Designing Security for the Future of Your Network

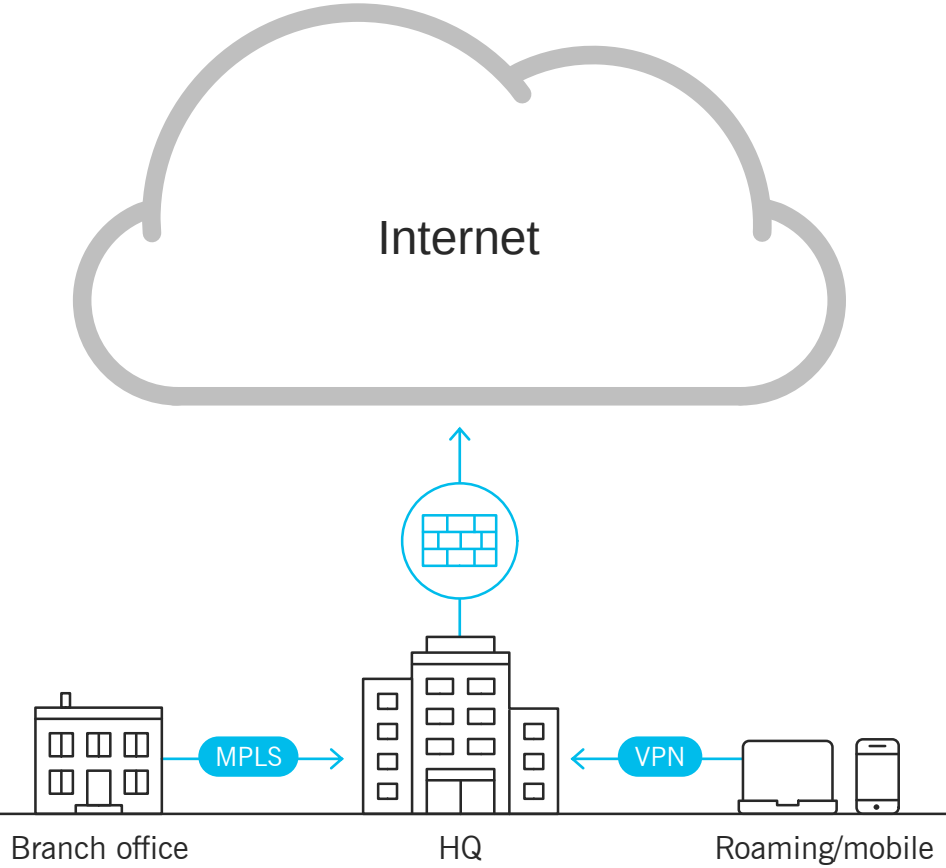
Secure internet gateway

Andreas Schober
Cybersecurity Specialist
October 2019

Traditional model

Network:
Centralized

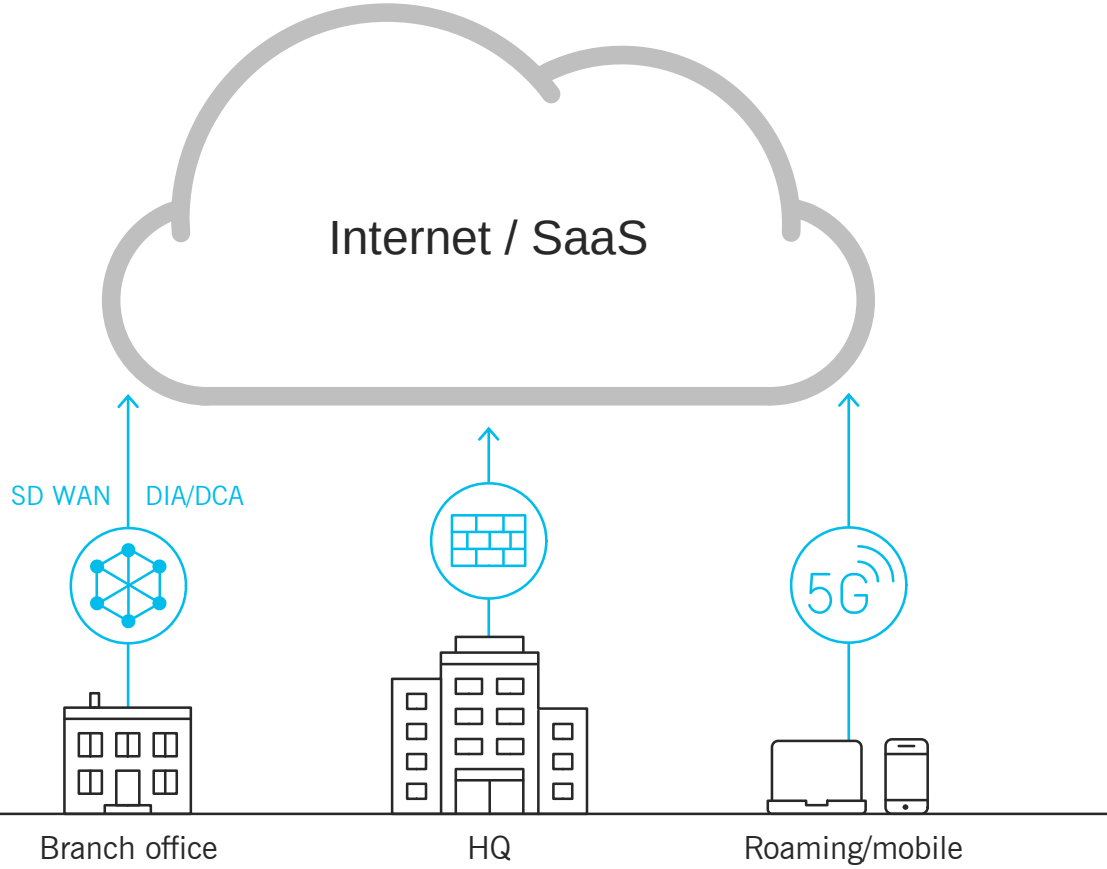
Security:
Single place to enforce policies and protection



Today's model

Network:
Decentralized

Security:
Protect at data center, cloud, and branch edge



Challenges you face

Malware and ransomware

Gaps in visibility and coverage

Volume and complexity of security tools

Limited security resources

2018 ESG market research

Access the report:
cs.co/ESG-SIG-research

- Surveyed 450 respondents in Nov 2018
- North America & Western Europe $50M in annual revenue
- 500+ employees
- Cybersecurity, IT, and networking security professionals

Roaming users

of employees considered roaming users

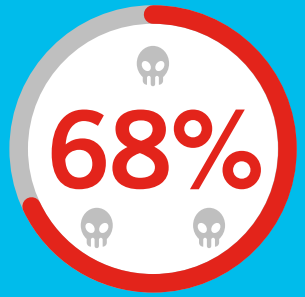
While 82% mandate use of VPNs…

8 out of 10

sometimes or frequently avoid VPN use

of branch office security deployments take over a month

Branch office vulnerabilities

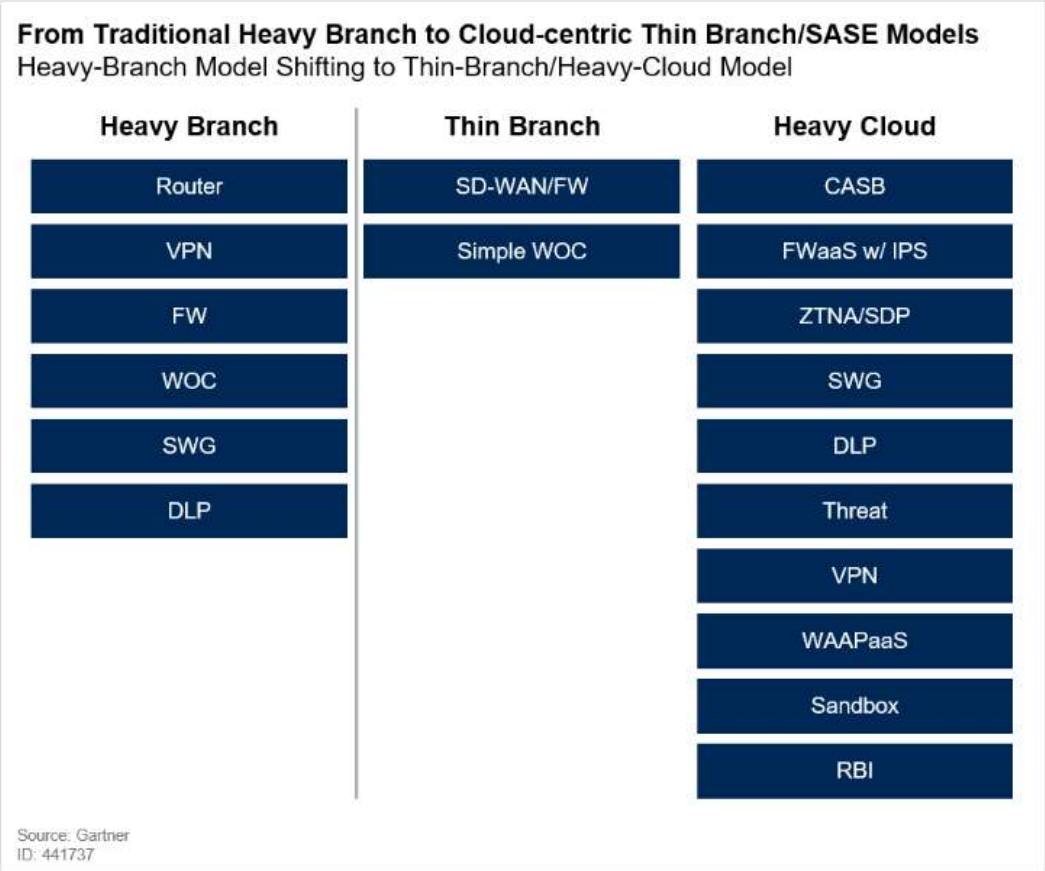


of branch offices and roaming users were the **source of compromise** in recent attacks

Source: ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019

Gartner view on shift

Gartner, The Future of Network Security Is in the Cloud, Figure 5, August 2019



Transformation to the secure internet gateway

- DNS-layer security
- Web gateway
- Firewall
- Data loss prevention

On-premises security converges in the cloud for more effective protection of branch offices

Secure internet gateway

Secure onramp to the internet, providing the first line of defense and inspection

Cisco Umbrella

Secure internet gateway

Secure onramp to the internet, everywhere

Visibility

On & off corporate network

All internet & web traffic

All apps

All devices

Protection

DNS-layer security

Web inspection

File inspection

Threat intel access

Control

URL block/allow lists

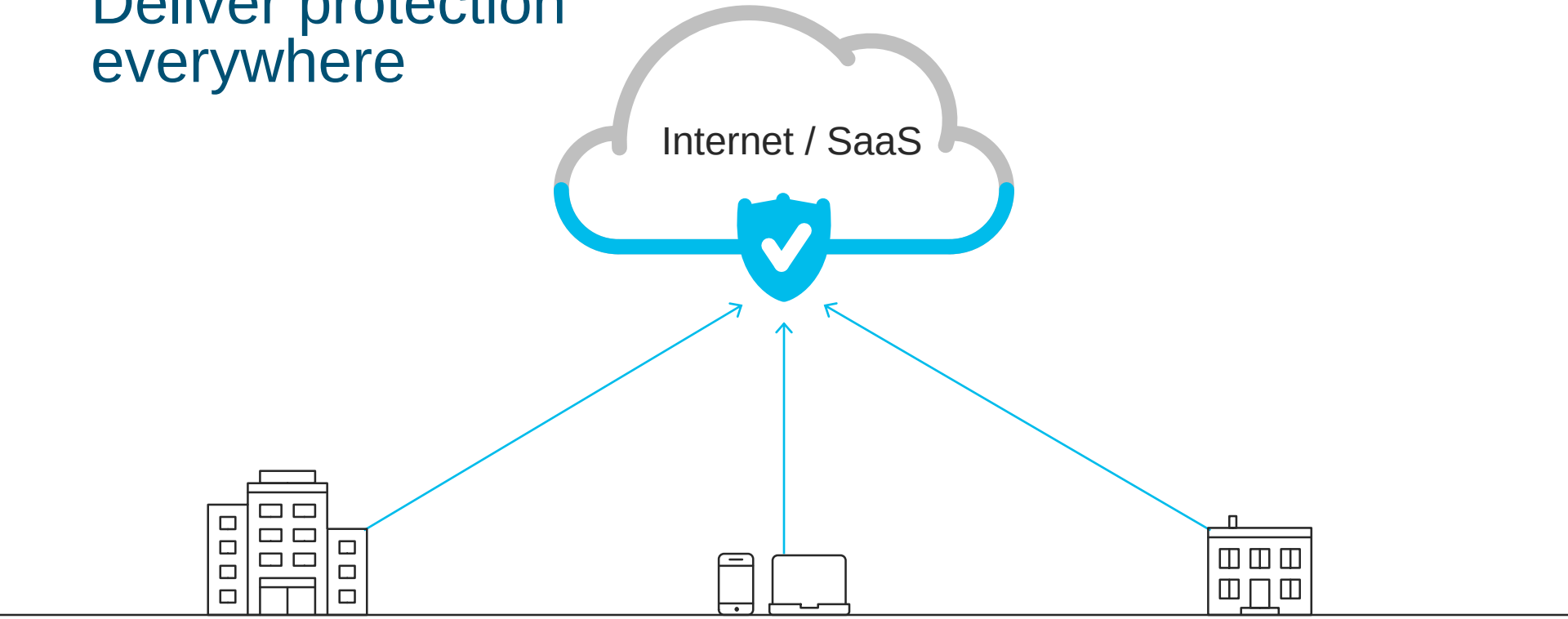
Port & protocol rules

Content filtering

App control

Powered by Cisco Talos threat intelligence

Deliver protection everywhere

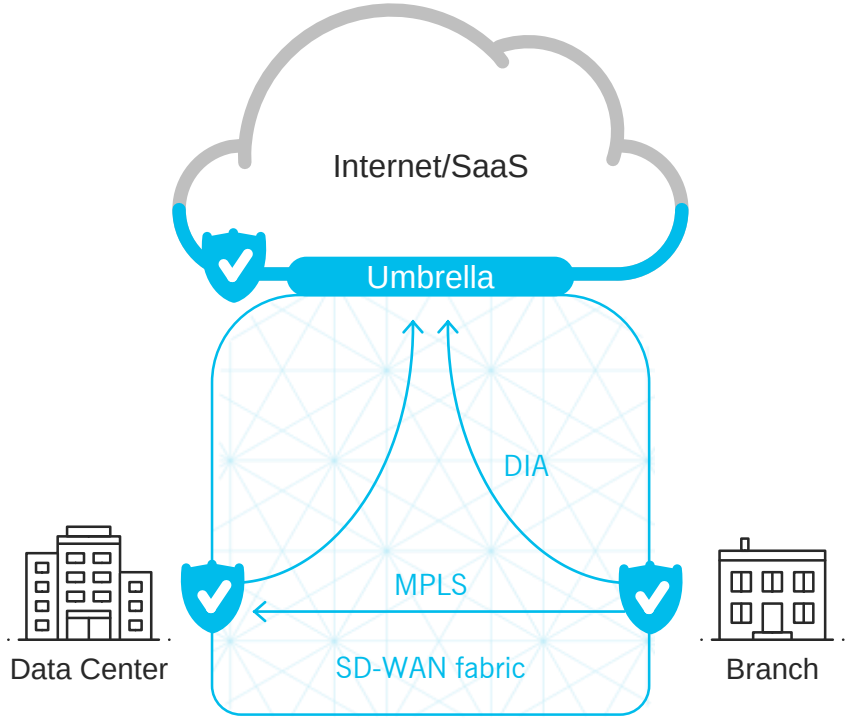


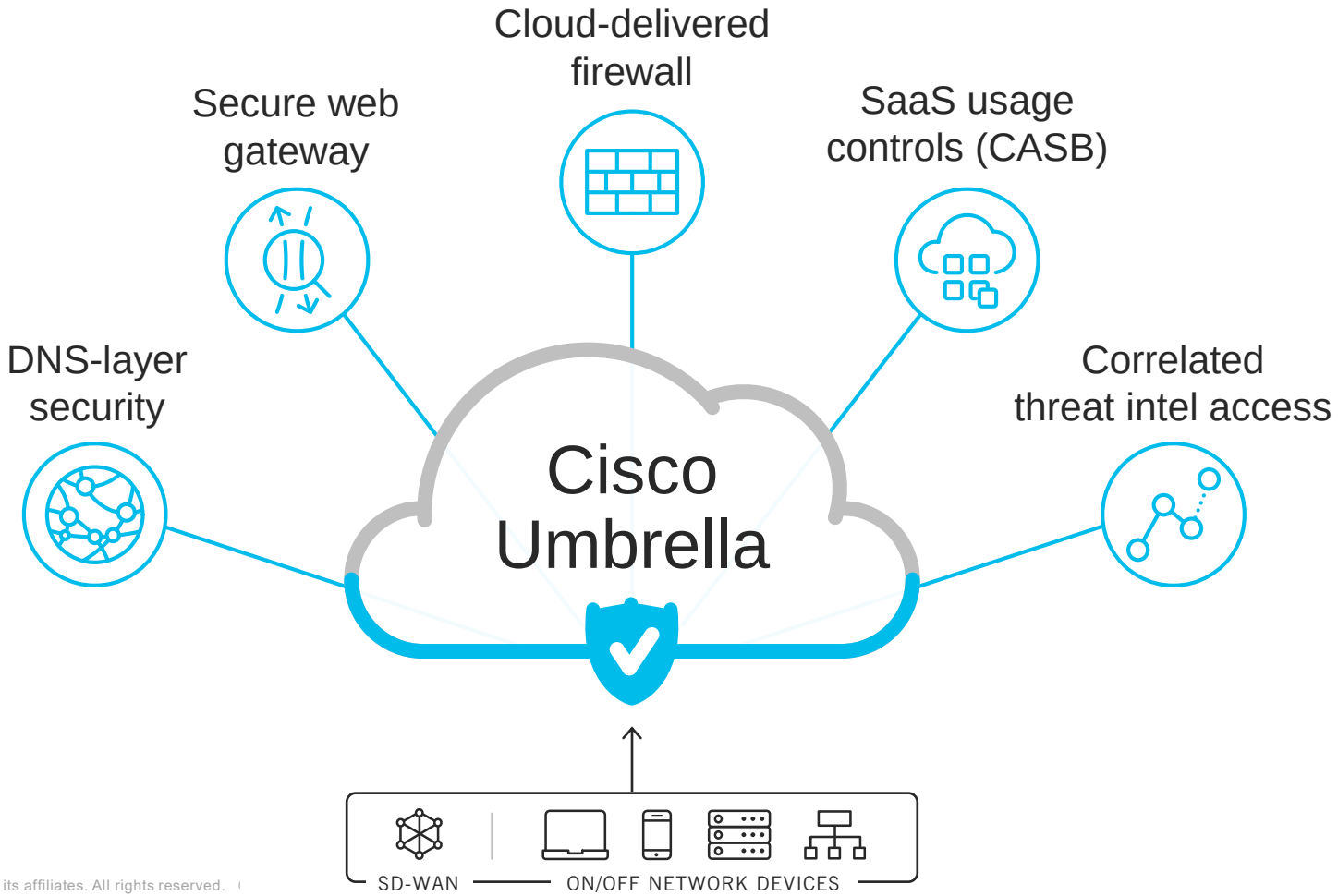
Boost existing security

Enable off-network

Transform edge security

Simple, effective protection across your Cisco SD-WAN fabric





DNS-layer security

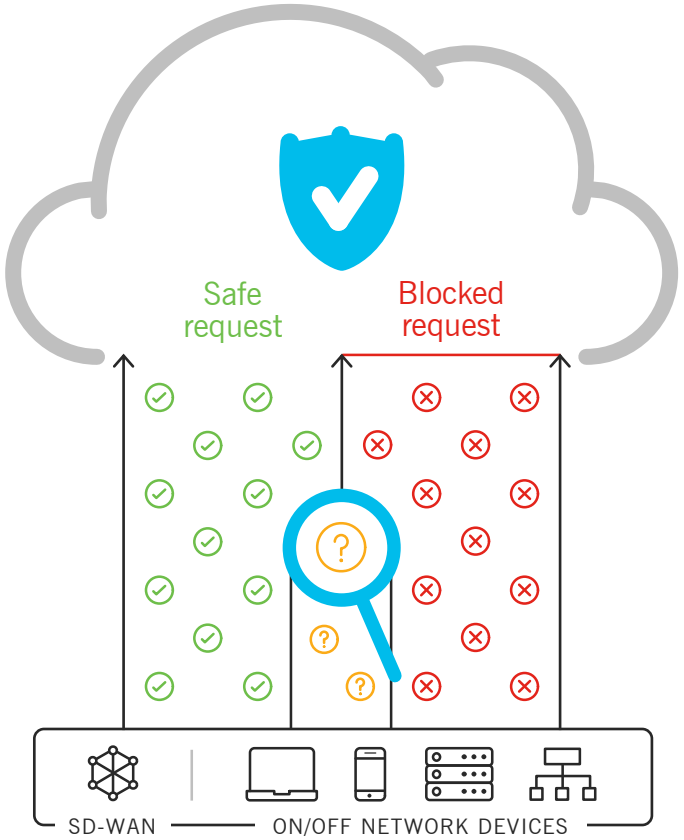
First line of defense

Deploy enterprise wide in minutes

Block domains associated with malware, phishing, command and control callbacks anywhere

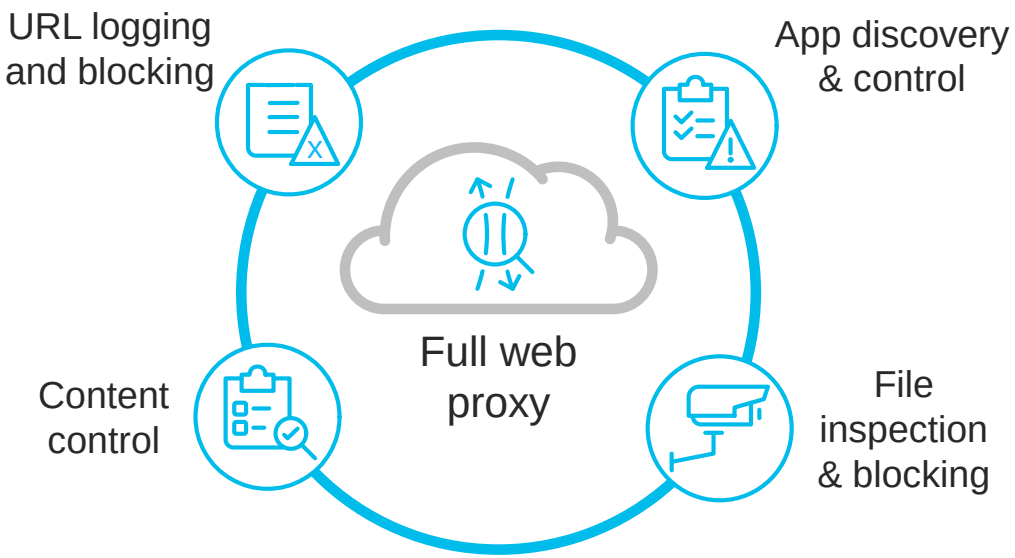
Stop threats at the earliest point and contain malware if already inside

Amazing user experience — faster internet access; only proxy risky domains



Secure web gateway: full web proxy

Deep inspection and control of web traffic



Capture all web traffic with full URL logging and blocking capabilities

Enforce acceptable use policies with content filtering and URL blocking

Block more malware with SSL decryption and file inspection

Additional functionality to be delivered in phases as developed

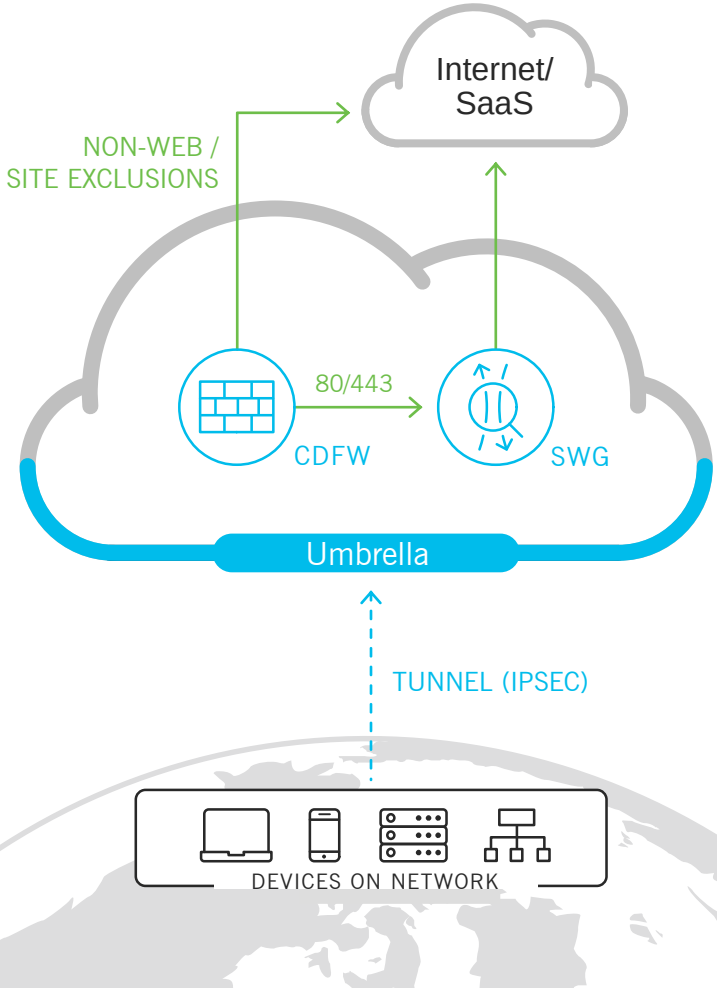
Cloud-delivered firewall

Firewall for the cloud edge

Tunnel all outbound traffic to Umbrella

Centrally manage IP, port, and protocol rules (L3/L4)

Anonymize IP to separate guest and employee traffic to eliminate negative impact on security rating (e.g. BitSight)



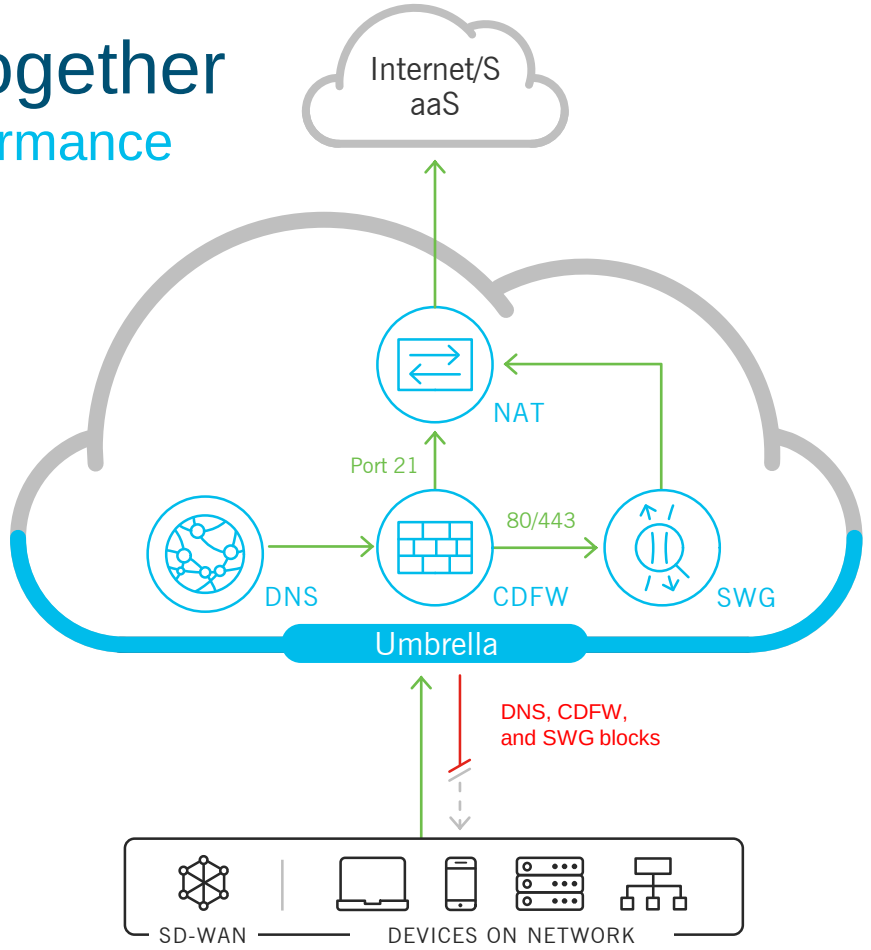
Enforcement that works together

Improved responsiveness and performance

DNS-layer security: First check for domains associated with malware

Cloud-delivered firewall (CDFW): Next check for IP, port, and protocol rules

Secure web gateway (SWG): Final check of all web traffic for malware and policy violations



Ability to easily block unapproved apps

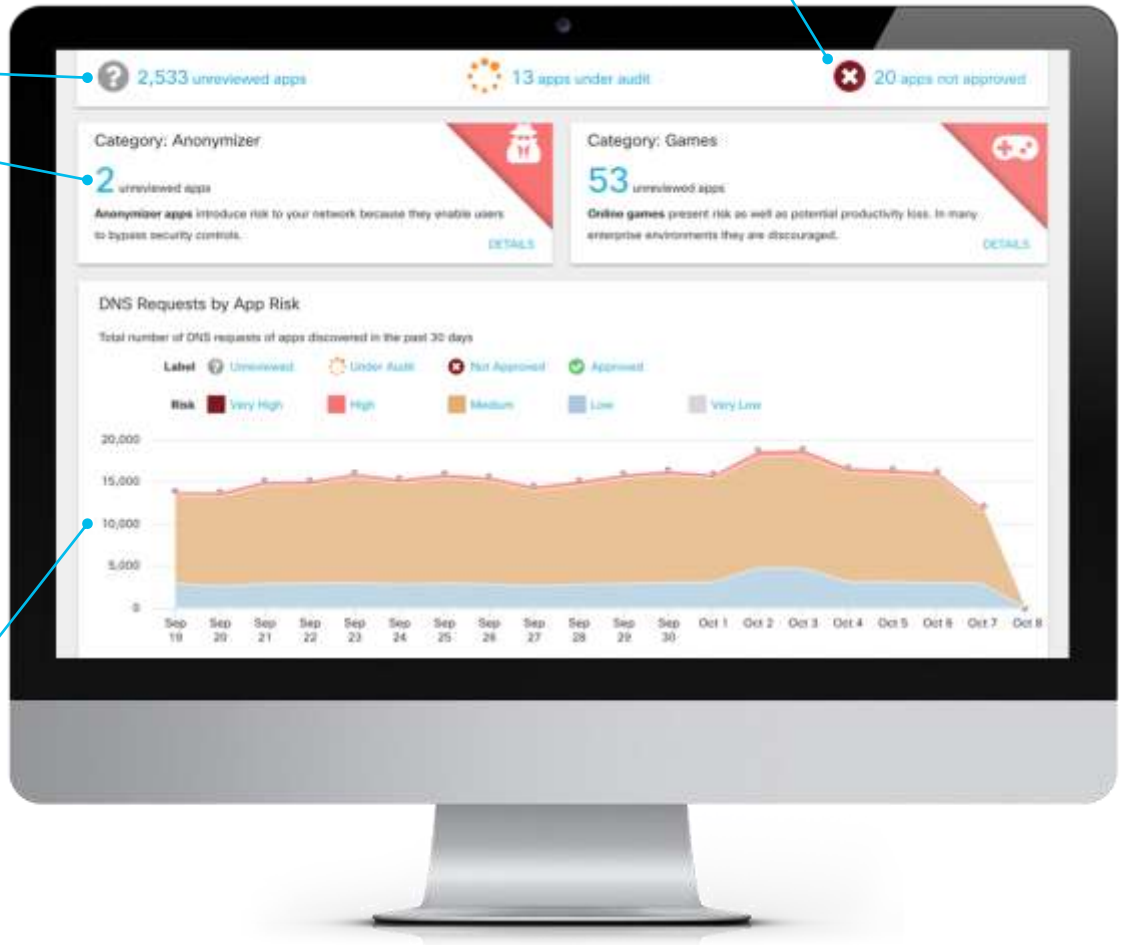
Status of discovered apps

Summary of high risk categories

APP DISCOVERY & BLOCKING

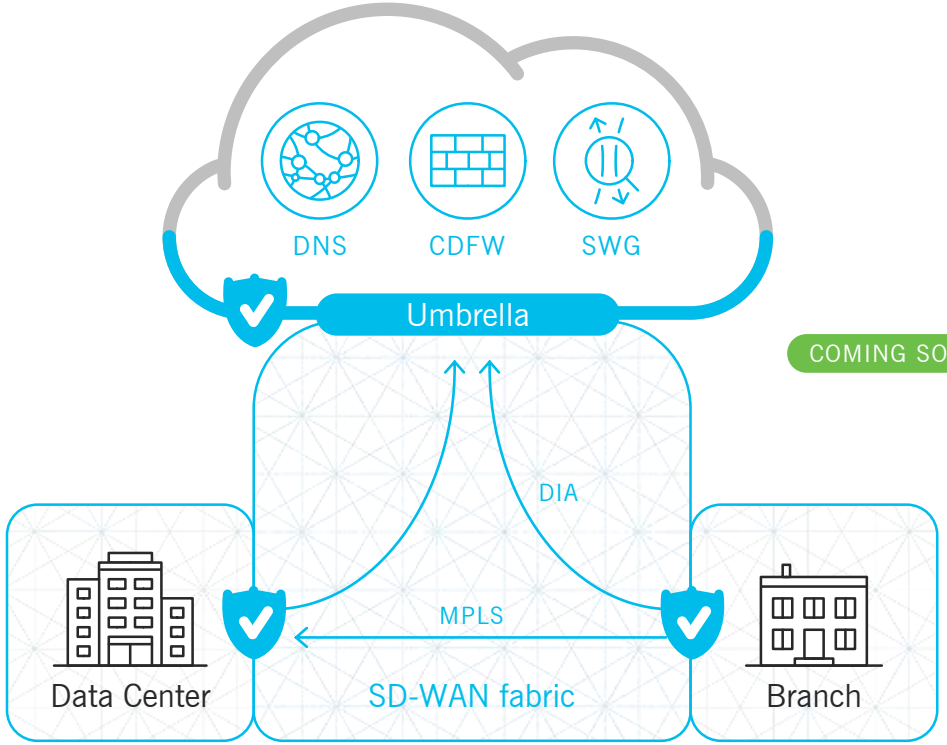
CASB functionality to address Shadow IT and enable secure cloud adoption

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



Cisco SD-WAN integration

Simple, effective protection across your Cisco SD-WAN fabric



COMING SOON!

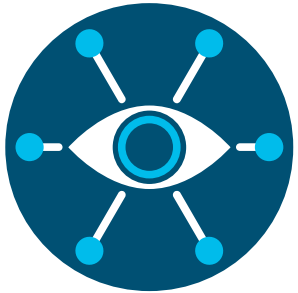
Quickly deploy DNS-layer security as first line of defense

Add deeper inspection and control with cloud-delivered firewall and secure web gateway capabilities

Easily scale security with future SaaS and web traffic growth

Cisco Talos: the largest non-government threat intelligence organization on the planet

250+ full-time threat researchers and data scientists



Analyzing 1.5 million unique malware samples daily

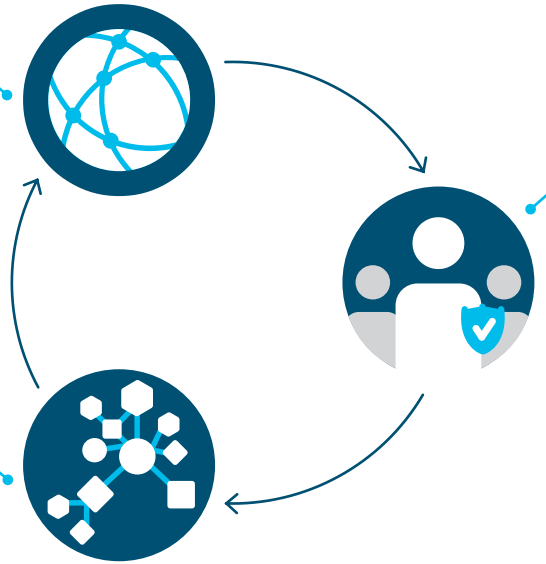
Blocking 20 billion threats daily. More than 20x any other vendor.

We **see more** so you can **block more** and **respond faster** to threats.

Statistical and machine learning models

Massive & diverse data

- 175B requests per day
- Represents 90 M active users, 16K enterprise customers
- From 160+ countries



Security researchers

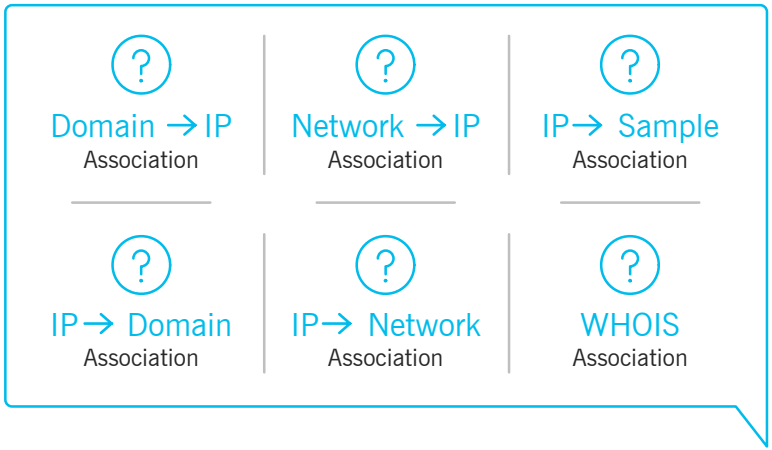
- Industry renown researchers
- Build models that can automatically classify and score domains and IPs

Models

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

Ransomware example

Ransomware: mapping attacker infrastructure



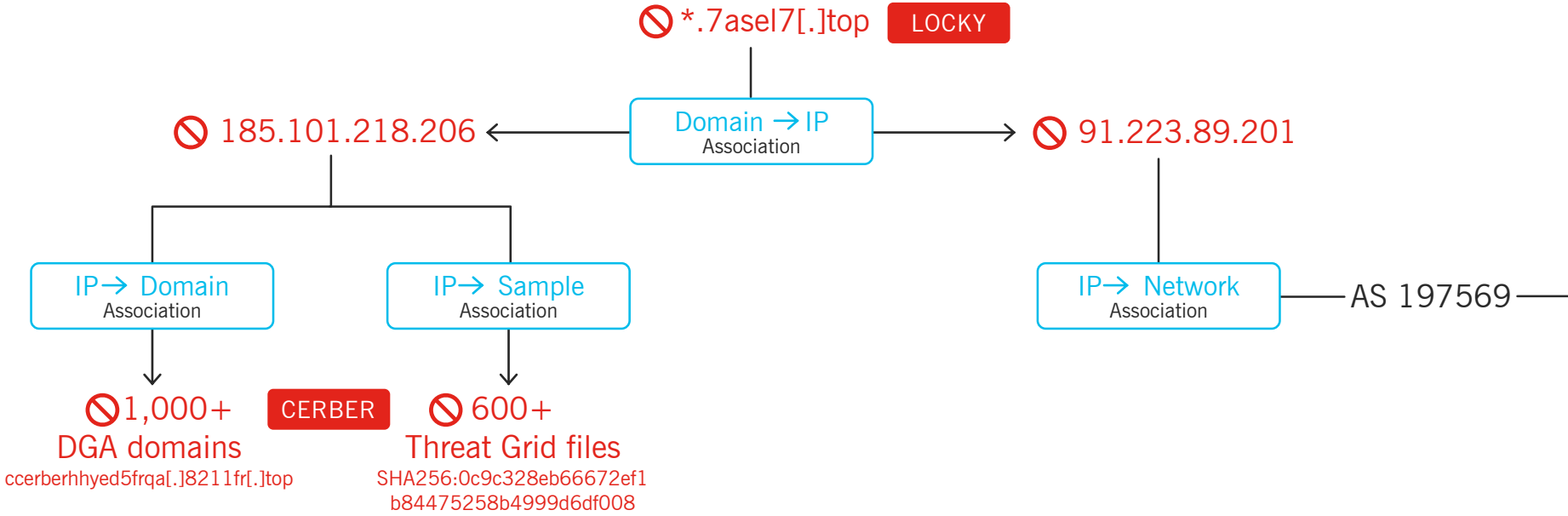
AUG 17 -26 DAYS SEP 12

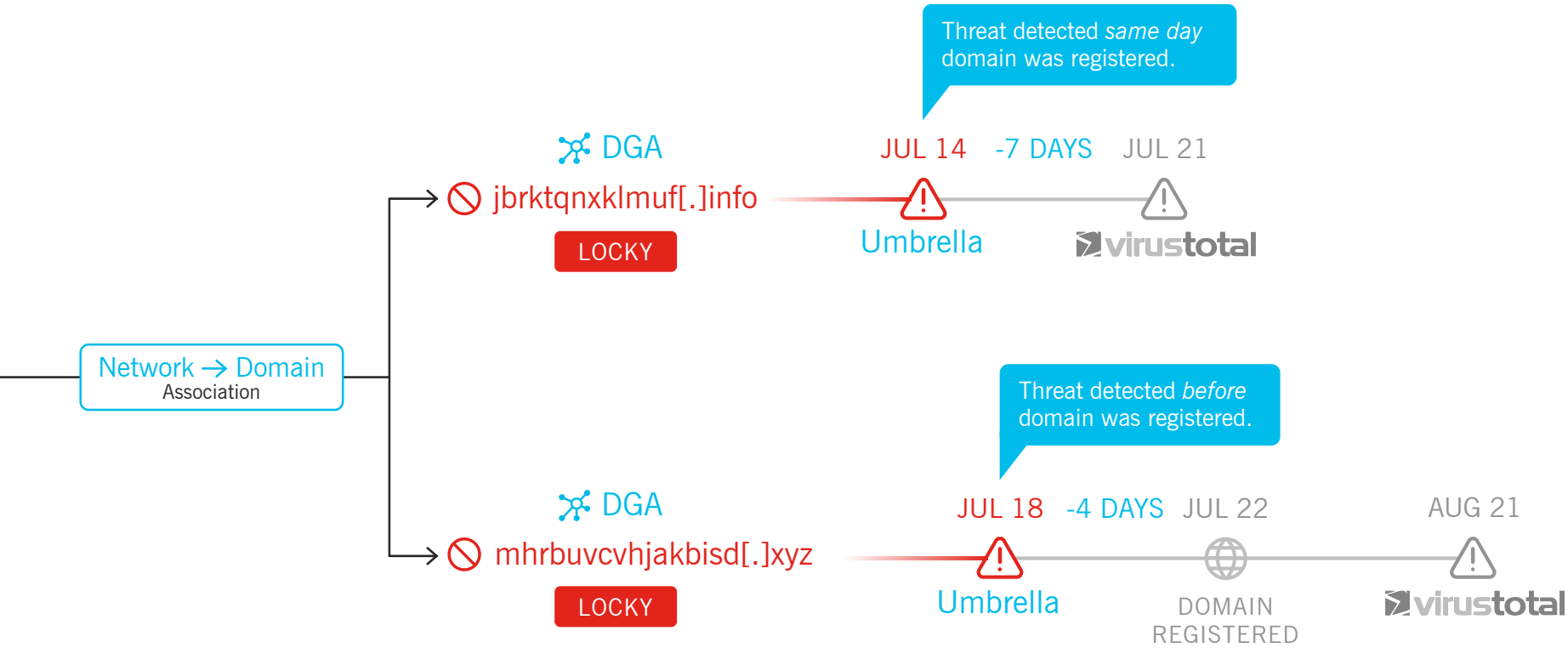
*.7asel7[.]top

LOCKY

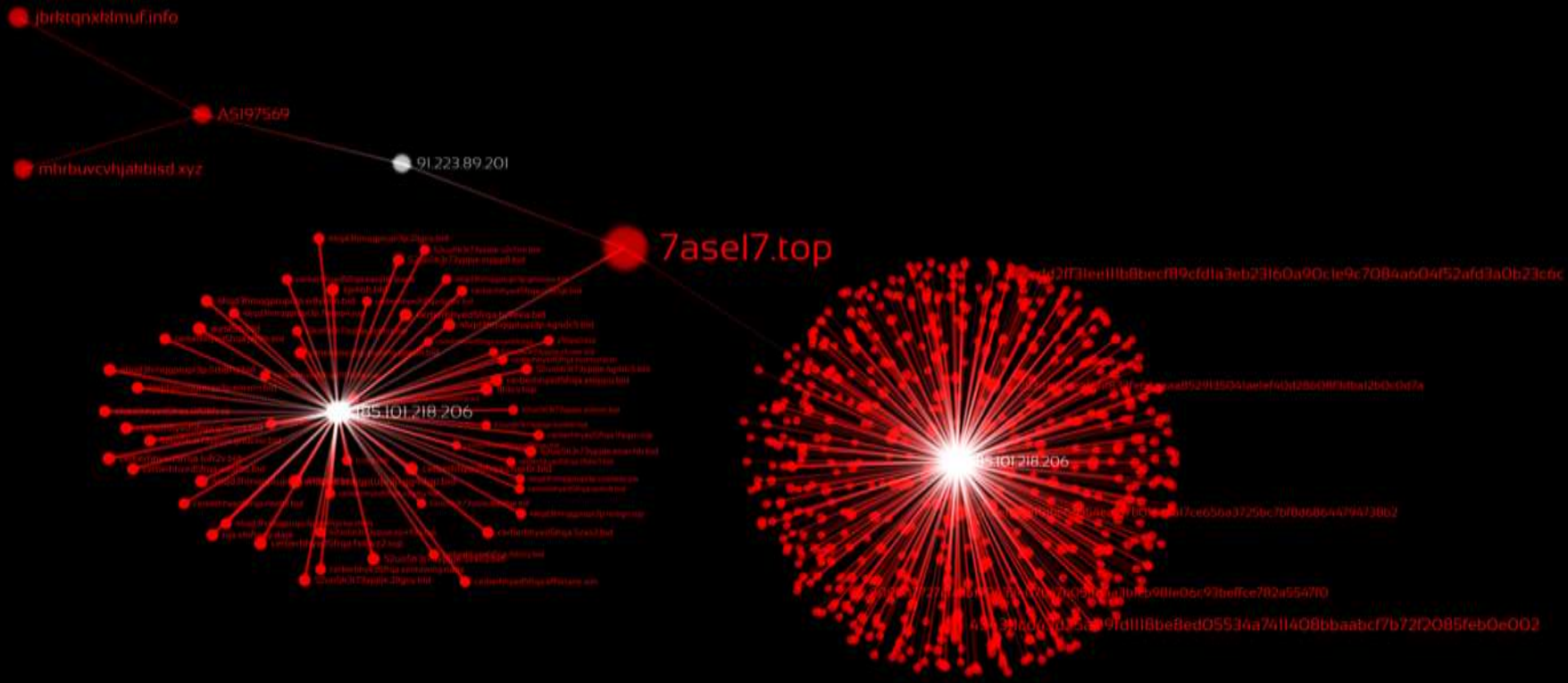
Umbrella

virustotal



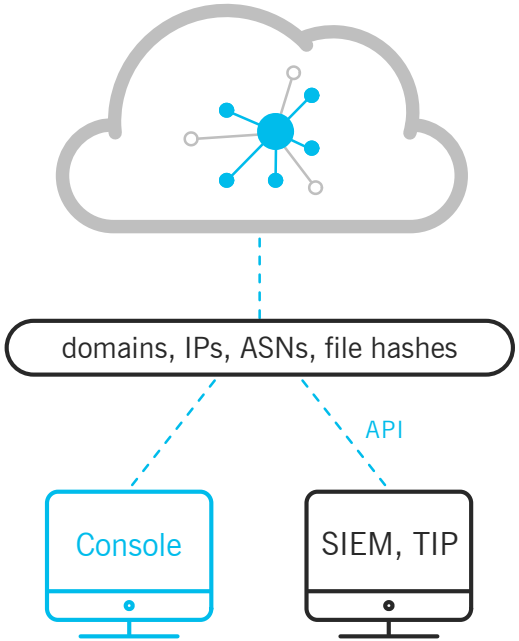


Visualizing attacker infrastructure



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 security data with global intelligence

Umbrella Infrastructure

Data centers co-located at major IXPs

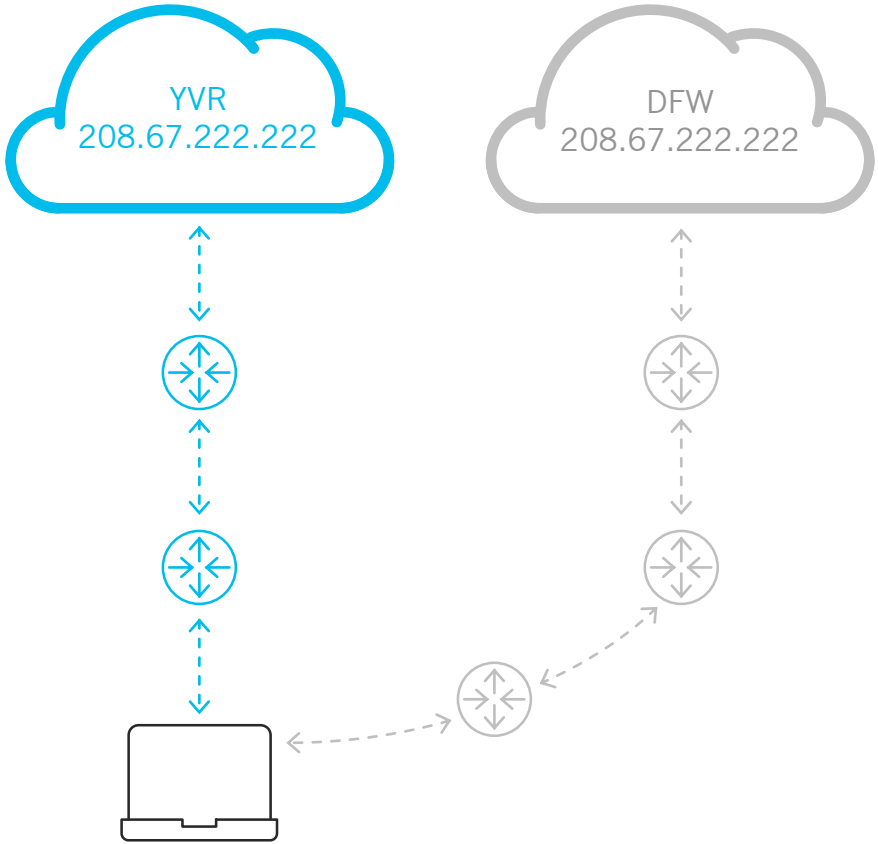
100%
business uptime
since 2006

Anycast IP routing for reliability

All data centers announce same IP address

Customer points DNS traffic to our IP address

Requests transparently sent to fastest available with automated failover

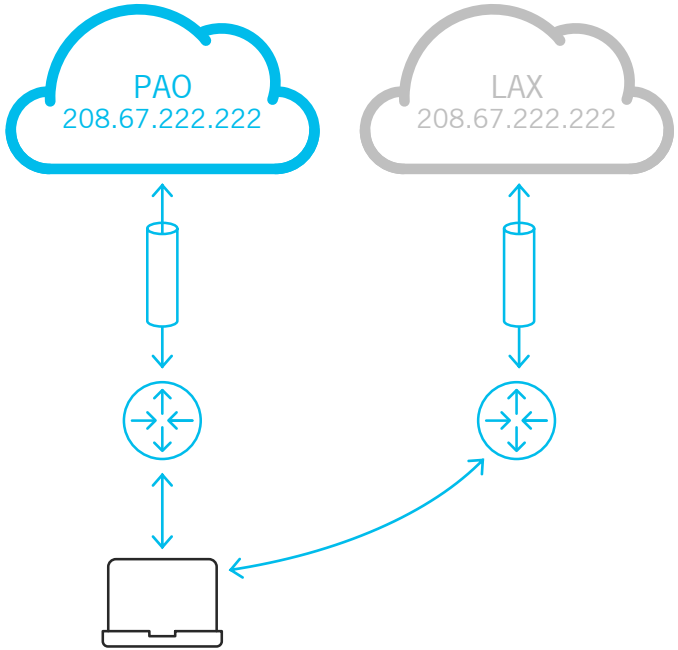


Leveraging Anycast for tunnel reliability and resilience

Customers choose data center to handle requests

Customers do not have to build a backup IPSec tunnel

If data center fails, customers' IPSec tunnel automatically moves with minimal downtime



Call to action

1. Consider where your organization is with remote trends and how your security stack must evolve
2. Ensure security is tied into the SD-WAN conversation from the beginning
3. Explore cloud security platforms focusing on reliability, deployment/management, coverage/ integrations, and efficacy


CISCO

Current Umbrella Packages

SIG Essentials

Includes all features in Platform plus:

- Secure web gateway
  - Send all web traffic via proxy chaining, IPSec tunnel, and PAC file
  - Decrypt and inspect SSL traffic (HTTPS)
  - Block URLs based on Cisco Talos and other third party feeds
  - Block files based on AV engine and Cisco Advanced Malware Protection
  - Enable URL filtering and block custom URLs
  - Log full URLs
  - Analyze unknown files via Cisco Threat Grid (200 files per day)* *Future functionality; not yet available
- Cloud-delivered firewall (L3/L4)
  - Send all outbound traffic via IPSec tunnel
  - Enforce rules based on IPs, ports, and protocols
- Cisco Enhanced Support

Simplified view of seat-based packages

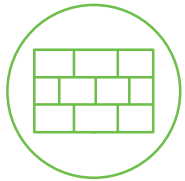
Tested/integrated Cisco deployment options

DNS, SWG, & CDFW

ISR

CSR

SD-WAN
(Viptela)



ASA

DNS only

AnyConnect

WLAN
controller

Meraki MX

Security
Connector for iOS

Mobility
Express

Meraki MR

Data center availability

	Proxy chaining & PAC files Web gateway	IPSec tunnel Web gateway & cloud-delivered firewall
North America		
Ashburn, VA	•	•
Atlanta, GA		
Denver, CO		
Dallas, TX	•	•
Los Angeles, CA	•	•
Miami, FL	•	•
New York City, NY	•	•
Palo Alto, CA	•	•
Seattle, WA	•	
Vancouver, Canada	•	
Toronto, Canada	•	
South America		
Sao Paulo, Brazil		
EMEA		
Amsterdam, NL	•	•
Paris, FR		
Copenhagen, DK	•	
Dublin, IE		
Dubai, AE	•	
Frankfurt, DE	•	•
London, GB	•	•
Milan, IT		
Prague, CZ		
Bucharest, RO		
Warsaw, PL		
APJ		
Johannesburg, ZA	•	
Hong Kong, CN	•	
Melbourne, AU		
Mumbai, IN	•	
Tokyo, JP	•	targeted Q3
Singapore, SG	•	targeted Q3
Sydney, AU	•	