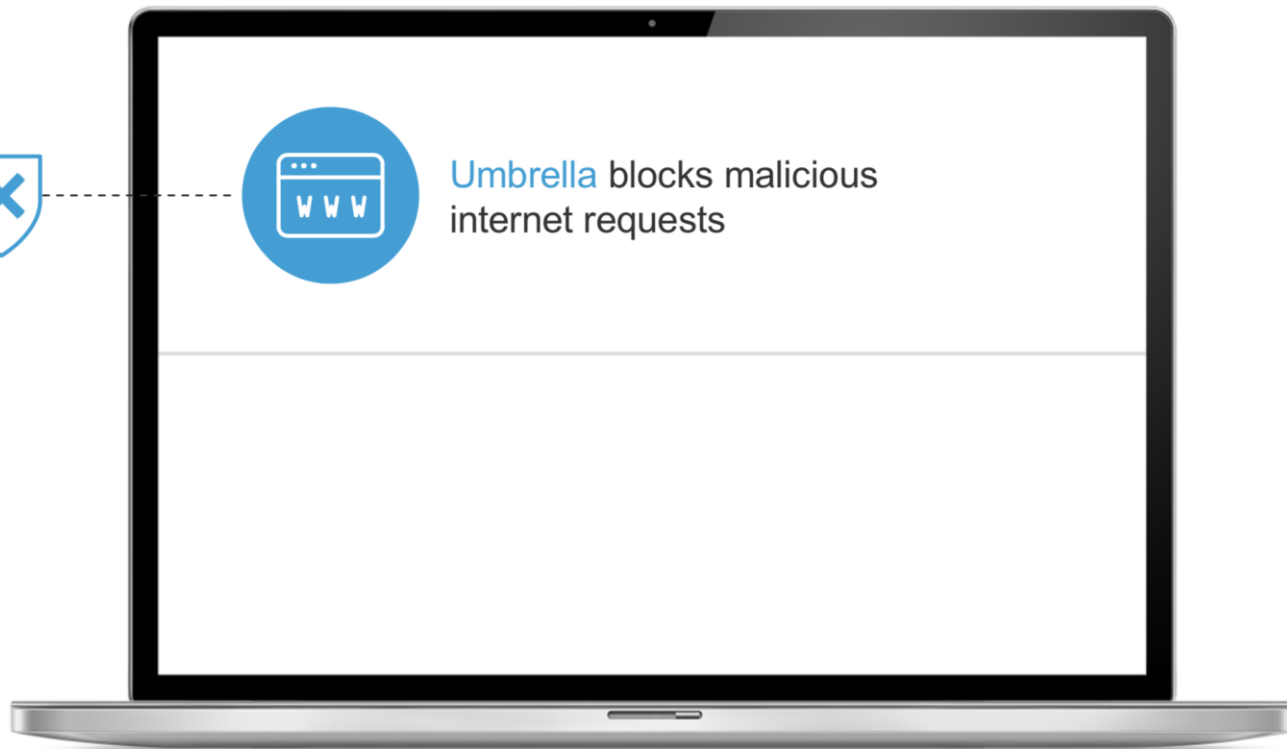




# 預防



Umbrella blocks malicious internet requests

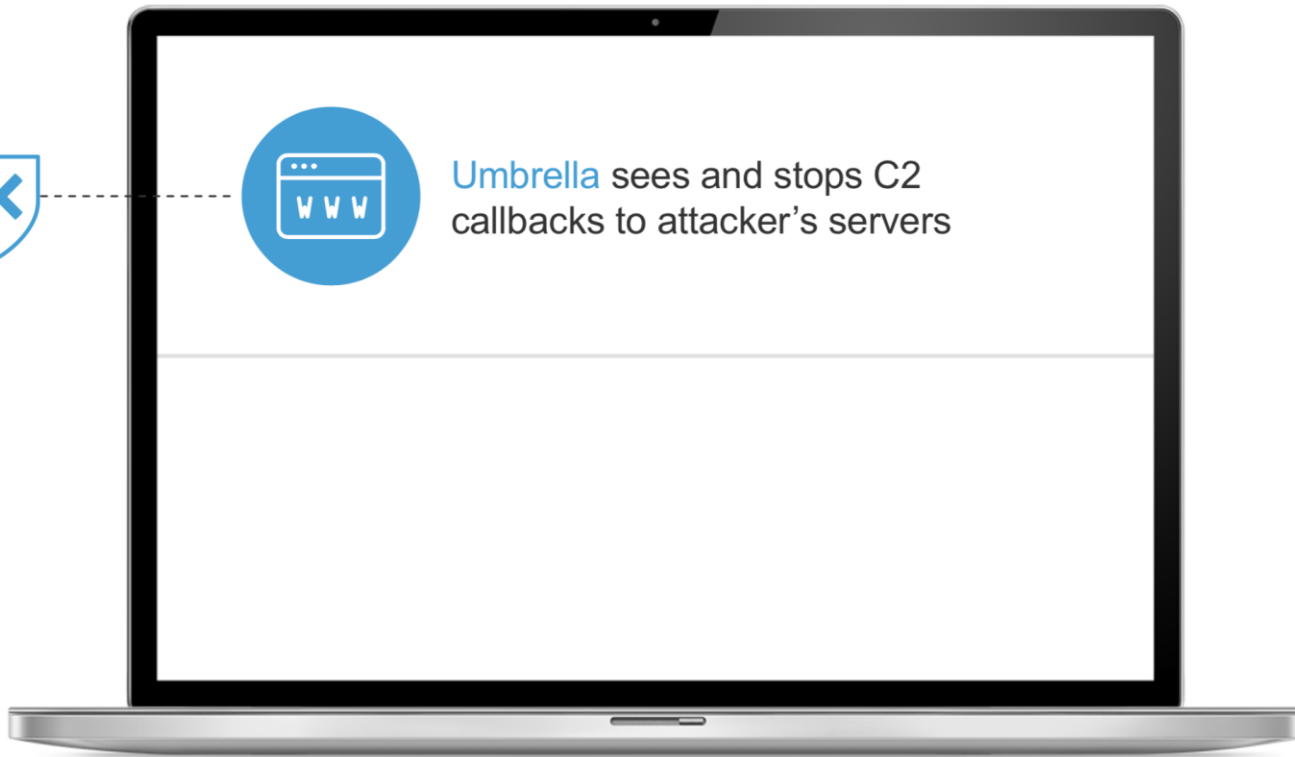


User endpoint

# 偵測



Umbrella sees and stops C2  
callbacks to attacker's servers

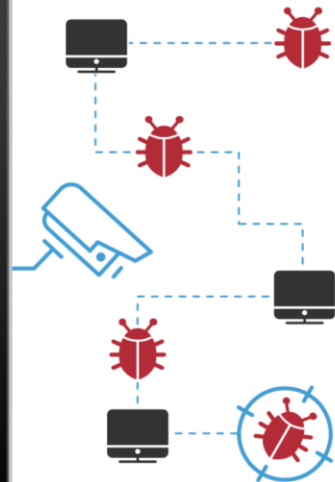


User endpoint

# 回應



Umbrella Investigate provides current and historical data on domains, IPs, and file hashes



Security team

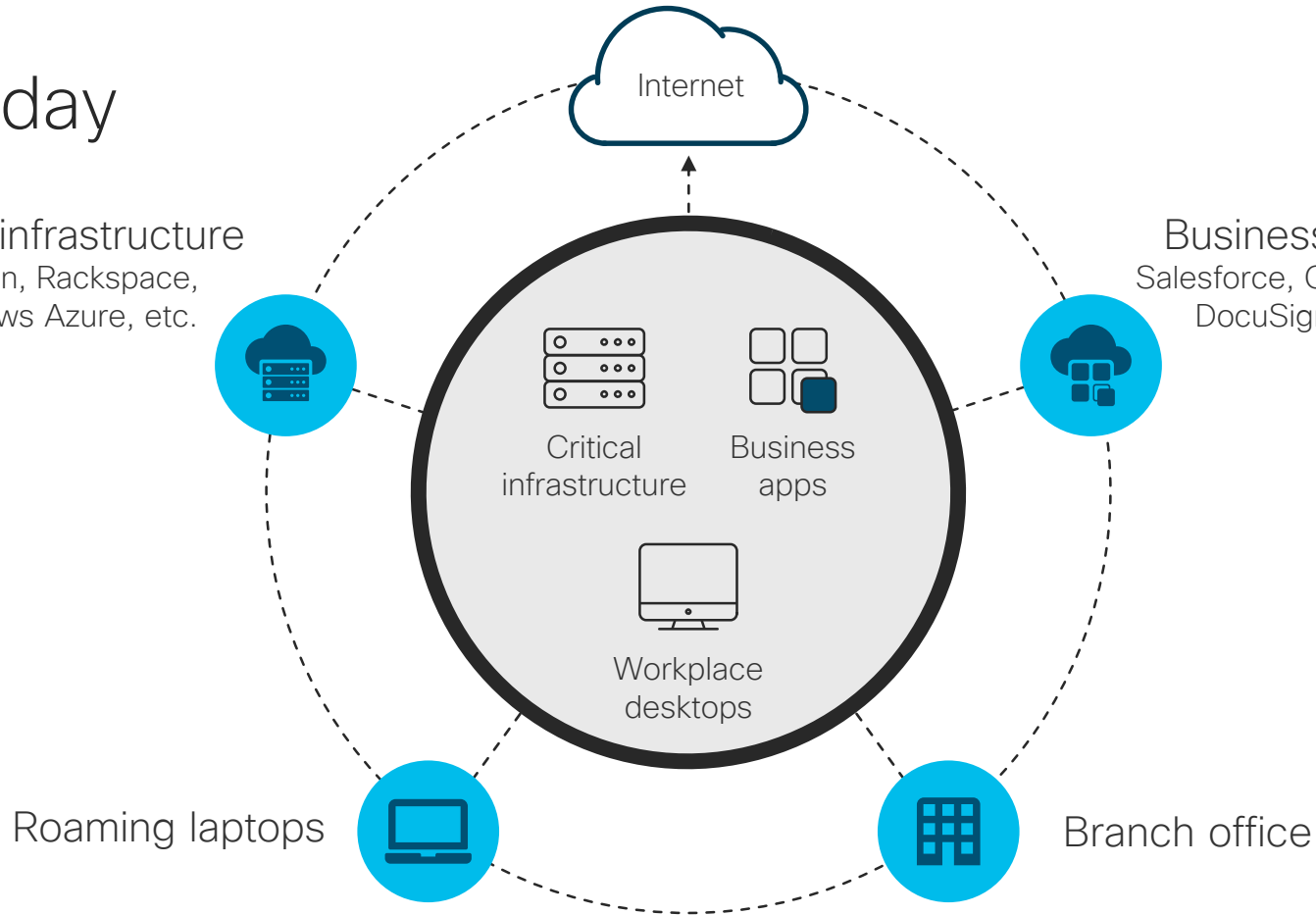
.. ..

# IT today

## Critical infrastructure

Amazon, Rackspace,  
Windows Azure, etc.

Business apps  
Salesforce, Office 365,  
DocuSign, etc.



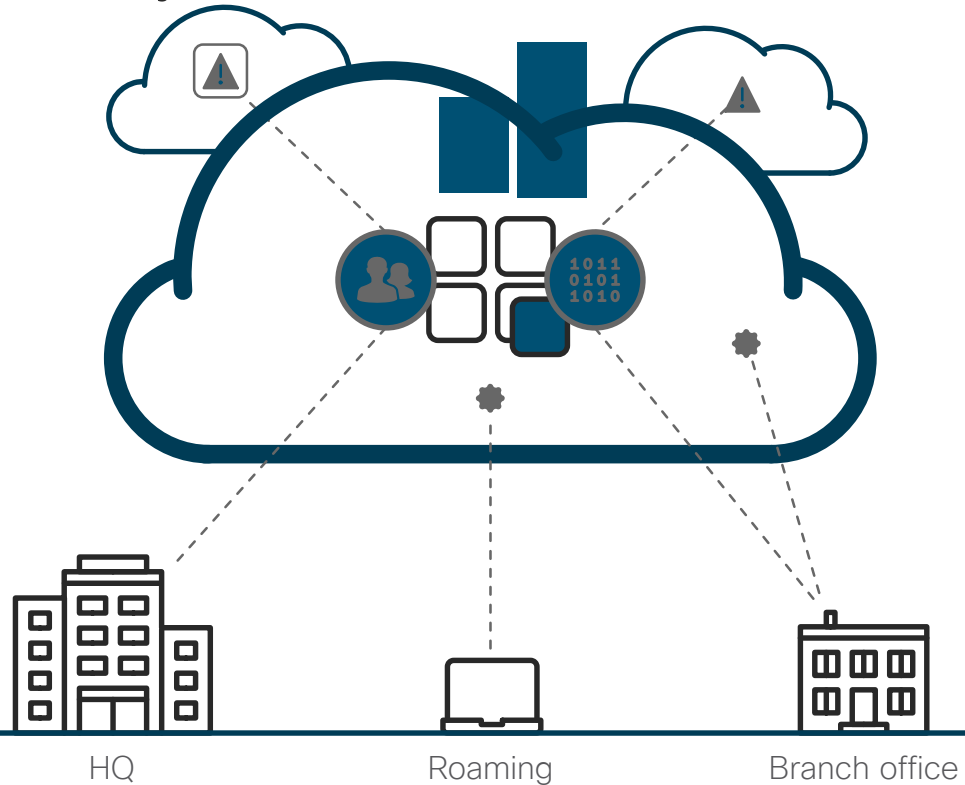
# How risk is different today

Users not protected by traditional security stack

Gaps in visibility and coverage

Expose sensitive info (inadvertently or maliciously)

Users can install and use risky apps on their own





# What is Umbrella?



## Umbrella

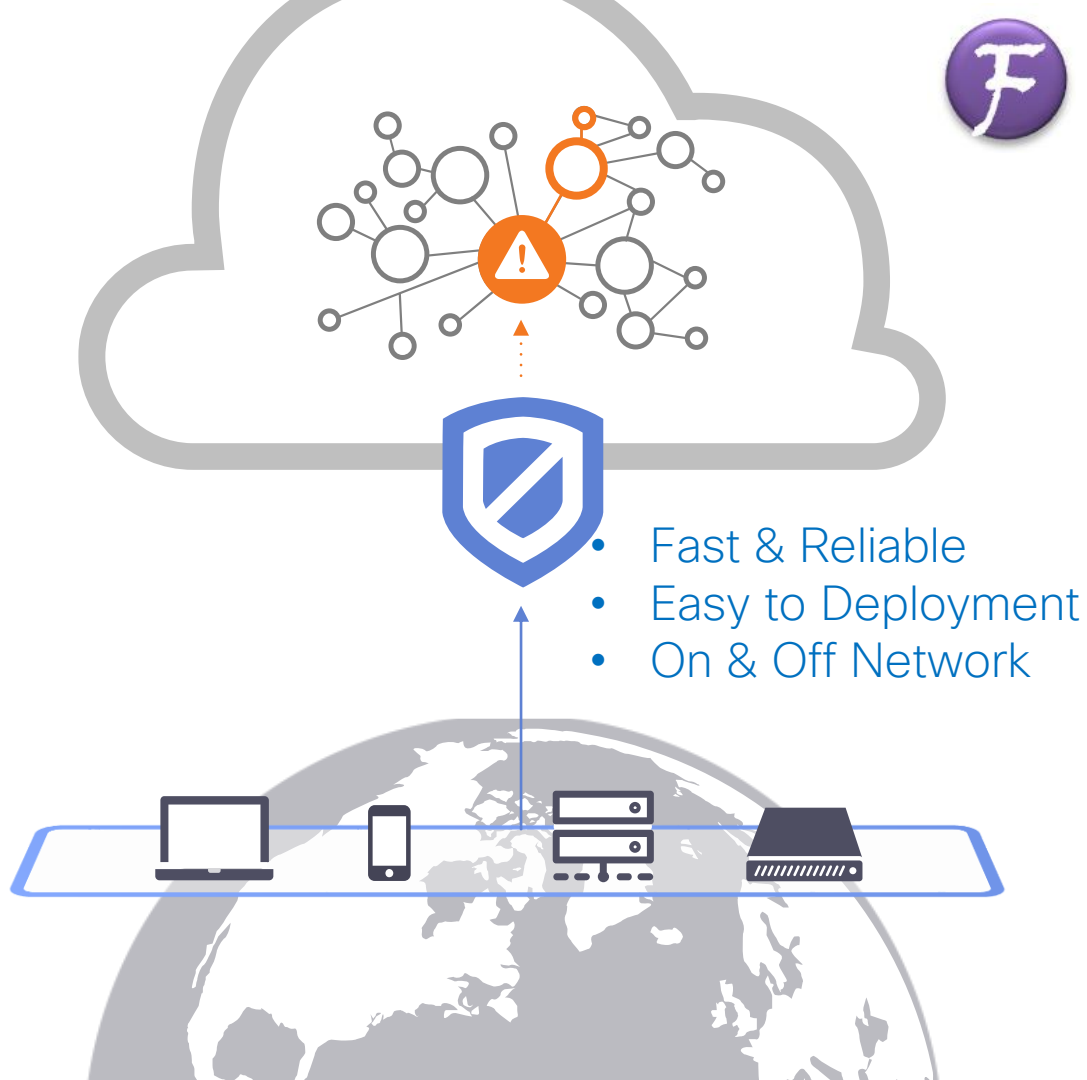
### Investigate & intelligence

Insight into the Internet infrastructure use for attacks and uncovers current and future malicious places

### Enforcement

Enforce security at the DNS & IP layers

Block malware, phishing, & C2 callbacks

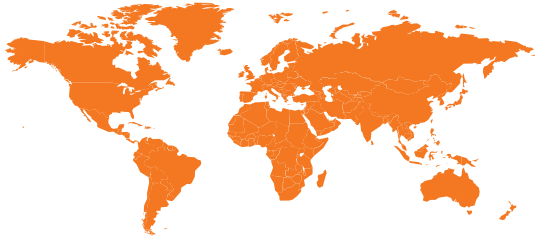


# From OpenDNS to Umbrella

DNS Service Built for World's Largest Security Platform

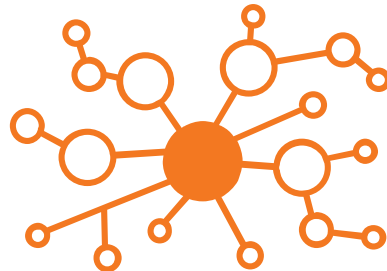
## GLOBAL NETWORK

- 70B+ DNS requests/day
- 65M+ biz & home users
- 100% uptime
- Any port, protocol, app



## UNIQUE ANALYTICS

- security research team
- automated classification
- BGP peer relationships
- 3D visualization engine



80M+

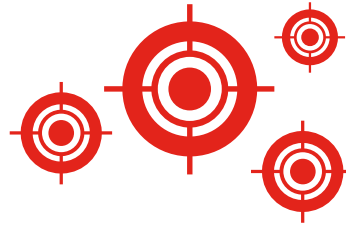
malicious requests  
blocked/day

# Common Security Challenges



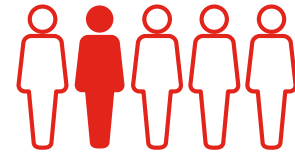
50% of PCs are Mobile  
70% of Offices go Direct

Most mobile & remote workers don't keep VPN always on, most branch offices don't backhaul traffic, and most new endpoint tools only detect



70-90% of Malware is Unique to Each Org

Signature-based tools, reactive threat intelligence, and isolated security enforcement cannot stay ahead of attacks



Shortage of Security Talent

Many tools require more resources than you have available to make work



# Umbrella Is Known For Two Things:

## 1. An incredibly powerful cloud delivery model for security.

- Recreating the benefits of a traditional network perimeter without appliances.
- Providing visibility, enforcement, audit, and compliance.
- Simple to deploy, easy to manage, security that doesn't sacrifice performance.

## 2. Identifying and blocking threats other vendors miss.

- Security Graph technology enables proactive security protection.
- Adding unique context to security intelligence and incident response.

# Intelligence

## Co-occurrence model

Identifies other domains looked up in rapid succession of a given domain

## Natural language processing model

Detect domain names that spoof terms and brands

2M+ live events per second

11B+ historical events

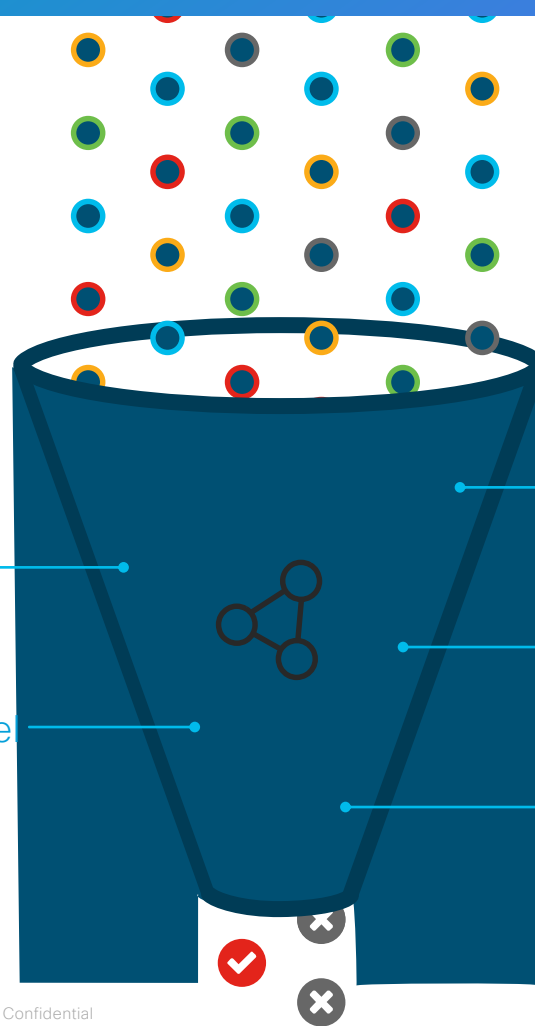
## Spike rank model

Detect domains with sudden spikes in traffic

## Predictive IP space monitoring

Analyzes how servers are hosted to detect future malicious domains

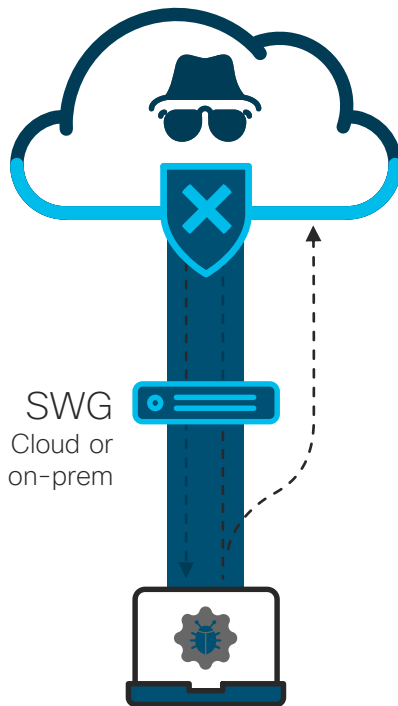
## Dozens more models



# Protection for command and control (C2) callbacks

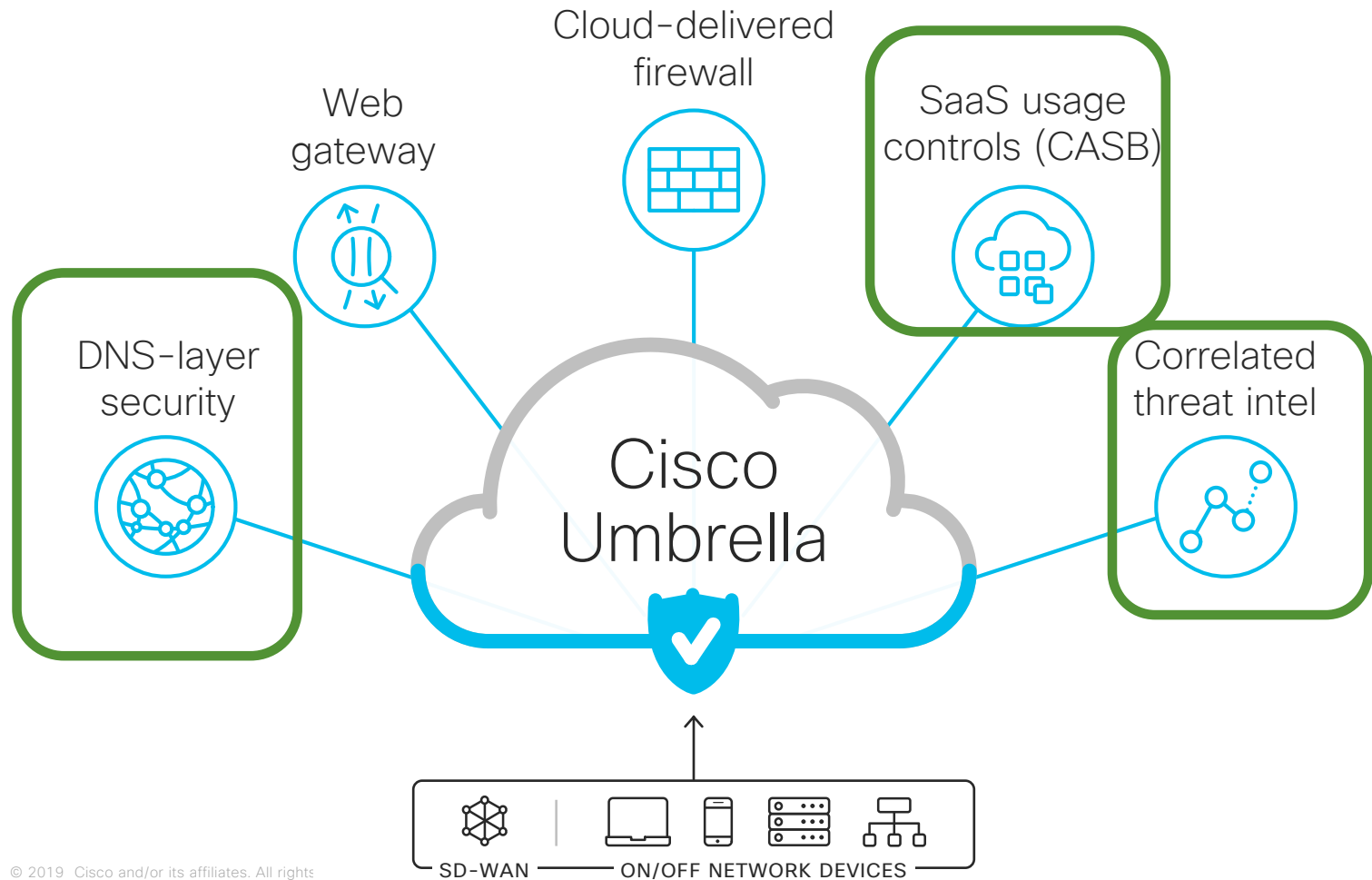
91%

of C2 can be blocked  
at the DNS layer



15%

of C2 bypasses  
web ports 80 &  
443



Allowed, blocked, and proxied  
traffic per device or network

## IDENTITY REPORTS

Quickly spot and  
remediate  
victims

Top activity and  
categories  
per device or network

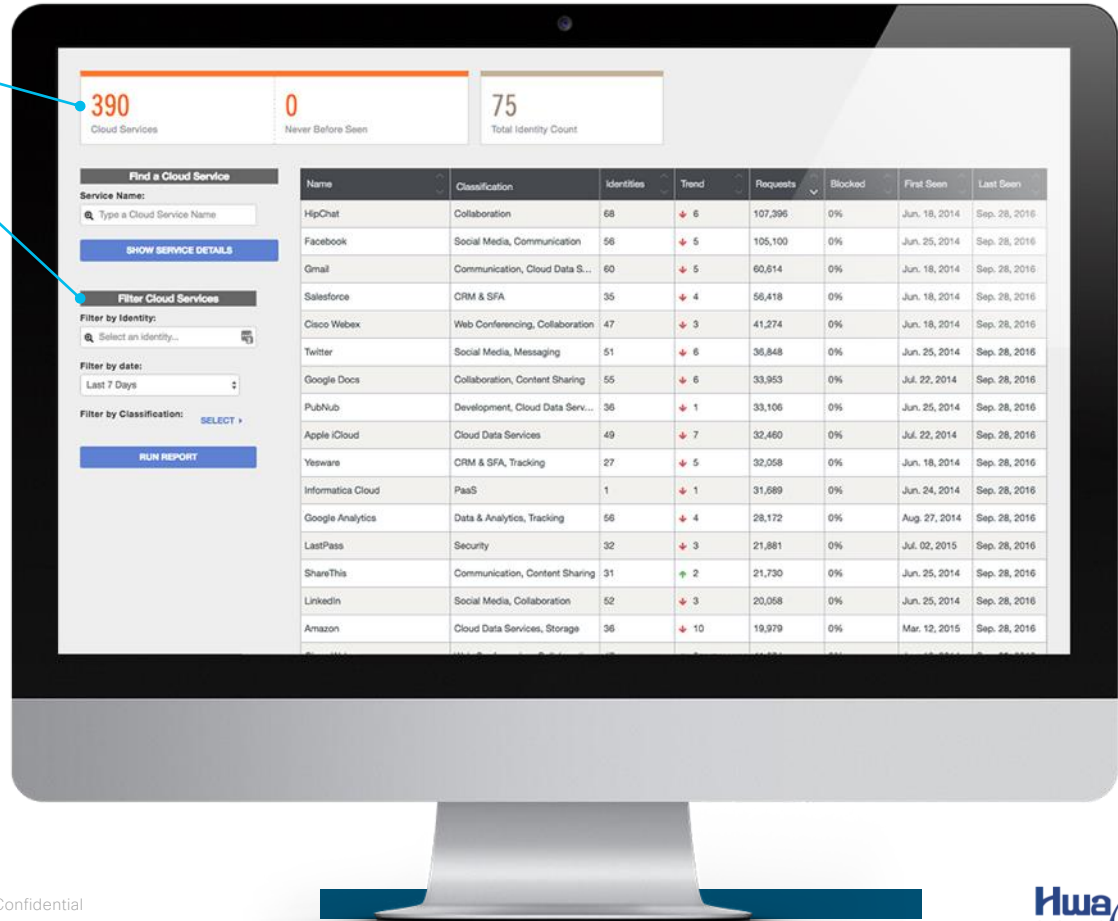


Total and newly seen  
cloud services

Cloud apps by classification  
and traffic volume

## CLOUD SERVICES REPORT

# Effectively combat shadow IT



# Updated Package - DNS Monitoring

## Provides....

- Real-time visibility  
Insight into events, including the occurrence of threats such as malware, ransomware, and phishing
- Fast and Reliable Recursive DNS

## Enhancements:

- Re-branded UI
- On-boarding wizard
- Network Devices API

## Reporting:

- Security Overview
- Security Activity
- Activity Search
- Total Requests
- Activity Volume
- Top Domains
- Top Categories
- Top Identities



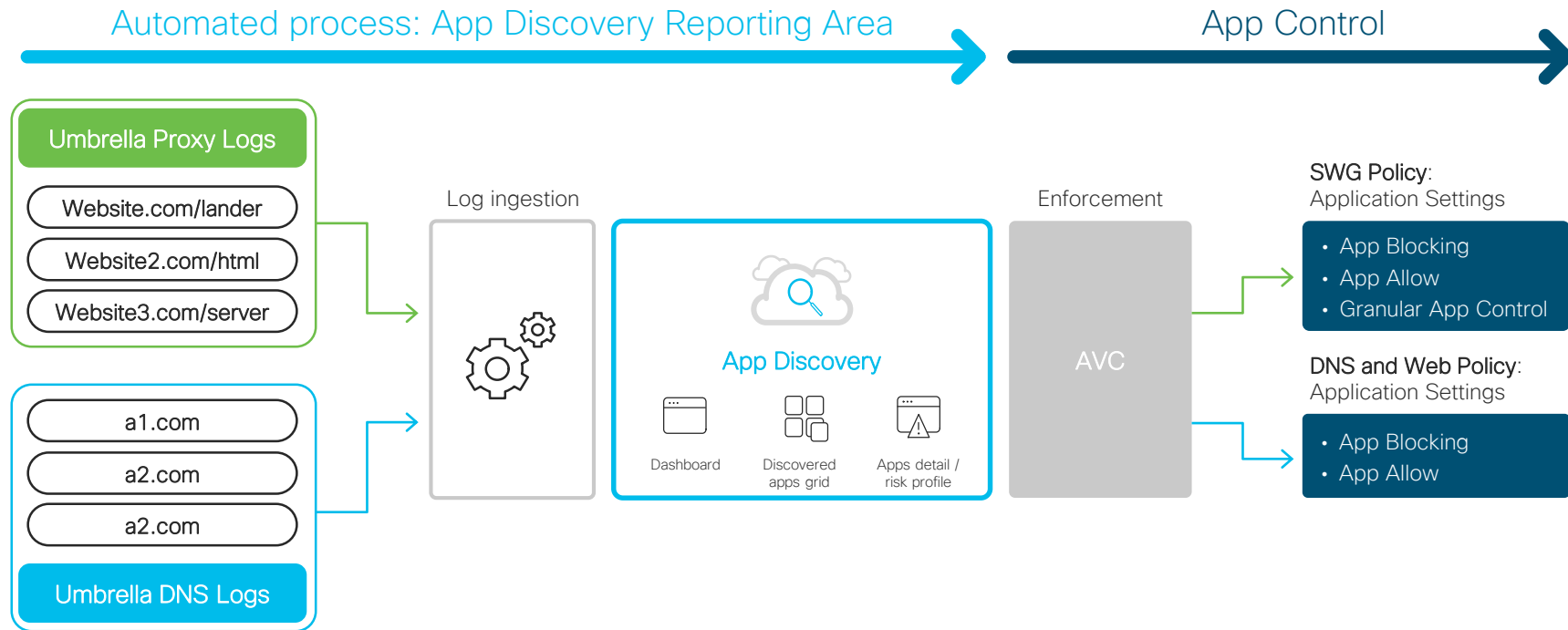
No Blocking

## How does a customer get DNS Monitoring?

- Sign-up on our website
- Automatically with DNA packages
- Post free-trial/POV

<https://dnsmonitoring.umbrella.com/>

# Umbrella App Discovery and Blocking

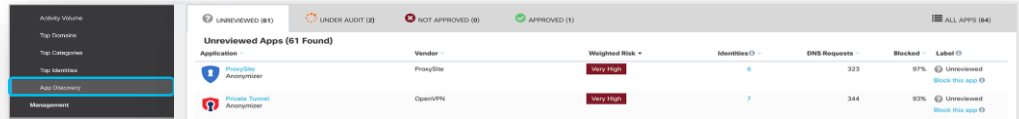




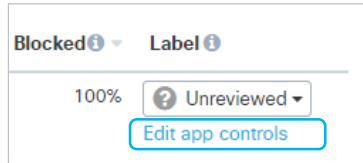
# App Discovery Update

### App Blocking – Enhanced Workflow

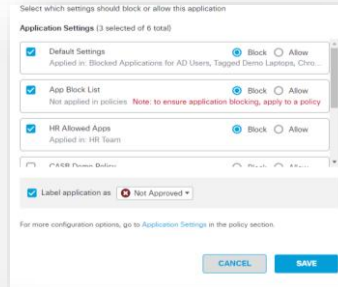
#### 1 Identify apps in App Discovery



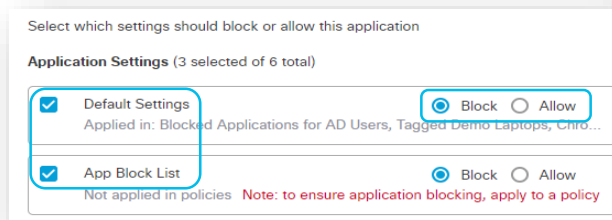
#### 2 Select the “Edit app controls” link under the app



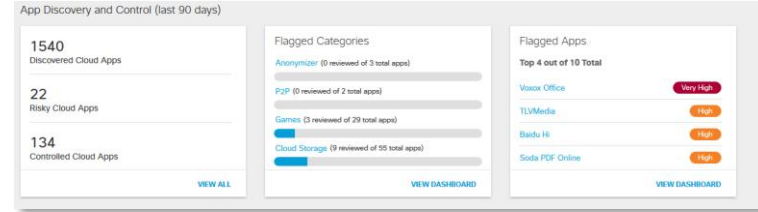
#### 3 Splash screen appears



#### 4 Apply Application Settings to appropriate Policy



### App Discovery now in the Overview page



App Discovery now part of the Overview page, includes:

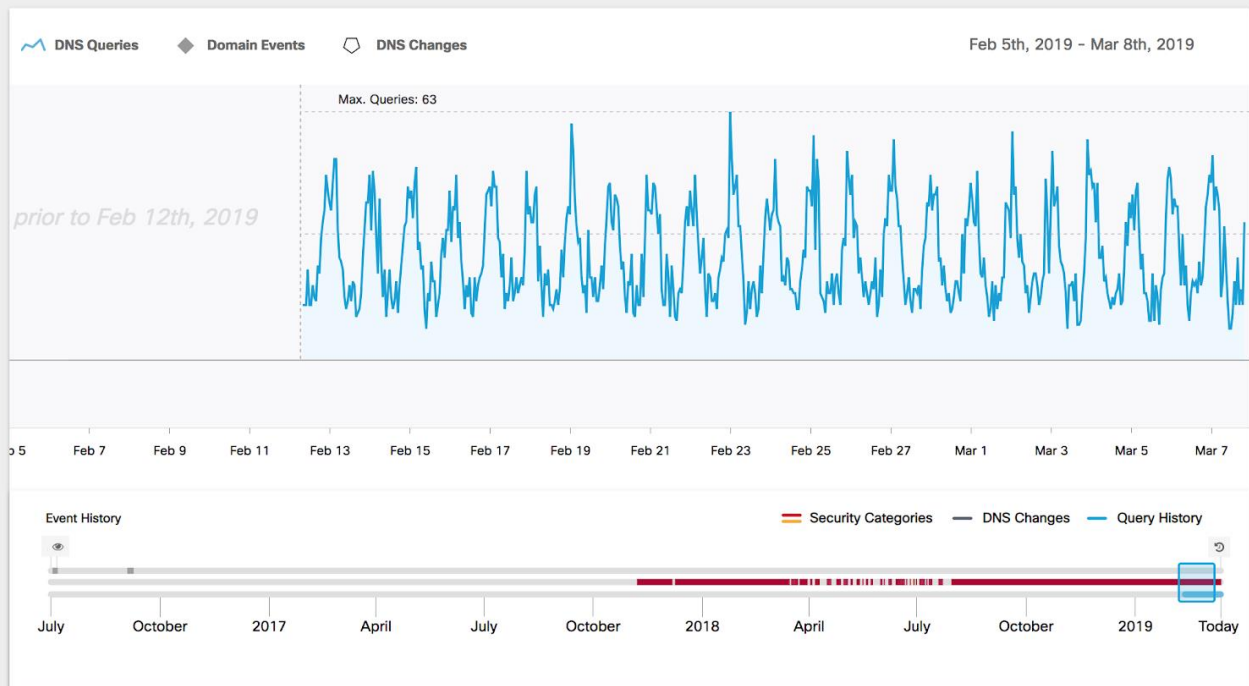
- Total discovered apps
- Number of Risky apps
- Number of apps controlled
- Flagged Categories
- Top Flagged apps

# Passive DNS in Investigate

INVESTIGATE

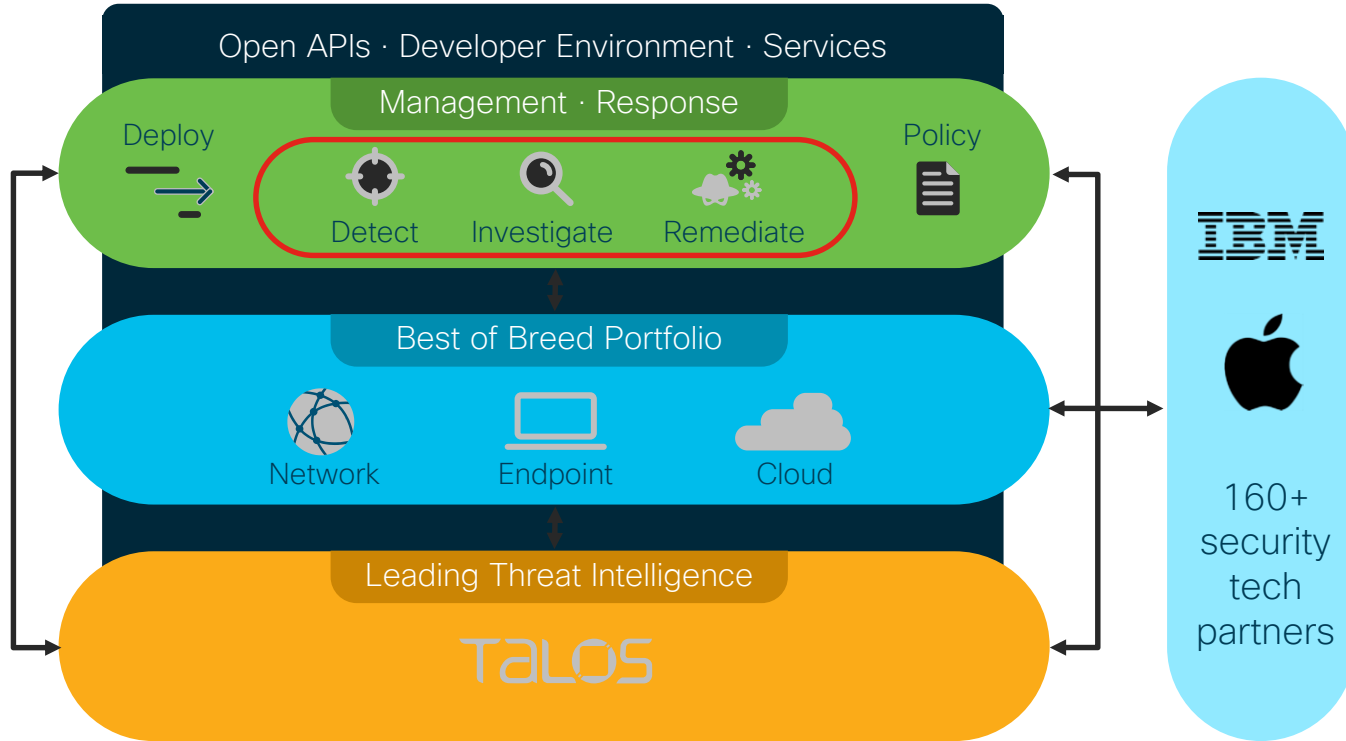
[BACK TO TOP](#)

## Timeline (Beta)

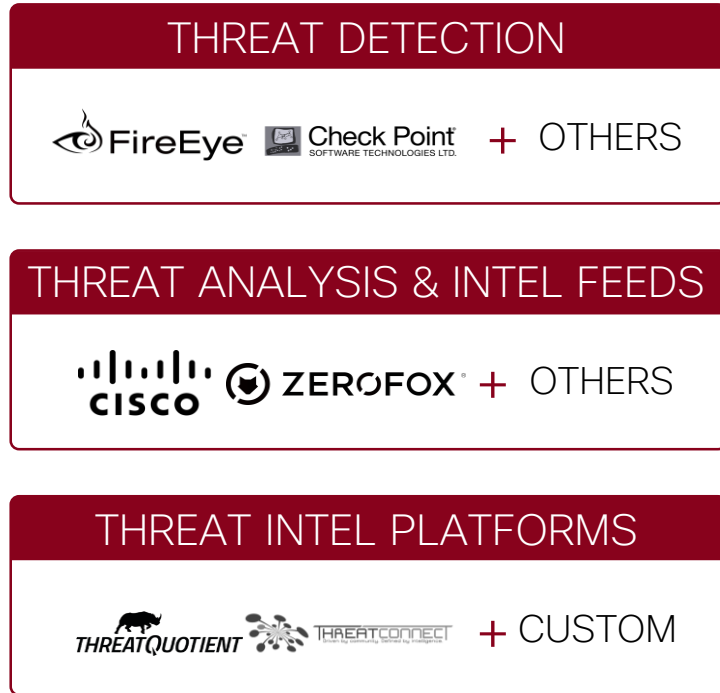


- What is Passive DNS? Historical database of DNS records
- Useful for threat hunters to go back in time to find missed compromises
- Further inspect the track record of a domain without tipping off bad actors that infrastructure they may still use is under suspicion
- Shows up to 4 years of history
- More than just DNS record values: Also includes security categorization history for a full sense of a domain's security history
- Will be included in all Investigate packages (including API)
- Full availability in a few weeks

# An integrated portfolio creates value for customers



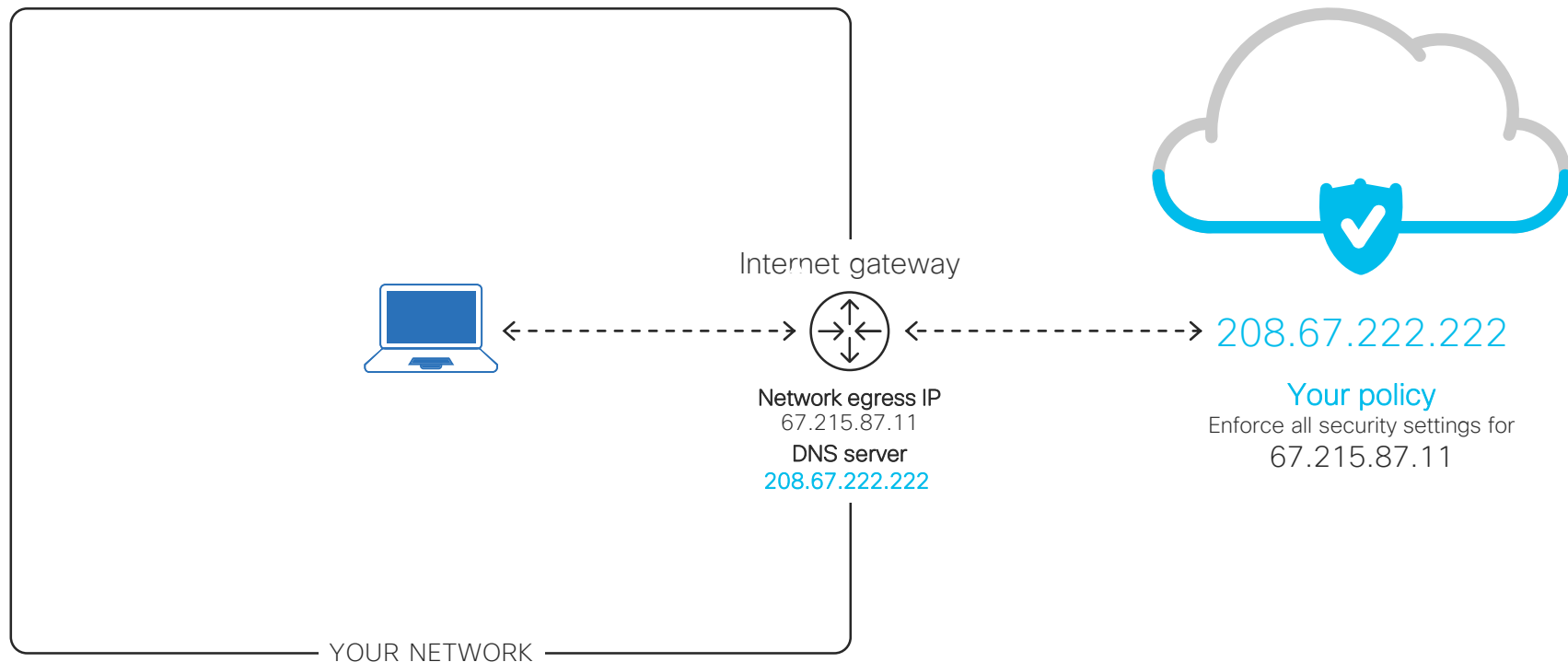
# Turn-Key and API-Based Integrations



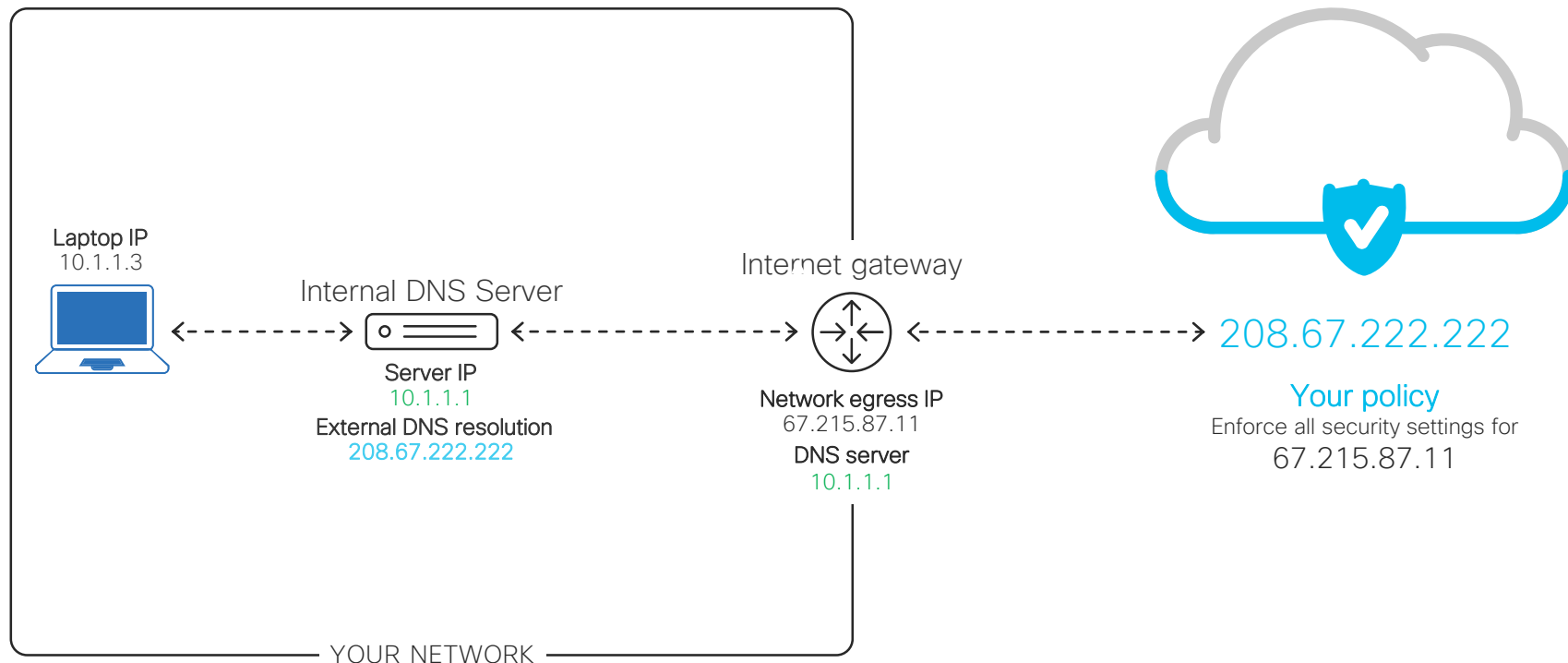
**UMBRELLA**  
Enforcement & Visibility  
Logs or blocks domains sent from partner or custom systems

# Umbrella的快速部署方式

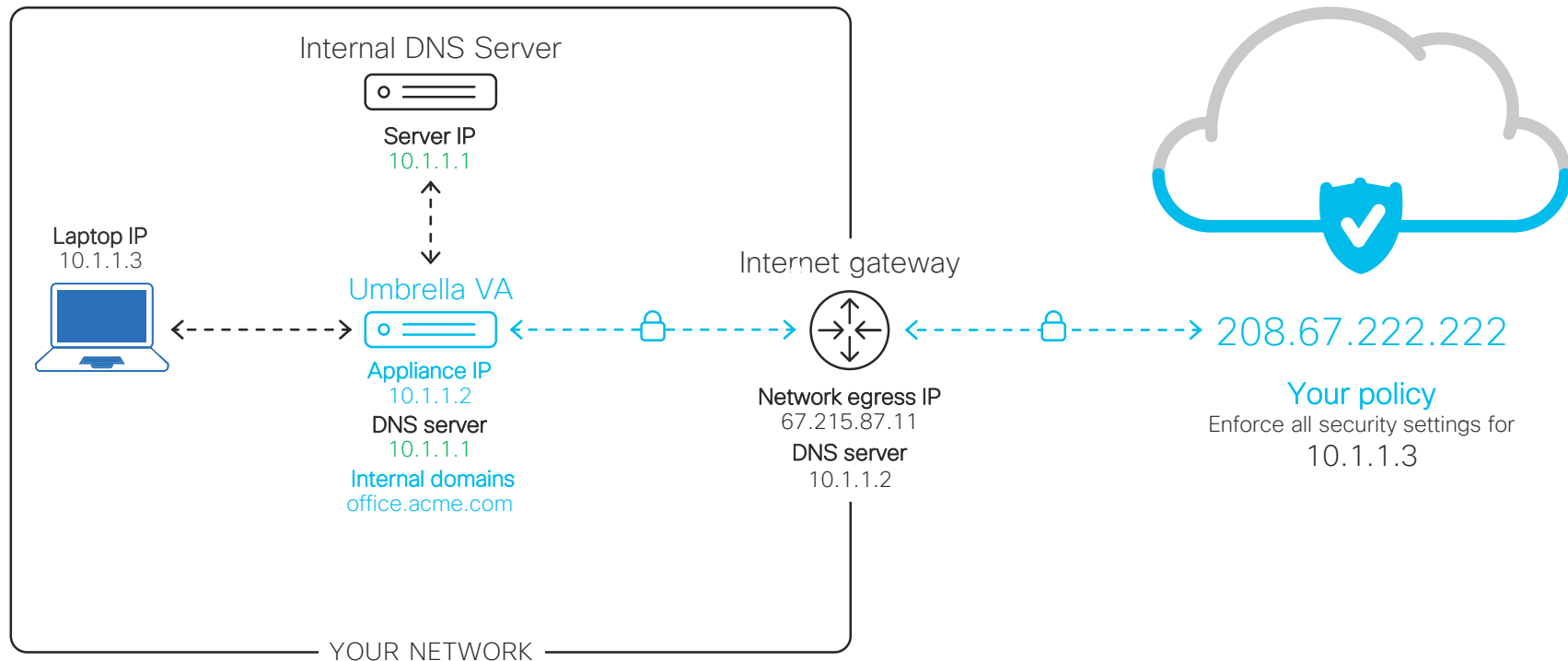
# Protect on-network devices via gateway's DHCP



# Protect on-network devices via DNS server

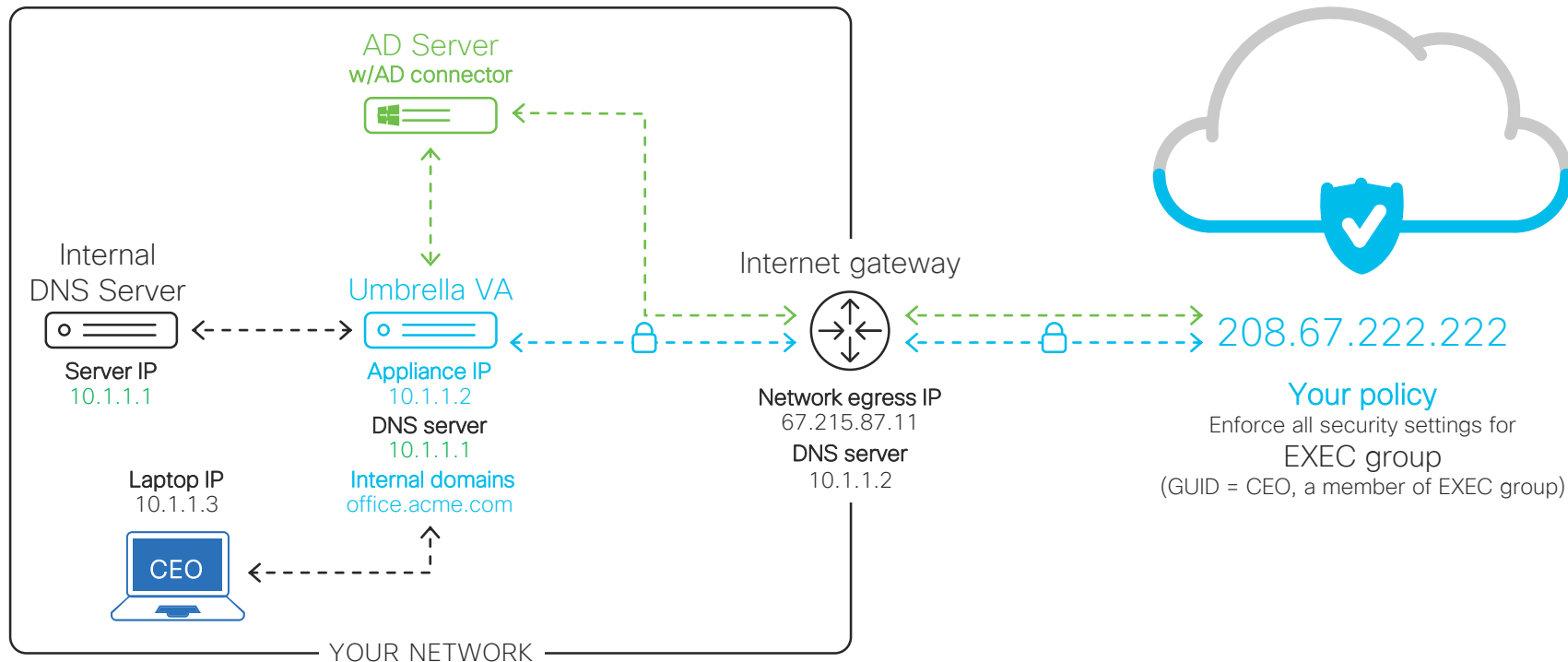


# Protect internal networks via Umbrella virtual appliance

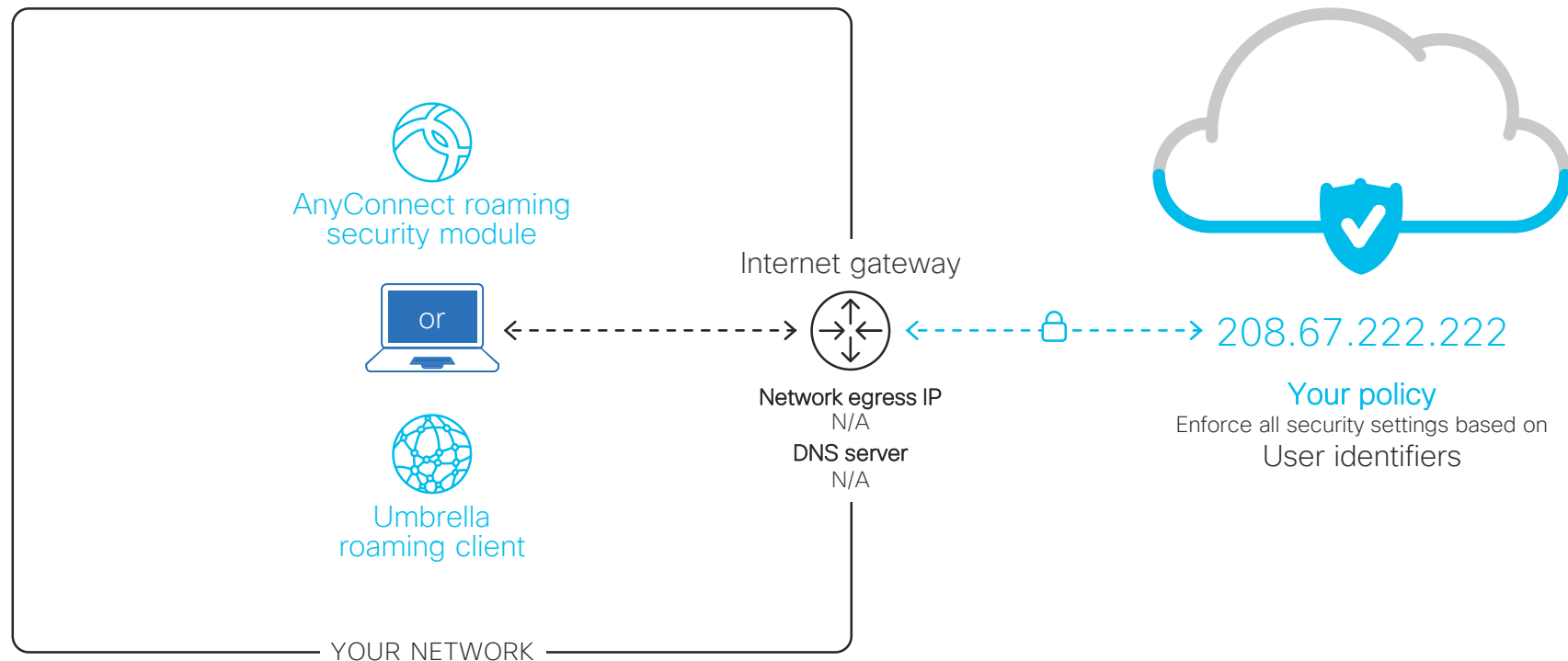




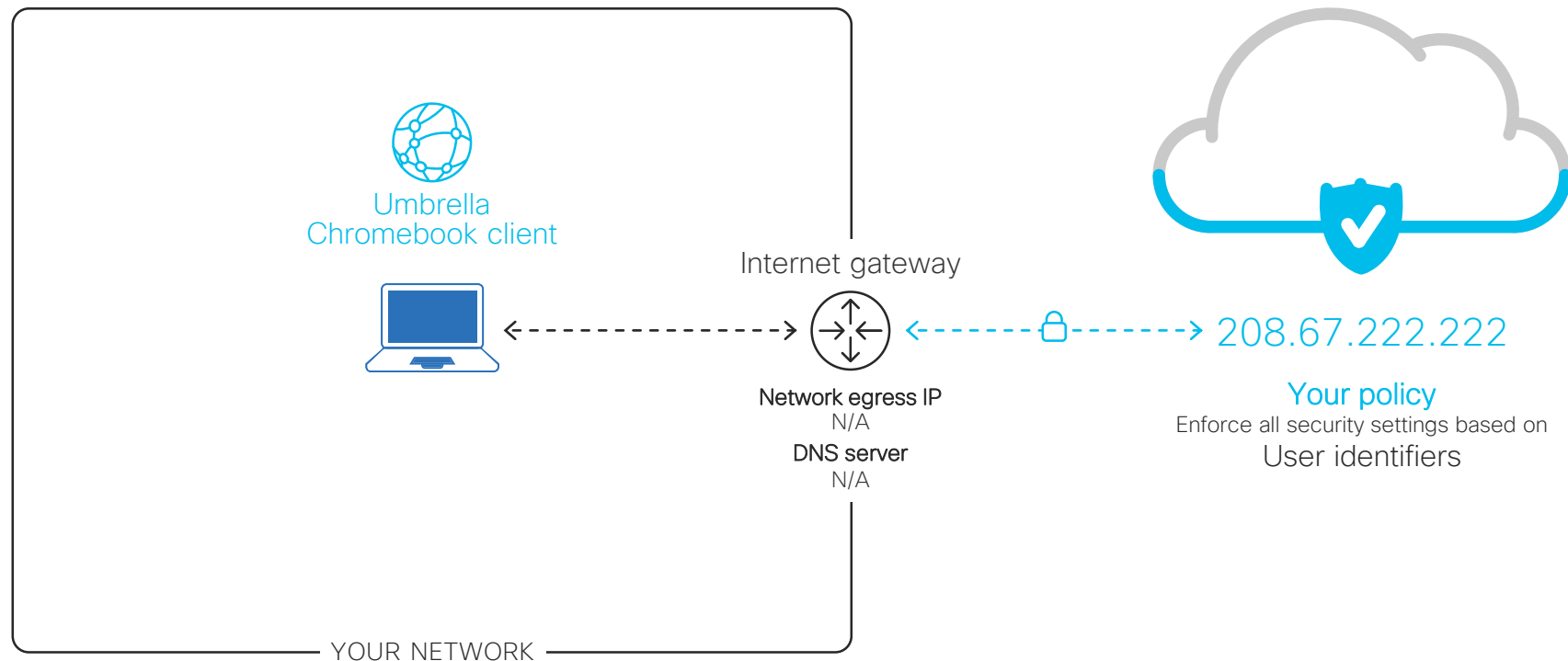
# Protect AD users via Connector and Umbrella virtual appliance



# Protect off-network Windows & macOS devices via AnyConnect or Umbrella roaming client



# Protect on and off-network Chromebook devices via Umbrella Chromebook client

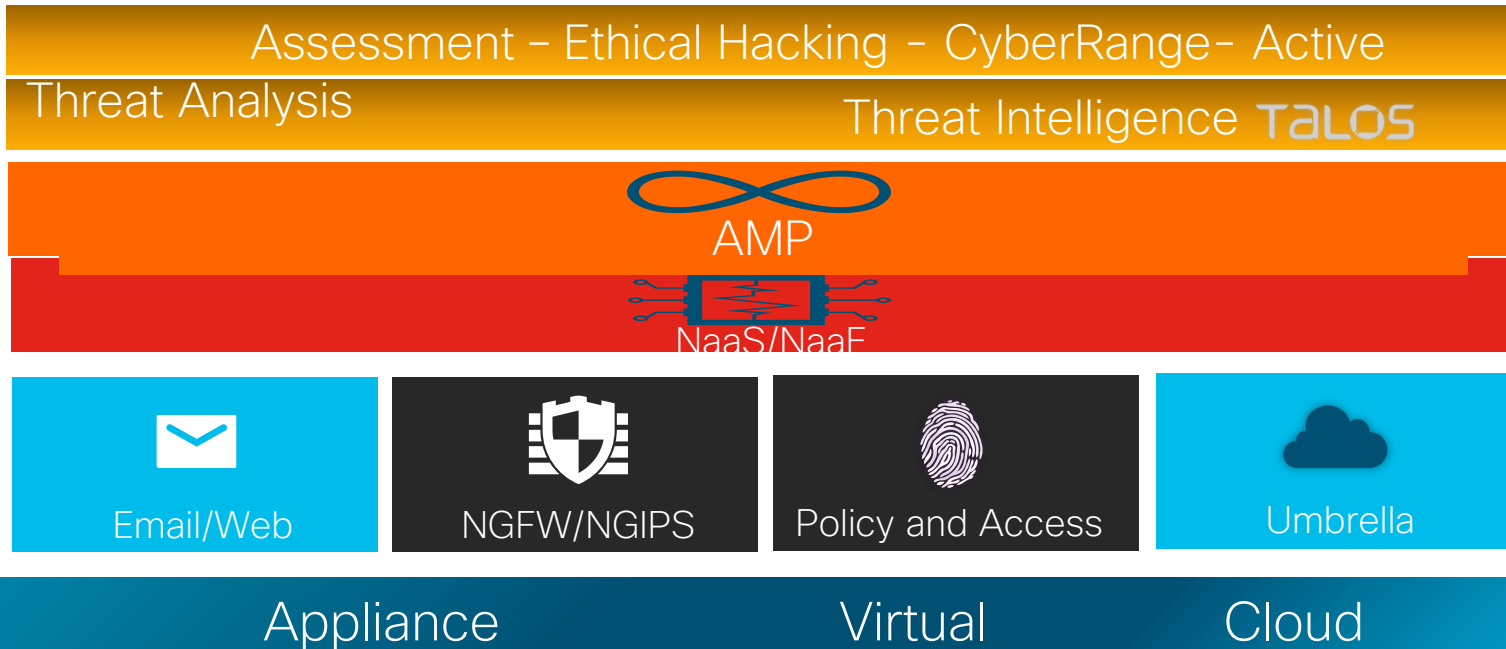


# Summary

# Cisco's Differentiation

## Best of Breed + Architectural Approach

### EcoSystem



# 思科的資安產品和方案



Firepower NGFW下一代防火牆  
和ESA郵件安全防護

識別用戶到用戶的C&C連接  
攔截含有惡意附件的郵件  
識別或改寫郵件的URL釣魚鏈接  
零日威脅爆發過濾  
整合AMP防護



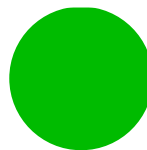
AMP高級惡意程式碼保護

利用雲智慧分析技術  
惡意程式碼一旦被發現後，則實現後續的檢測  
和攔截  
對已知的惡意文件攔截最有效



Umbrella與Web防護

防止惡意網站的DNS解析  
攔截超過95%的C&C域名解析請求  
URL信譽過濾攔截C&C網站訪問



StealthWatch(Lancope)

檢測和發現感染主機與C&C僵屍網路的通信  
對連接C&C的通信企圖進行告警  
借助網絡設備作為探針來發現和降低風險

# The Power of OpenDNS + Cisco

INTERNET

MALWARE  
BOTNETS/C2  
PHISHING

MID LAYER

LAST LAYER

FIRST LAYER

DNS LAYER

FIREPOWER // ●  
WSA (+ESA) /// ●  
LANCOPE /// ●



HQ

Mobile

Mobile

MID LAYER

MID LAYER

LAST LAYER

ASA



Branch

MERAKI



Branch

## BENEFITS

Alerts Reduced 2x;  
Improves your SIEM

Block malware before it  
hits the enterprise

Contains malware if  
already inside

Internet access is  
faster; Not slower

Provision globally in  
under 30 minutes



and/or its affiliates. All rights reserved.





# Top Ways to Add Umbrella to Your Security Stack

OFF-  
NETWORK  
SECURITY



Umbrella  
+  
ASA / AnyConnect

SECURE  
DIRECT-TO-  
NET OFFICES



Umbrella  
+  
ISR / Meraki

NEW LAYER OF  
PREDICTIVE  
SECURITY



Umbrella  
+  
AMP for Endpoints

AUTOMATE  
ENFORCEMENT &  
VISIBILITY



Umbrella  
+  
Threat Grid

SPEED UP  
INCIDENT  
RESPONSE



Investigate  
+  
Threat Grid



# Strong Adoption Amongst Global Enterprises

## TECH



## FINANCE



## MEDIA



## LEGAL



## HIGHER ED



## ENERGY



## RETAIL



## HEALTHCARE



## ENGR'ING



## MFG



第一線的雲  
防禦

快速建置

價格具競爭  
力

API協同資安  
整合

