

Cisco Umbrella

The first line of defense:
DNS-layer security

Emanuel Almeida
Technical Solutions Architect
October 2021



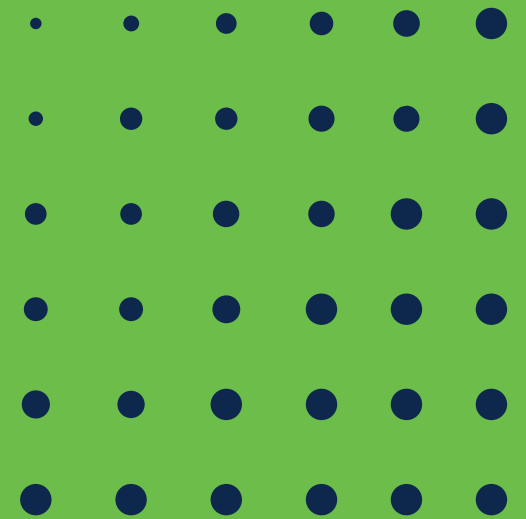


Agenda



- ▶ 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

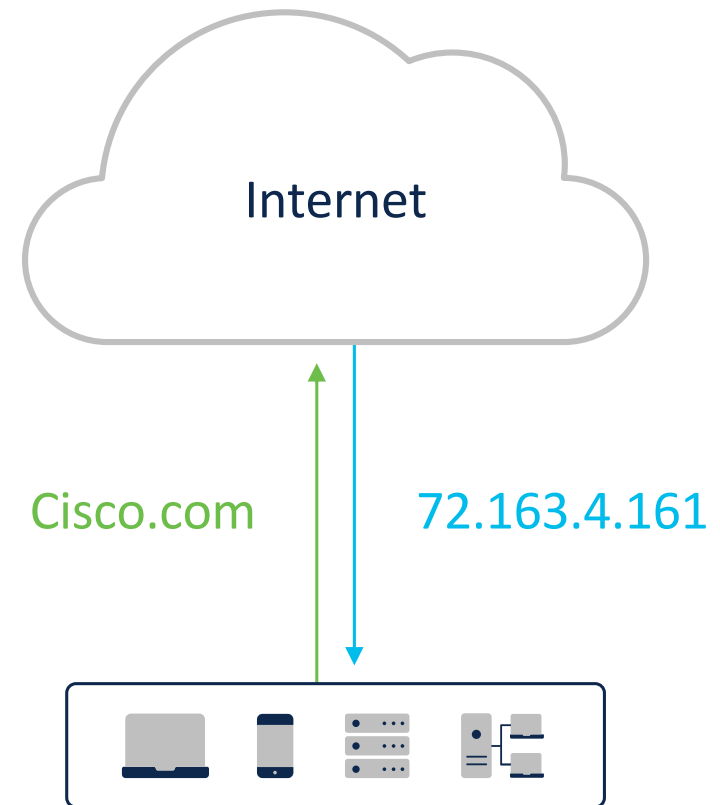


Reported breaches
could have been
controlled by DNS

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

2012

Launched

DNS-layer security offer (OpenDNS Umbrella)

2015

Acquired

by Cisco

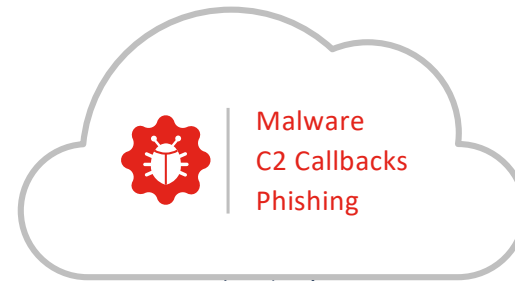
2019

Expanded

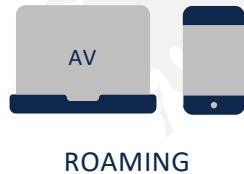
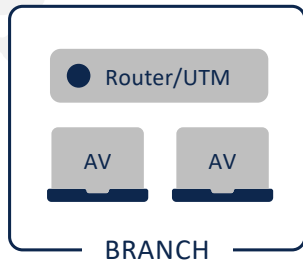
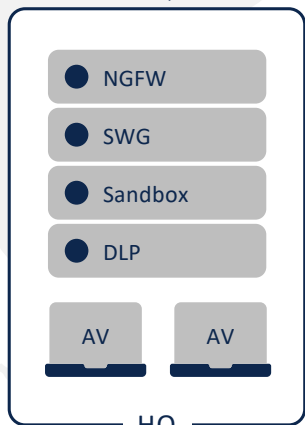
to integrate more security services in single platform



Umbrella DNS-layer security



Umbrella



First line

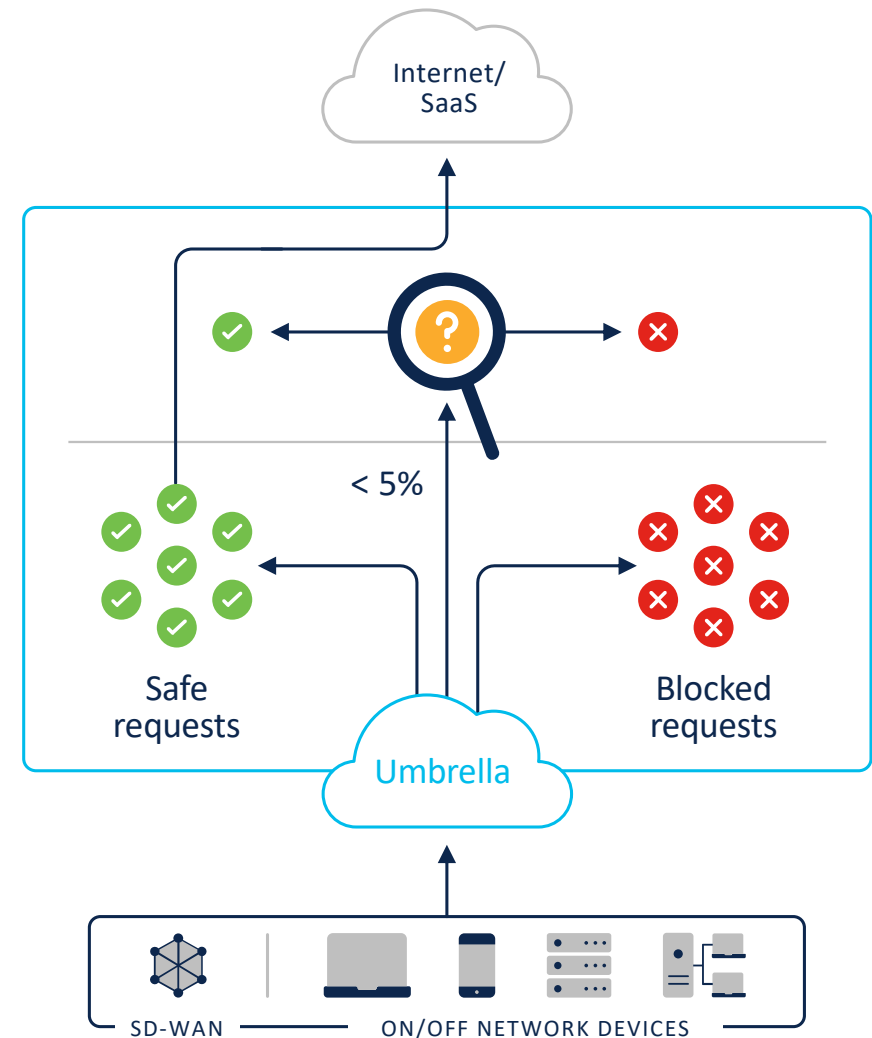
Benefits

- 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

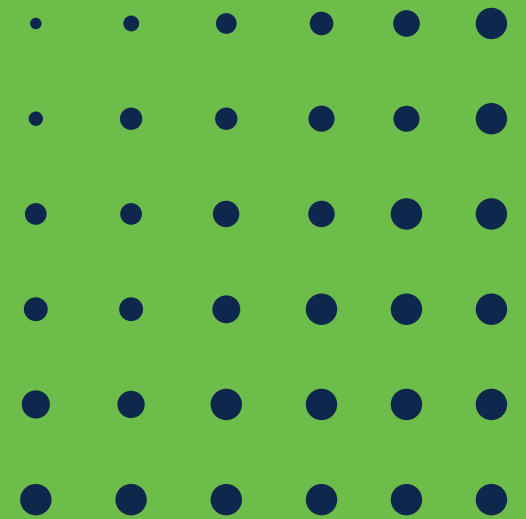
Umbrella DNS-layer security

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

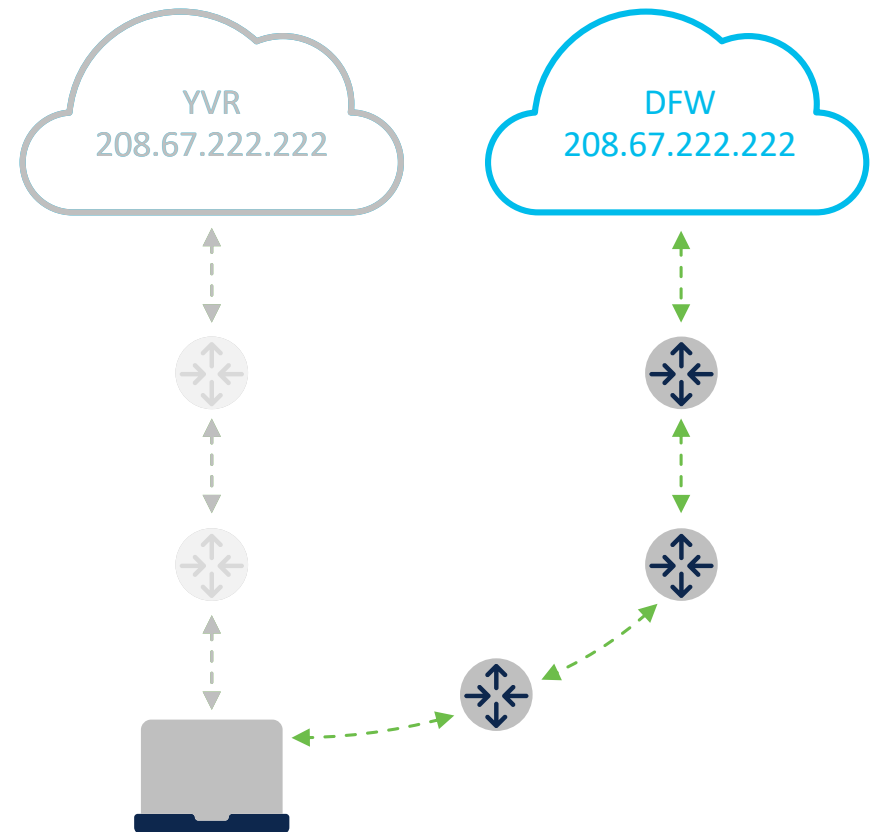
▶▶ 32+
data centers
worldwide



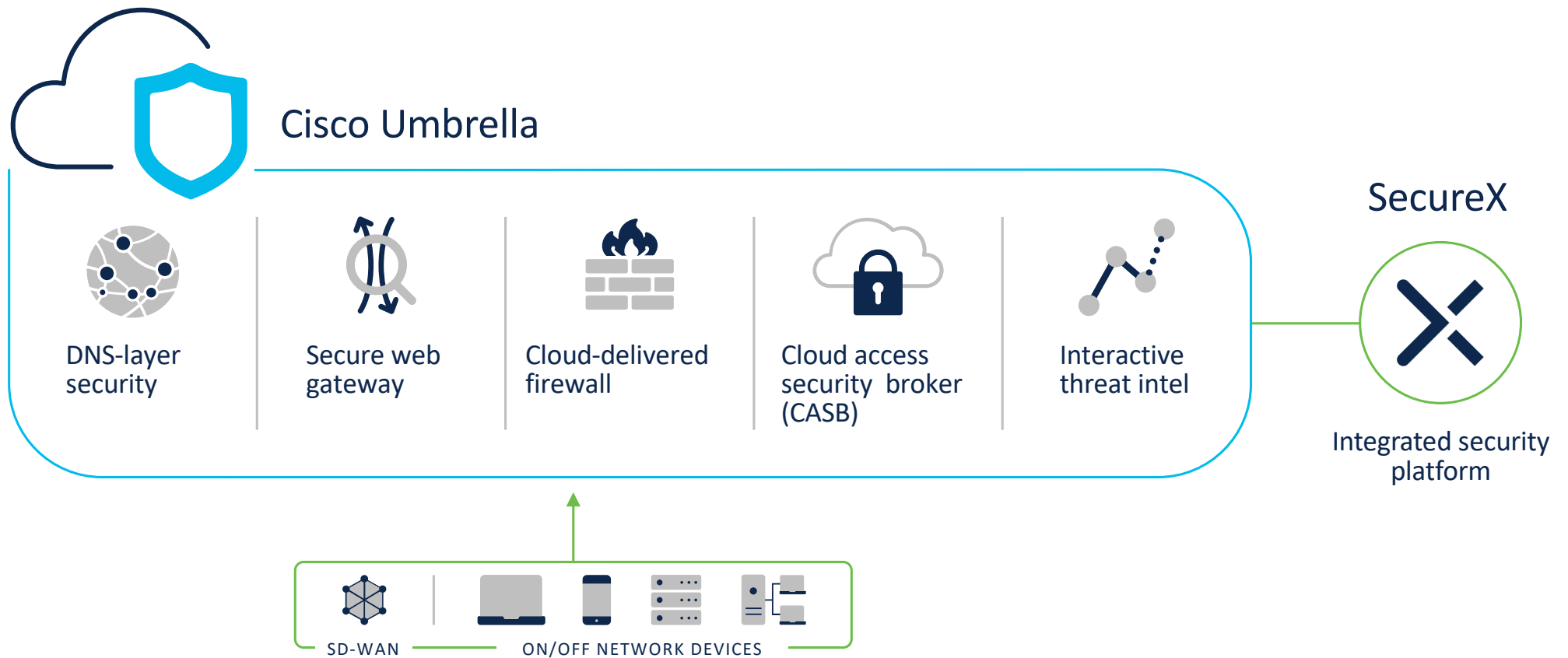
Anycast IP routing for reliability

DNS-layer security

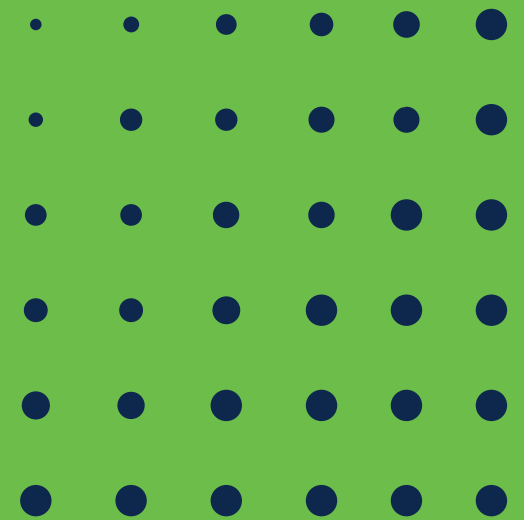
- All data centers announce same IP address
- Customer points DNS traffic to our IP address
- Requests transparently sent to fastest available with automated failover



The Umbrella multi-function security solution

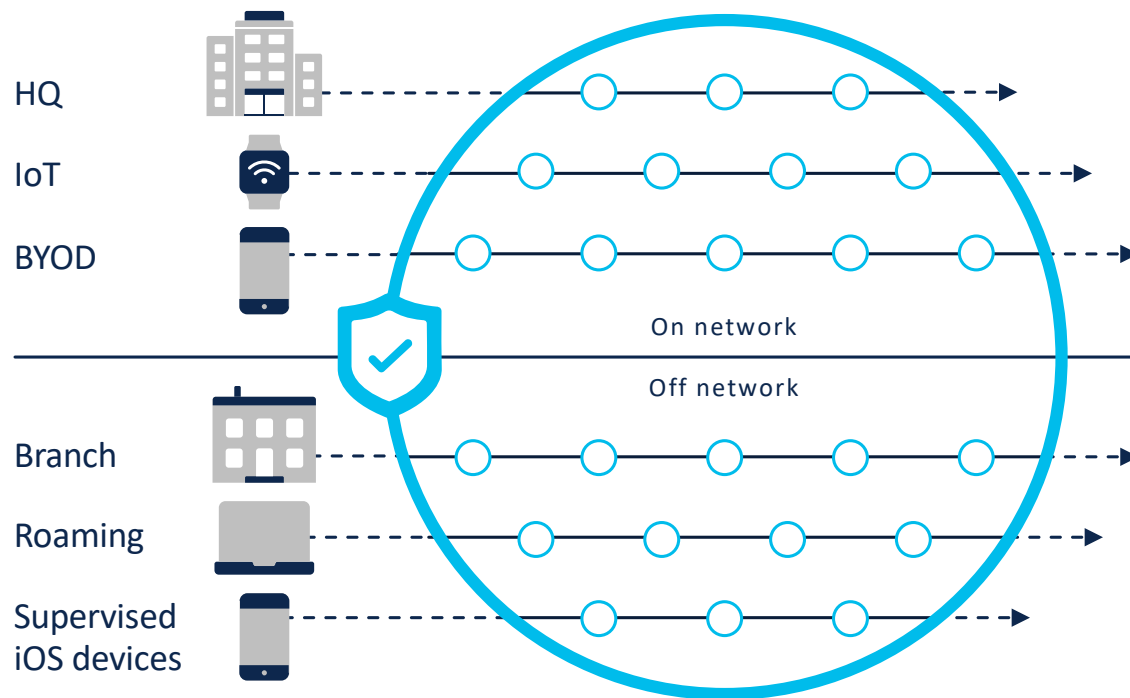


Enforcement



DNS security

Visibility and protection for all activity, anywhere

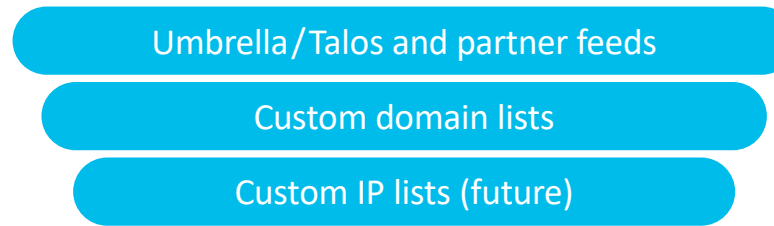


- All office locations
- Any device on your network
- Roaming laptops and supervised iOS devices
- Every port and protocol

Breadth to cover all ports and depth to inspect risky domains

DNS and IP layer

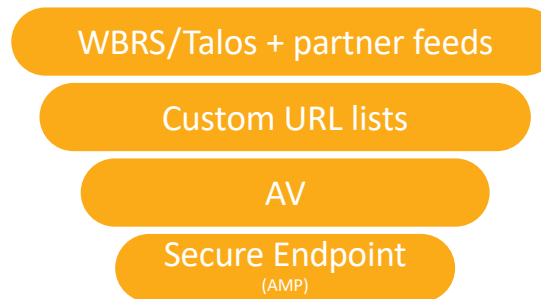
- Domain request
- IP response (DNS-layer) or connection (IP-layer)



Allow, block, proxy

HTTP/S layer

- URL request
- File hash



Allow or block

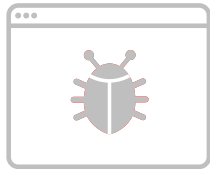
Predictive updates



Umbrella statistical & machine learning models

Internet-wide telemetry

Prevents connections before and during the attack



Web- and email-based infection

- Malvertising / exploit kit
- Phishing / web link
- Watering hole compromise



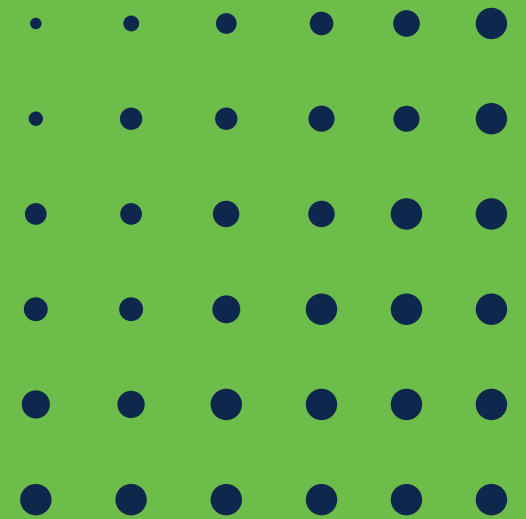
Command and control callback

- Malicious payload drop
- Encryption keys
- Updated instructions



Stop data exfiltration and ransomware encryption

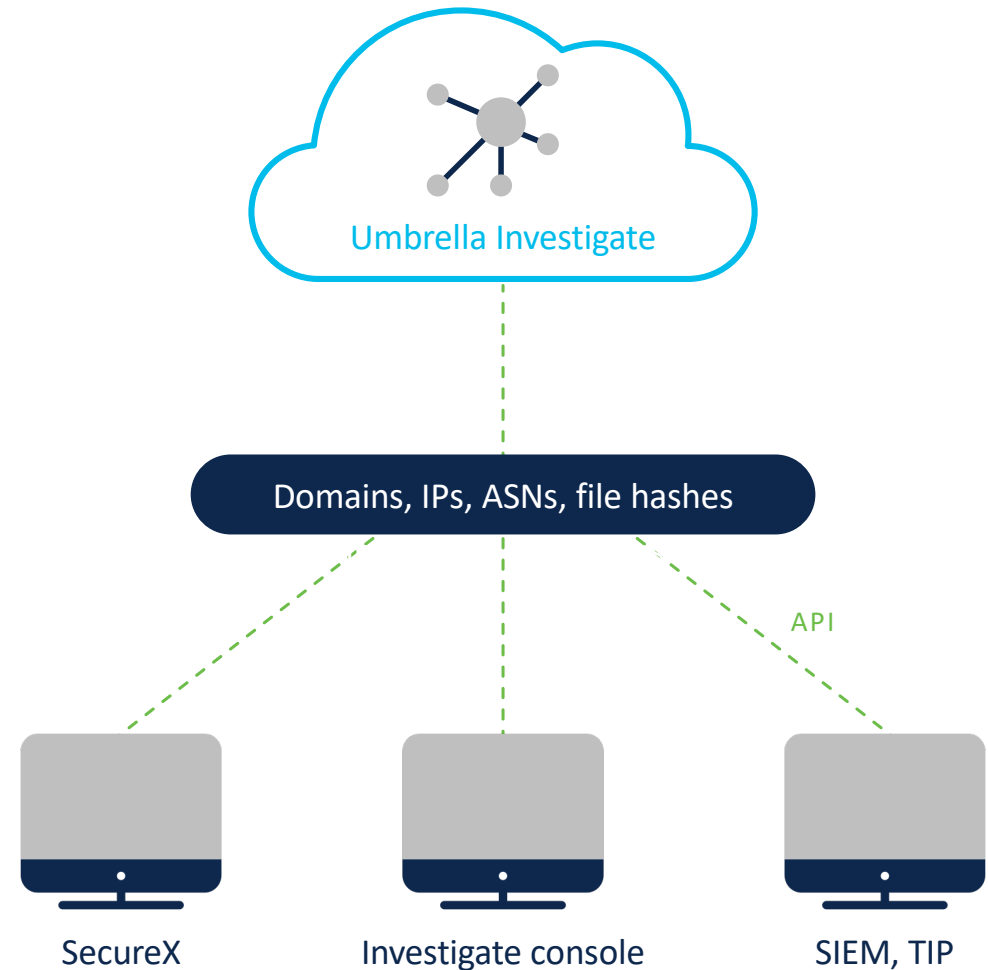
Threat Intelligence



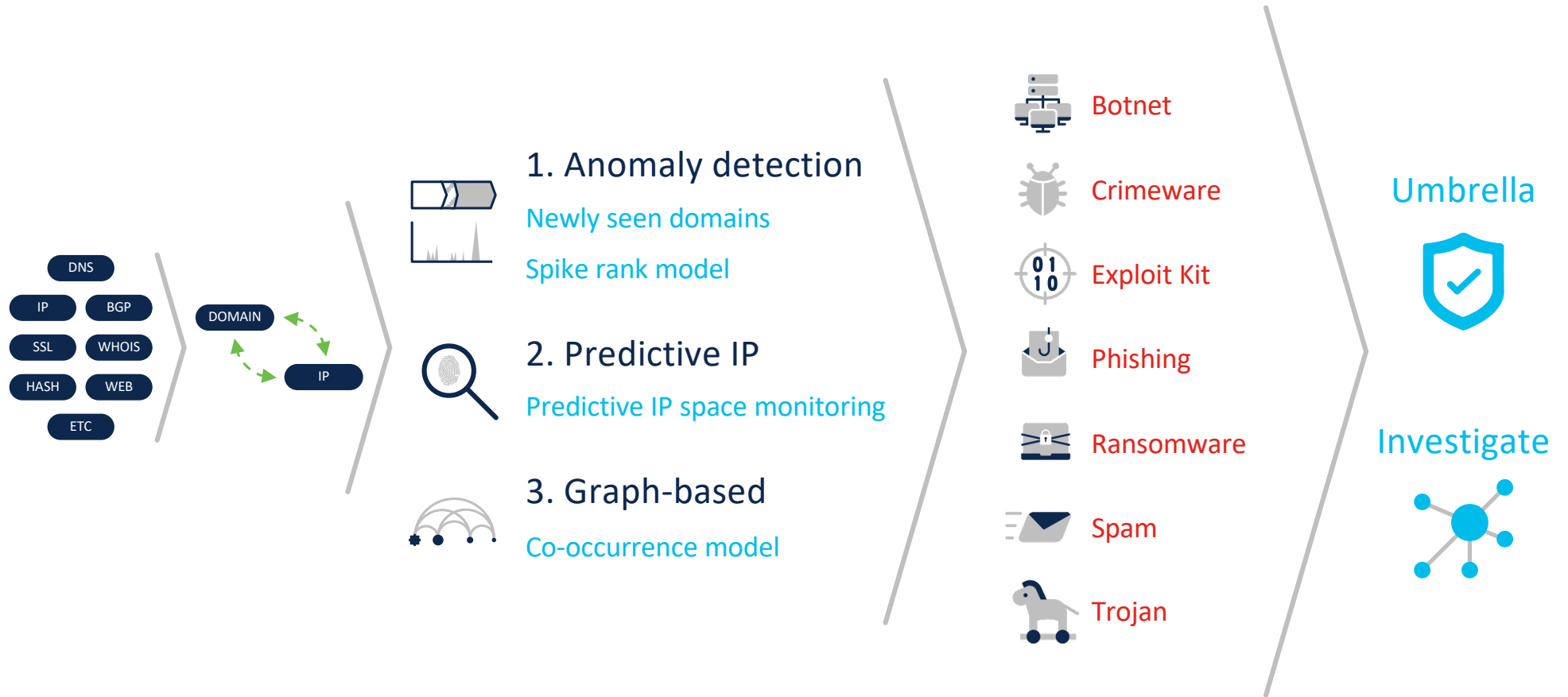
Umbrella Investigate

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

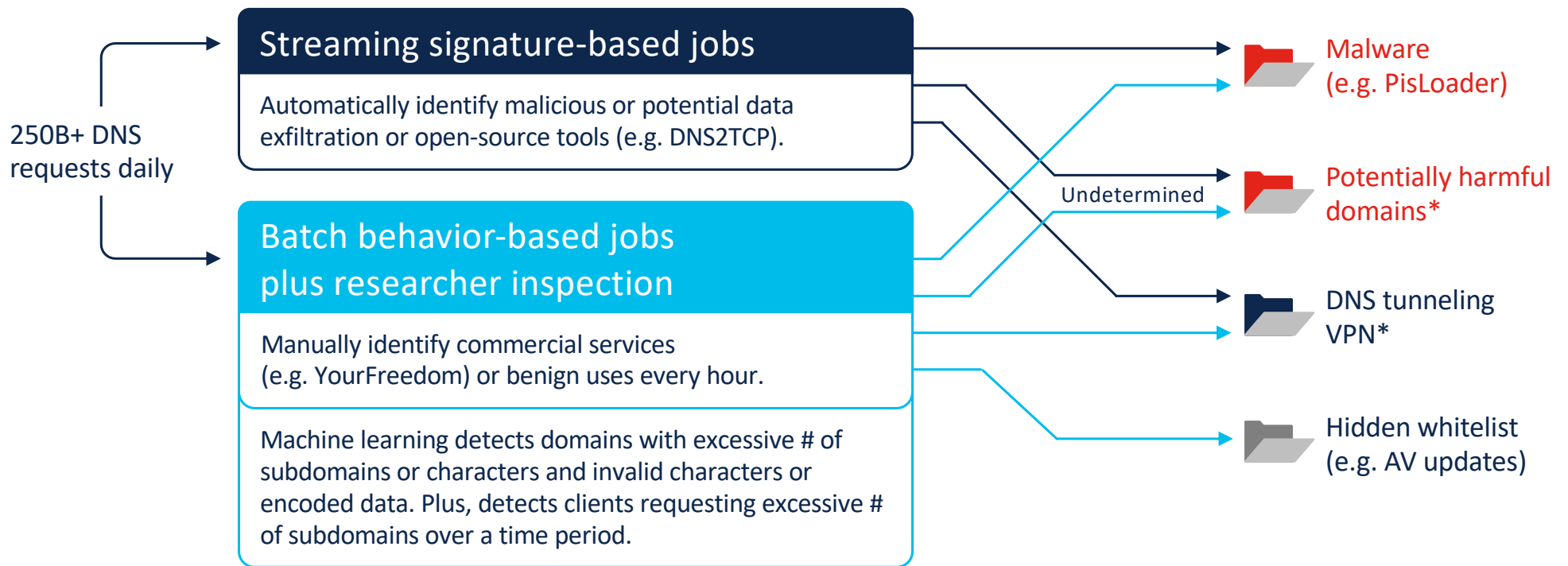


Multi-faceted threat intel



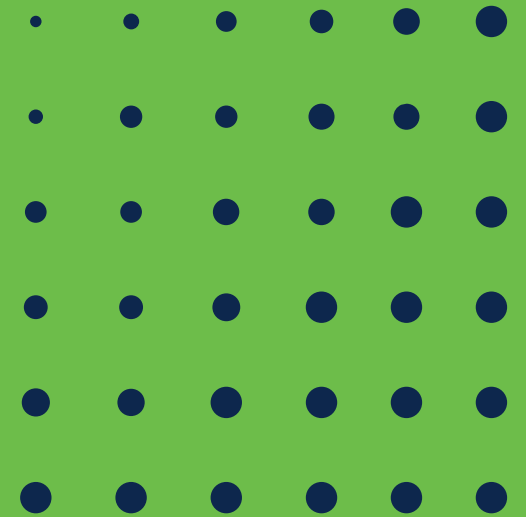
New analysis and categories

To combat DNS tunneling



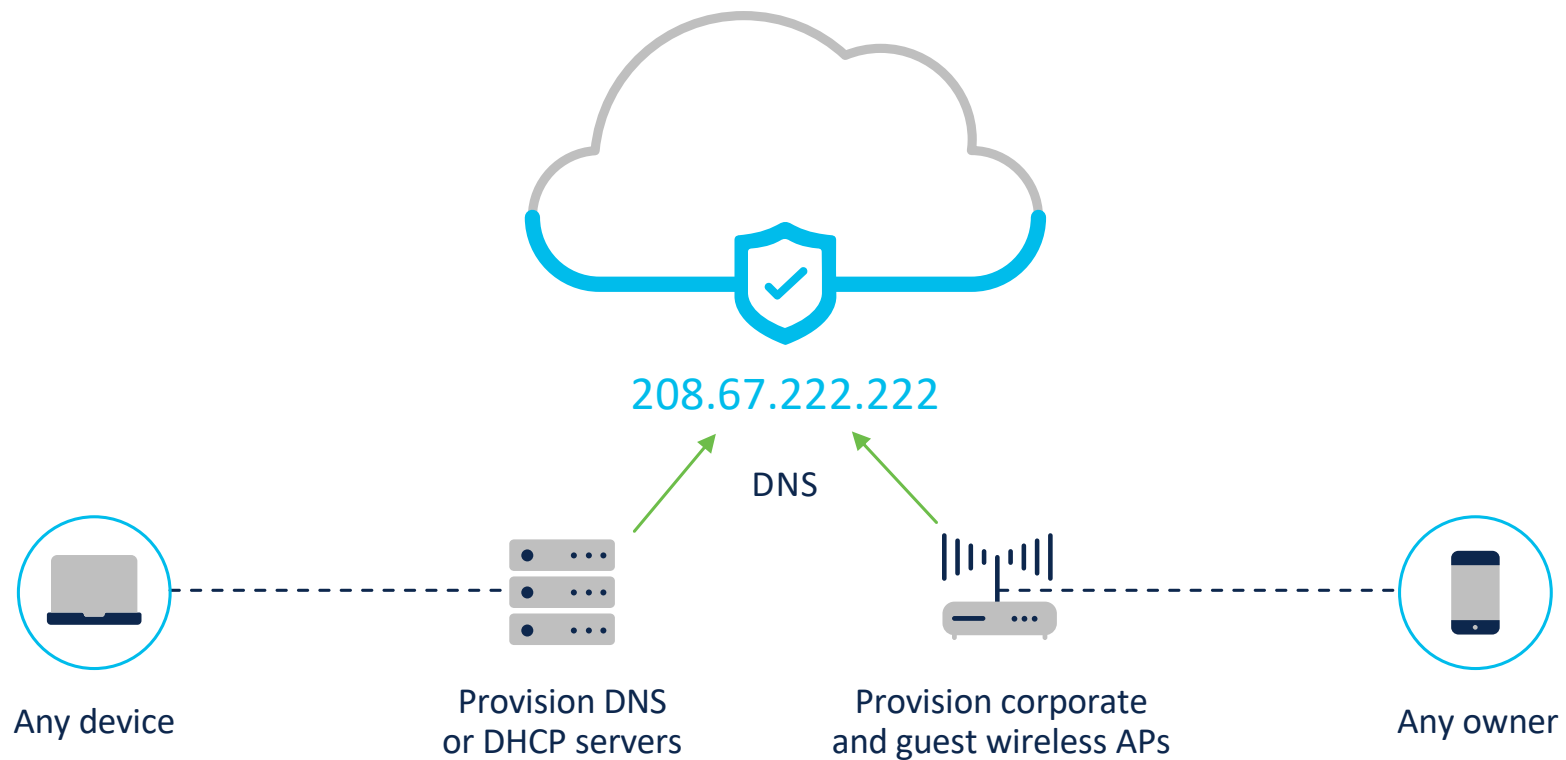
*New categories: These are allowed by default, but can be blocked. And domains in these categories may have already been categorized as Malware or Botnet (a.k.a. C2 callbacks) by many other Umbrella statistical models.

Deployment

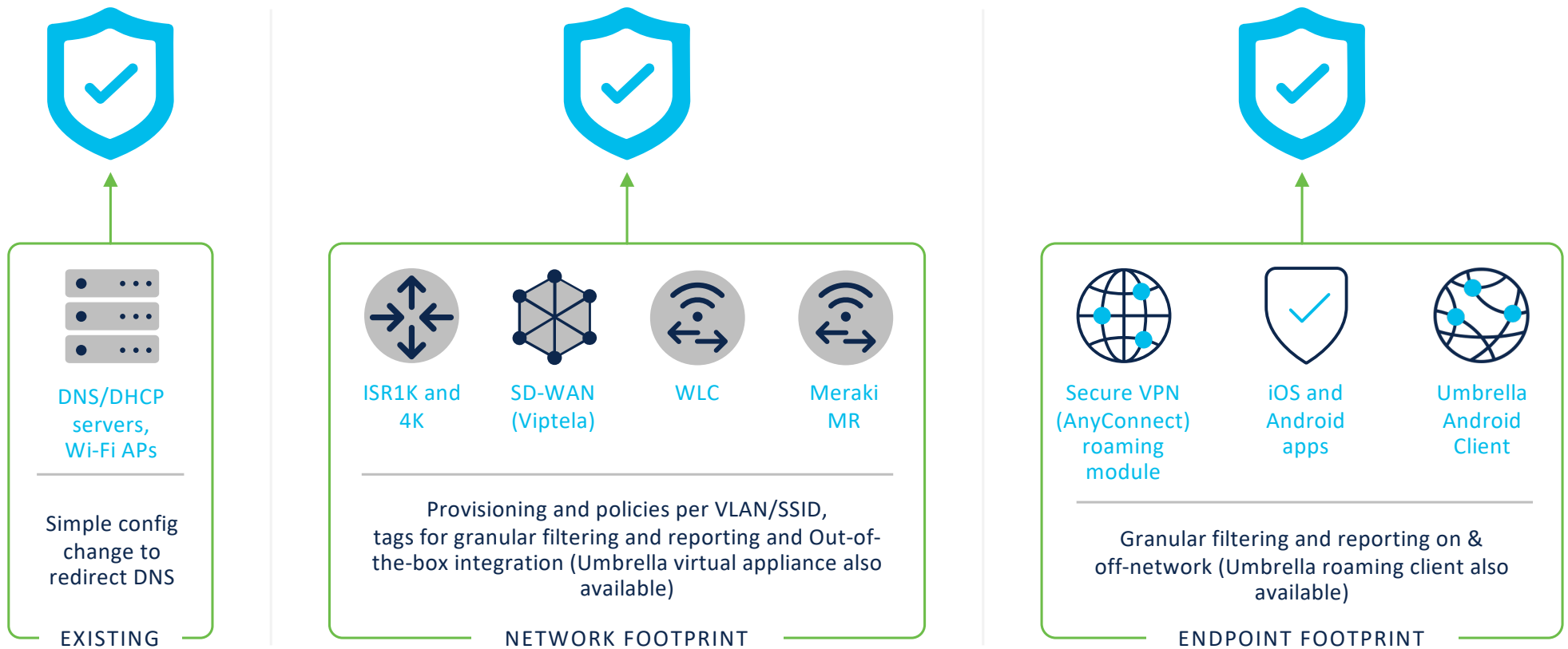


Simplest way to protect any device on-network

Point external DNS traffic to Umbrella



Enterprise-wide deployment in minutes



Reports



ACTIVITY SEARCH

Find the result of every DNS request

Destination Domain

Action Taken

The screenshot shows the Cisco Activity Search interface. At the top, there's a search bar with the text "Search by domain, identity, or URL" and buttons for "Advanced" and "CLEAR". Below the search bar, there are filter sections for "RESPONSE" (Blocked), "Protocol" (HTTP, HTTPS), and "Event Type" (Antivirus, Application, Cisco AMP, Content Category, Destination List, Integration, Security Category, Tenant Controls). The main table displays activity from Apr 5, 2021 at 9:00 AM to Apr 6, 2021 at 3:25 PM. The table has columns for Identity, Destination, Identity Used by Policy/Rule, Internal IP, External IP, Action, and Categories. The results show several blocked requests to various domains, including www.icloud.com, star-mini.c10r.facebook.com, and redirector.googlevideo.com, with categories like File Storage, Software/Technology, Webmail, Social Networking, and Malware.

Identity	Destination	Identity Used by Policy/Rule	Internal IP	External IP	Action	Categories
Network B	www.icloud.com	Network B	209.165.202.132	209.165.202.132	Blocked	File Storage, Software/Technology, Webmail
Network B	star-mini.c10r.facebook.com	Network B	209.165.202.132	209.165.202.132	Blocked	Social Networking
Network B	star-mini.c10r.facebook.com	Network B	209.165.202.132	209.165.202.132	Blocked	Social Networking
Network B	star-mini.c10r.facebook.com	Network B	209.165.202.132	209.165.202.132	Blocked	Social Networking
Network B	star-mini.c10r.facebook.com	Network B	209.165.202.132	209.165.202.132	Blocked	Social Networking
Network B	redirector.googlevideo.com	Network B	209.165.202.132	209.165.202.132	Blocked	Video Sharing
Network B	redirector.googlevideo.com	Network B	209.165.202.132	209.165.202.132	Blocked	Video Sharing
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWfjstGluZ2kP...	Network T	209.165.201.12	209.165.201.12	Blocked	Malware
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWfjstGluZ2kP...	Network T	209.165.201.12	209.165.201.12	Blocked	Malware
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWfjstGluZ2kP...	Network T	209.165.201.12	209.165.201.12	Blocked	Malware
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWfjstGluZ2kP...	Network T	209.165.201.12	209.165.201.12	Blocked	Malware
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWfjstGluZ2kP...	Network T	209.165.201.12	209.165.201.12	Blocked	Malware

Categories (Including Security)

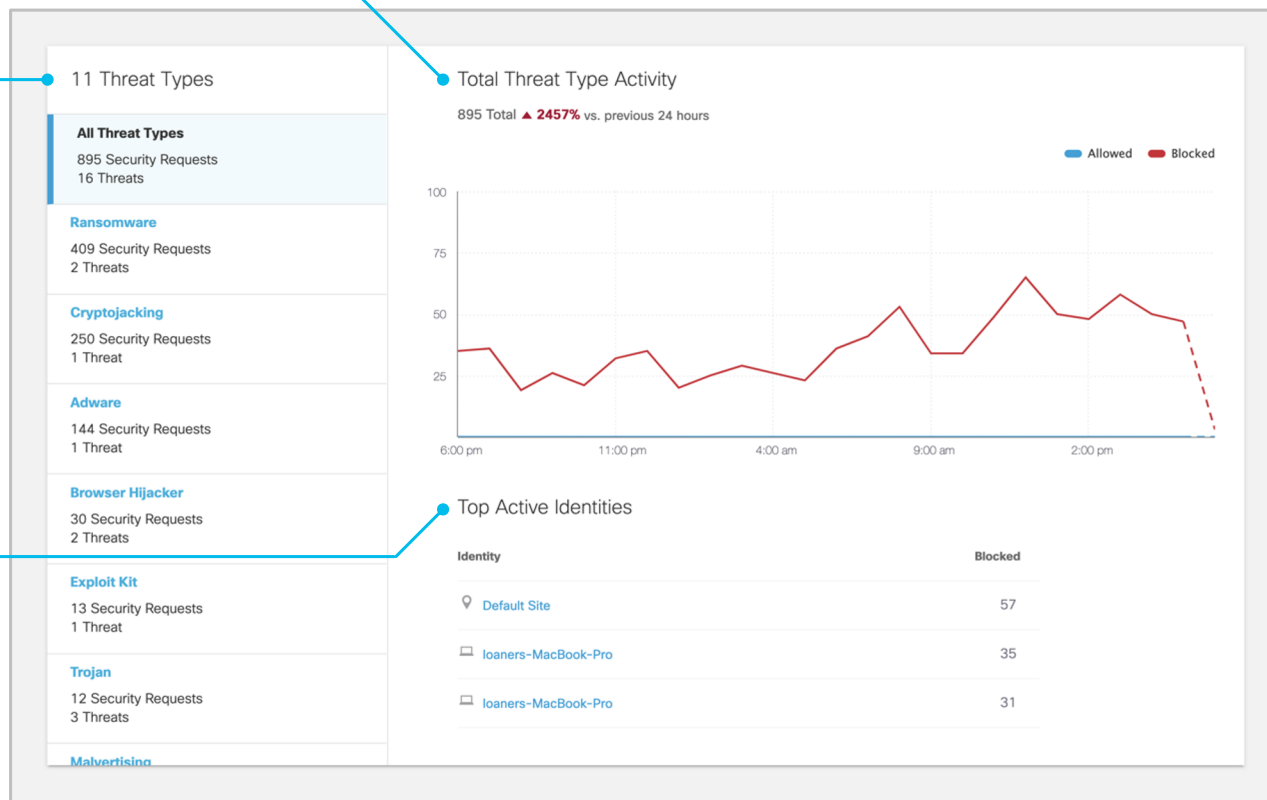
THREATS REPORT

Quickly spot and remediate victims

Top identities impacted by threats with ability to drill down

Recent threat trends

Breakdown of threat types



APP DISCOVERY REPORT

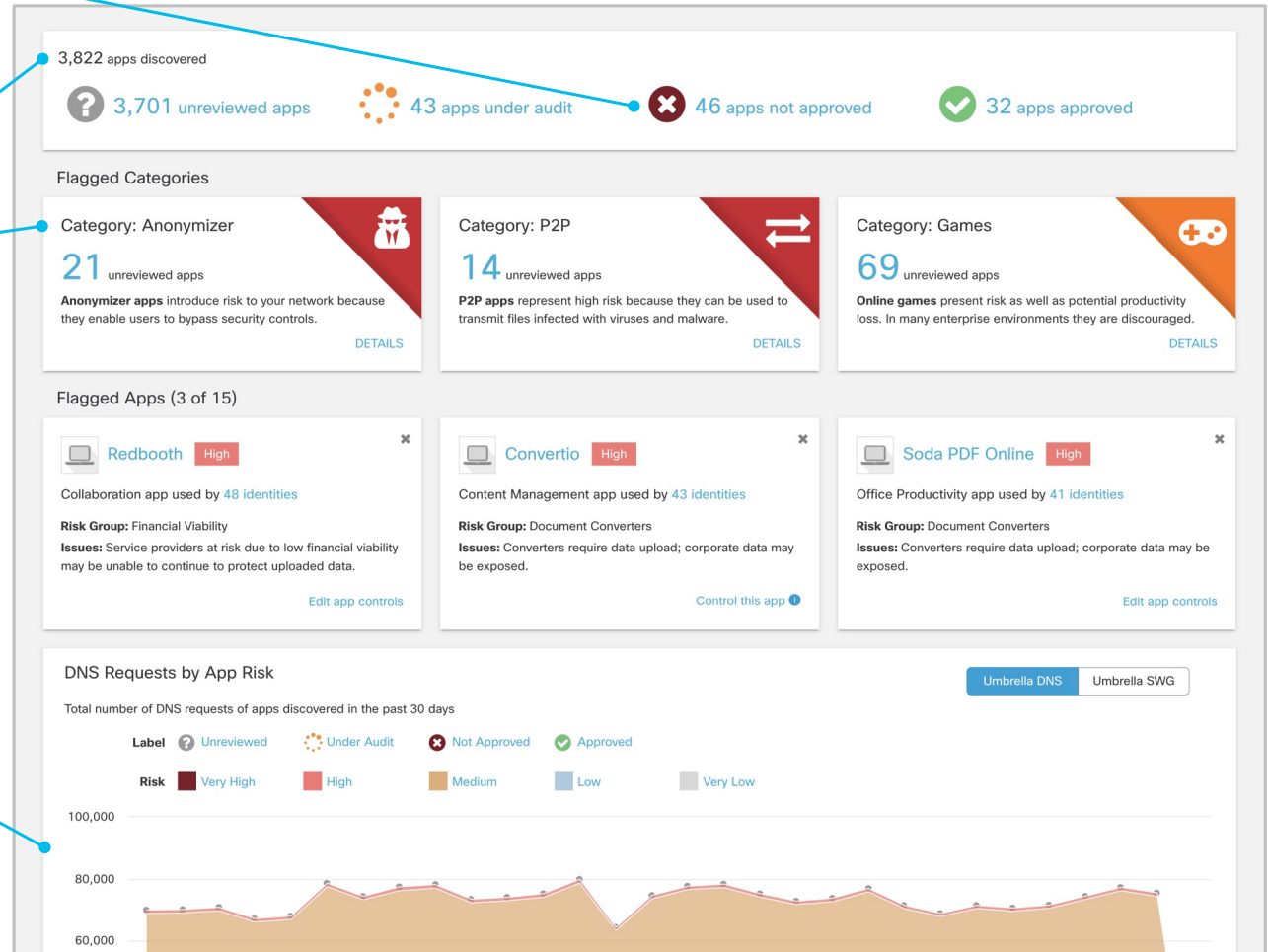
Manage Shadow IT to enable secure cloud adoption

Ability to easily block unapproved apps

Status of discovered apps

Summary of high-risk categories

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





SECURE