CISCO
SECURE

The bridge to possible

Cisco Umbrella

The first line of defense: DNS-layer security

Emanuel Almeida
Technical Solutions Architect
October 2021

Agenda

- Challenges
- Umbrella DNS-layer security
  - Cloud Security Service
  - Enforcement
  - Threat Intelligence
- Deployment
- Reporting

Challenges

Often used, not often monitored

90%

Of malware use
DNS in attacks

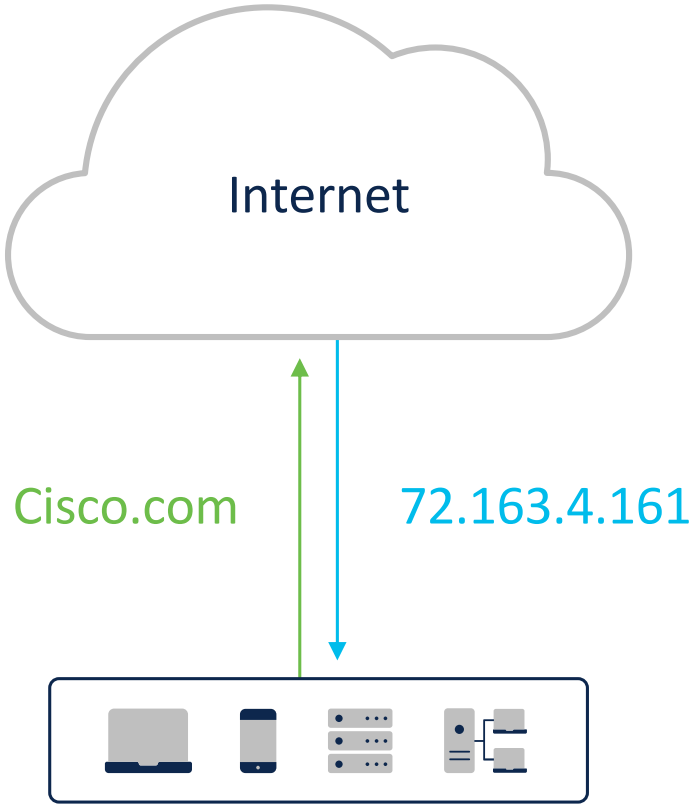
1 in 3

Reported breaches
could have been
controlled by DNS

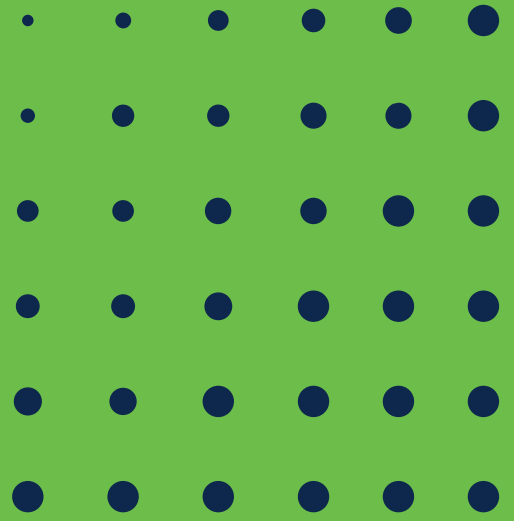
Source: Cisco Security Research Report

Why is DNS useful for security?

- First step in connecting to the internet
- Precedes file execution and IP connection
- Used by nearly all devices



Meet Cisco Umbrella



History

Founded
as a recursive DNS provider (OpenDNS)

2006

Launched
DNS-layer security offer (OpenDNS Umbrella)

2012

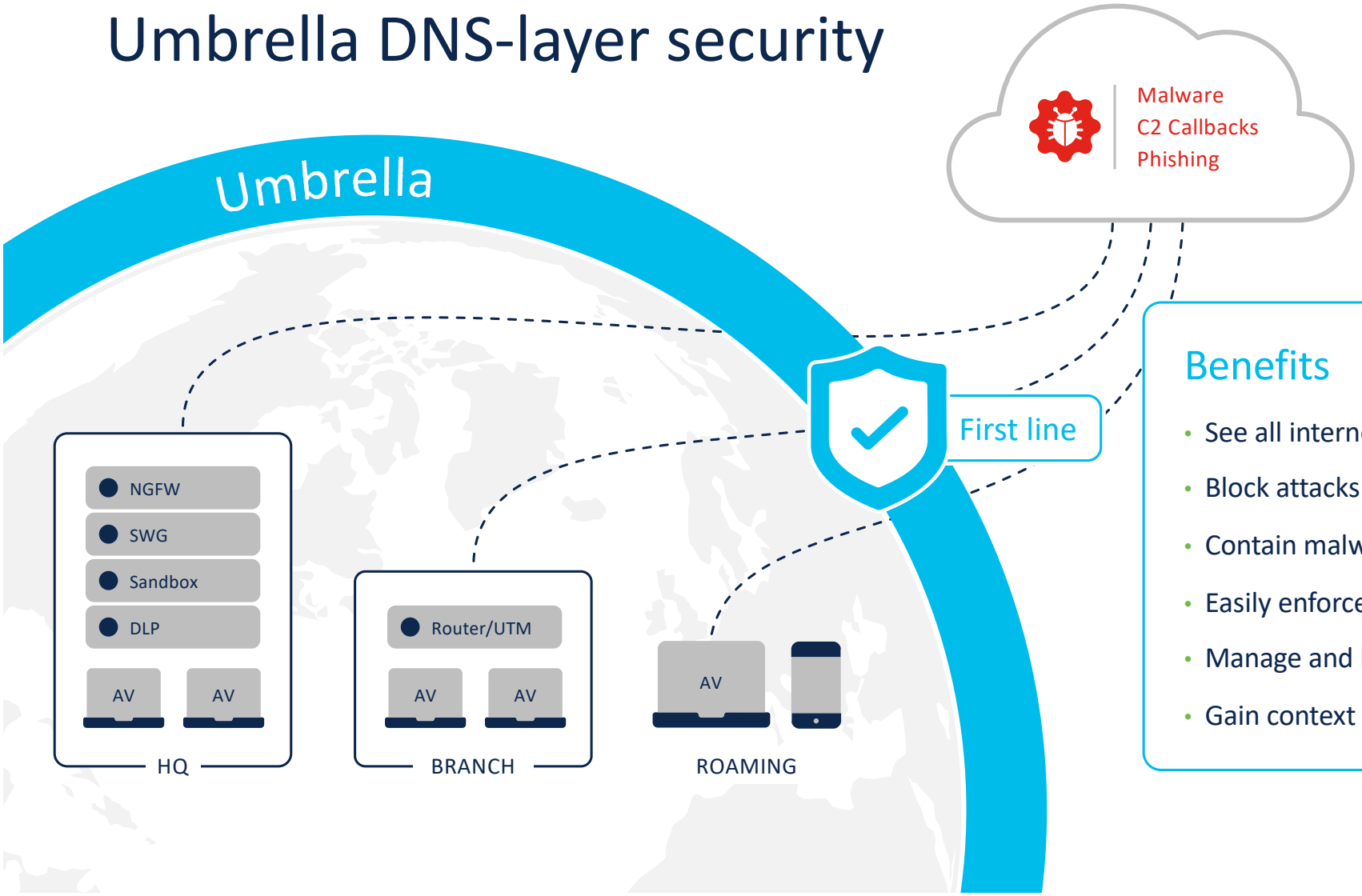
Acquired
by Cisco

2015

Expanded
to integrate more security services in single platform

2019

Umbrella DNS-layer security



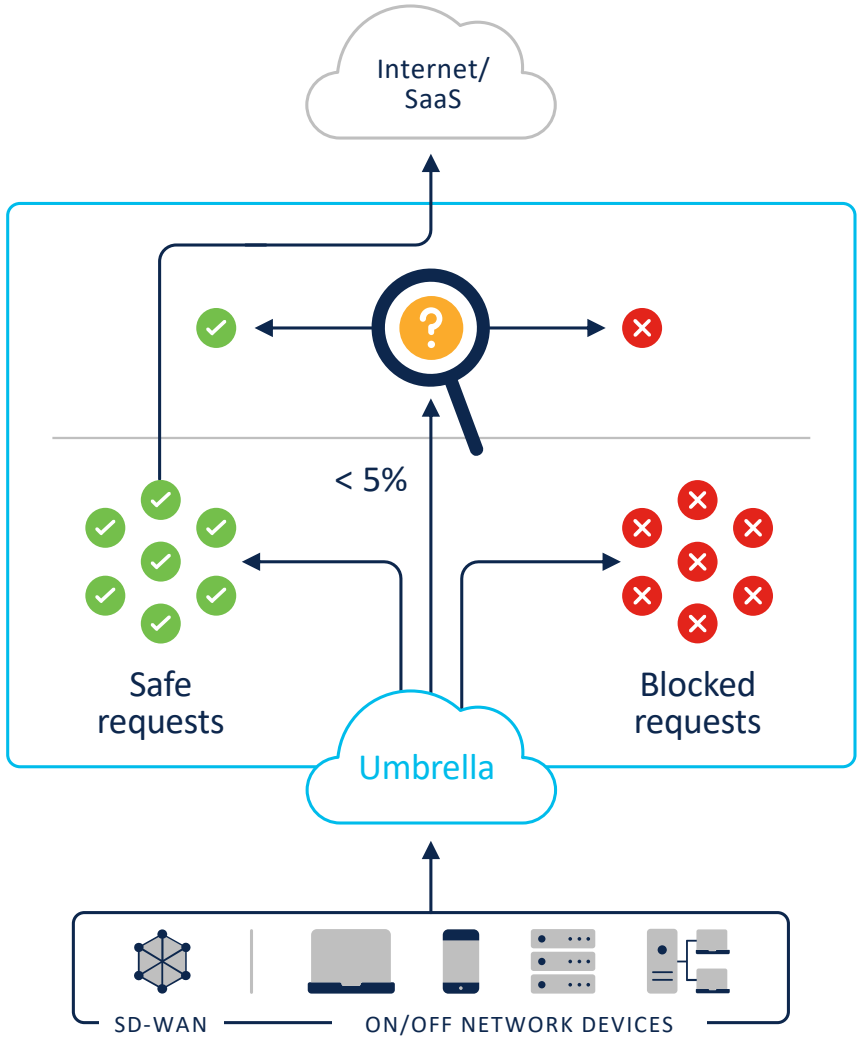
Benefits

- See all internet traffic across users
- Block attacks earlier
- Contain malware if already inside
- Easily enforce content web filtering
- Manage and block cloud apps
- Gain context for faster investigation

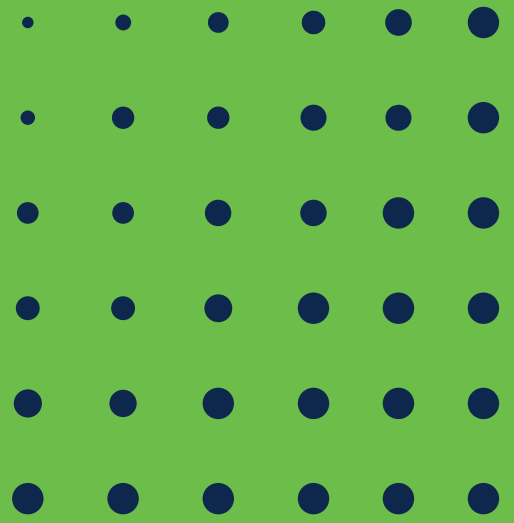
Umbrella DNS-layer security

First line of defense

- Block domains associated with malware, phishing, command and control callbacks anywhere
- Stop threats at the earliest point and contain malware if already inside
- Accelerate threat response with an integrated security platform
- Amazing user experience — faster internet access; only proxy risky domains



Cloud Security Service



Large, global footprint

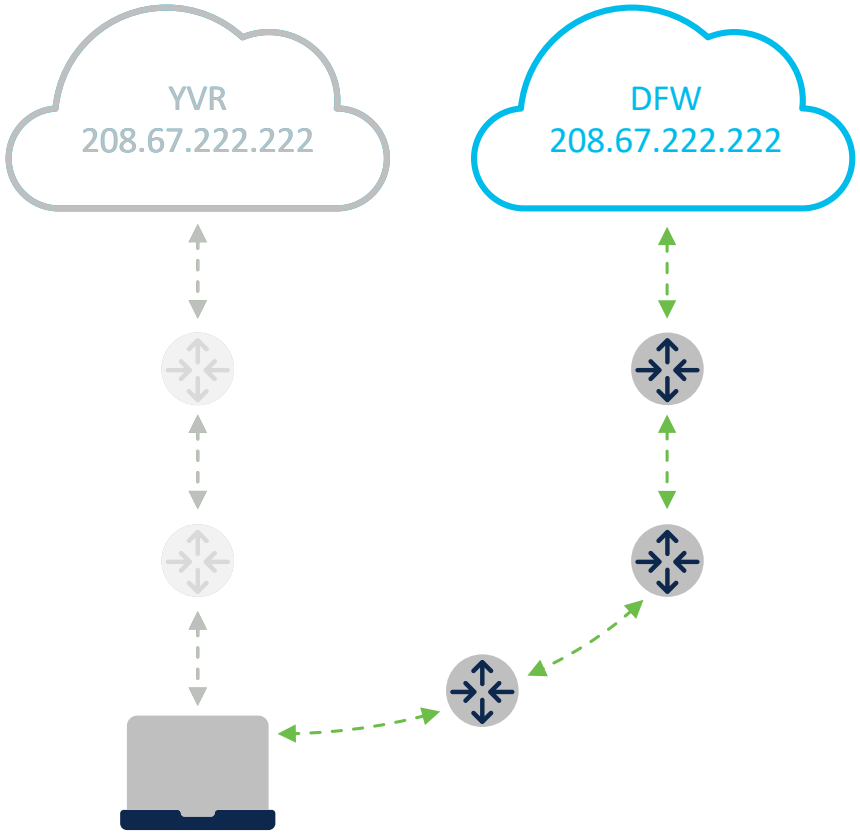
32+

data centers worldwide

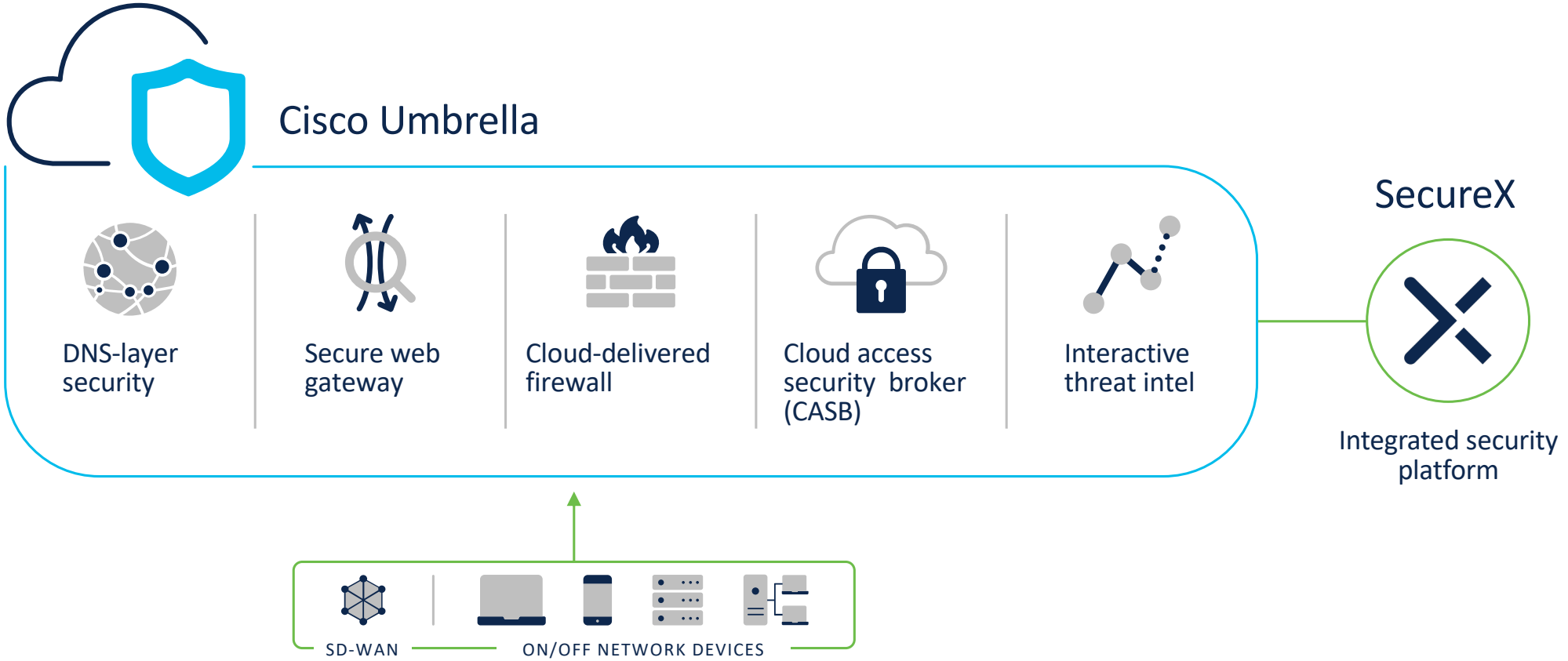
Anycast IP routing for reliability

DNS-layer security

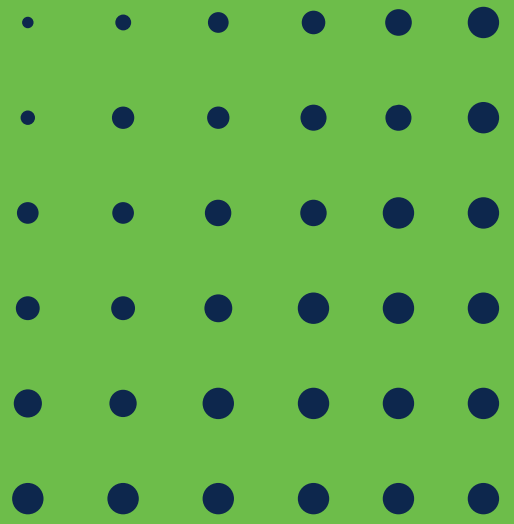
- All data centers announce same IP address
- Customer points DNS traffic to our IP address
- Requests transparently sent to fastest available with automated failover



The Umbrella multi-function security solution

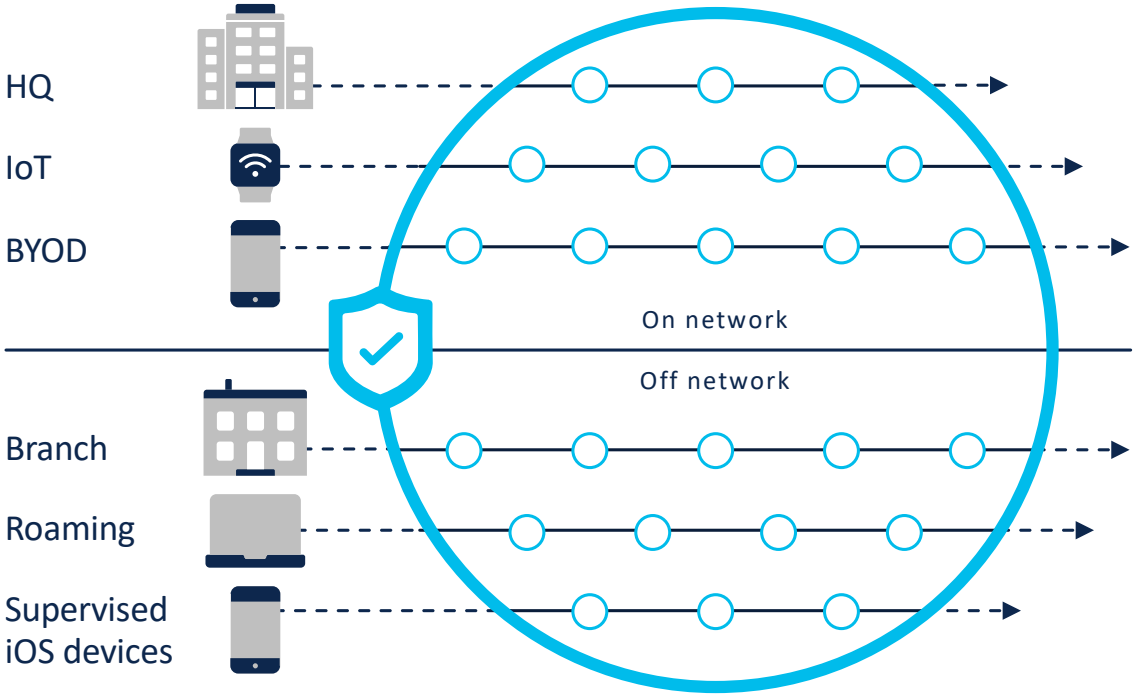


Enforcement



DNS security

Visibility and protection for all activity, anywhere

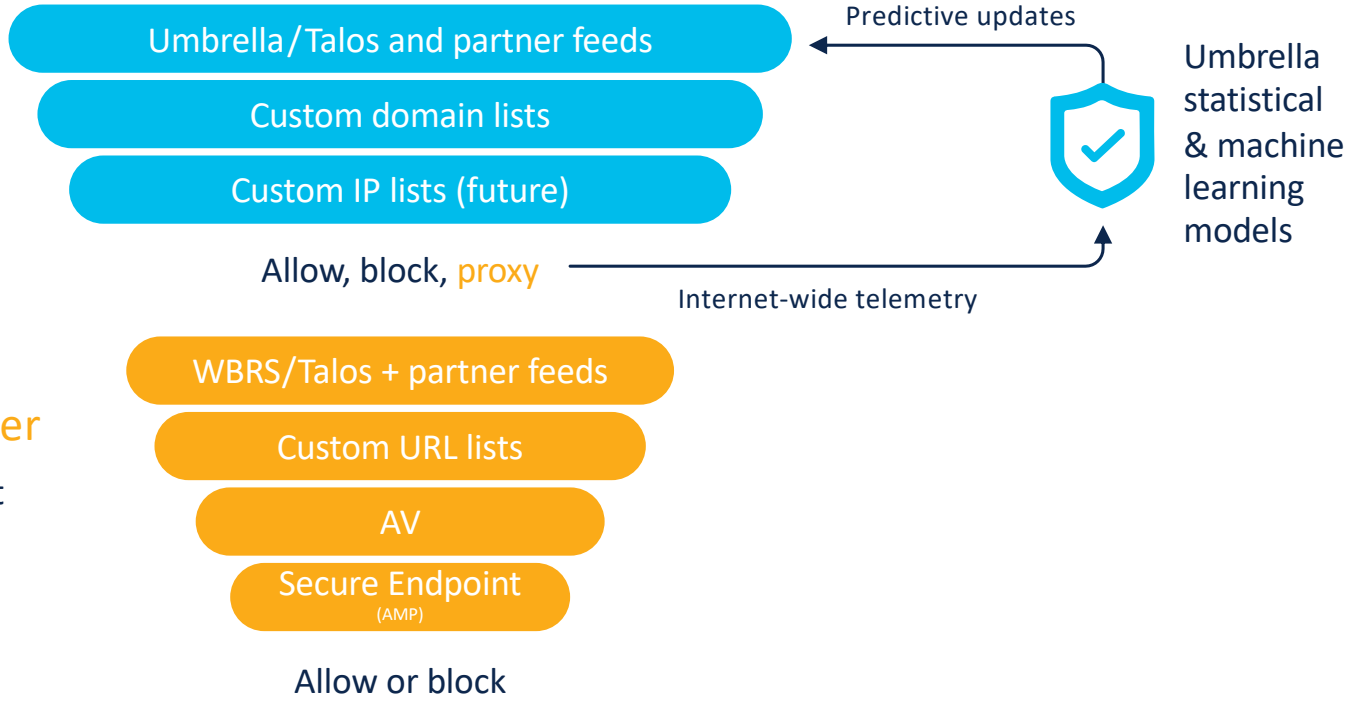


- All office locations
- Any device on your network
- Roaming laptops and supervised iOS devices
- Every port and protocol

Breadth to cover all ports and depth to inspect risky domains

DNS and IP layer

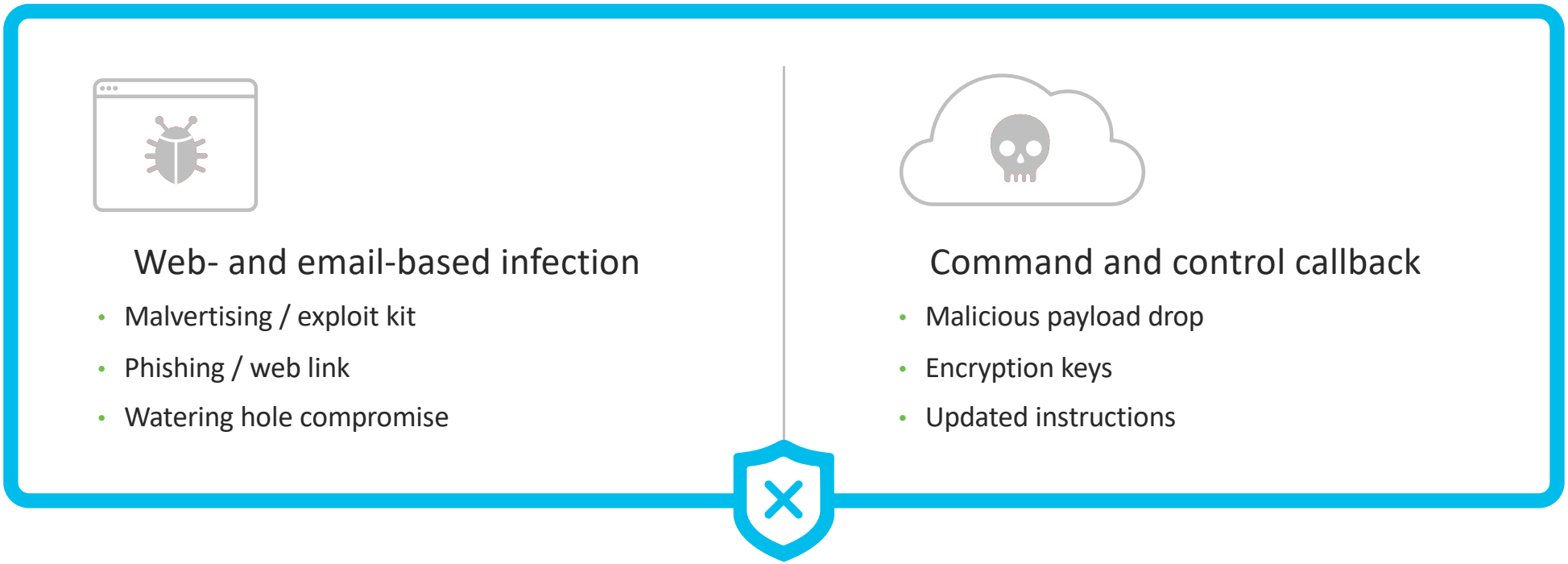
- Domain request
- IP response (DNS-layer) or connection (IP-layer)



HTTP/S layer

- URL request
- File hash

Prevents connections before and during the attack



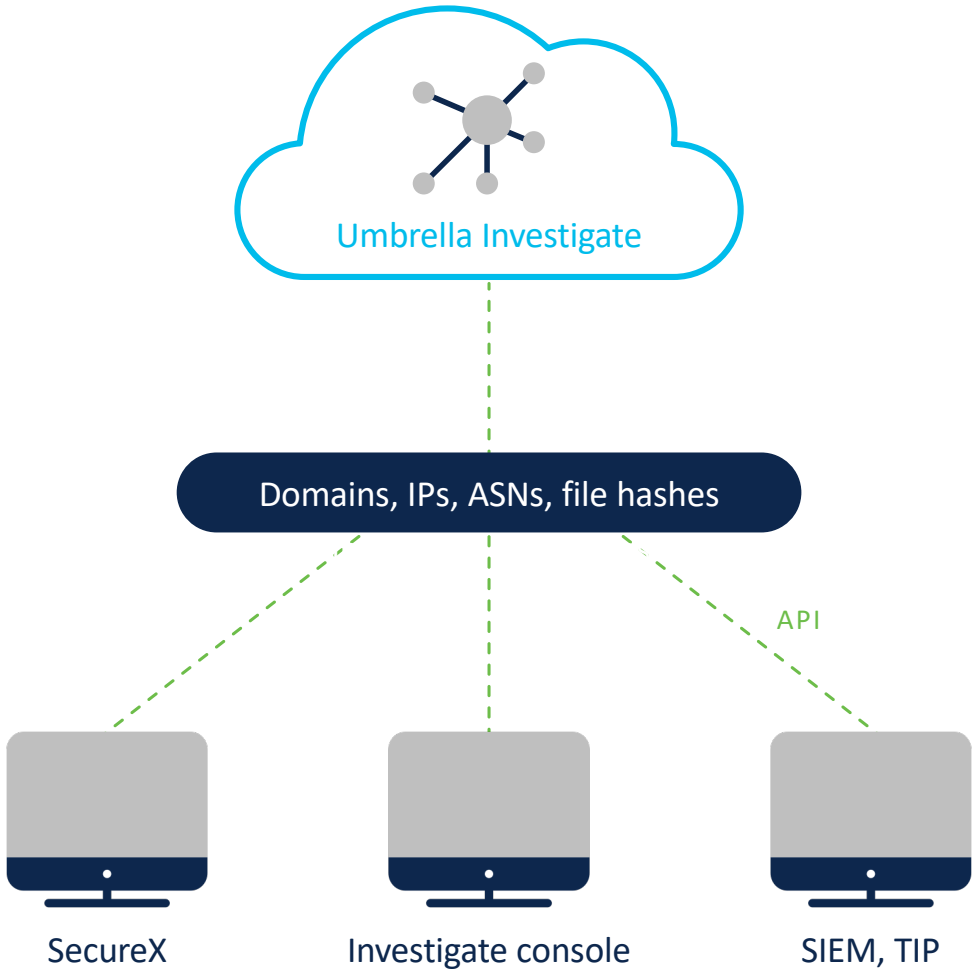
Stop data exfiltration and ransomware encryption

Threat Intelligence

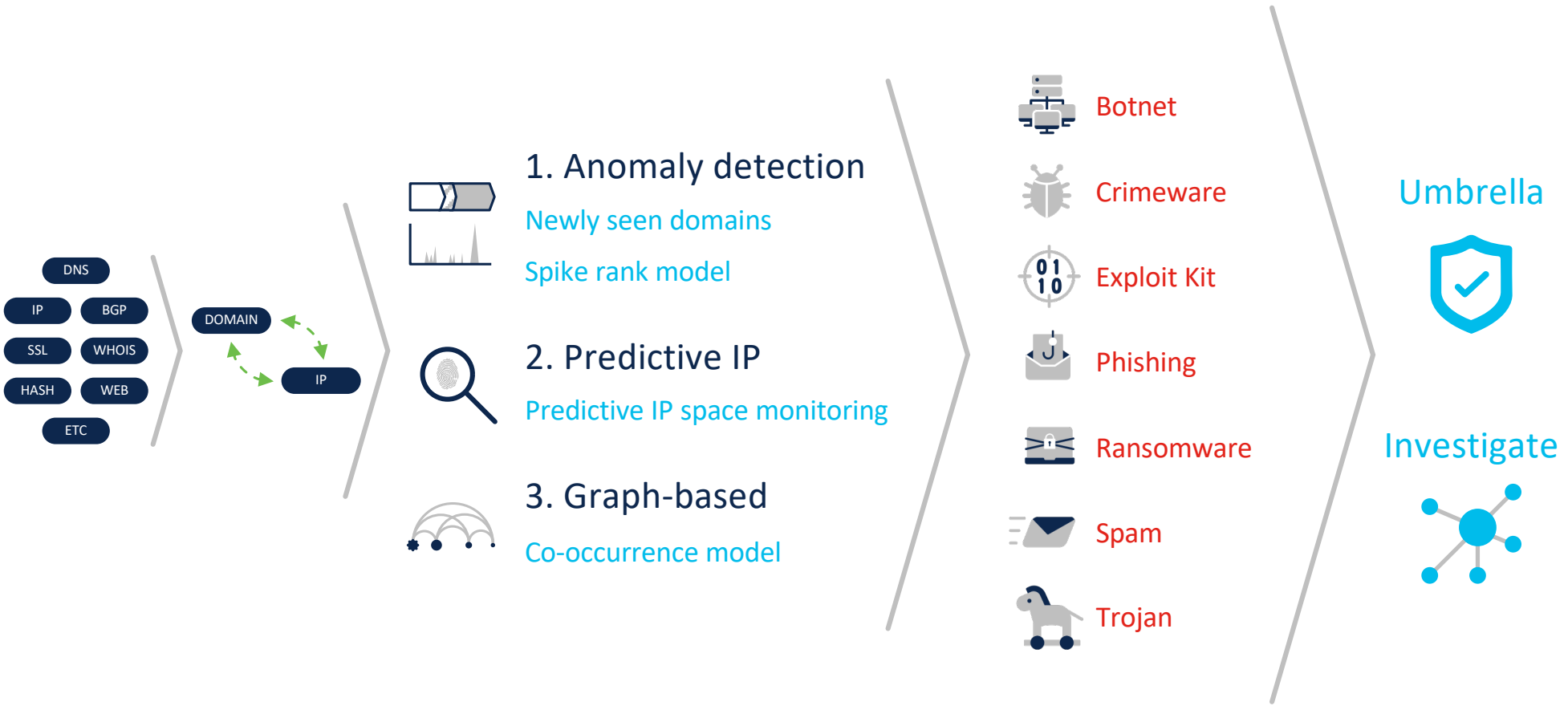
Umbrella Investigate

Rich threat intelligence for fast triage

- Gain deeper visibility into threats with the most complete view of the internet
- Speed up incident investigations and response
- Discover and predict malicious domains and IPs
- Enrich data and alerts across your security infrastructure with global intelligence

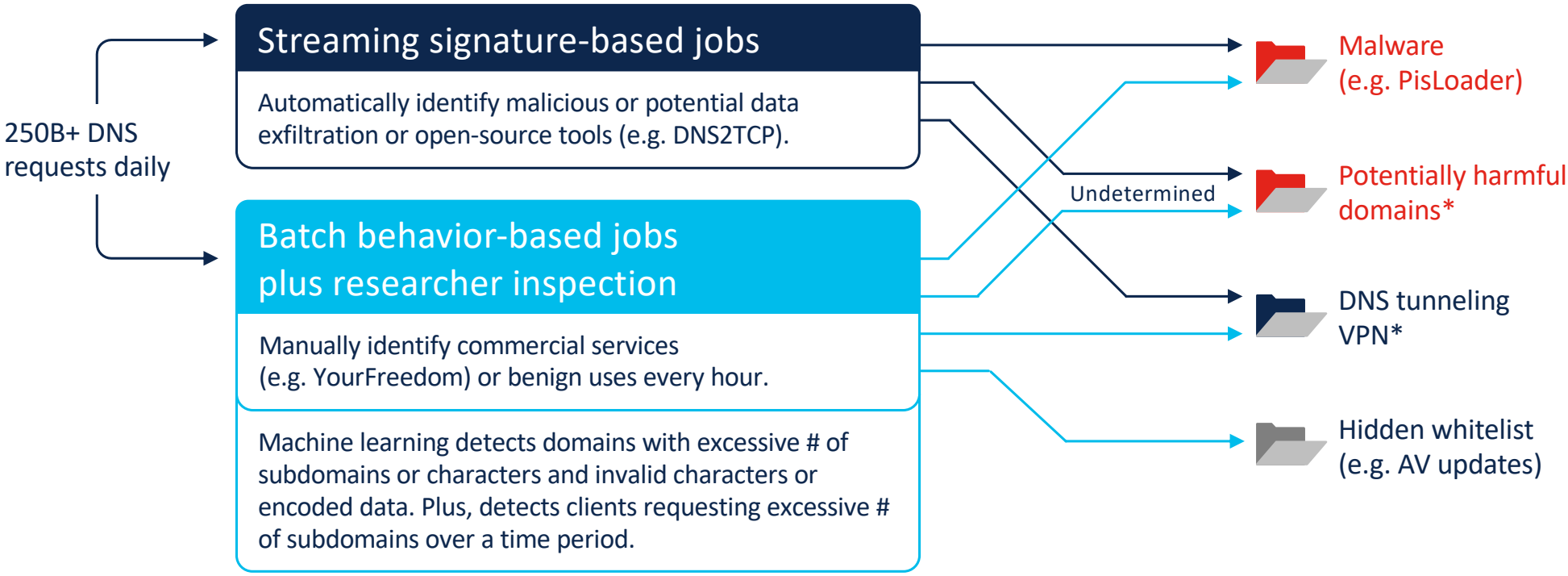


Multi-faceted threat intel



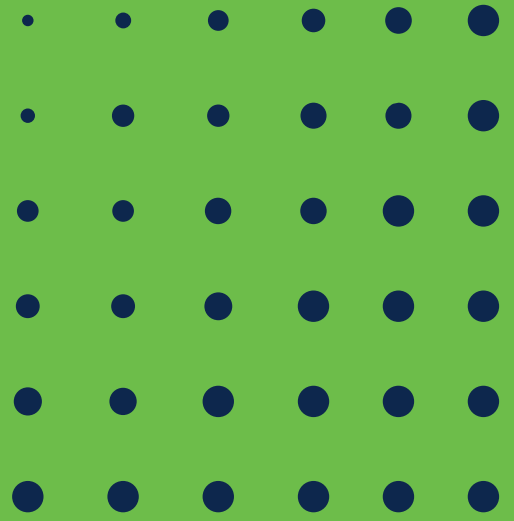
New analysis and categories

To combat DNS tunneling



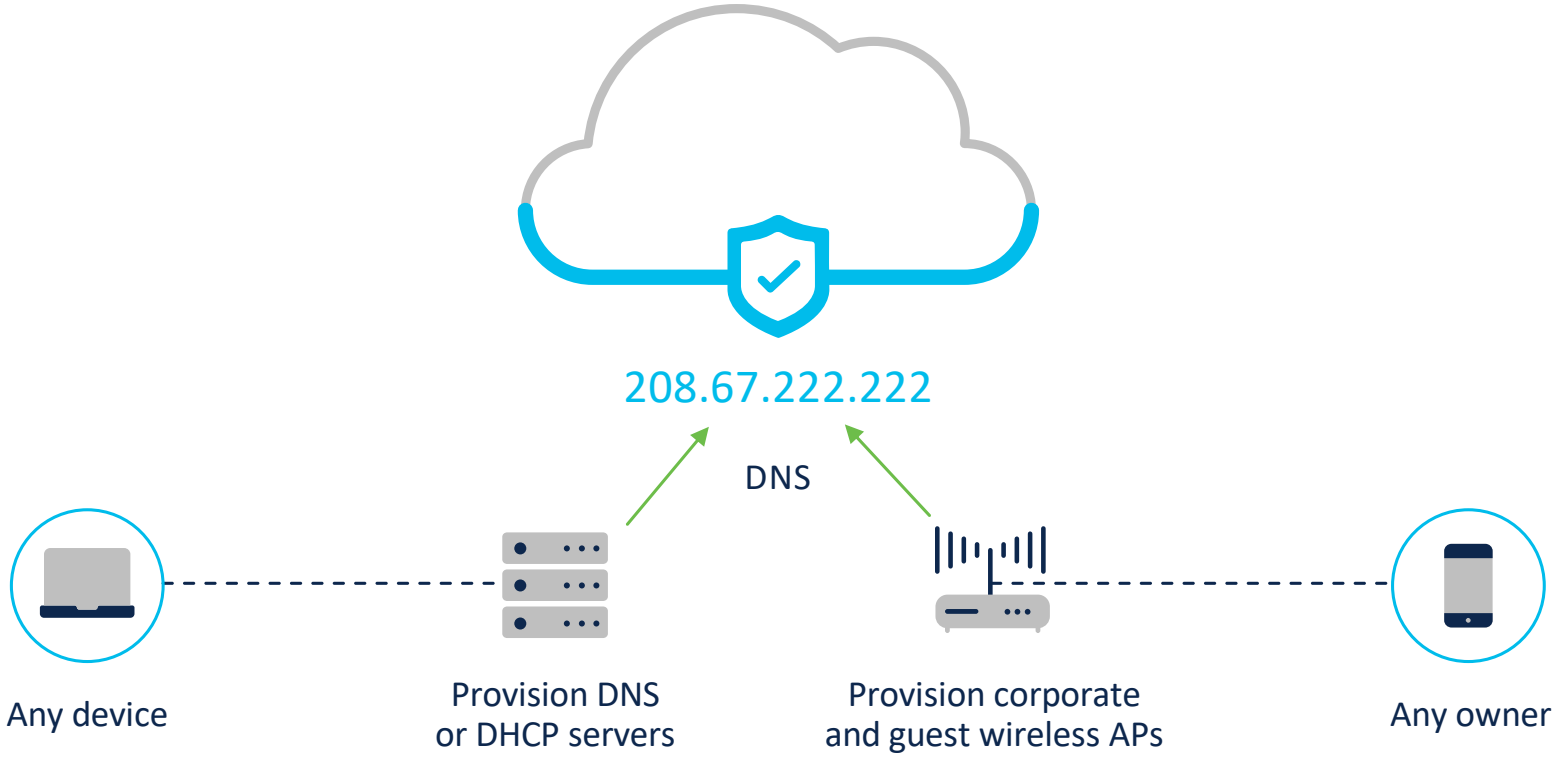
*New categories: These are allowed by default, but can be blocked. And domains in these categories may have already been categorized as Malware or Botnet (a.k.a. C2 callbacks) by many other Umbrella statistical models.

Deployment

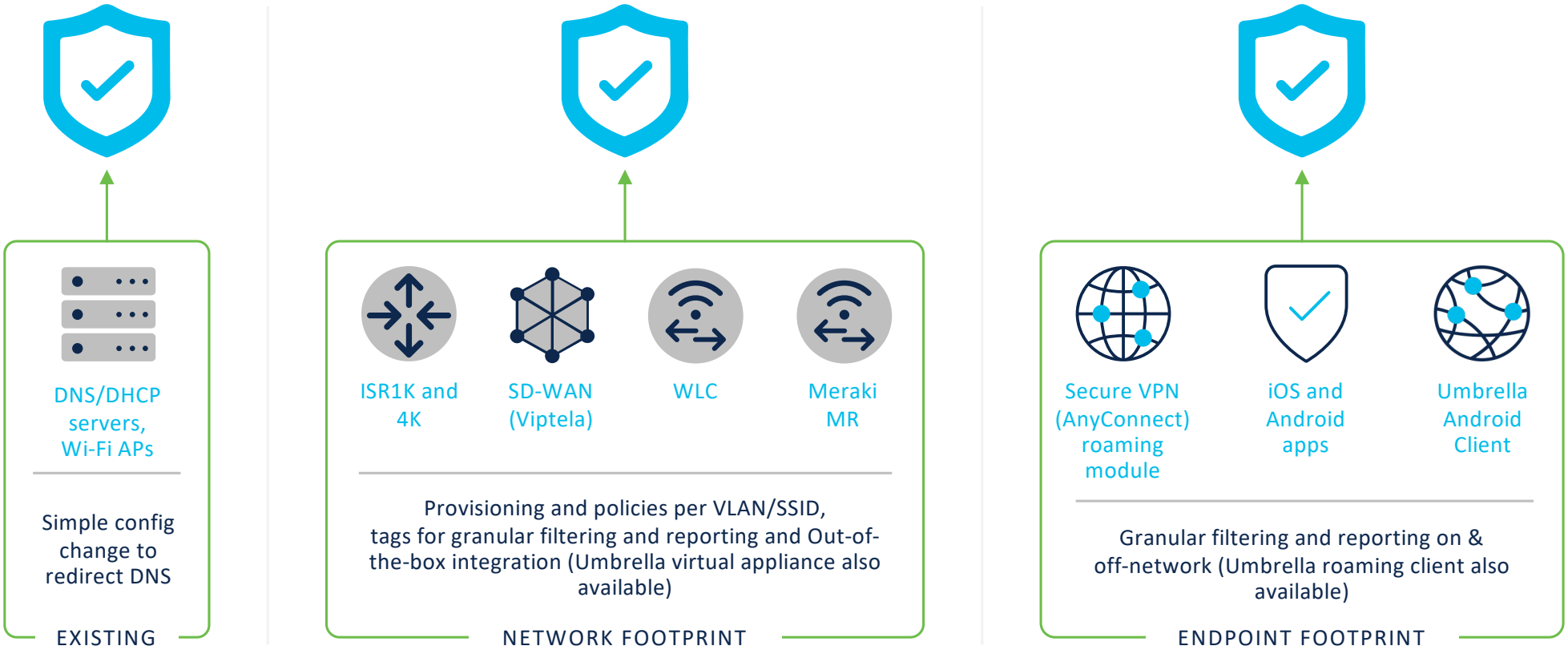


Simplest way to protect any device on-network

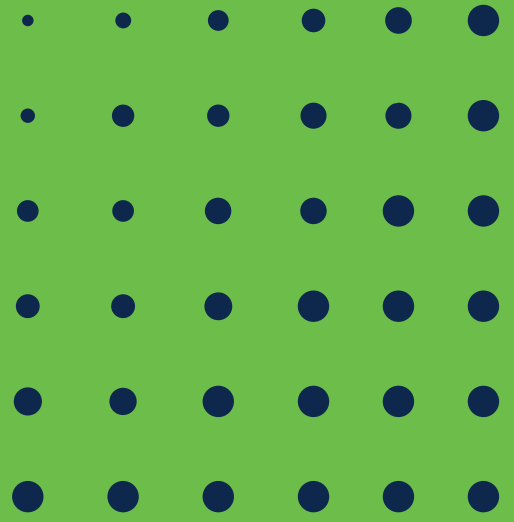
Point external DNS traffic to Umbrella



Enterprise-wide deployment in minutes



Reports

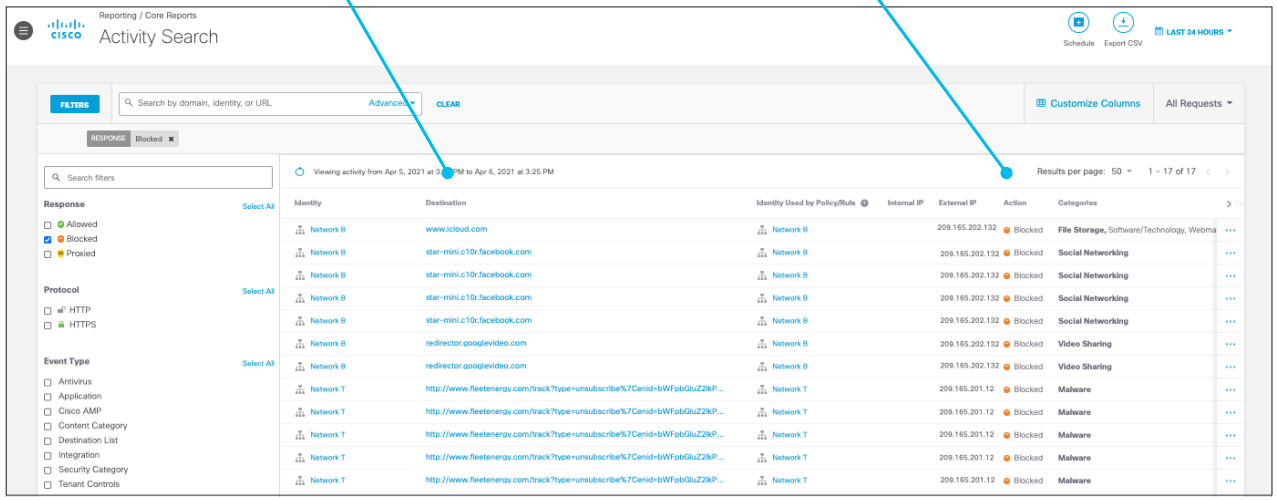


ACTIVITY SEARCH

Find the result of every DNS request

Action Taken

Destination Domain



Categories (Including Security)

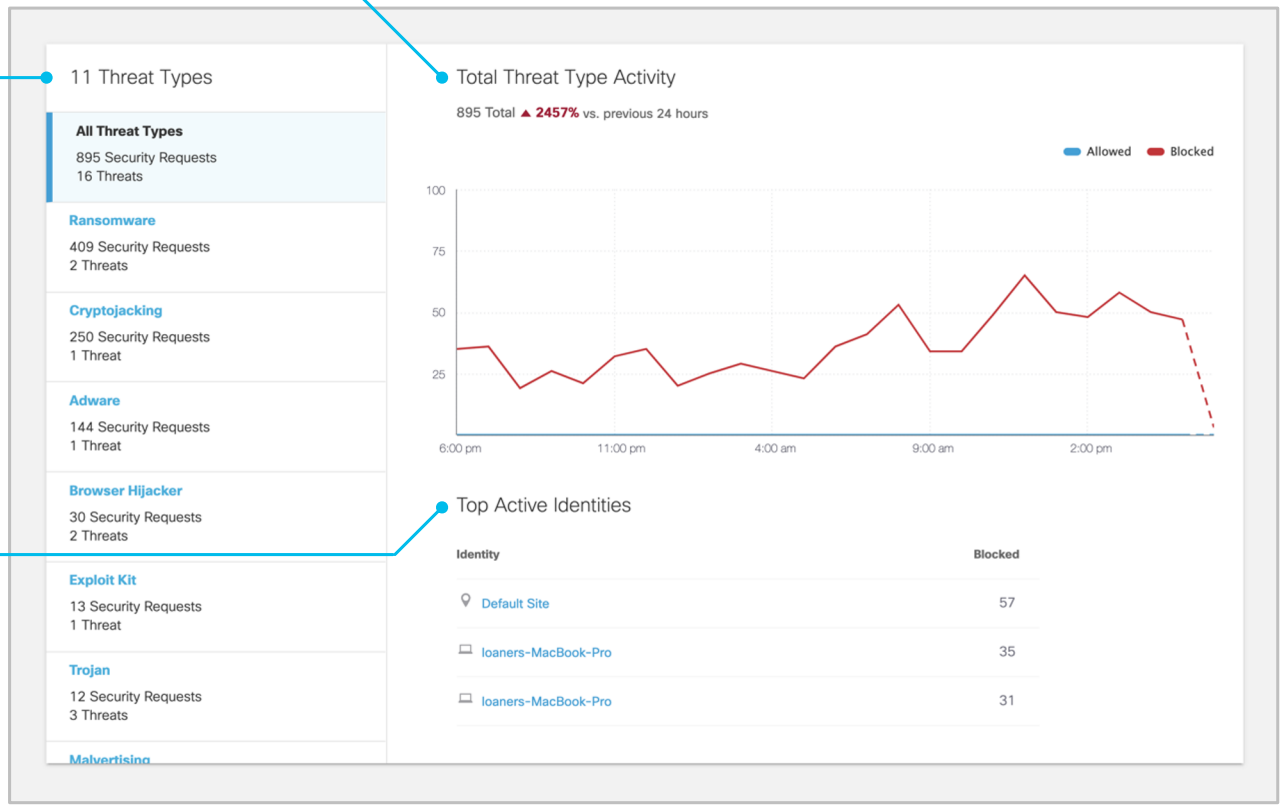
THREATS REPORT

Quickly spot and remediate victims

Recent threat trends

Breakdown of threat types

Top identities impacted by threats with ability to drill down



Ability to easily block unapproved apps

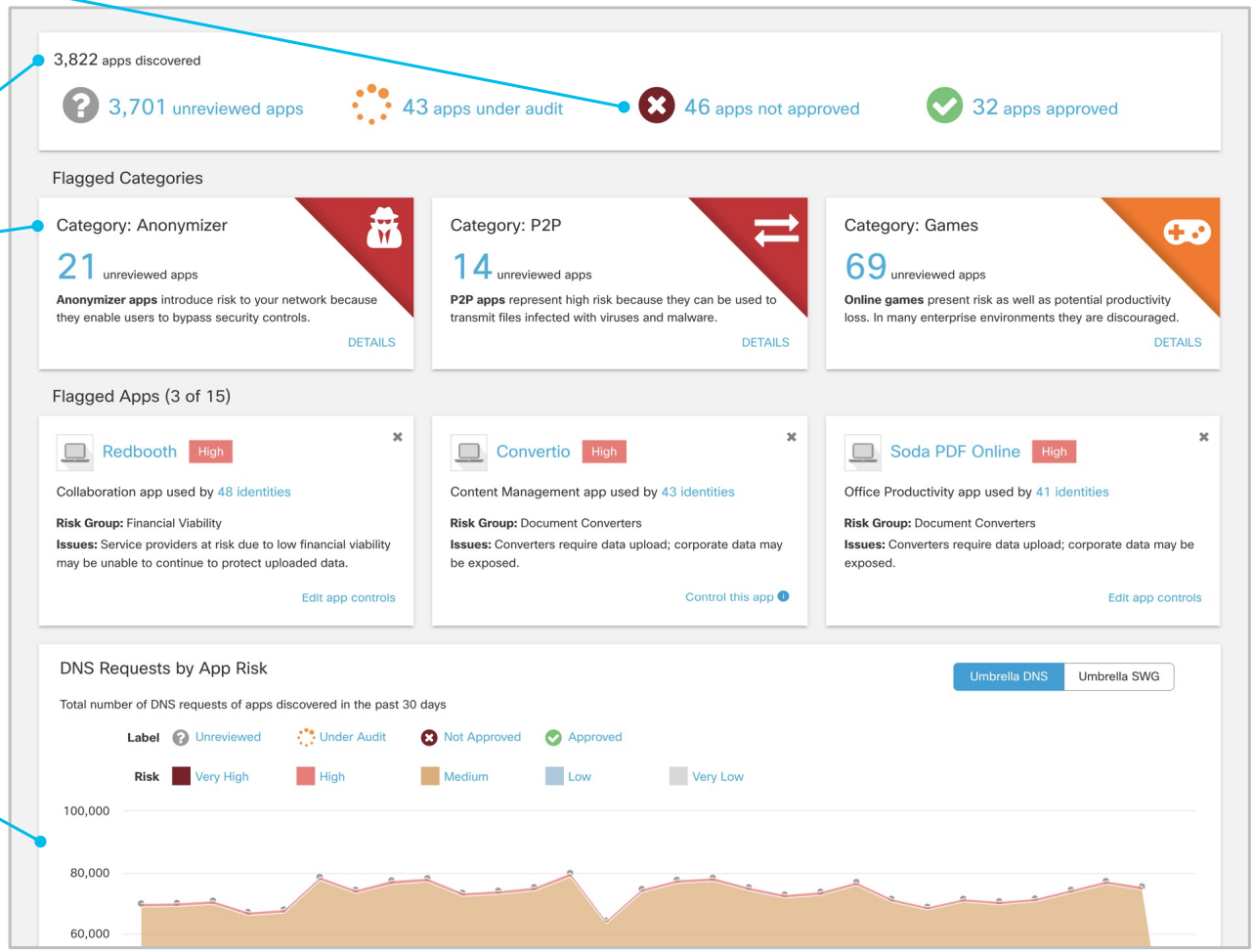
Status of discovered apps

Summary of high-risk categories

APP DISCOVERY REPORT

Manage Shadow IT to enable secure cloud adoption

Visibility into cloud app usage by risk with links to app details



SECURE