



Cisco Umbrella

Introducing Cisco Umbrella for cloud based threat protection

First line of defense for threats on the internet

Dragan Novakovic
Security CSE
April 2017

Hackers hijacked banks entire online operation

Hacking a bank isn't so different from the old-fashioned method of robbing one

The attackers compromised the bank's account at Registro.br - the domain registration service of NIC.br, the registrar for sites ending in the Brazilian .br top-level domain, which also managed the DNS for the bank. With that access, the attackers were able to change the registration simultaneously for all of the bank's domains, redirecting them to servers the attackers had set up on Google's Cloud Platform.



Agenda

Challenges
DNS
Product overview
Enforcement
Intelligence
Cloud platform
Deployment
Reporting and retention
Ransomware example

Challenges

The way we work has changed

Critical infrastructure

Amazon, Rackspace,
Windows Azure, etc.



Internet

Business apps

Salesforce, Office 365,
G Suite, etc.



Critical
infrastructure Business
apps



Workplace
desktops

Roaming laptops



Branch office

Users and apps have adopted the cloud, **security must too**

49%
of the workforce
is mobile

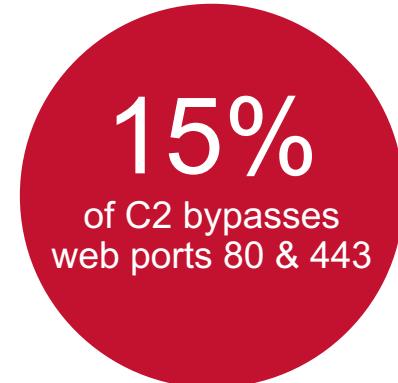
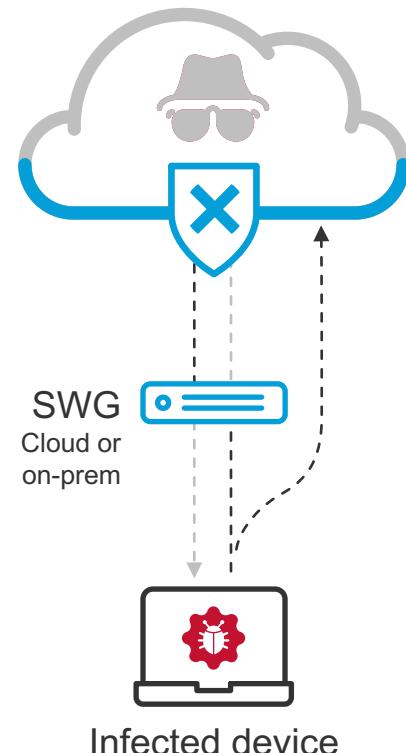
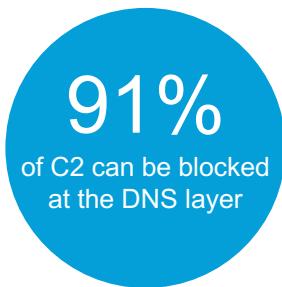
82%
admit to not
using the VPN

70%
increase in
SaaS usage

70%
of branch offices
have DIA



Protection for command and control (C2) callbacks



DNS

DNS

Overview



Domain registrar

Maps and records names
to #s in “phone books”



 Cisco Umbrella



Authoritative DNS

Owns and publishes
the “phone books”



Recursive DNS

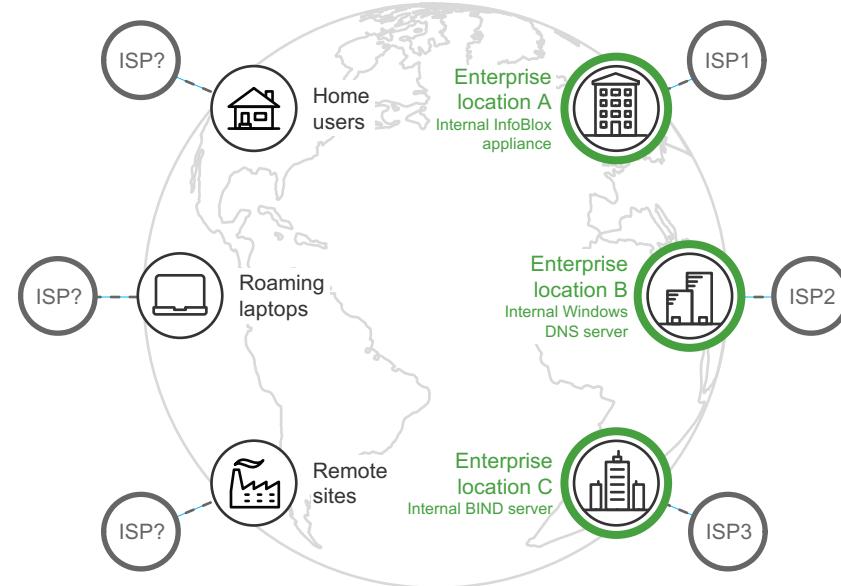
Looks up and remembers
the #s for each name



Who resolves your DNS requests?

Challenges

- Multiple internet service providers
- Direct-to-internet branch offices
- Users forget to always turn VPN on
- Different DNS log formats

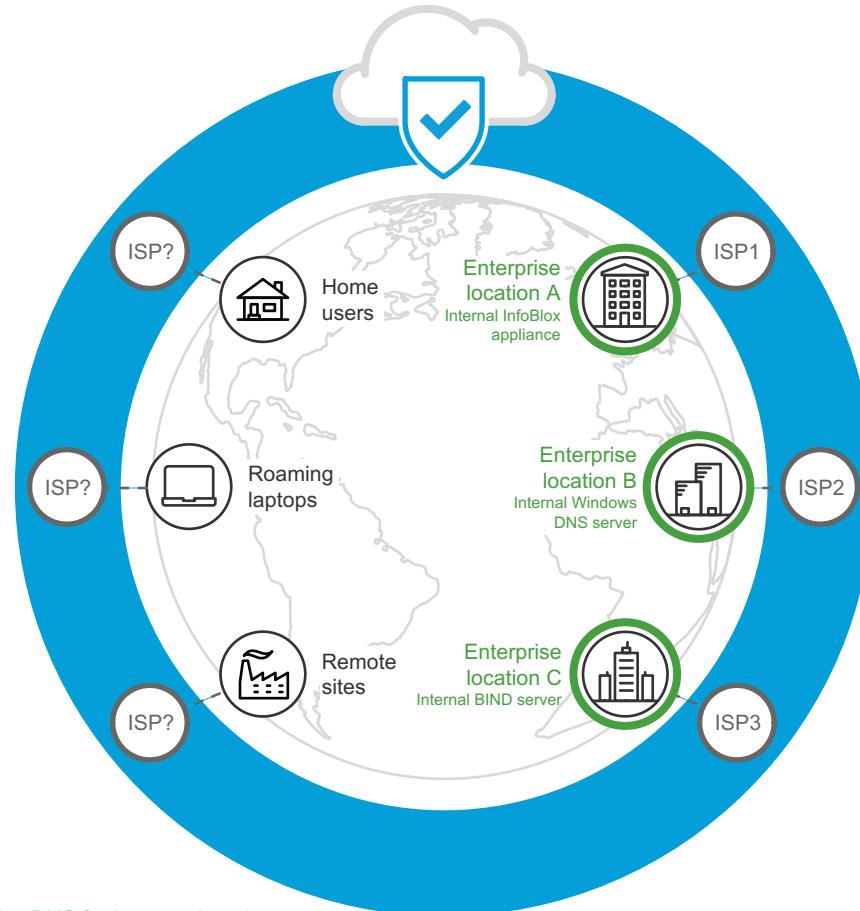


- Recursive DNS for internet domains
- Authoritative DNS for intranet domains

Using a single global recursive DNS service

Benefits

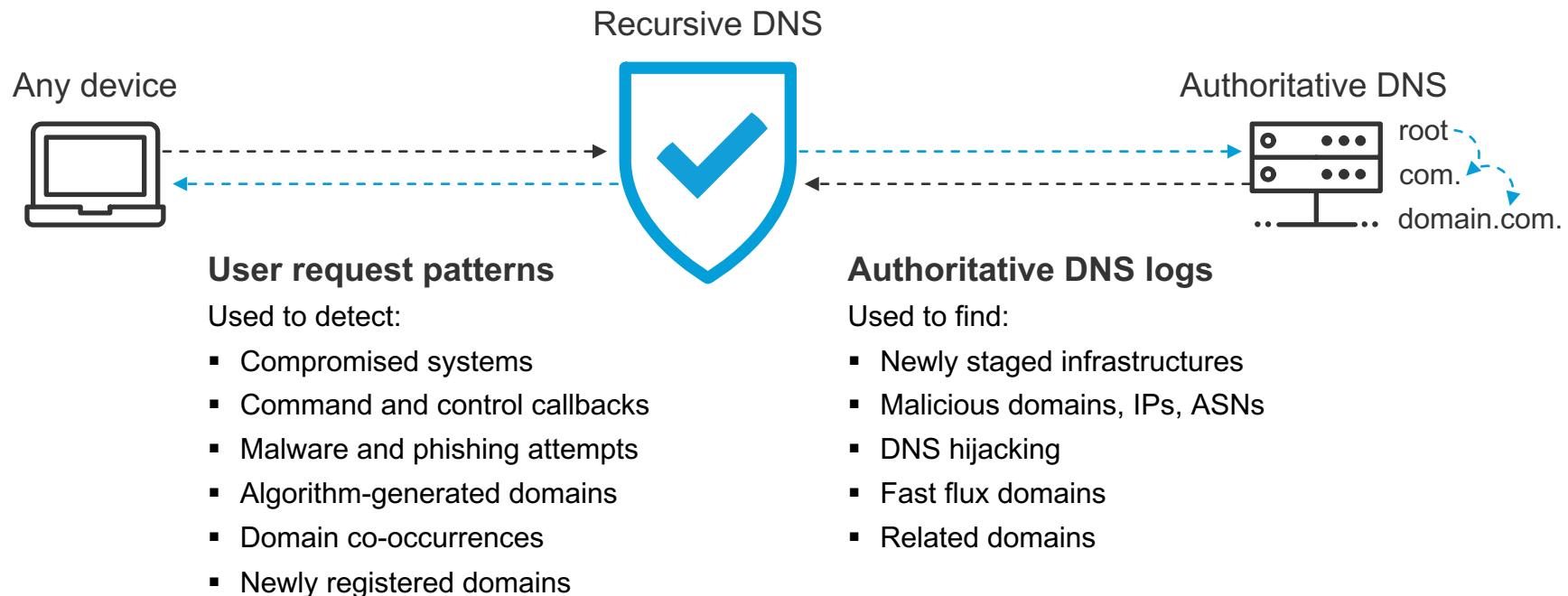
- Global internet activity visibility
- Network security w/o adding latency
- Consistent policy enforcement
- Internet-wide cloud app visibility



Recursive DNS for internet domains

Authoritative DNS for intranet domains

Gather intelligence and enforce security at the DNS layer



Product overview

Enforcement
Intelligence
Cloud platform
Deployment
Reporting and retention

Cisco Umbrella

Cloud security platform

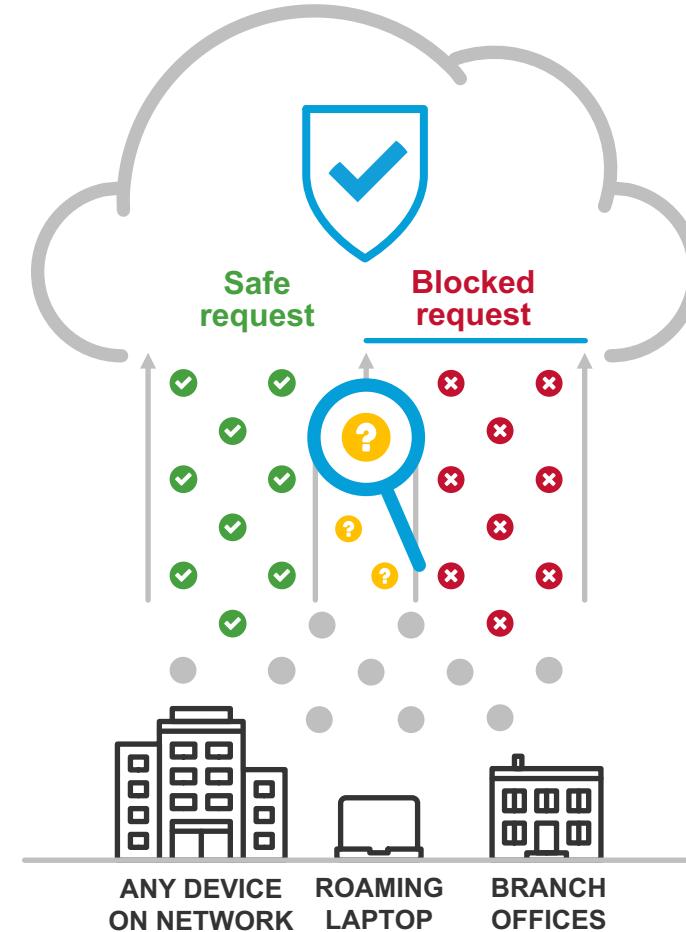
Built into the foundation of the internet

Intelligence to see attacks before launched

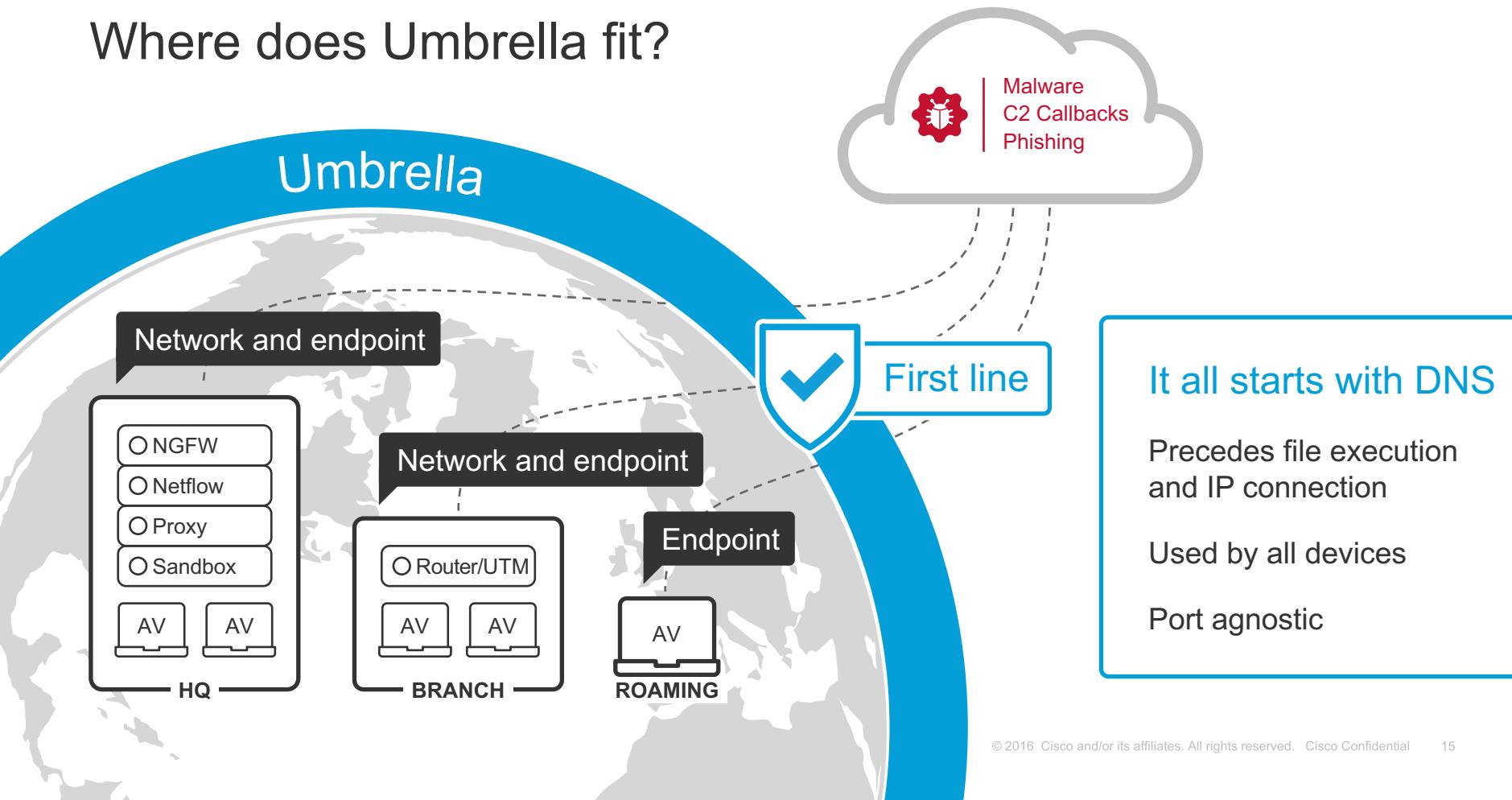
Visibility and protection everywhere

Enterprise-wide deployment in minutes

Integrations to amplify existing investments



Where does Umbrella fit?



Built into foundation of the internet

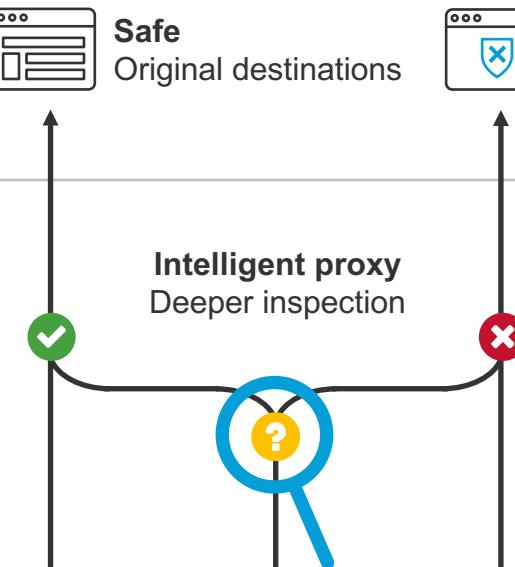
Destinations

Original destination or block page



Security controls

- DNS and IP enforcement
- Risky URL inspection through proxy
- SSL decryption available



Internet traffic

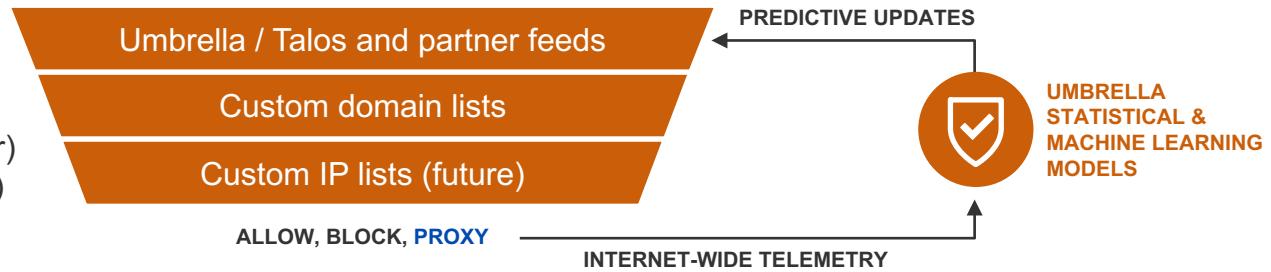
On and off-network

 Cisco Umbrella

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



Web and email-based infection

Malvertising / exploit kit

Phishing / web link

Watering hole compromise



Command and control callback

Malicious payload drop

Encryption keys

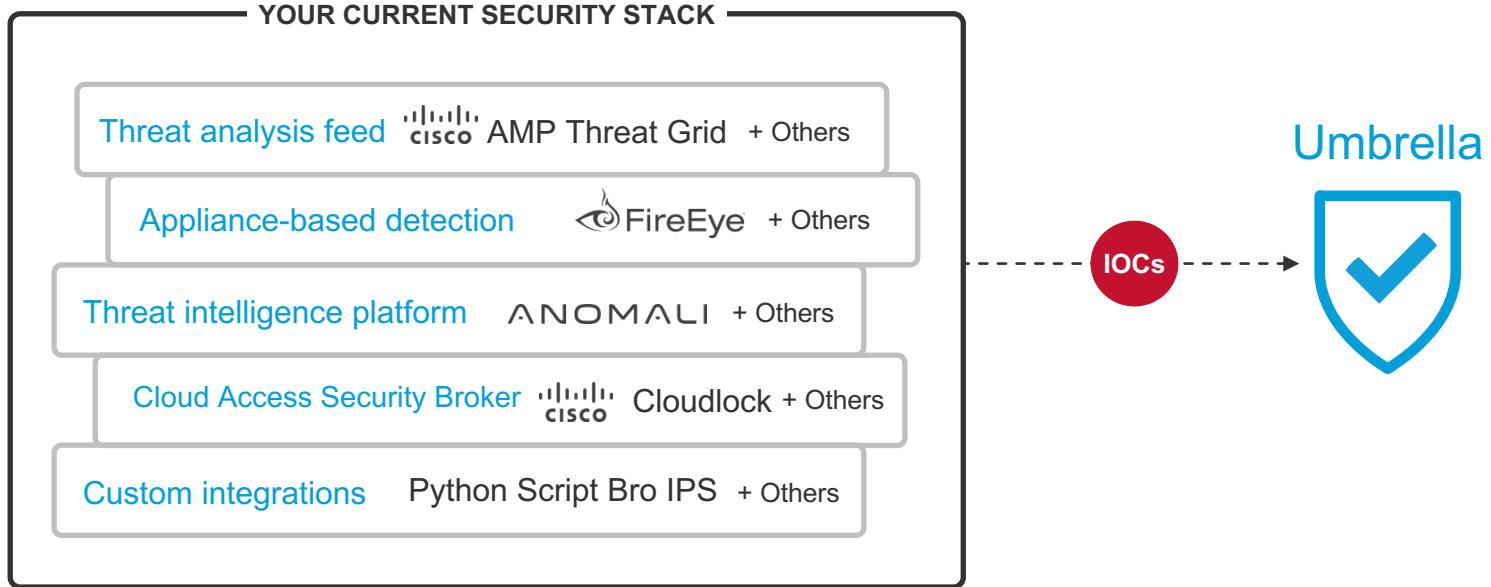
Updated instructions



Stop data exfiltration and ransomware encryption

Integrations to amplify existing security

Block malicious domains from partner or custom systems



Our view of the internet

100B

requests
per day

85M

daily active
users

12K

enterprise
customers

160+

countries
worldwide

Intelligence to see attacks before launched

Data

- Cisco Talos feed of malicious domains, IPs, and URLs
- Umbrella DNS data — 100B requests per day



Models

- Dozens of models continuously analyze millions of live events per second
- Automatically uncover malware, ransomware, and other threats

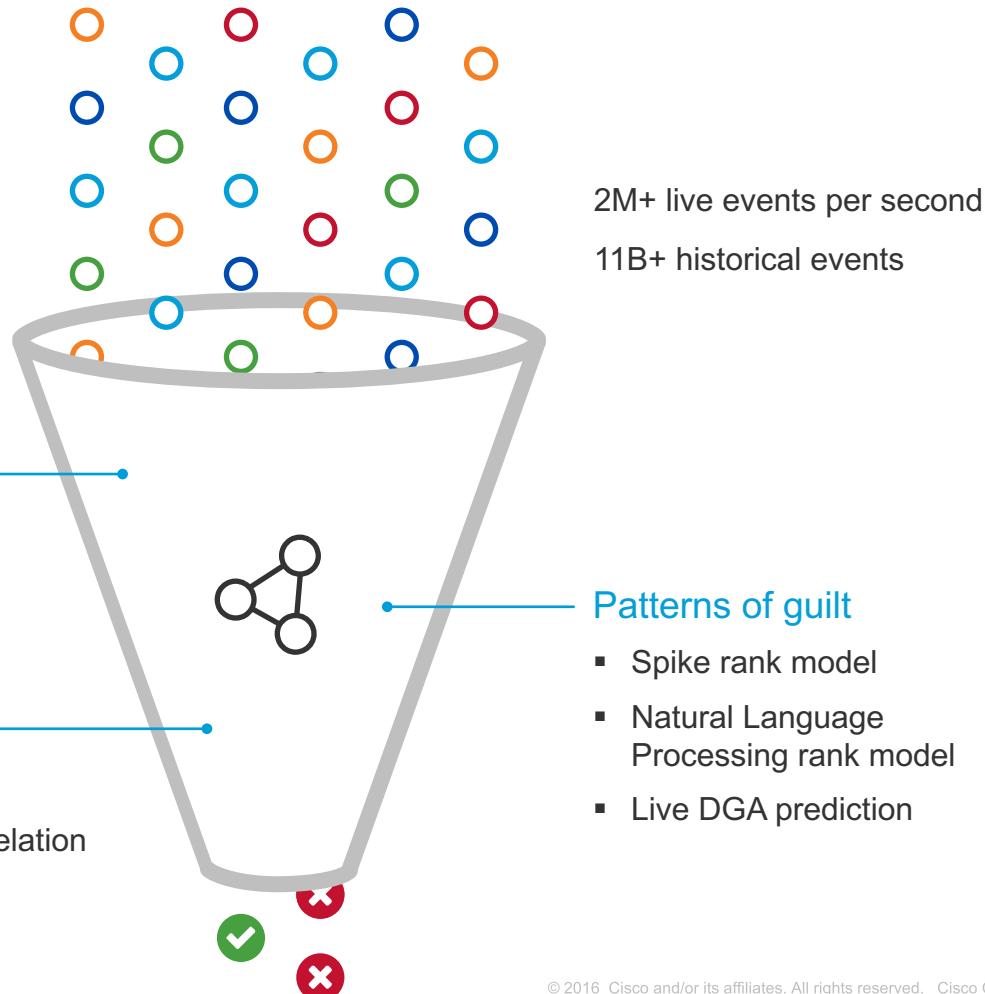


Security researchers

- Industry renown researchers
- Build models that can automatically classify and score domains and IPs

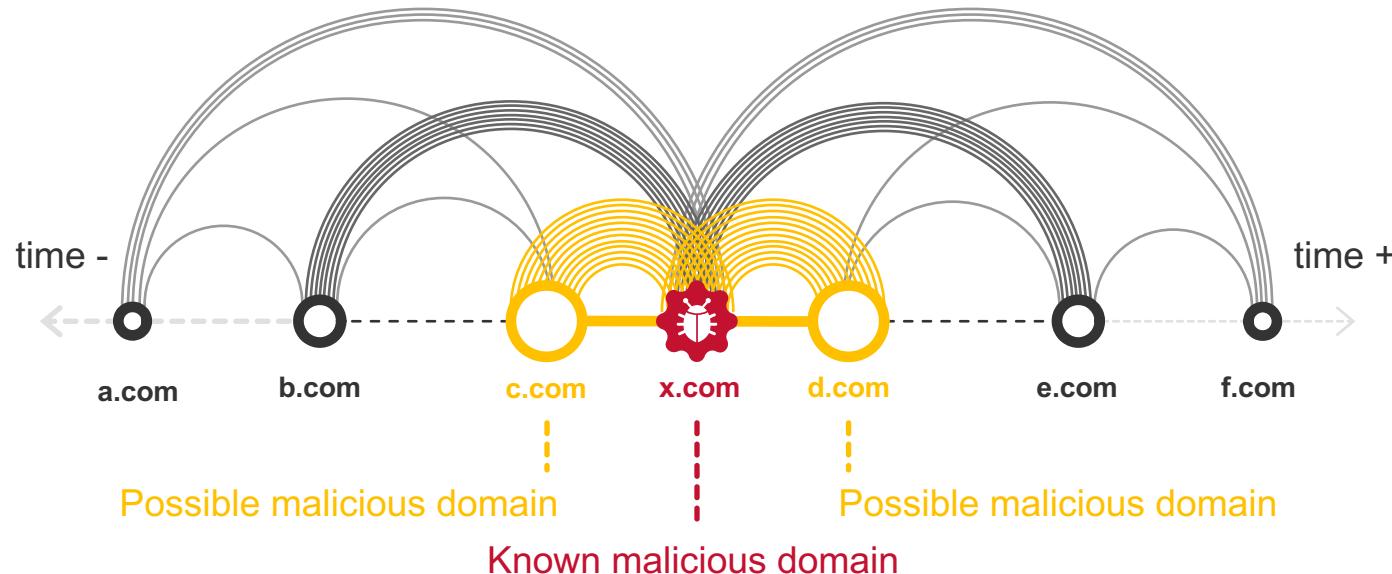


Statistical models



Co-occurrence model

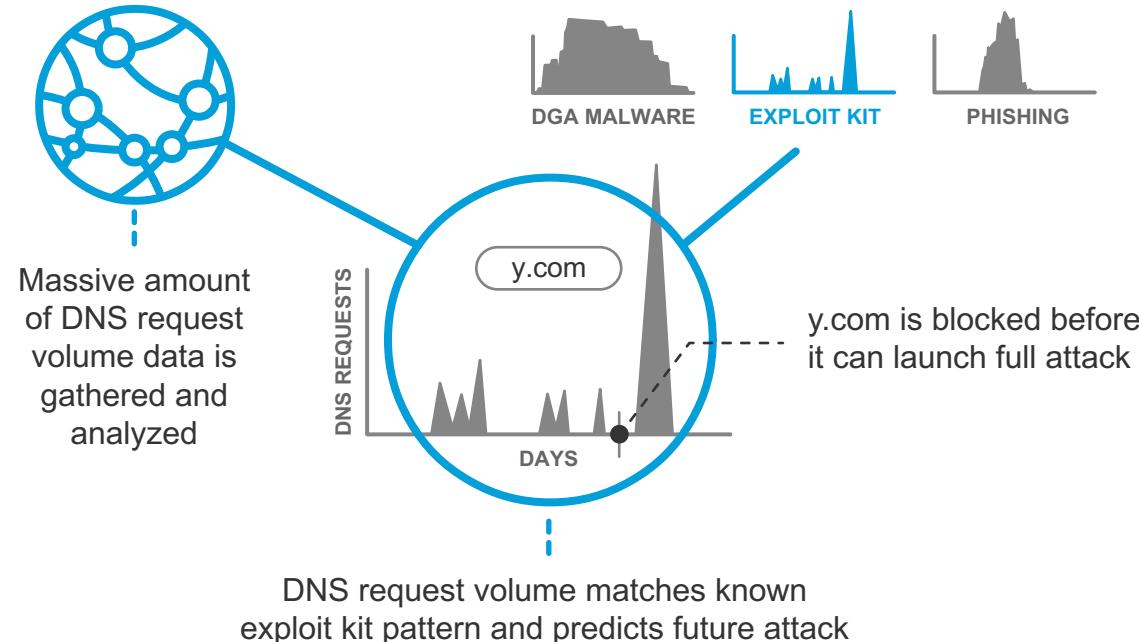
Domains guilty by inference



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

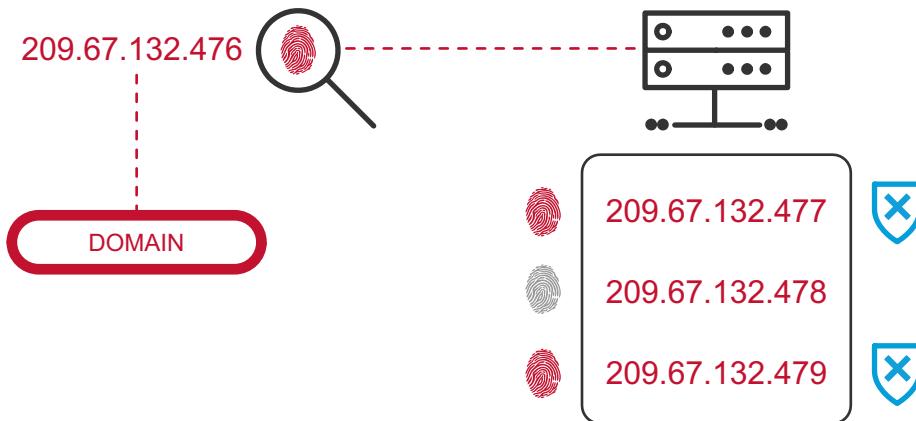
Spike rank model

Patterns of guilt



Predictive IP Space Monitoring

Guilt by association



Pinpoint suspicious domains and observe their IP's fingerprint

Identify other IPs – hosted on the same server – that share the same fingerprint

Block those suspicious IPs and any related domains

IP geo-location analysis

Host Infrastructure

Location of the server
IP addresses mapped to domain



Hosted across 28+ countries

DNS Requesters

Location of the network and off-network device
IP addresses requesting the domain

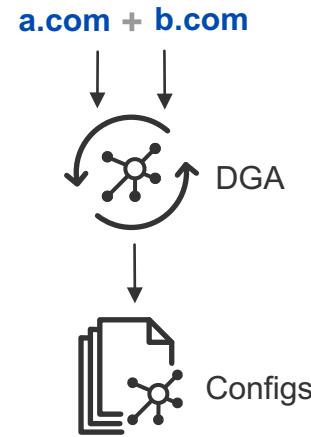


Only US-based customers
requesting a .RU TLD

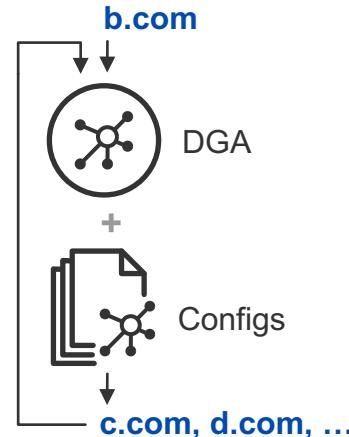
'Live DGA Prediction' automated at an unparalleled scale



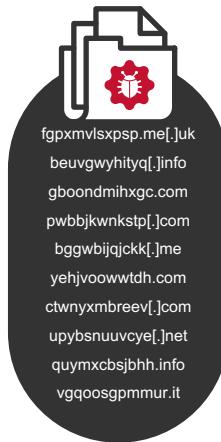
Identify millions of domains, many used by DGAs and unregistered



Combine C2 domain pairs and known DGAs to identify unknown configs

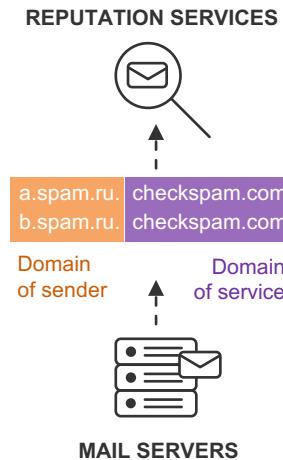


Combine newly-identified configs with DGA to identify C2 domains continuously



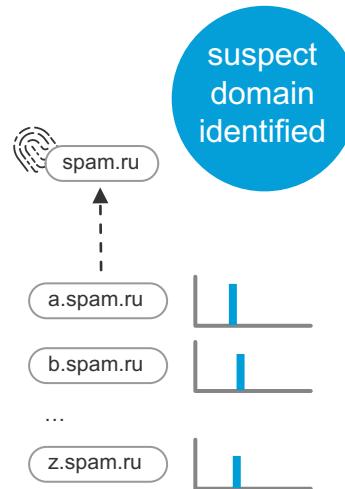
Used by thousands of malicious samples now and in the future

'Sender Rank' model: predict domains related to spammers



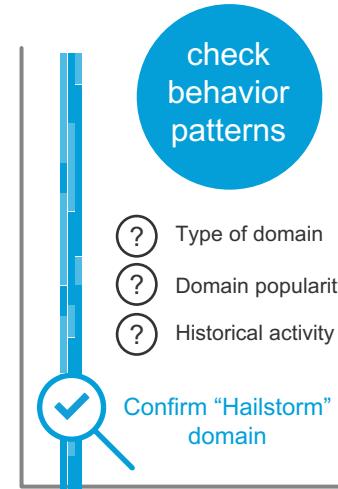
Identify queries to spam reputation services

85M+ DNS users are attacked by various spam campaigns and use reputation services



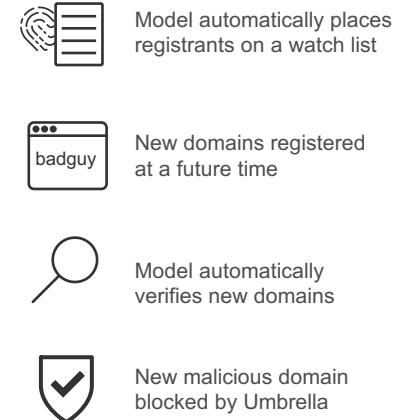
Model aggregates hourly graphs per domain

Short bursts of 1000s of "Hailstorm" spam uses many FQDNs, e.g. subdomains, to hide from reputation services



Model identifies owners of "Hailstorm" domains

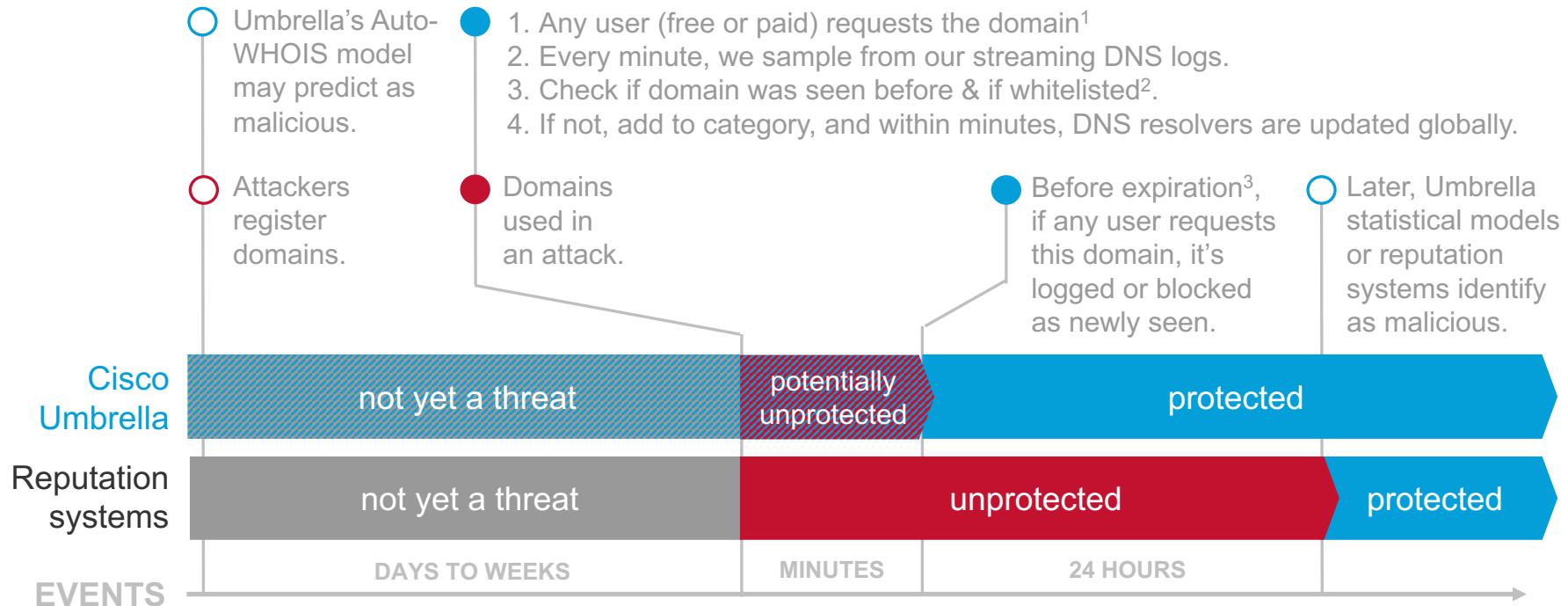
After confirmation, query WHOIS records to get registrant of sender domain



Block 10,000s of domains before new attacks happen

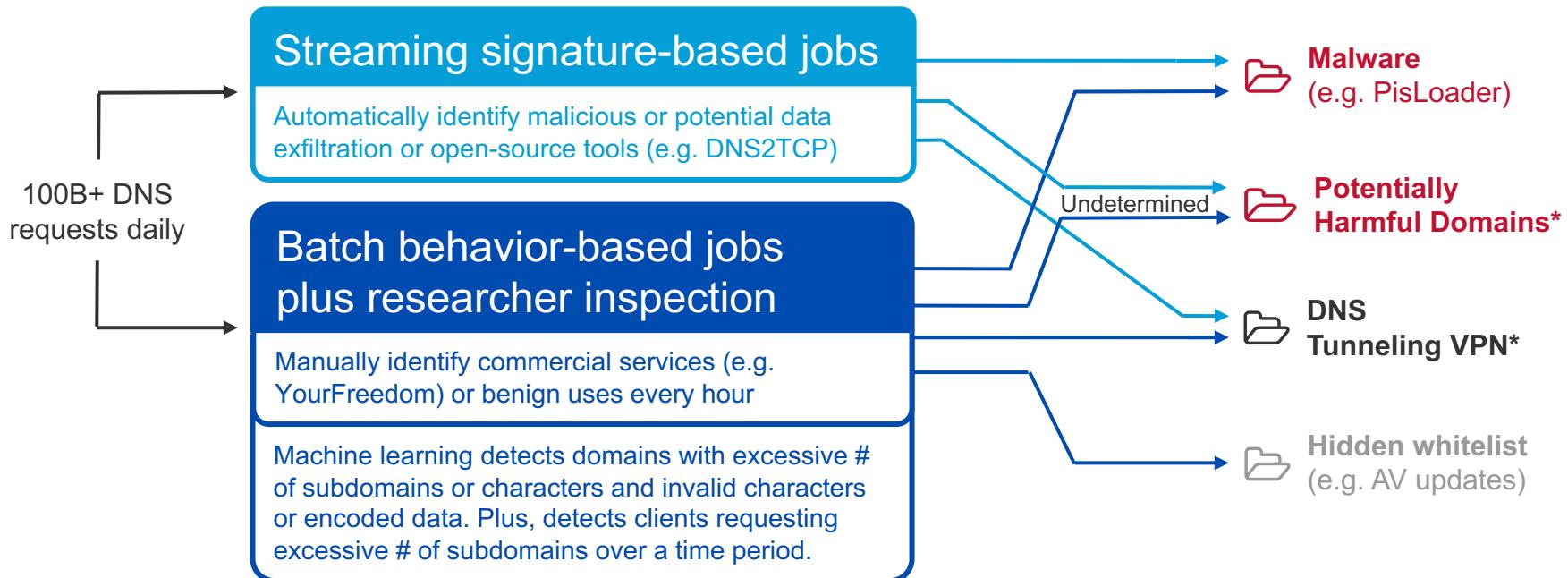
Attackers often register more domains to embed links in phishing or C2 callbacks in malware

'Newly Seen Domains' category reduces risk of the unknown



- May have predictively blocked it already, and likely the first requestor was a free user.
- E.g. domain generated for CDN service.
- Usually 24 hours, but modified for best results, as needed.

New analysis and categories to combat DNS tunneling



Our efficacy

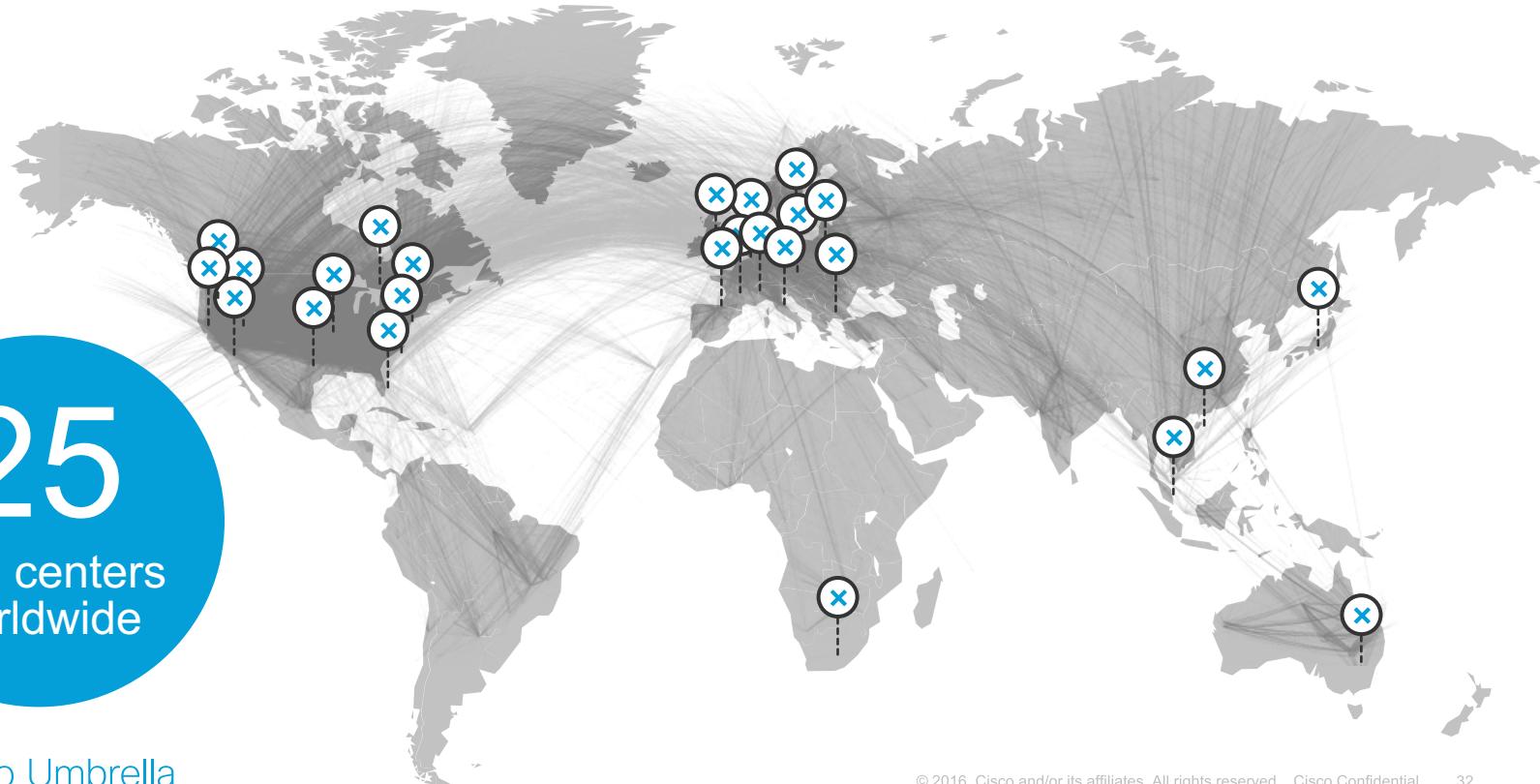
Discover
3M+
daily new
domain names

Identify
60K+
daily malicious
destinations

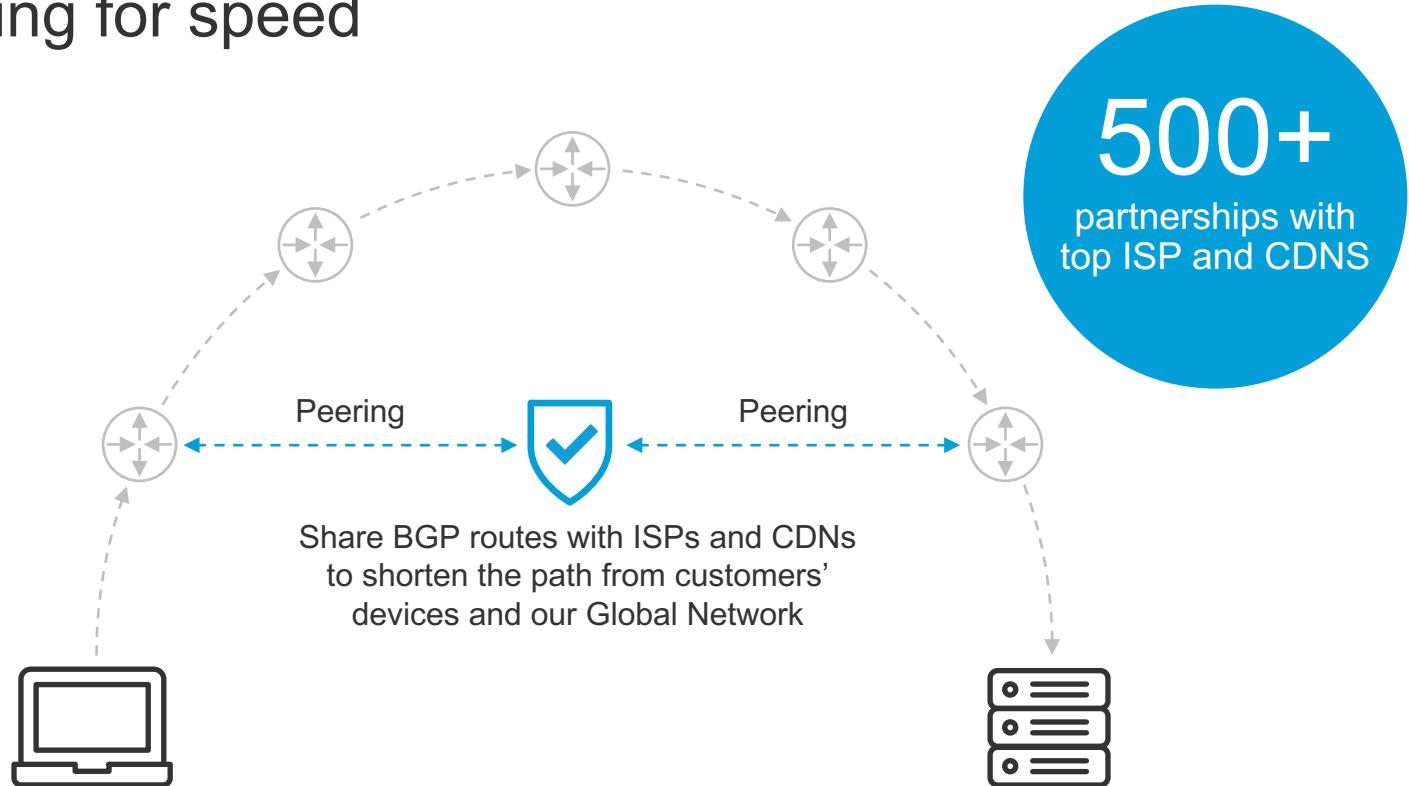
Enforce
7M+
malicious destinations
while resolving DNS

Data centers co-located at major IXPs

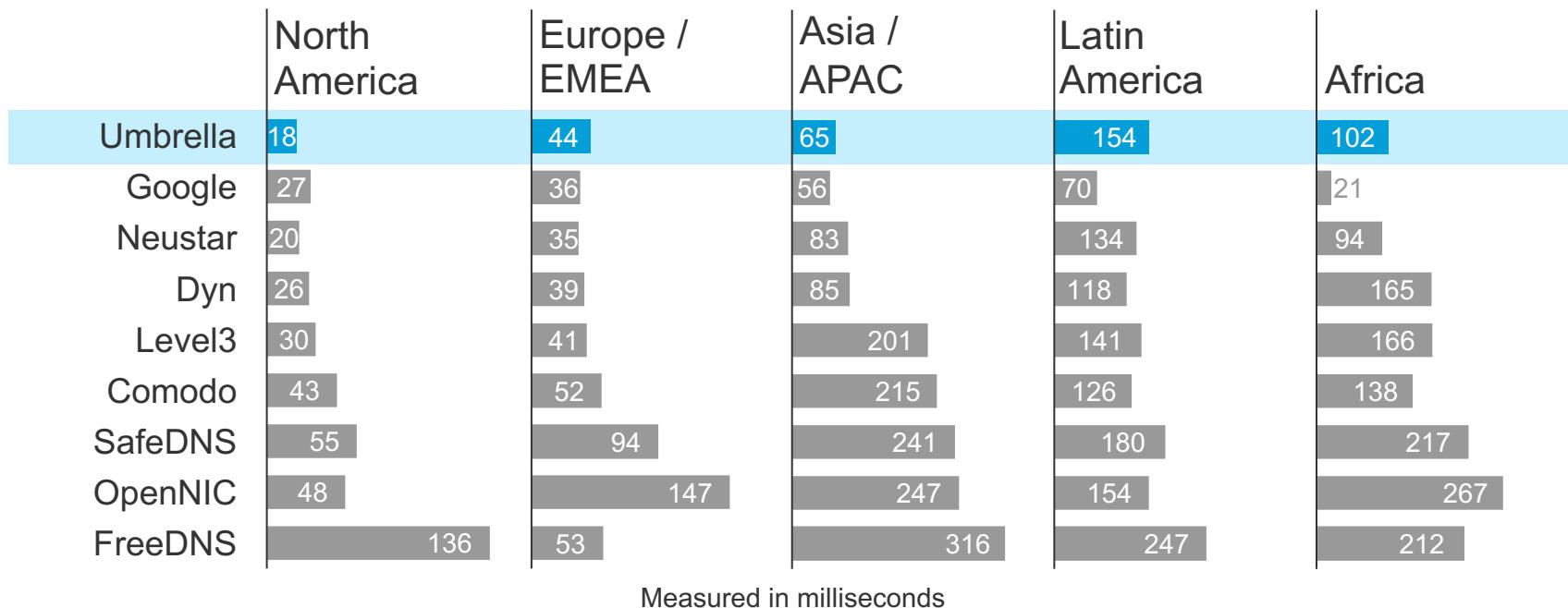
25
data centers
worldwide



BGP peering for speed



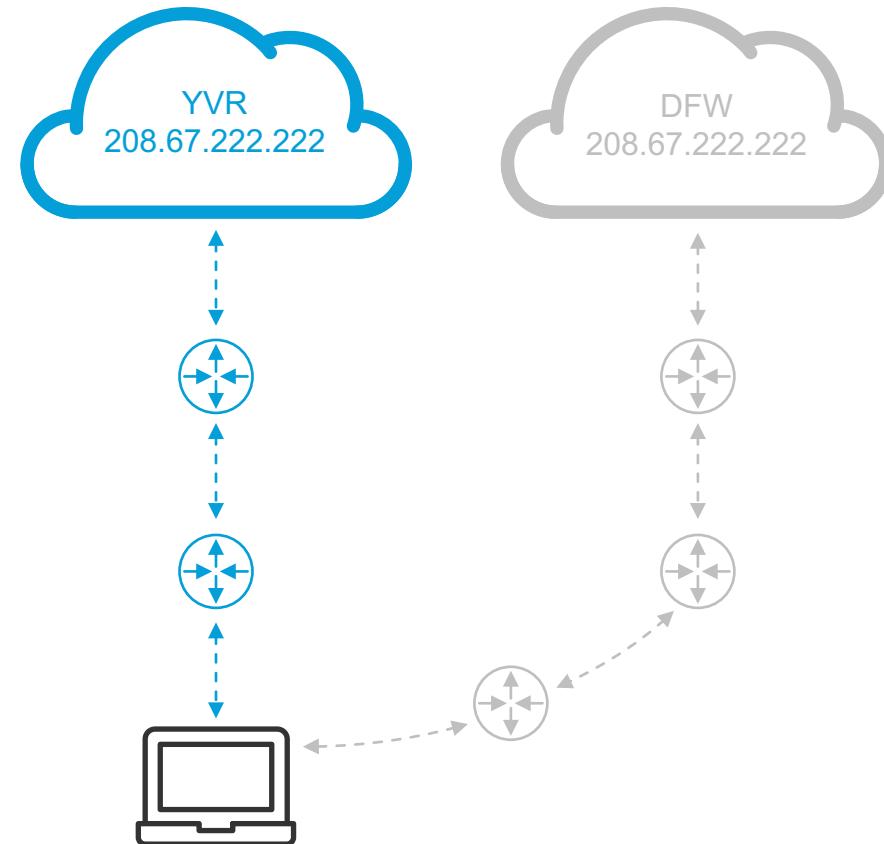
How fast do we resolve DNS requests?



Anycast IP routing for reliability

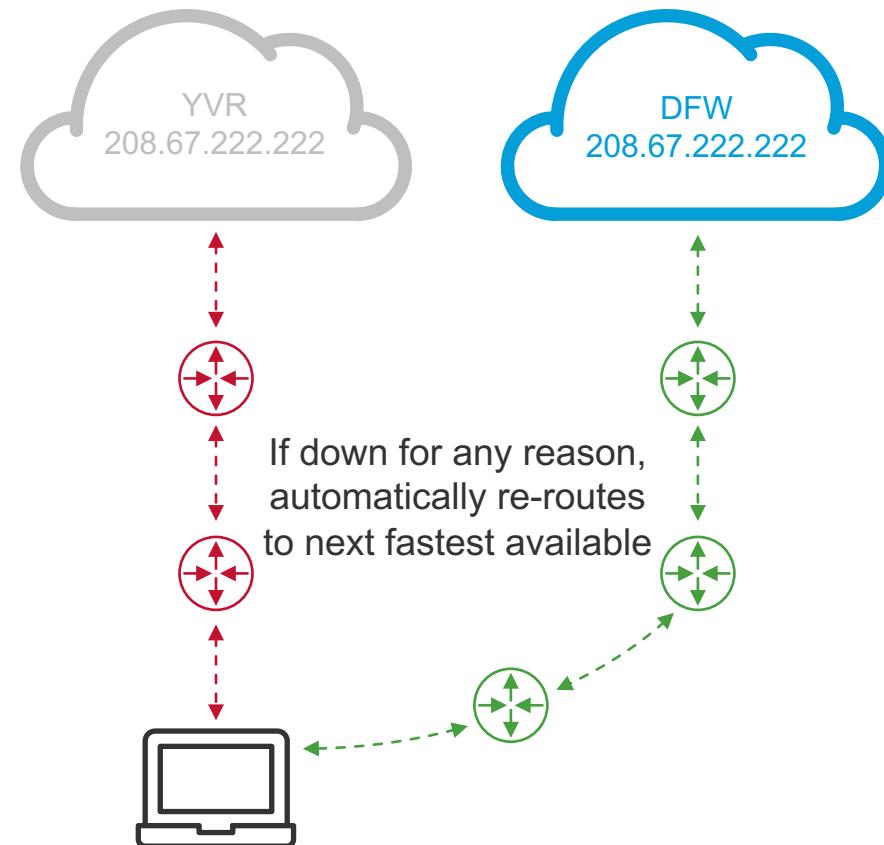
All data centers announce
same IP address

Requests transparently sent
to fastest available



Anycast IP routing for reliability

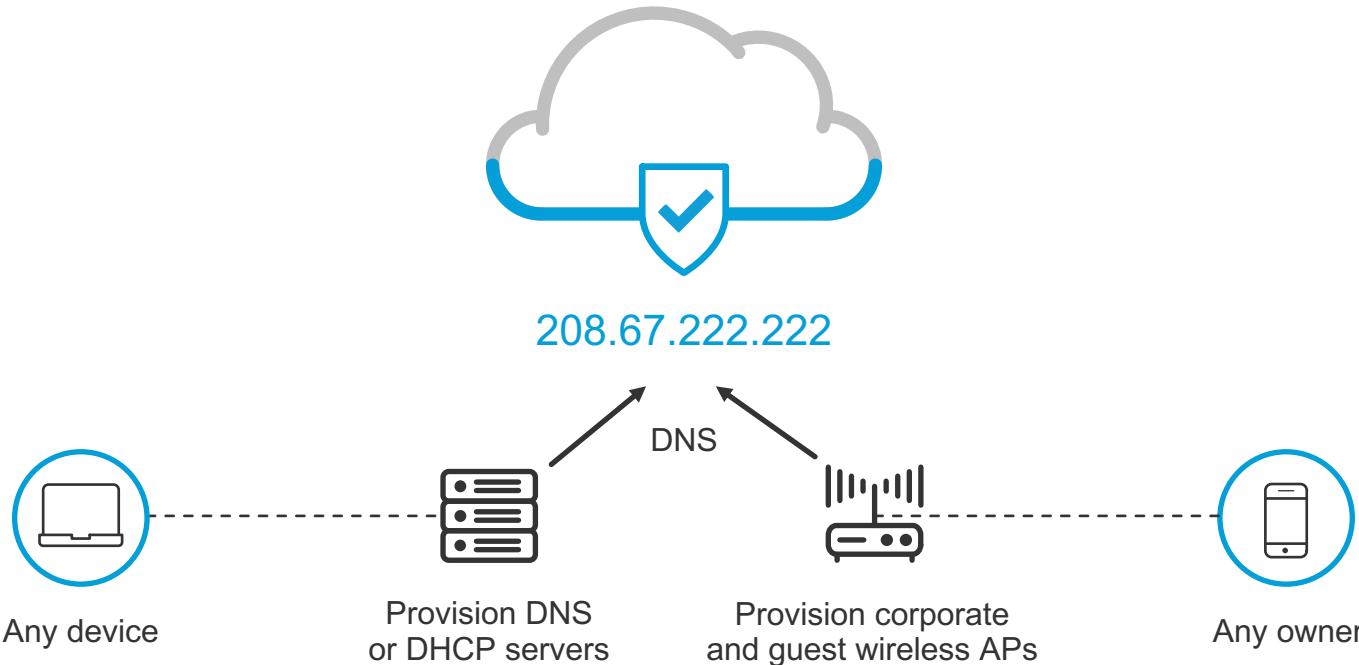
100%
uptime since 2006
DDoS protection and
global fail-over



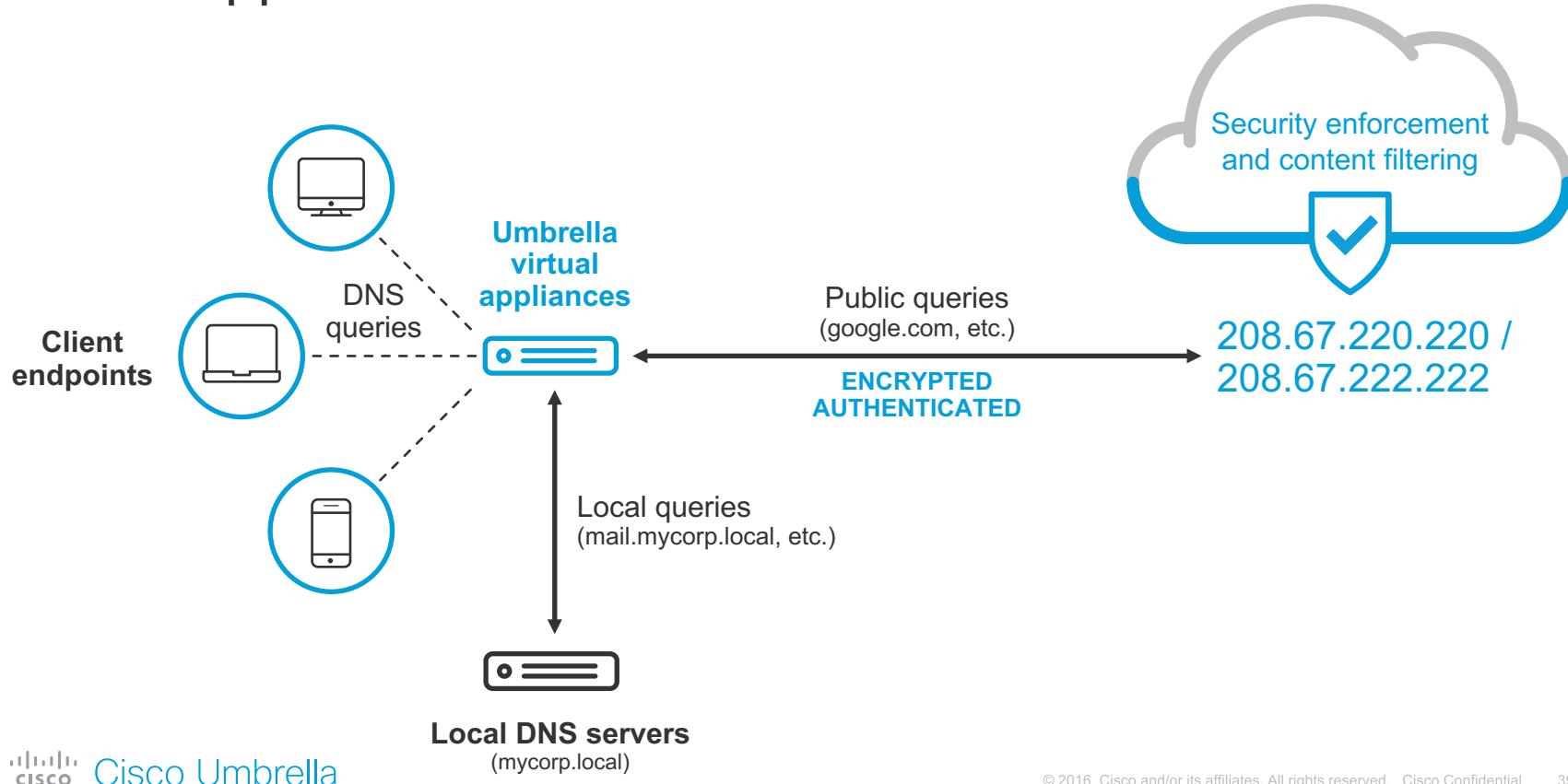
Deployment

Simplest way to protect any device on-network

Point external DNS traffic to Umbrella



Virtual appliance for AD and internal networks



Cisco AnyConnect module

Roaming protection without another agent

- 1 Enable roaming security module
- 2 Set roaming policy in Umbrella
- 3 Gain visibility into internet activity
and detailed logs for incident response

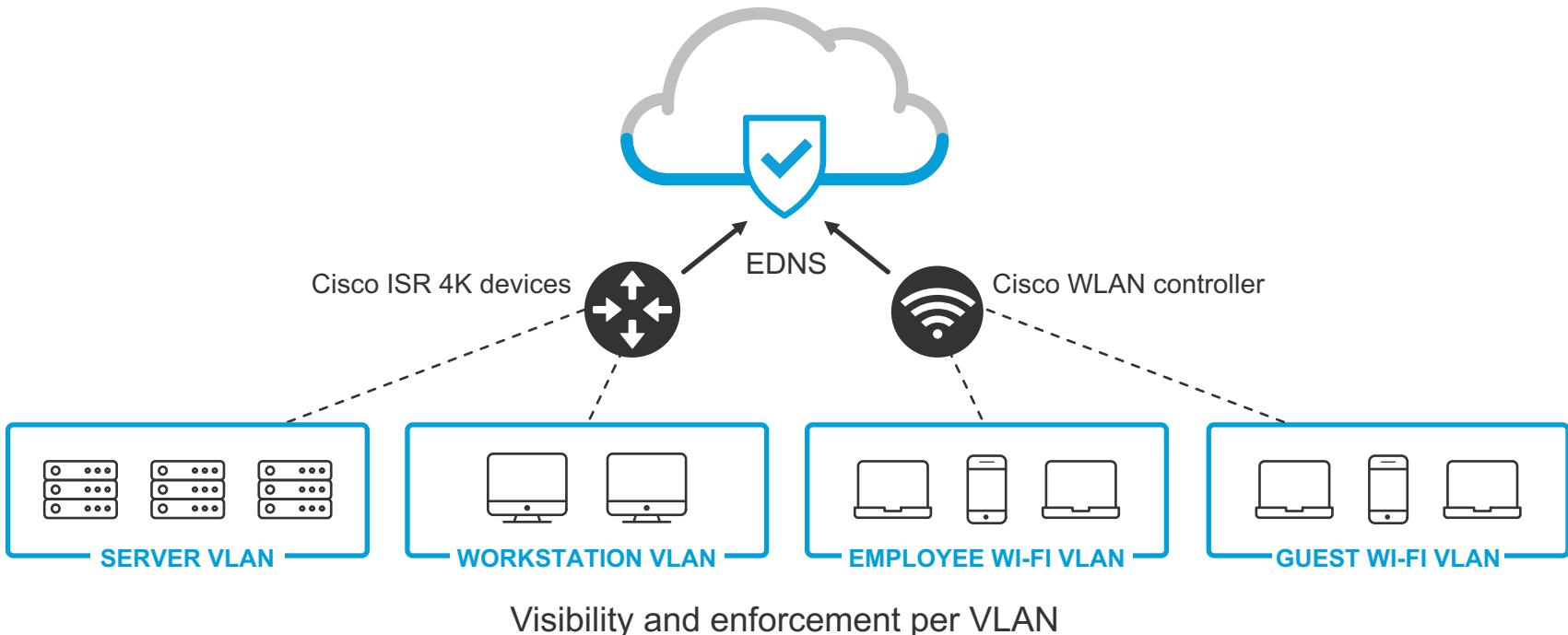


208.67.222.222



Integration with Cisco ISR 4K devices and WLAN controllers

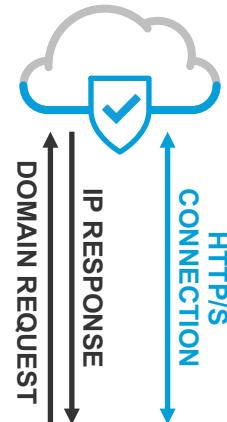
Protection for branch offices and Wi-Fi users



DEPLOYMENT

Enforcement and visibility per Umbrella identity

Securely embed identities within query using a RFC-compliant mechanism, differing granularity based on deployment



Web-based redirects transparent to user enable same identity for proxy

NETWORK VIA EGRESS IP FOR ALL DEPLOYMENTS					
Umbrella deployments	Your DNS or DHCP server	Umbrella roaming client (RC)	Umbrella AD Connector	Umbrella virtual appliance (VA)	Umbrella API for network devices
Umbrella identities	N/A	Hostname (GA) Internal IPs (LA) Usernames* (LA)	*Usernames with groups for RC and VA	Internal IPs Subnets Usernames*	Network device names or VLAN IDs

How Umbrella fits with Cisco Web Security Appliance (WSA)

Flexibility to fit customers' use cases



Umbrella provides safe internet access anywhere users go, even off the VPN

WSA solves on-prem requirements for usage/bandwidth controls and compliance

Cisco Defense Orchestrator (CDO) for ongoing policy management

Single place to add domains/URLs to block across cloud (Umbrella) and on-prem (WSA, NGFW)

DEPLOYMENT

On-network: simple to point external DNS without clients

DHCP server

Simple for locations without internal domains



DNS server

Simple for locations that manage internal domains

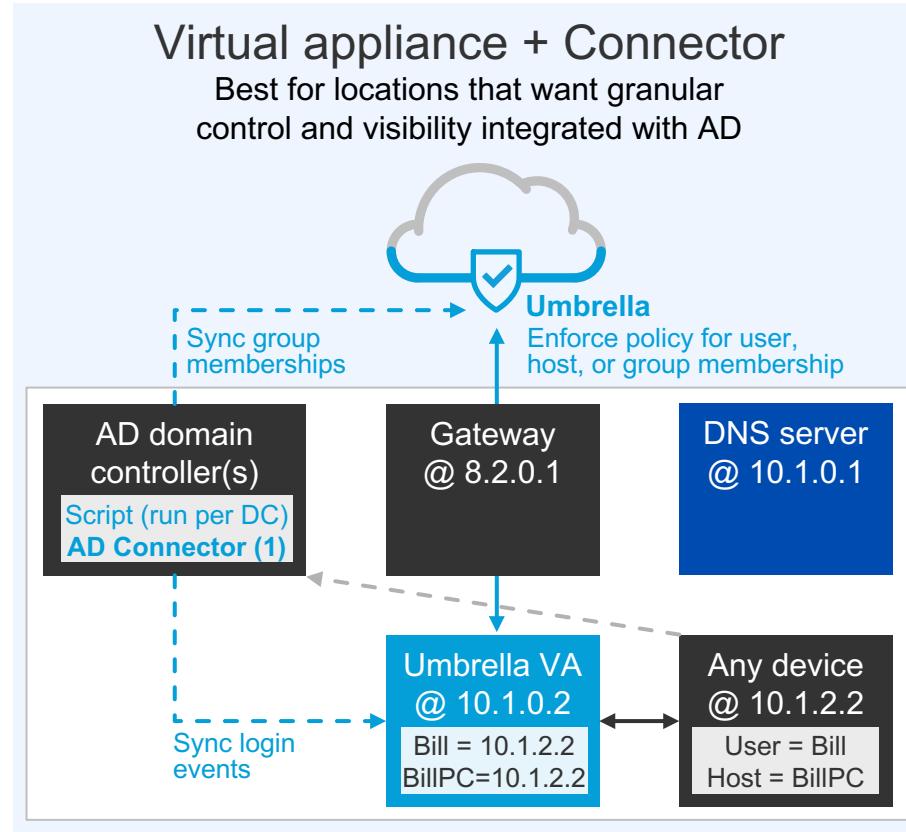


Virtual appliance

Best for locations that want granular control & visibility



On-network: adding user-based enforcement without clients

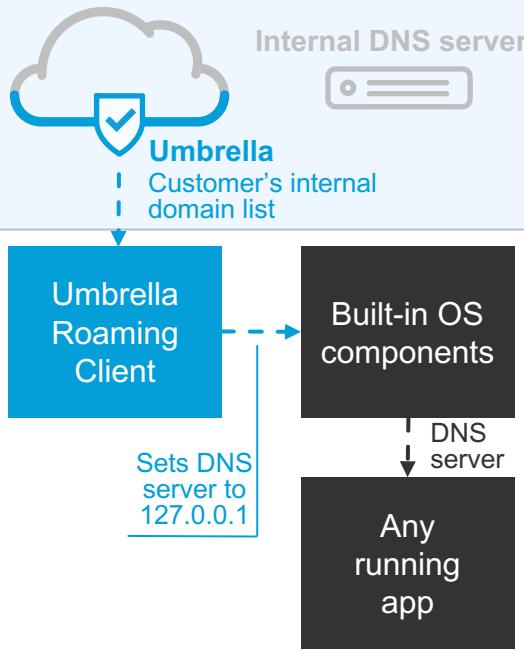


DEPLOYMENT

Roaming: DNS-layer security via Umbrella's roaming client

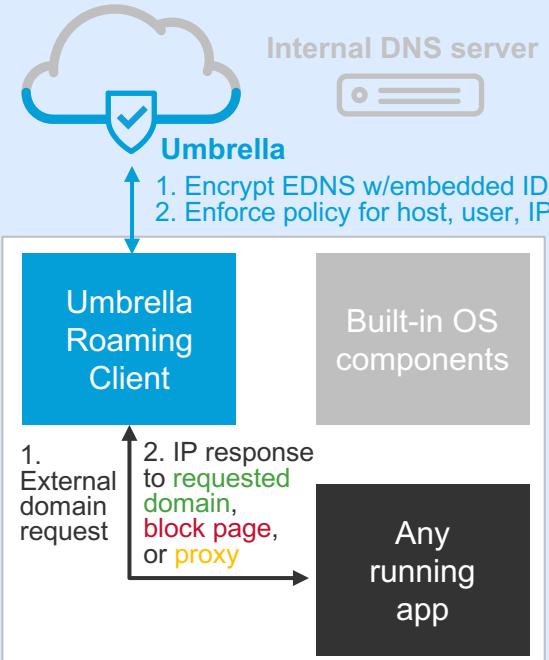
Step 1

Client watches for new networks and continuously sets DNS



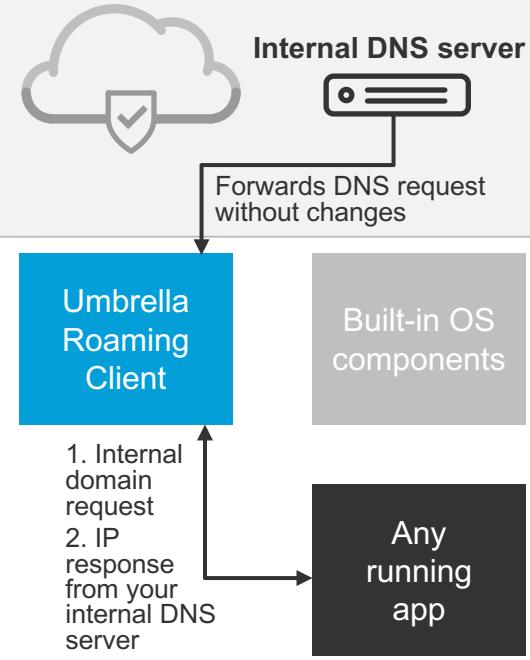
Step 2a

External (internet) domains resolved by Umbrella



Step 2b

Internal (intranet) domains resolved by your DNS server

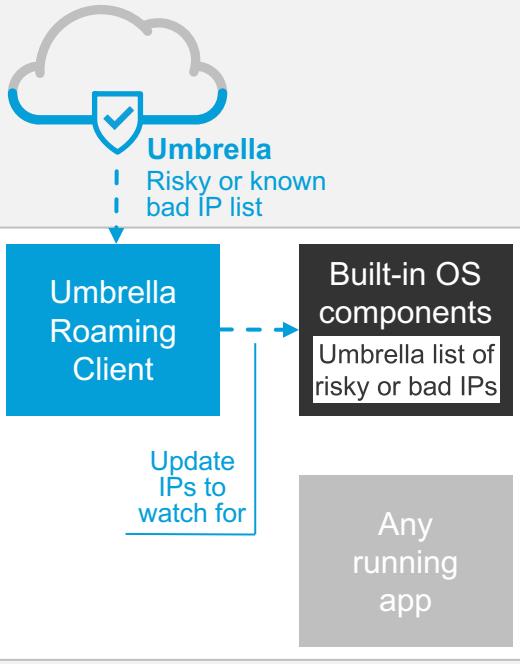


DEPLOYMENT

Roaming: adding IP-layer enforcement without a full VPN

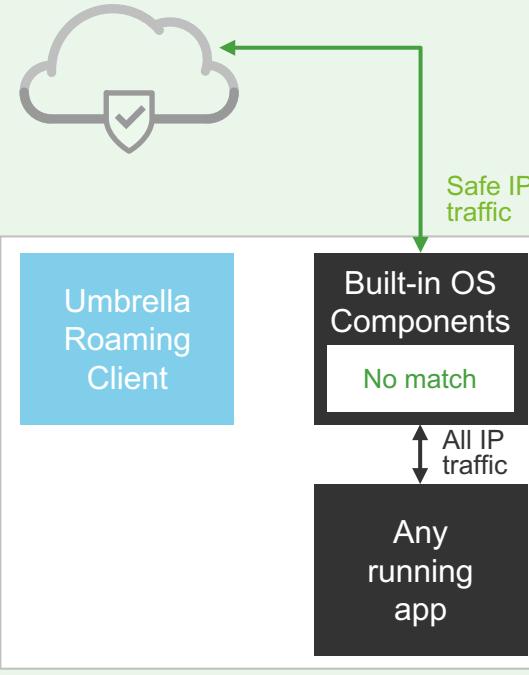
Step 1

Client continuously updates list and OS watches for matching IP traffic



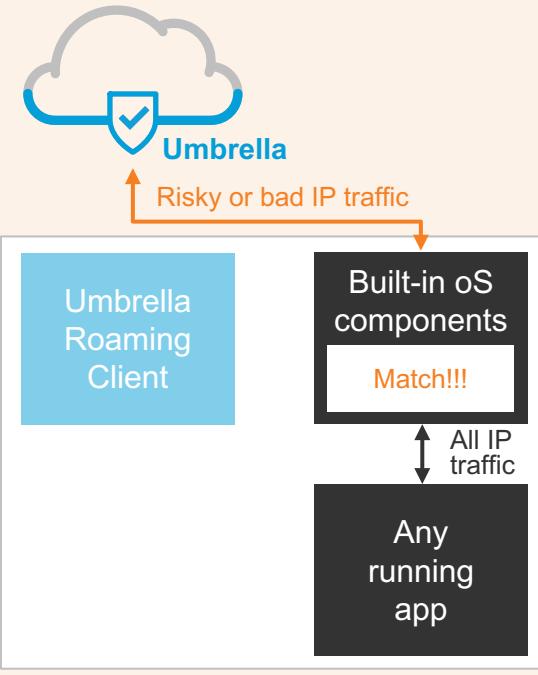
Step 2a

Most traffic routed directly to internet



Step 2b

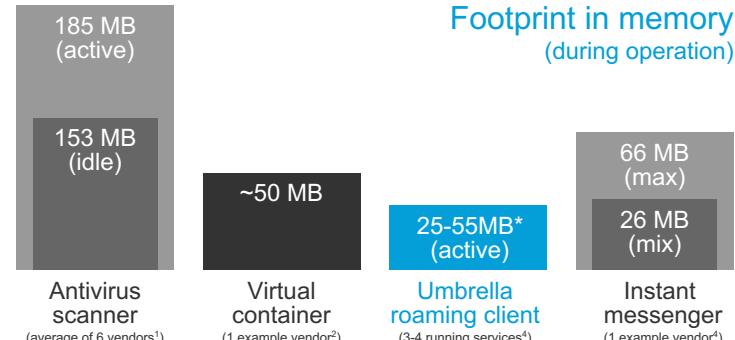
Some traffic tunneled through Umbrella



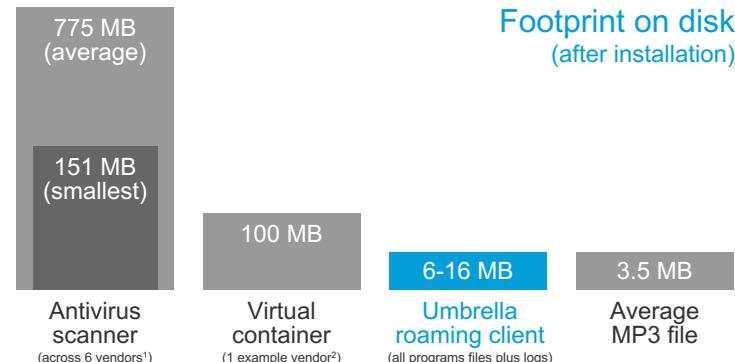
Umbrella's roaming client

Roaming protection with a lightweight agent

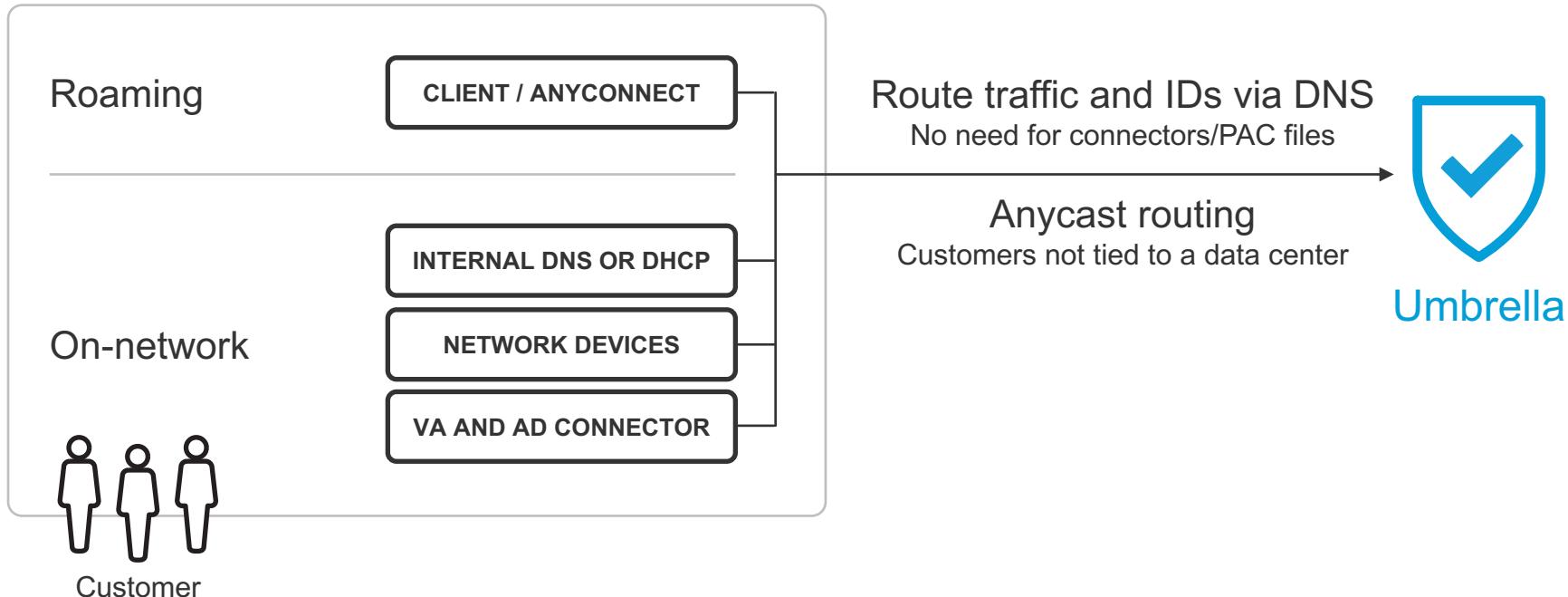
- 1 Install roaming client



- 2 Set roaming policy in Umbrella

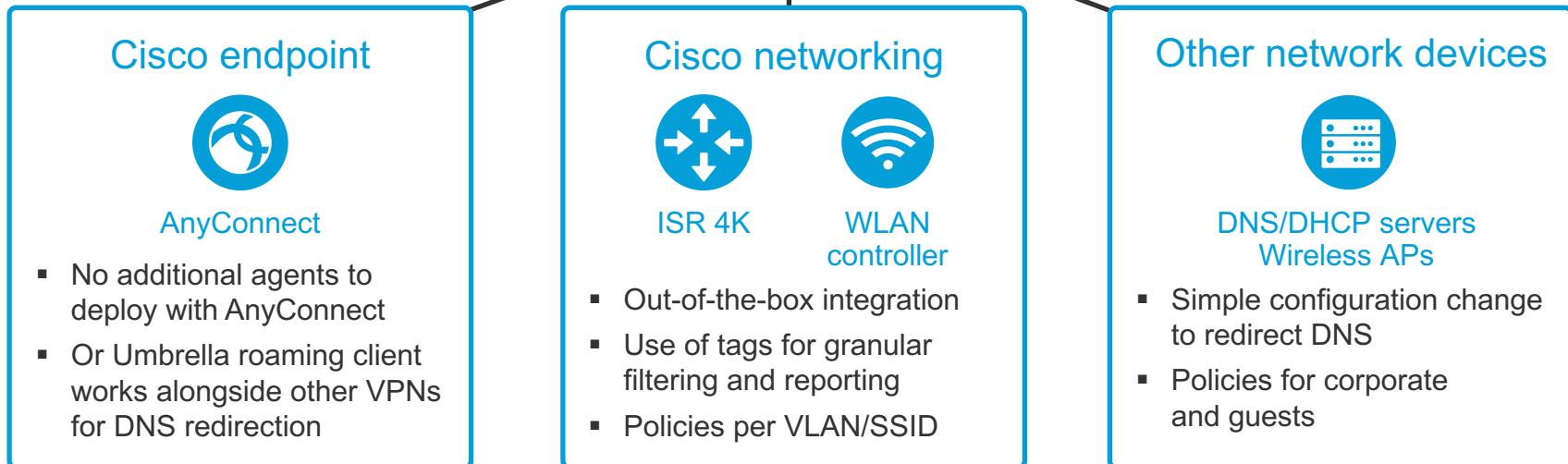


Connecting to Umbrella

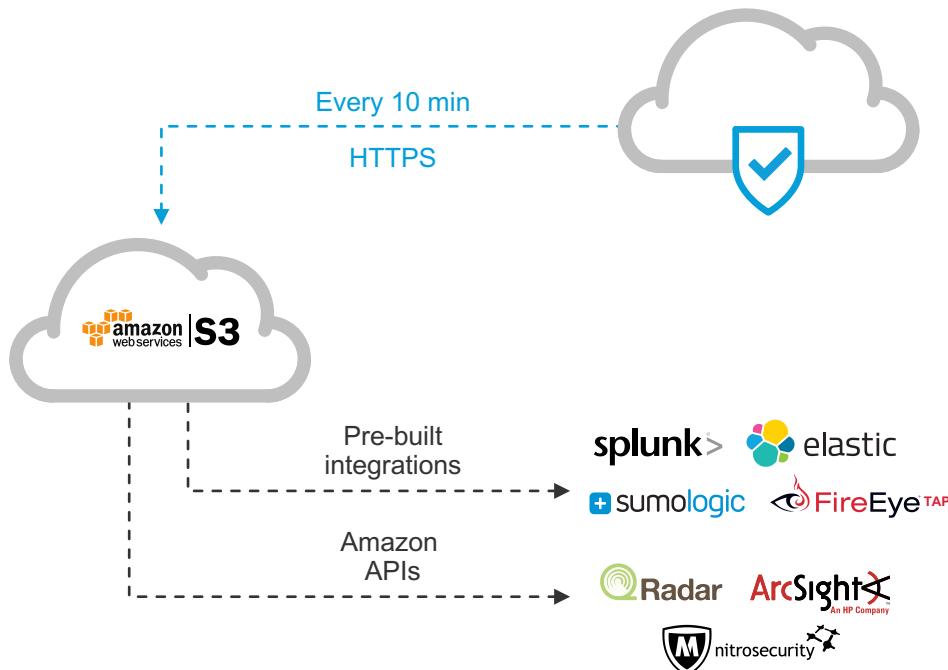


DEPLOYMENT

Enterprise-wide deployment in minutes



Log storage with Amazon S3

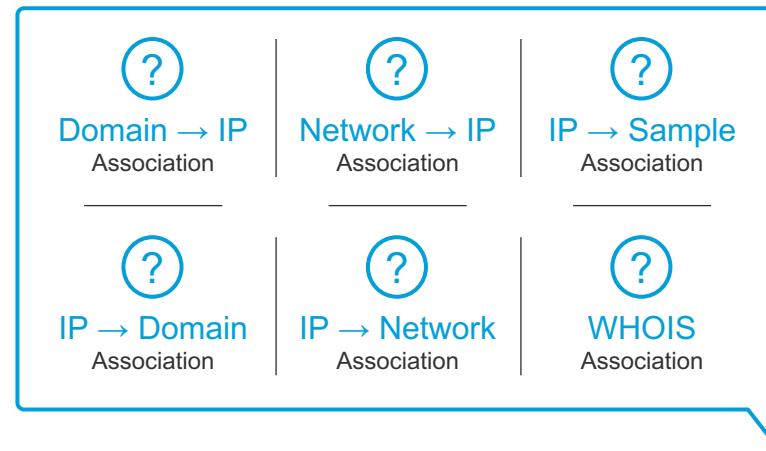


S3 Benefits

Triple redundant and encrypted storage
Pre-built SIEM / log analytic integrations
Elastic: pay only for the storage used

Ransomware example

Ransomware: mapping attacker infrastructure



AUG 17

-26 DAYS

SEP 12

🚫*.7asel7[.]top

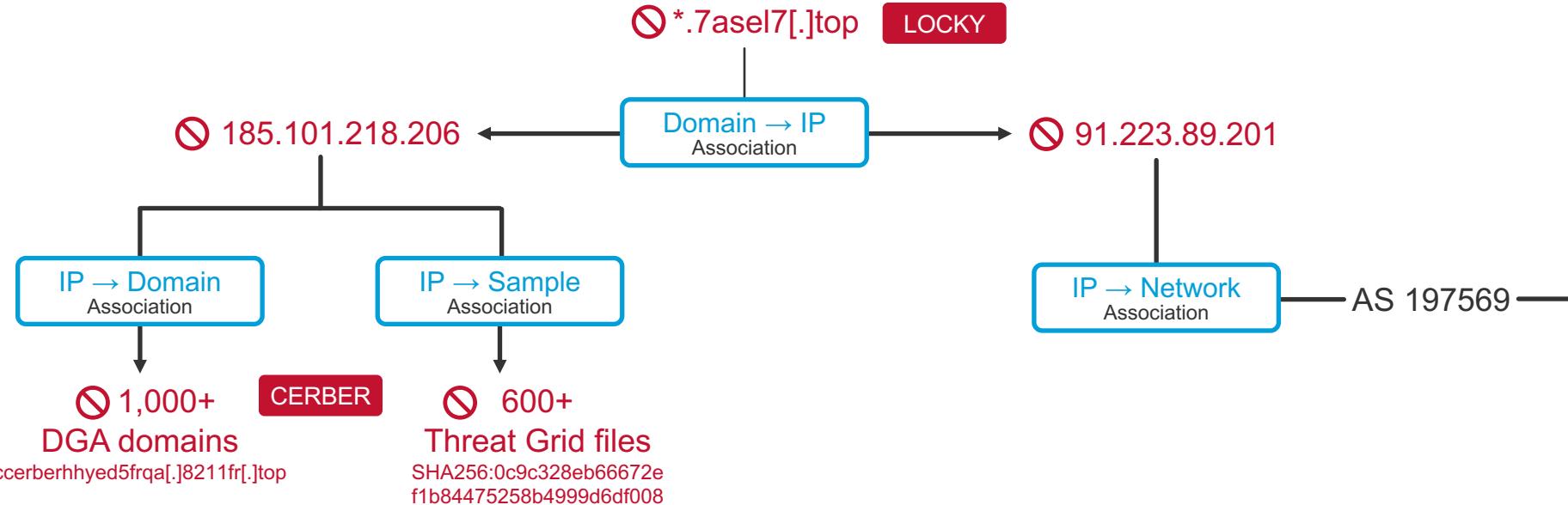
LOCKY

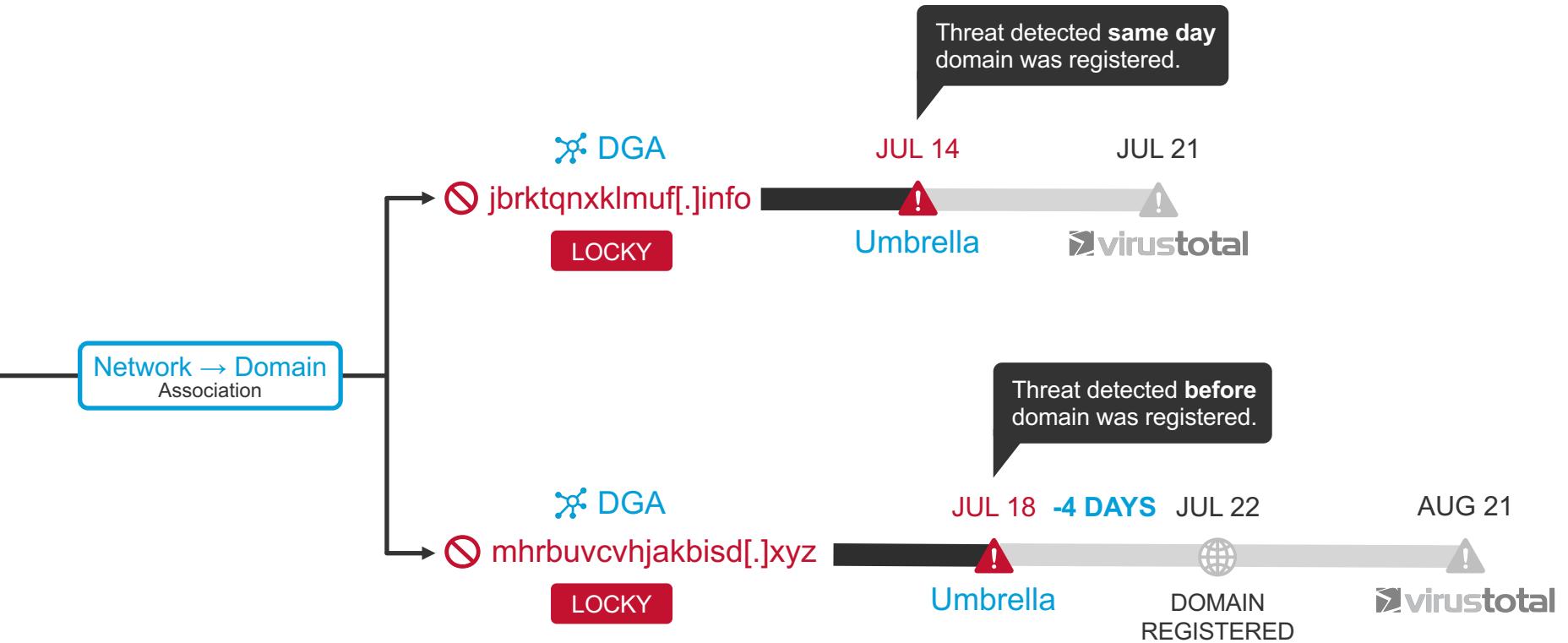


Umbrella

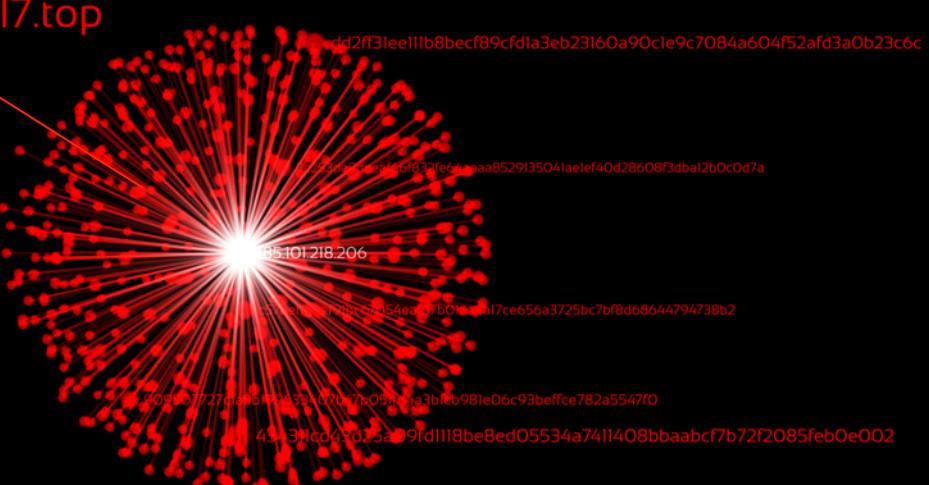
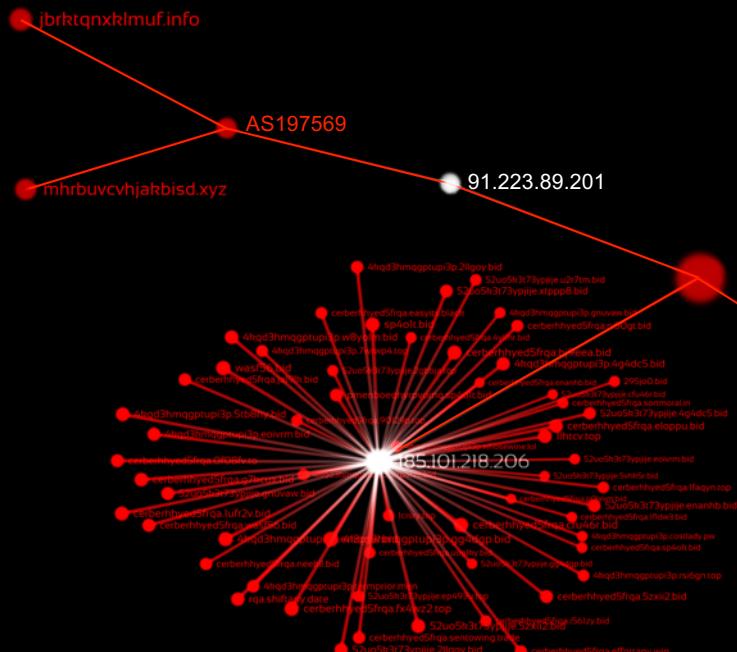


virustotal





Visualizing attacker infrastructure



Cisco Cloud Security



Umbrella

Secure Internet Gateway

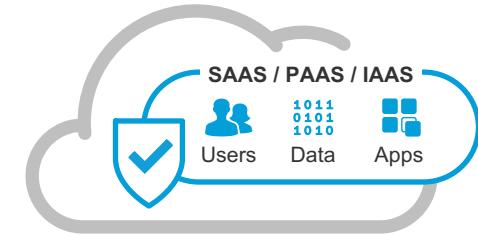
Secure access to the internet wherever users go, even off VPN



Umbrella Investigate

Threat intelligence

View relationships between malware, domains, and IPs across the internet



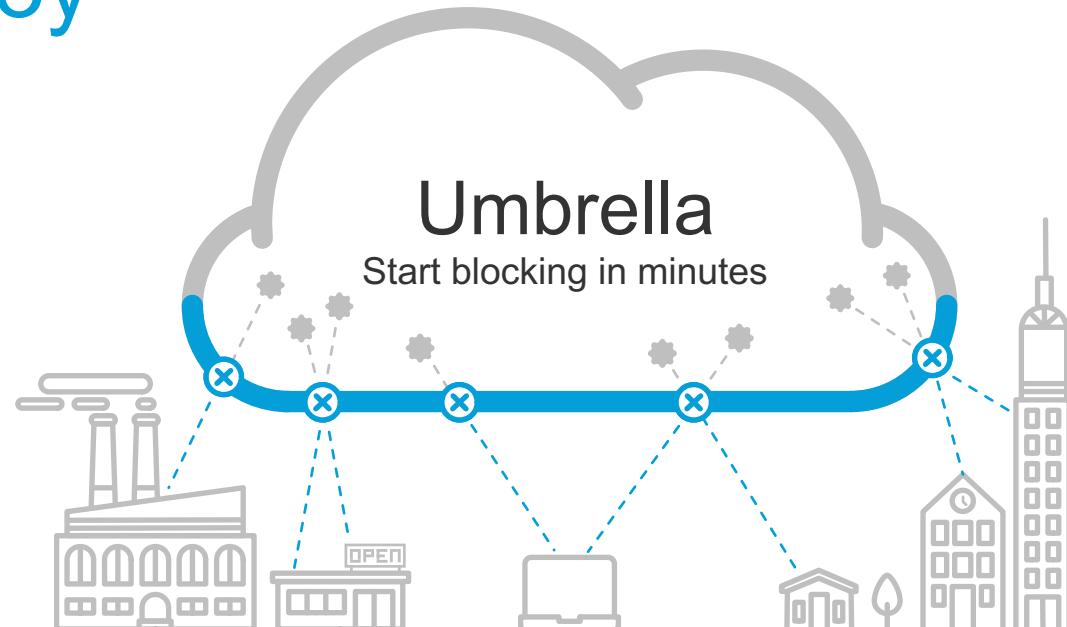
Cloudlock

Cloud Access Security Broker

Secure users, data, and apps across SaaS, PaaS, and IaaS

Easiest security product you'll ever deploy

- 1 Signup
- 2 Point your DNS
- 3 Done





Cisco Umbrella