Cisco Umbrella

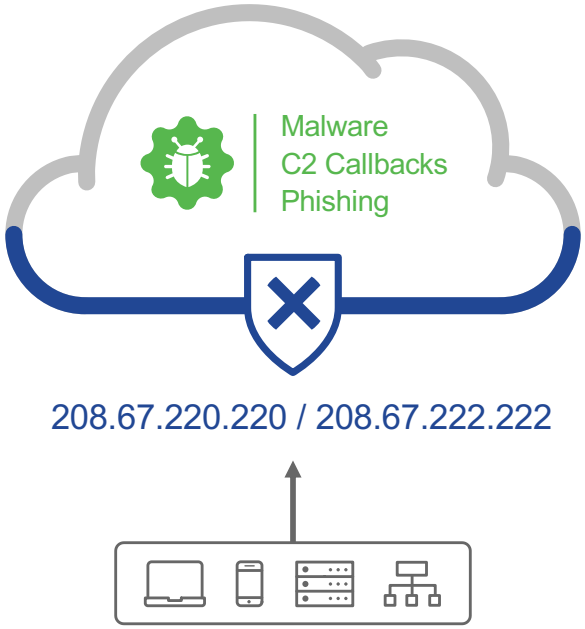
First line of defense for threats on the internet

Webinar Seguridad ORBE

Guillermo Gonzalez

03 / 2019

Cisco Umbrella



Built into the foundation of the internet

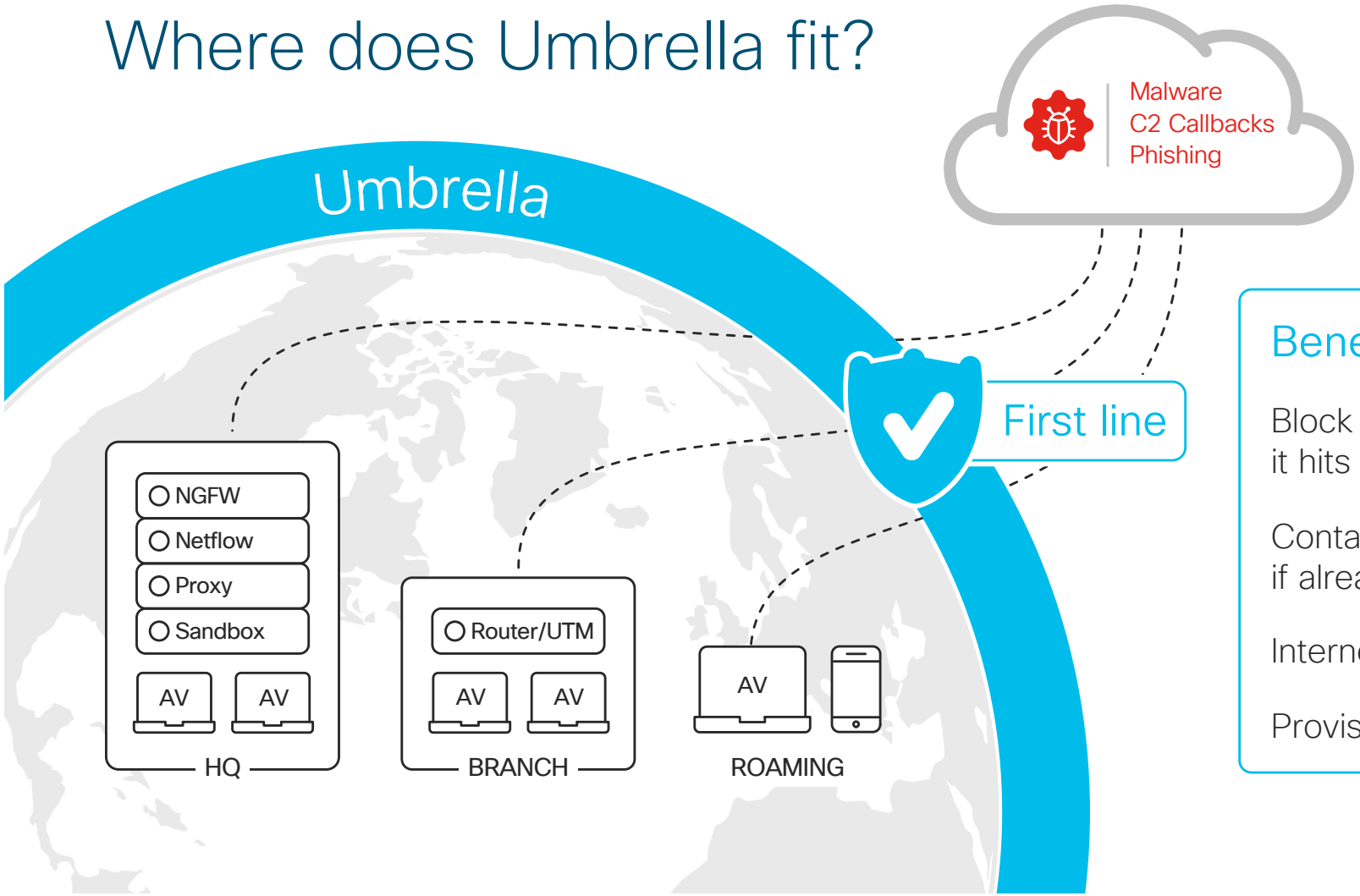
Intelligence to see attacks before launched

Visibility and protection everywhere

Enterprise-wide deployment in minutes

Integrations to amplify existing investments

Where does Umbrella fit?



Benefits

Block malware before it hits the enterprise

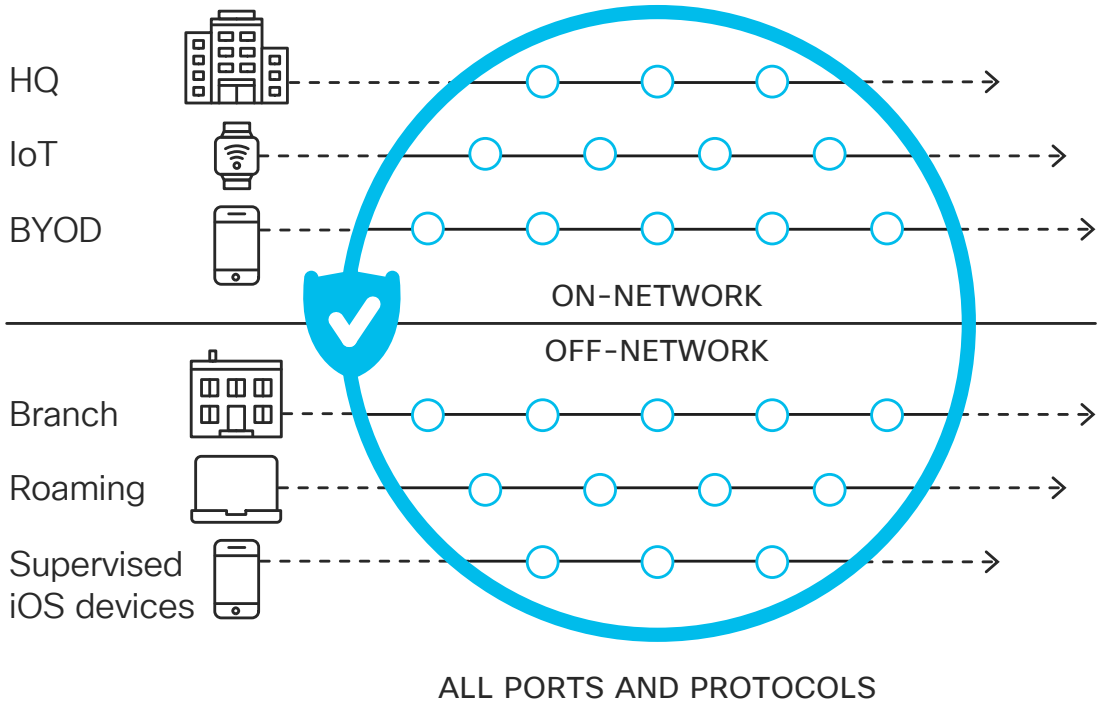
Contains malware if already inside

Internet access is faster

Provision globally in minutes

Visibility and protection for all activity, anywhere

Umbrella



All office locations

Any device on your network

Roaming laptops and supervised iOS devices

Every port and protocol

Cisco Umbrella

Built into foundation of internet

Destinations

Original destination or block page

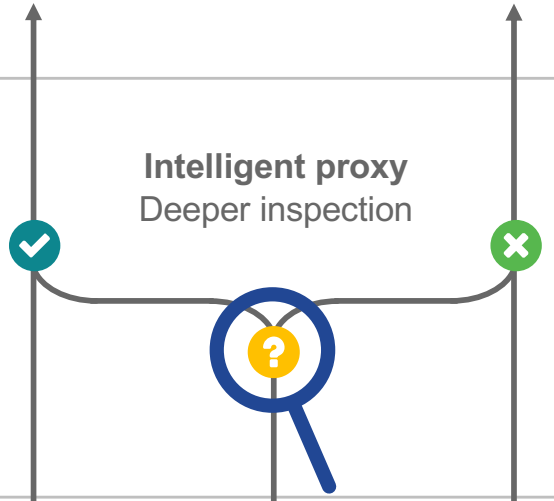
Safe
Original destinations

Blocked
Modified destination

Security controls

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

Intelligent proxy
Deeper inspection



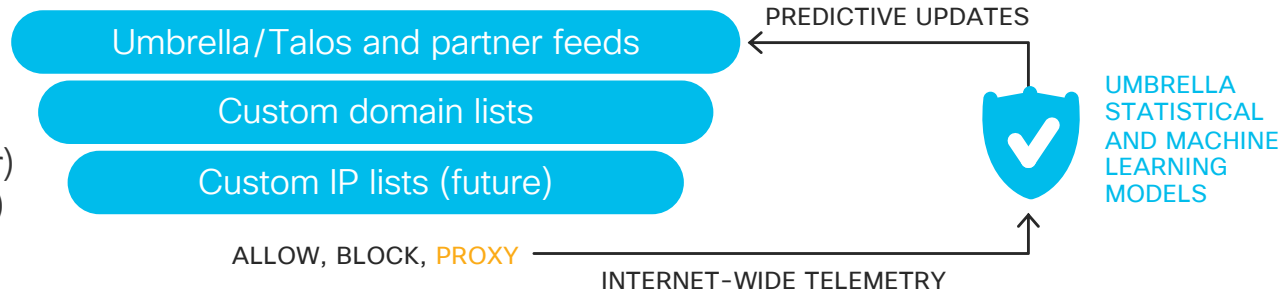
Internet traffic

On- and off-network

Breadth to cover all ports and depth to inspect risky domains

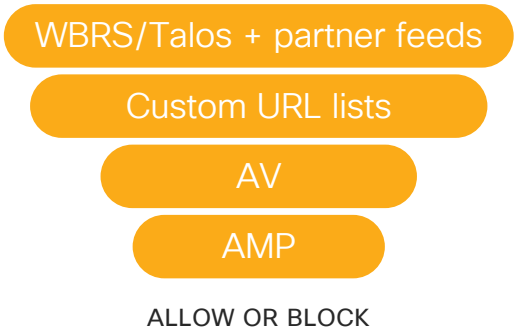
DNS and IP layer

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

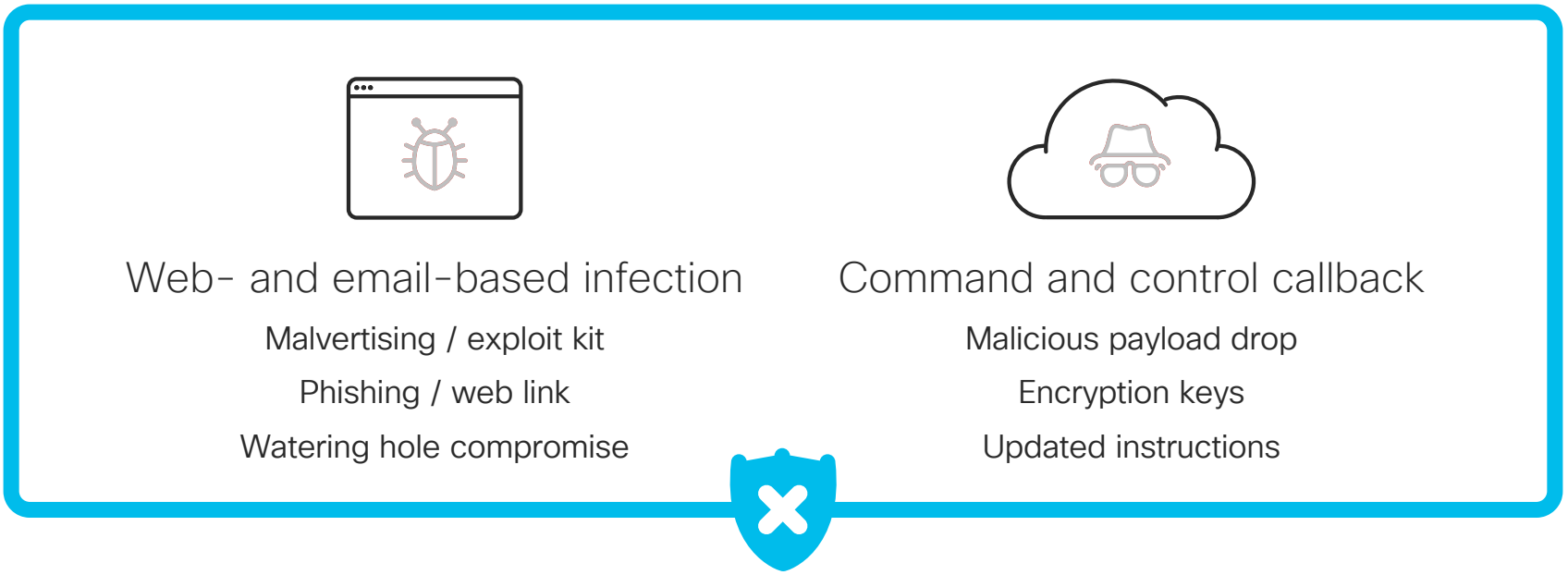


HTTP/S layer

- URL request
- File hash



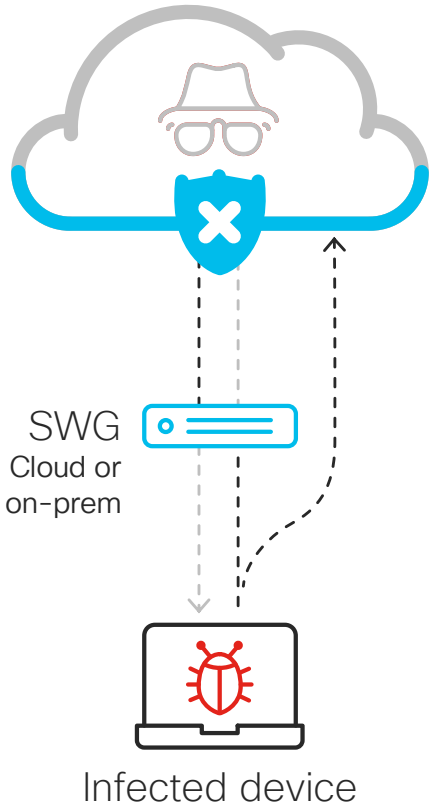
Prevents connections before and during the attack



Stop data exfiltration and ransomware encryption

Protection for command and control (C2) callbacks

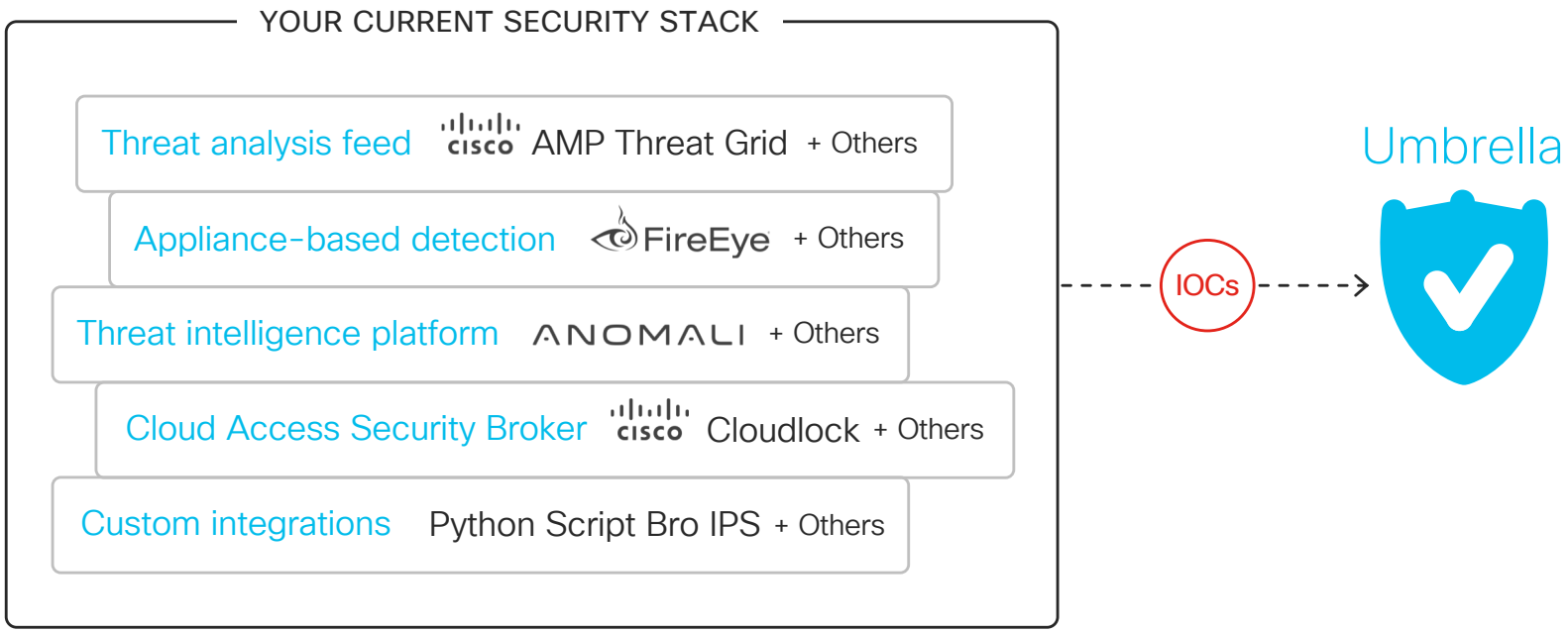
91%
of C2 can be blocked at the DNS layer



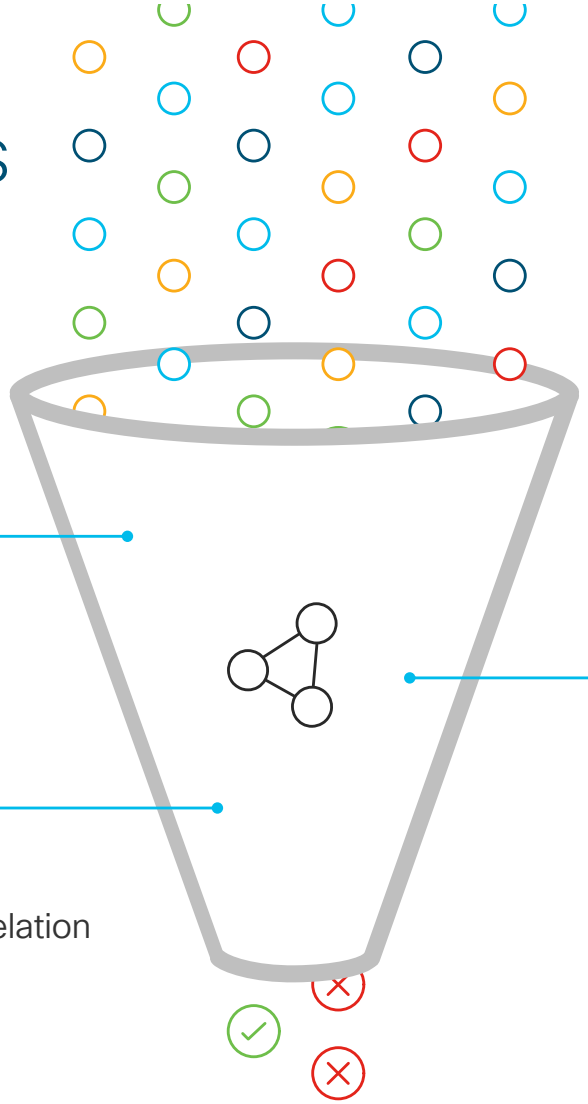
15%
of C2 bypasses web ports 80 & 443

Integrations to amplify existing security

Block malicious domains from partner or custom systems



Statistical models



2M+ live events per second

11B+ historical events

Guilt by inference

- Co-occurrence model
- Sender rank model
- Secure rank model

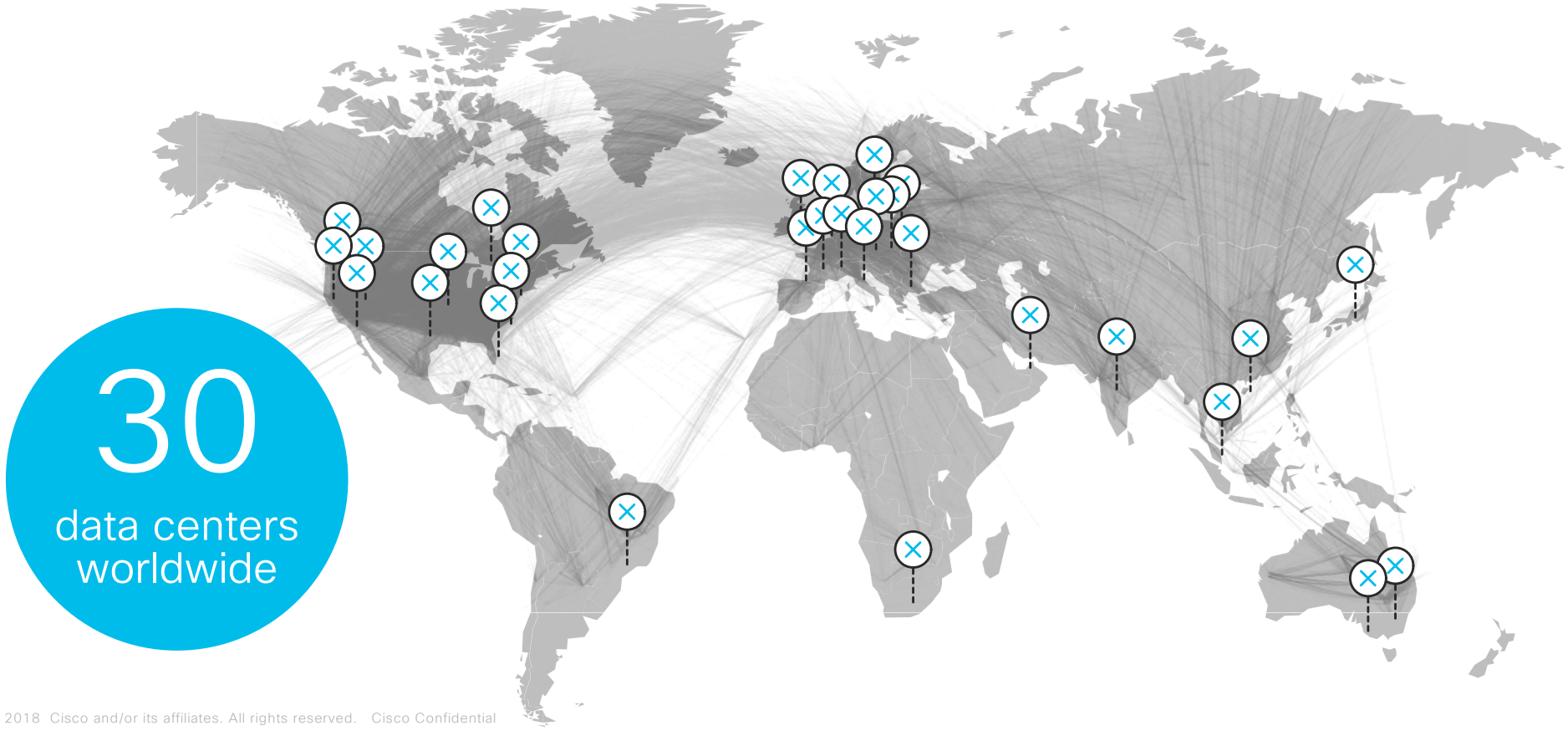
Guilt by association

- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

Patterns of guilt

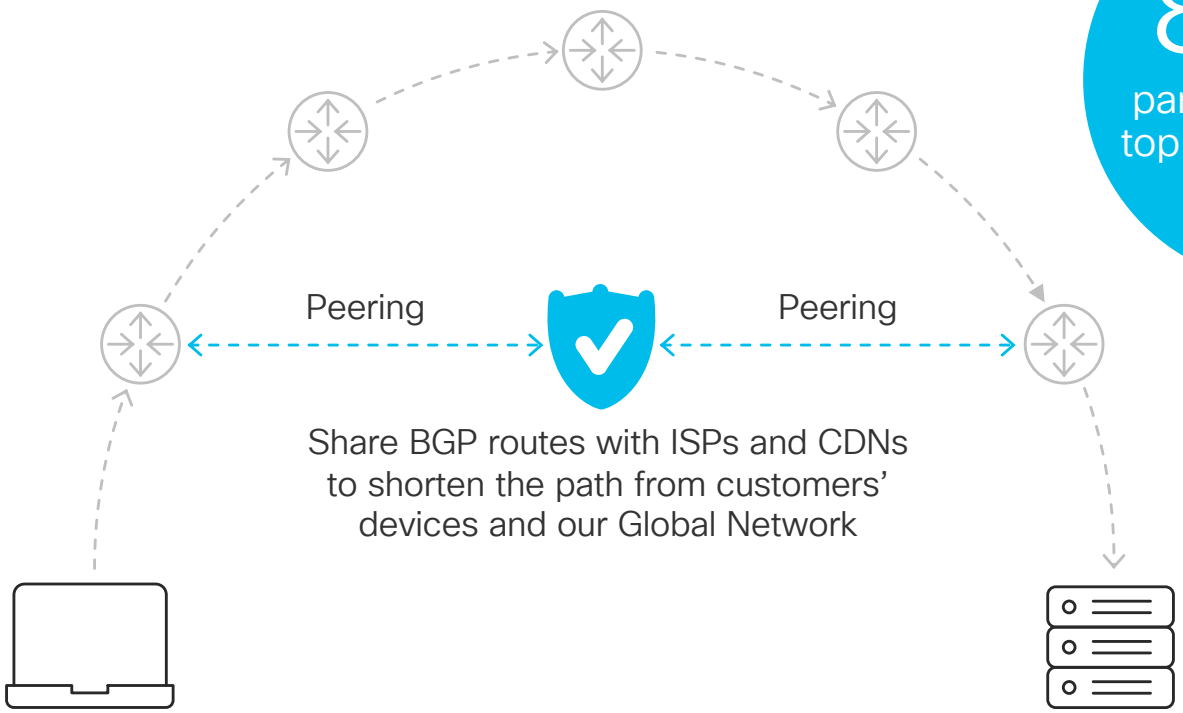
- Spike rank model
- Natural Language Processing rank model
- Live DGA prediction

Data centers co-located at major IXPs



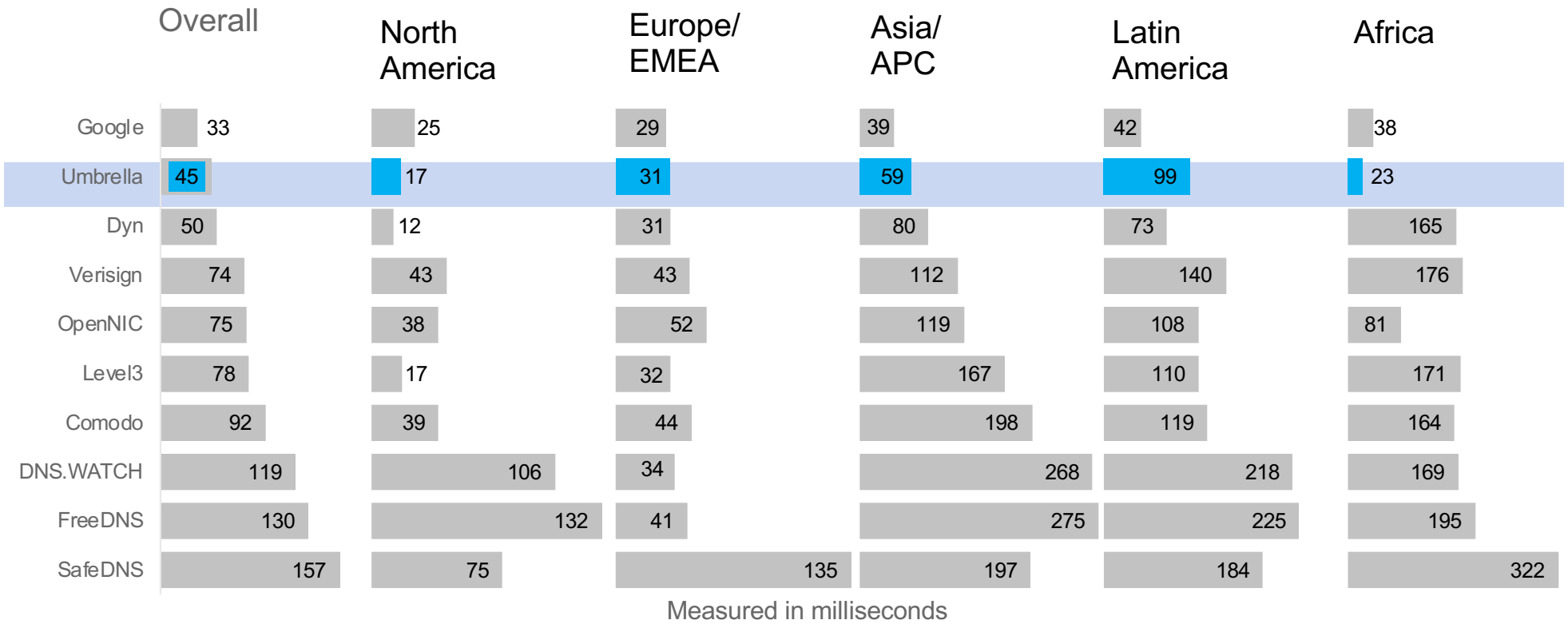
BGP peering for speed

800+
partnerships with
top ISP and CDNS



Share BGP routes with ISPs and CDNs
to shorten the path from customers'
devices and our Global Network

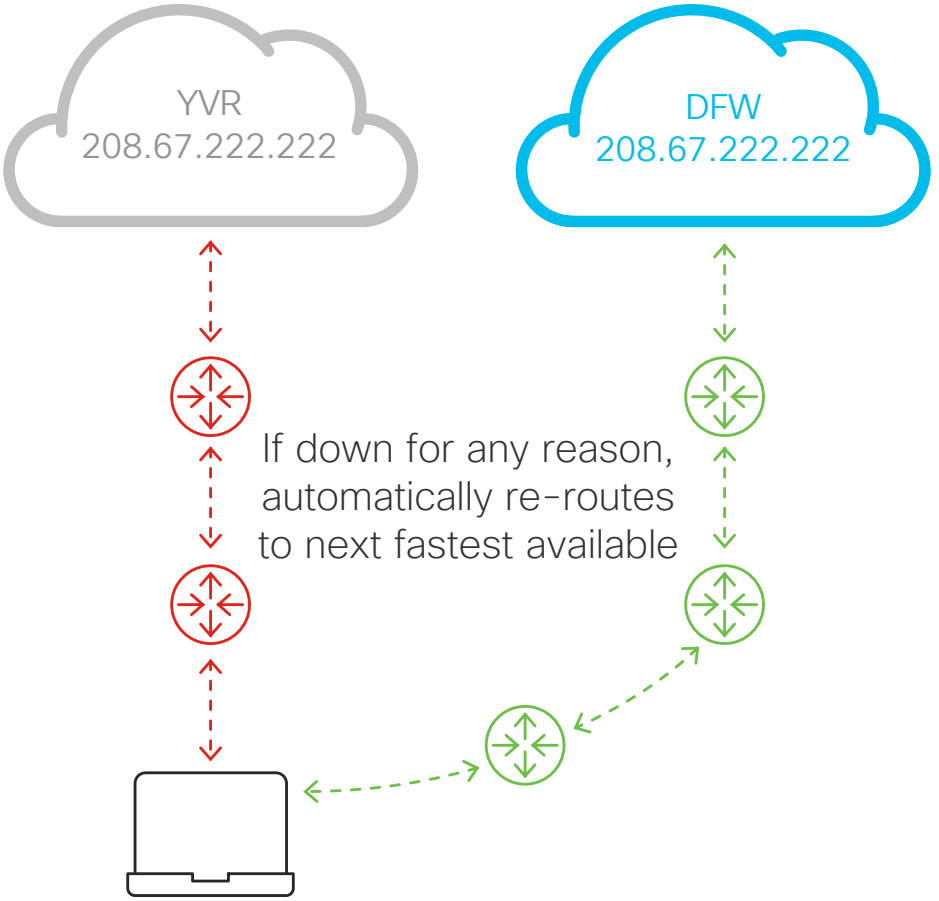
How fast do we resolve DNS requests?



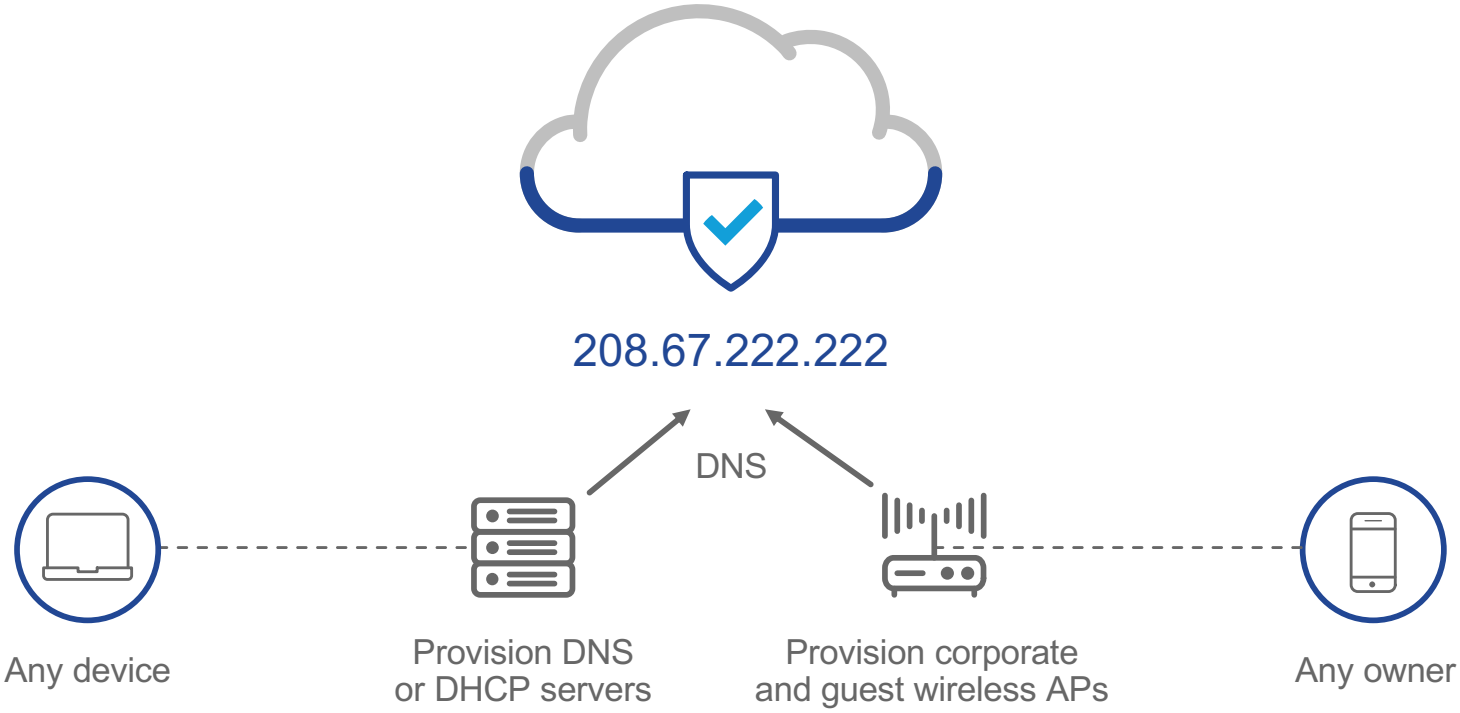
Source: MSFT Office 365 Researcher, ThousandEyes Blog Post, May 2017

Anycast IP routing for reliability

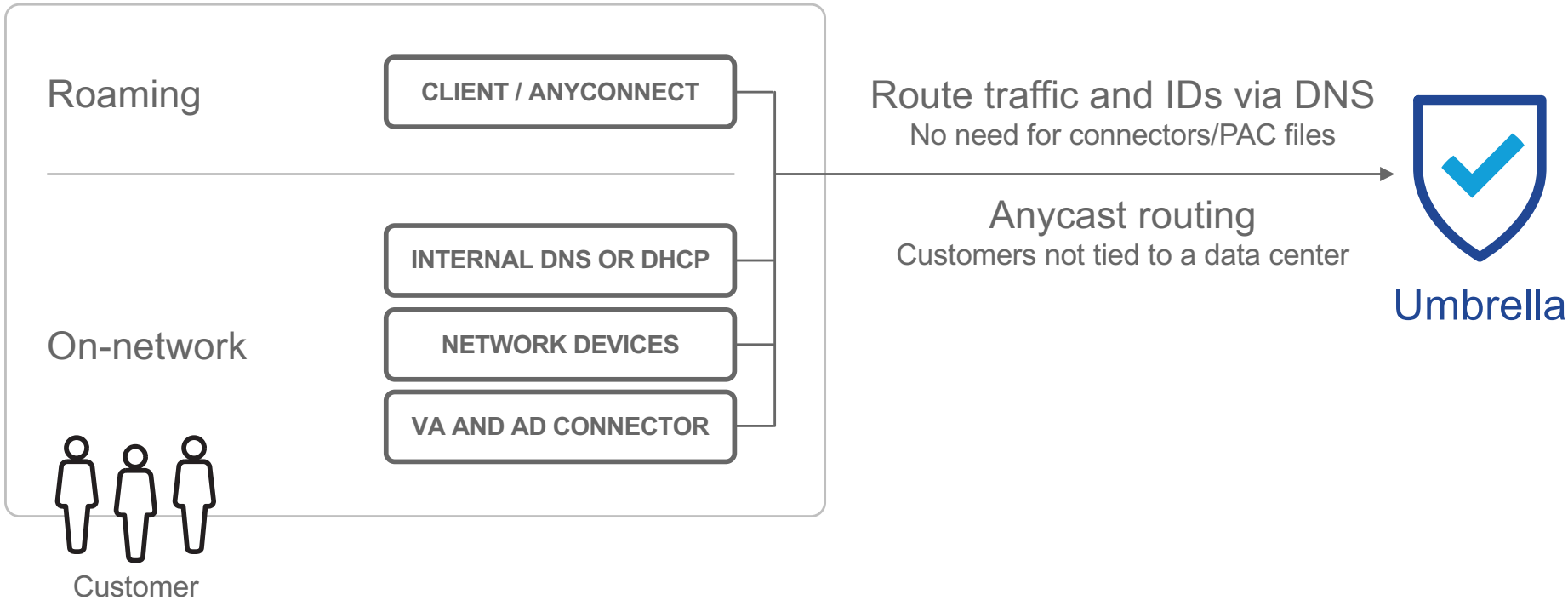
100%
business uptime since 2006
DDoS protection and global fail-over



Simplest way to protect any device on-network



Connecting to Umbrella



Enterprise-wide deployment in minutes

Existing

DNS/DHCP servers, Wi-Fi APs

Simple config change to redirect DNS

Network footprint

ISR1K and 4K

SD-WAN (Viptela)

WLC

Meraki MR

- Provisioning and policies per VLAN/SSID; tags for granular filtering and reporting
- Out-of-the-box integration (Umbrella virtual appliance also available)

Endpoint footprint

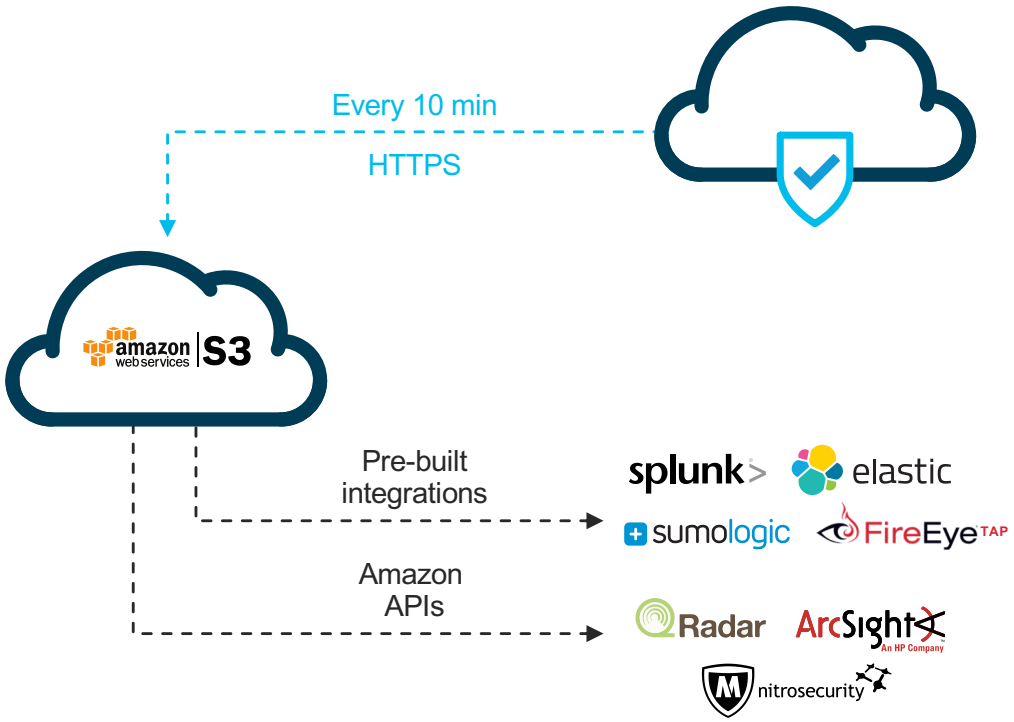
AnyConnect roaming module

Cisco Security Connector

Umbrella Chromebook client

Granular filtering and reporting on- & off-network (Umbrella roaming client also available)

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


CISCO