

# Cisco Secure Internet Gateway

SASE

Milan Habrcetl

Cisco Cyber Security Specialist, [mhabrcet@cisco.com](mailto:mhabrcet@cisco.com)

15.3.2022



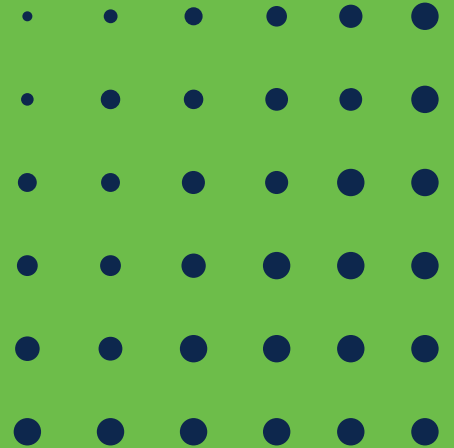


# Agenda



- ▶ SASE
- ▶ Global cloud architecture
- ▶ Threat intelligence
- ▶ Umbrella product overview
- ▶ Umbrella components / key functionality
  - Connections, integration and logging
  - DNS security
  - Secure web gateway
  - Cloud delivered firewall
  - Cloud access security broker (CASB)
  - Cisco SecureX

SASE



# SASE helps you get back in the driver's seat



Deliver secure access  
anywhere, anytime



Make your business  
more agile

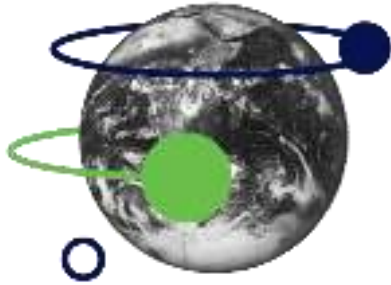


Move access control  
to the cloud edge



Gain efficiencies with an  
as-a-service model

# At Cisco, we're uniquely positioned to help



Networking

Largest SD-WAN solution provider



Security

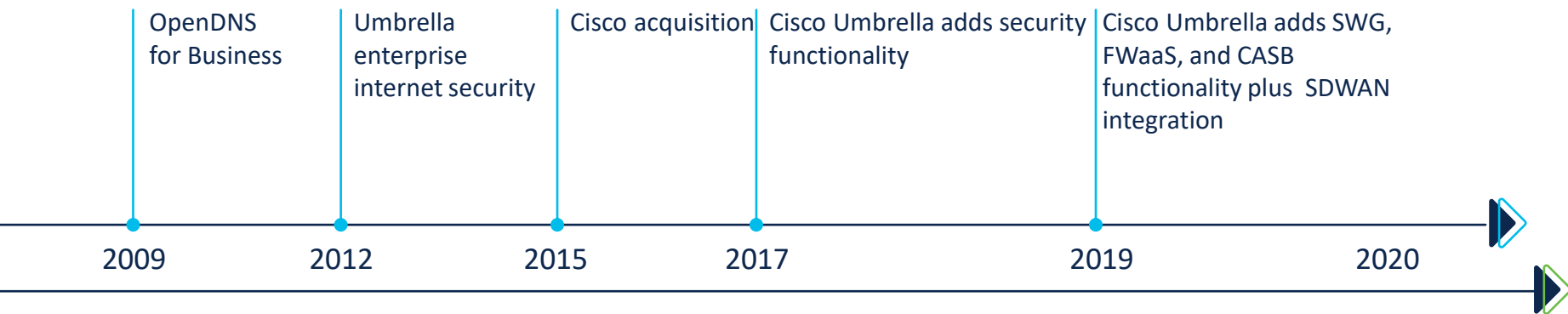
Defending 100% of the Fortune 100



Zero Trust

Leader in Zero Trust two years running

# Cisco Umbrella evolution



SIG



SASE



# Gartner: Secure Access Service Edge (SASE)

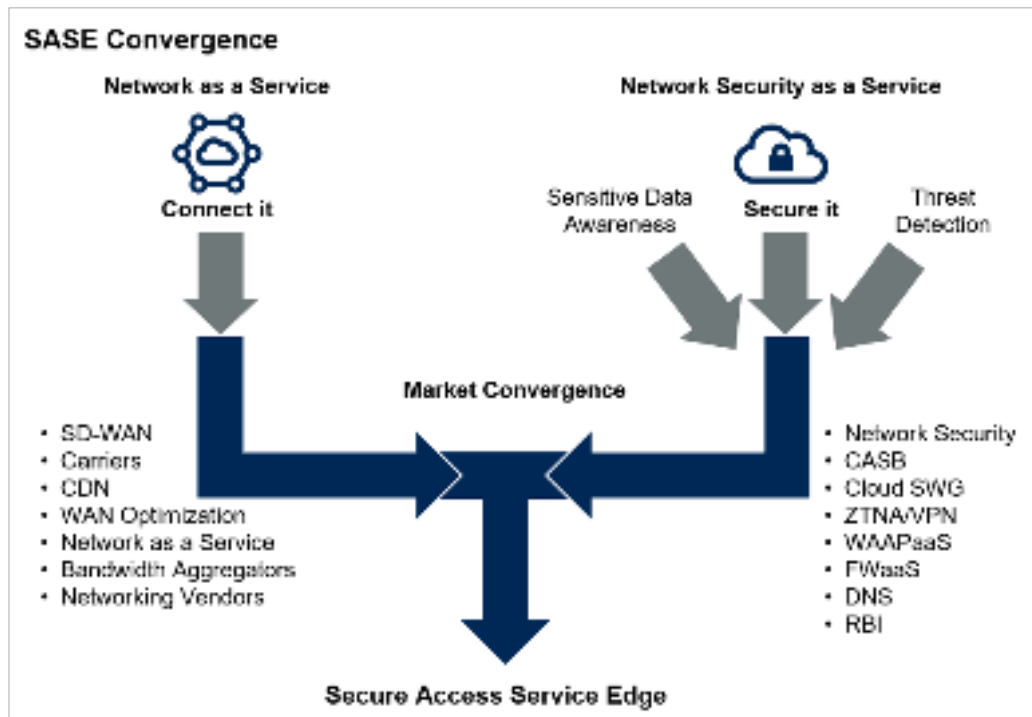
Convergence of networking and security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

Benefit rating:  
Transformational

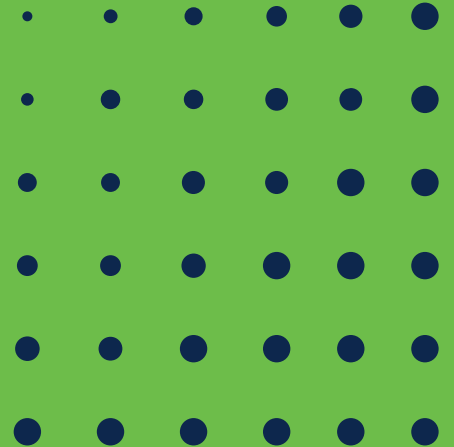
Market penetration:  
Less than 1% of target audience

Maturity:  
Emerging

Gartner, The Future of Network Security  
Is in the Cloud, Neil MacDonald, Aug 30, 2019



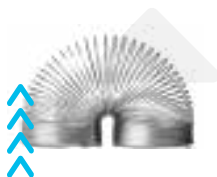
# Global cloud architecture



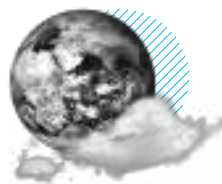


# Born in the cloud global architecture

Rapid scalability, continuous innovation, high performance – without downtime



Containerized, multi-tenant architecture powers scalability and reliability



Agile infrastructure delivers continuous innovation without customer downtime



Proven track record since 2006 with global data centers on six continents



Low latency delivers high performance and up to 73% latency reduction

# Lightning-fast performance

## Reduce latency and speed performance

- 1,000+ peering partnerships with ISPs, CDNs and SaaS platforms - fastest route
- 6,000 peering sessions to create shortcuts to major ISPs - decrease hop count
- Carrier neutral: locate data centers based purely on best and diverse connections and services



# Peering across the globe

## Umbrella peering accelerates application performance

- Peering lowers latency by providing more direct paths
- Peering from data centers to more than 1,000 organizations including leading SaaS & IaaS providers (always growing)
- Up to 50% performance increase with key applications

## Examples of peering partnerships (not comprehensive)

### SPs

- AT&T (Global)
- Bell
- Bharti Airtel Limited
- BT
- Charter
- China Mobile
- Google Fiber
- KDDI
- Rogers
- Swisscom
- Telkom
- Verizon
- Vodafone

### IaaS

- Alibaba
- Amazon
- Dell Services
- Digital Ocean
- Equinix
- Fastly
- Go Daddy
- Google
- Huawei Cloud
- Microsoft
- Rackspace

### SaaS

- Adobe
- Apple
- Baidu
- Box
- DocuSign
- Microsoft
- NS1
- Oracle
- Salesforce
- Square
- Webex
- Dropbox

# Performance validation by Miercom Labs

## Results

- Reduced hop count by up to 33%
- Improved latency and traffic consistency (jitter) by up to 73%
- Substantive network performance improvement, using real app use cases

## Testing setup

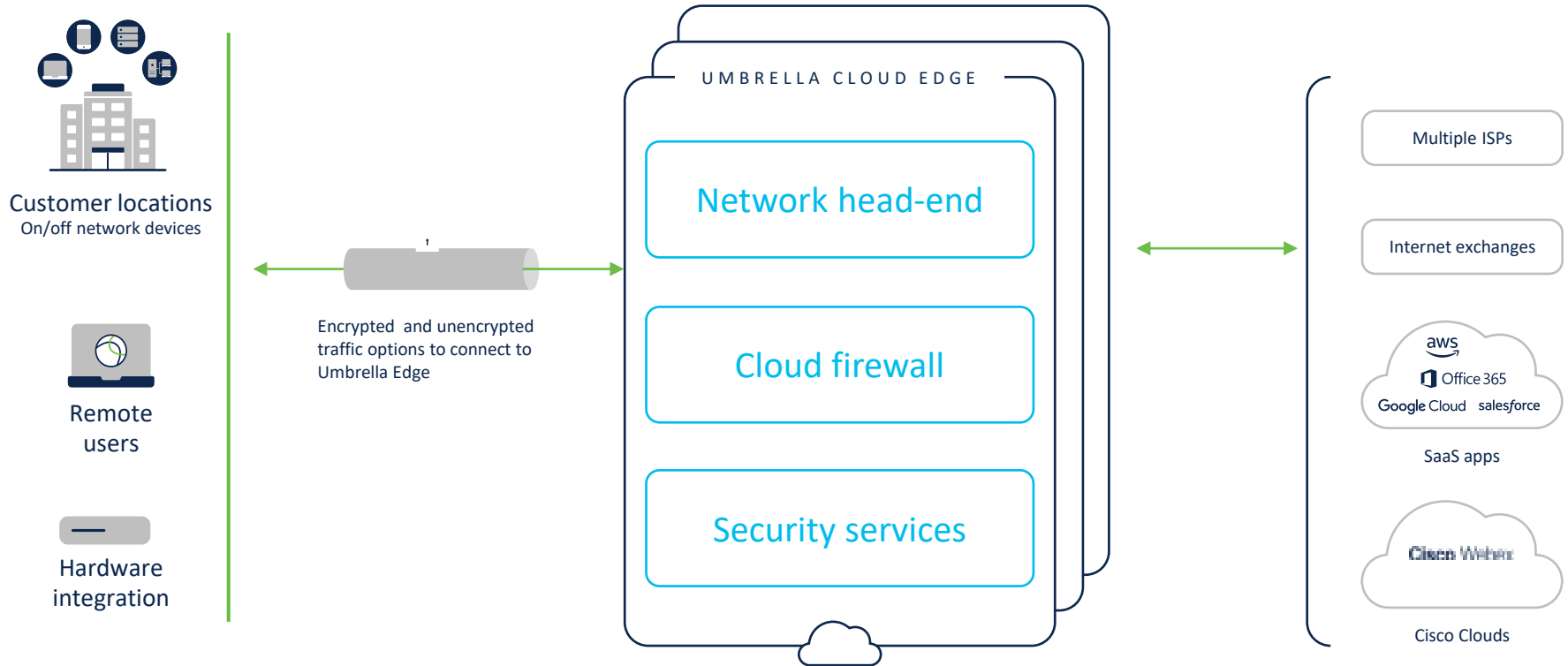
- Connection to seven popular SaaS applications (table below is BOX)
- Compared direct-to-internet vs. through Umbrella with secure web gateway (with decryption) and cloud firewall policies set

Data center location	Hop count			Latency (ms)		
	Before *	After *	Hop count improvement (%)	Before *	After *	Reduction in latency (%)
New York, NY	15	12	20.0	60	21	65
San Jose, CA	14	11	21.4	58	14	67.6
Ashburn, VA	16	13	18.8	62	22	64.5
Frankfurt, Germany	18	12	33.3	67	18	73.1

[Cisco Umbrella Performance Assessment Summary Report](#), Miercom Labs, December 2020

\* See "Testing setup" above

# Global cloud architecture: top-line

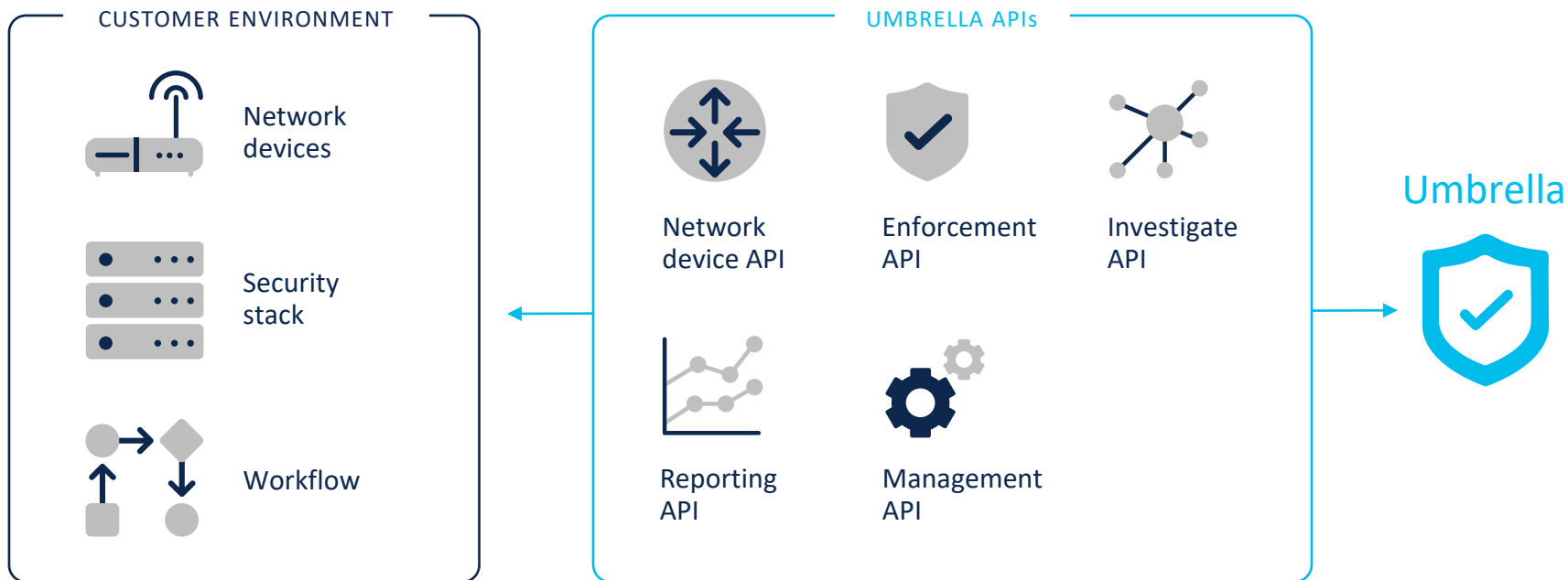


# Cisco Umbrella earns SOC 2 Type II Compliance

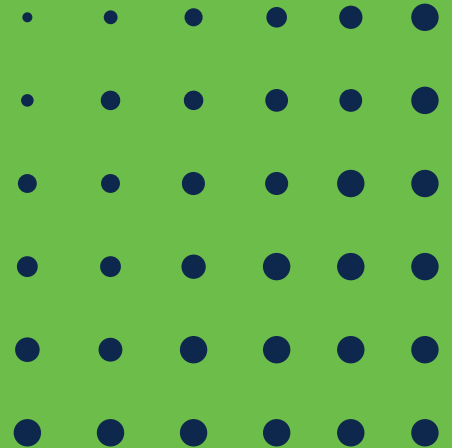


# APIs to easily enable integration

Enrich data and extend protection across existing tools and workflows



# Interactive threat intelligence





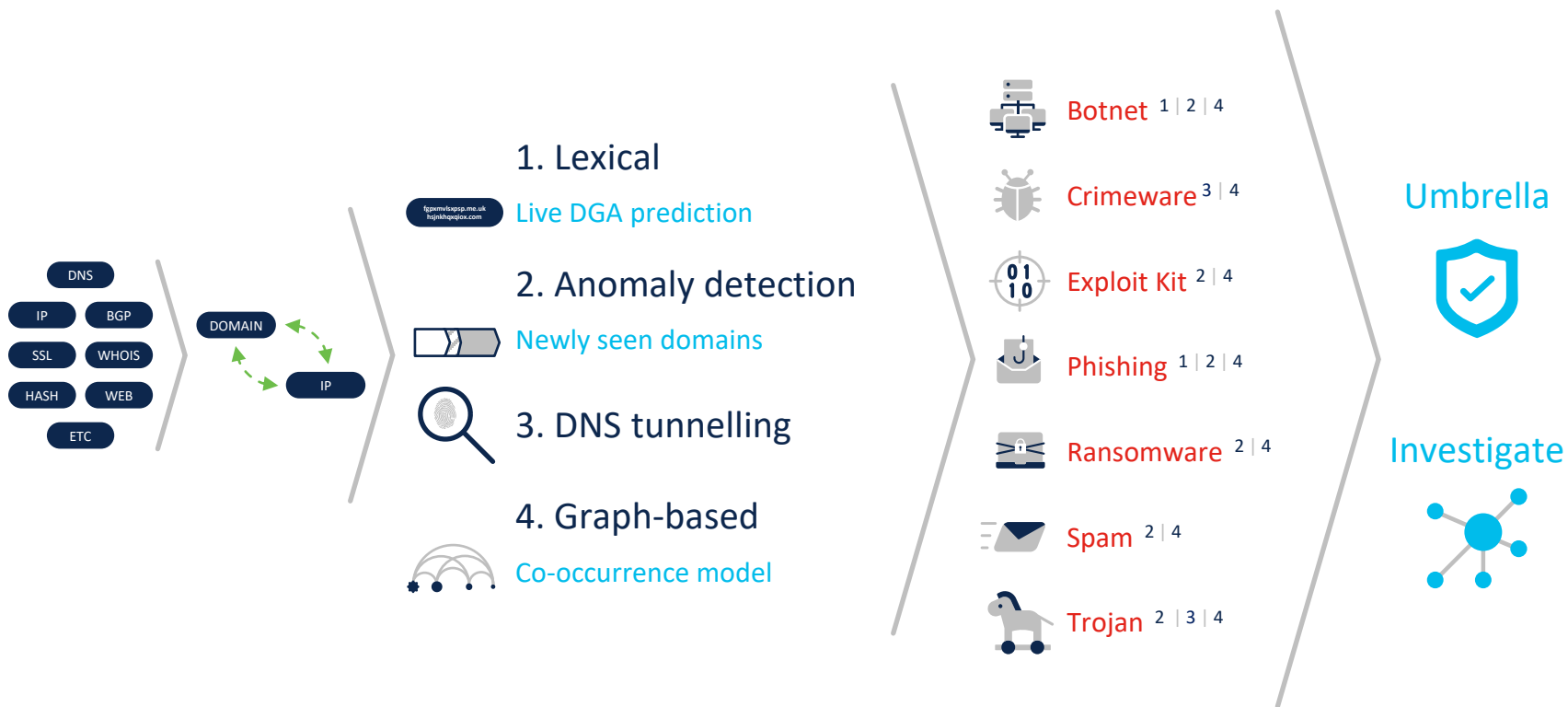
# Cisco Talos: the largest threat intelligence organization on the planet

- ▶ 400+ full-time threat researchers and data scientists
- ▶ 5 billion reputation requests, 2 billion malware samples seen daily
- ▶ 5 billion category responses, 200 million IPs & URLs blocked daily.

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

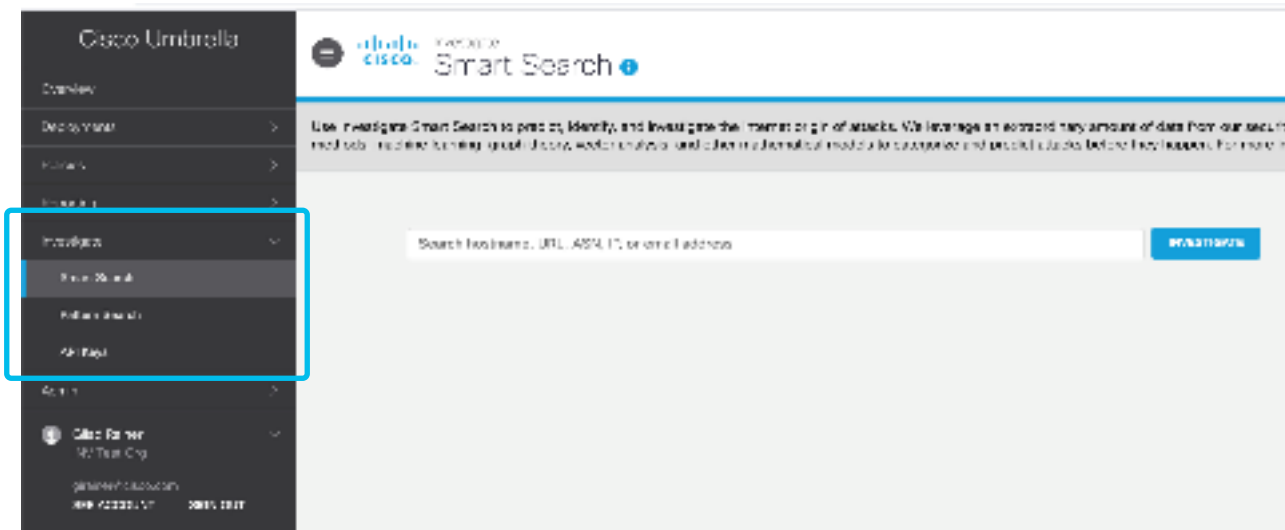


# Multi-faceted threat intel



# Streamlined navigation

## Investigate incorporated into Umbrella



- Accessing Investigate from the Umbrella dashboard has been simplified. Now, users can easily navigate to Investigate and start a Smart Search or Pattern Search.
- Customers can also quickly locate API Keys for their various orgs

# NEW AV-TEST security efficacy report!

Featuring Cisco Umbrella

Security efficacy is one of the top differentiators for Umbrella.

Umbrella is #1 in security efficacy- again!

- Focus of lab test: assessing each SWG vendor's ability to protect roaming and remote workers
- AV-TEST assessed both our SWG and DNS-layer protection security efficacy

The logo for AV-TEST, featuring the letters 'AV' in a stylized, bold font with a diagonal slash through them, followed by 'TEST' in a large, bold, sans-serif font.

The Independent IT-Security Institute  
Magdeburg Germany

Umbrella consistently performed better than the competition!

Get the report: <https://bit.ly/3jFNVwK>

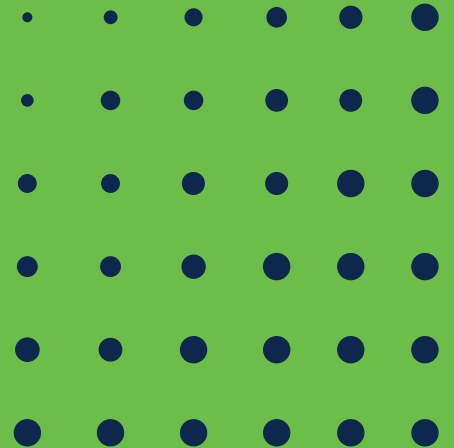
# Efficacy testing: SWG

- Data captured Sep-Oct 2020 by AV-TEST, using their samples (not Cisco's)
- Products configured to provide highest level of protection
- Umbrella SWG also with DNS security policy

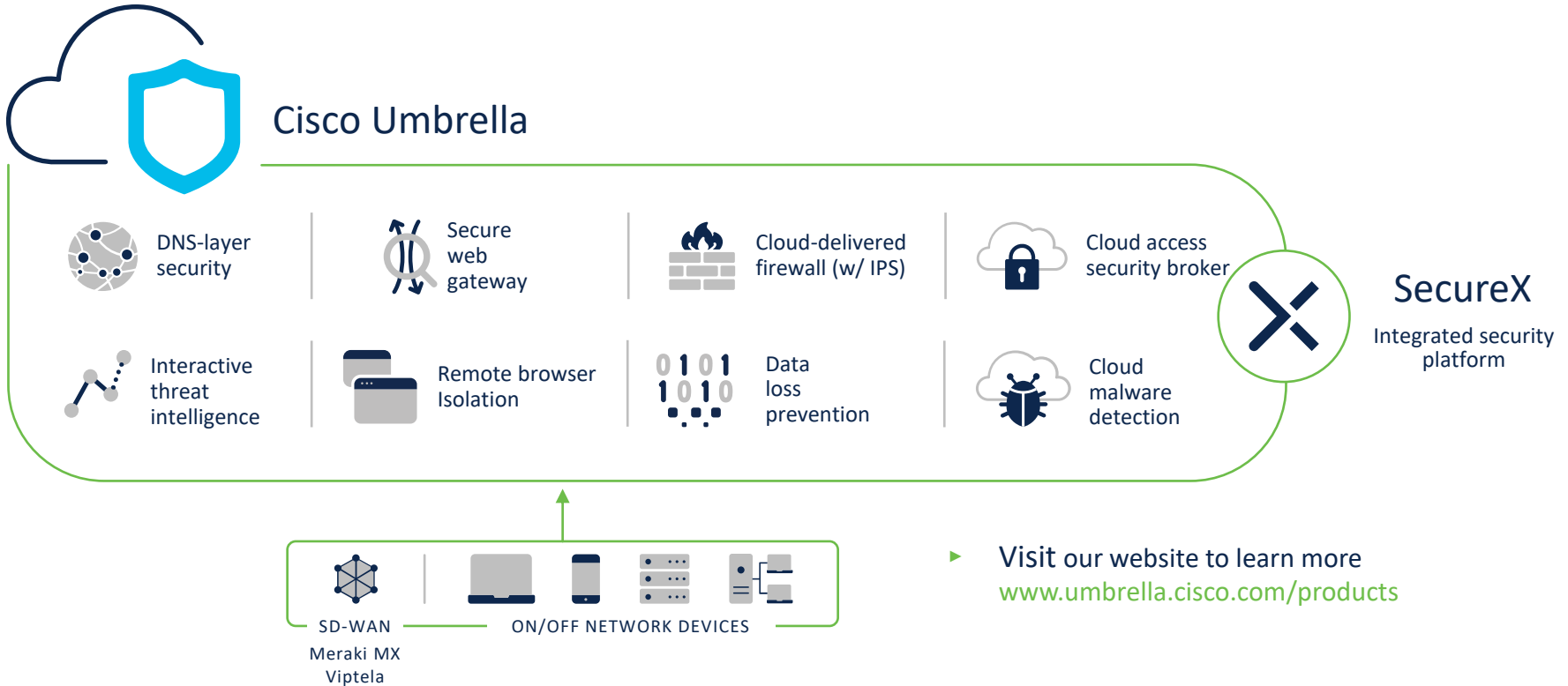
Type of test	Umbrella	Zscaler	Palo Alto	Netskope	Akamai
Malicious PE files (Portable executables)	93.65	87.29	83.88	82.12	61.41
Malicious destinations	99.15	93.28	57.68	55.52	48.35
Phishing links	93.79	85.20	91.51	48.35	74.12
<b>Total detection rate</b>	<b>96.39</b>	<b>89.67</b>	<b>73.15</b>	<b>61.90</b>	<b>58.43</b>

% Detected (higher is better)

# Product overview



# Cisco Umbrella



► Visit our website to learn more  
[www.umbrella.cisco.com/products](https://www.umbrella.cisco.com/products)

# Cisco Umbrella key capabilities

## Secure access to the internet & usage of cloud applications



### Visibility

- On & off corporate network
- All internet and web traffic
- All apps
- All devices
- SSL decryption
- Shadow IT
- Sensitive data transmitted

### Protection

- DNS-layer security
- Web inspection
- File inspection & sandboxing
- Data loss prevention
- Non-web traffic inspection
- Intrusion prevention system
- Remote browser isolation
- Data at rest cloud malware scanning



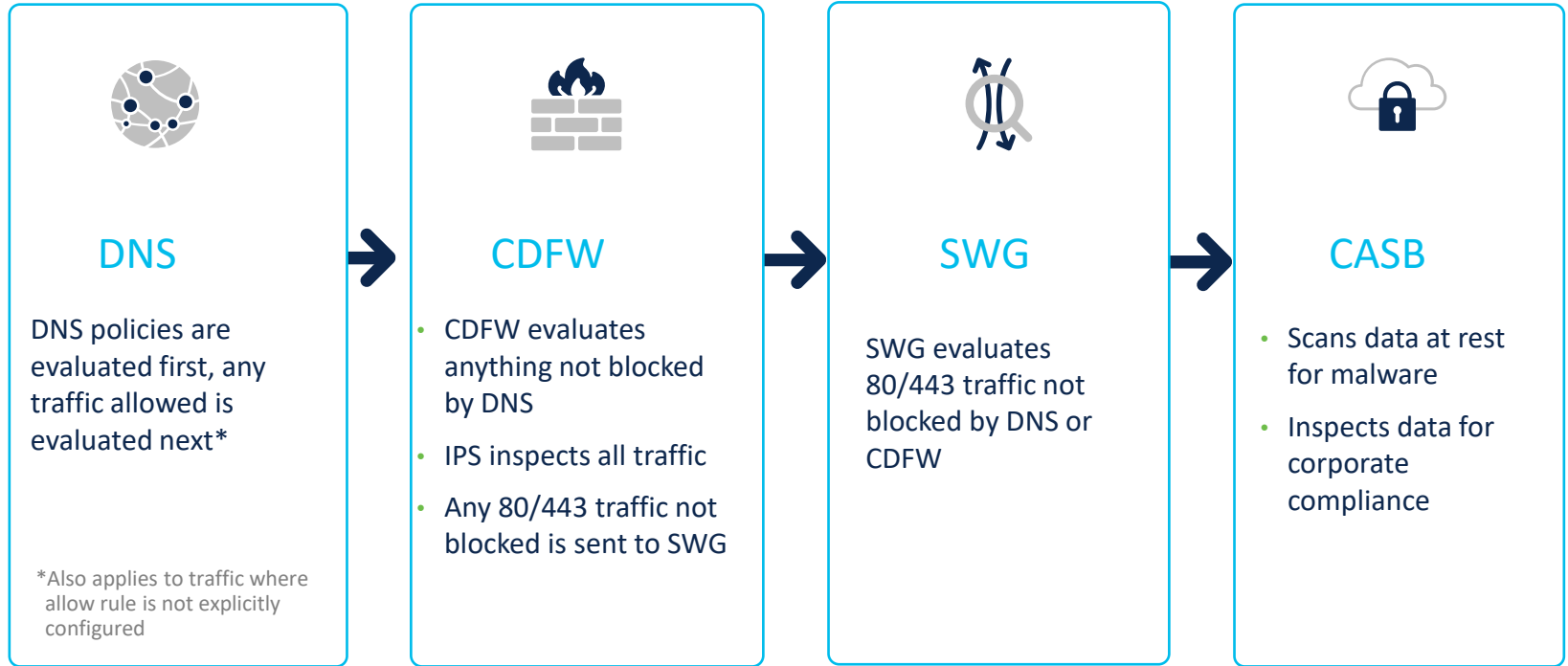
### Control

- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls

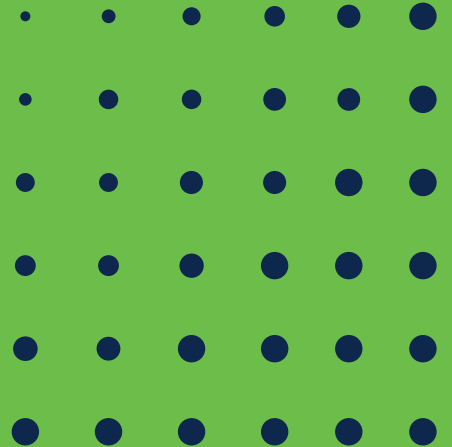
Built-in extended detection and response (XDR) platform with Cisco SecureX



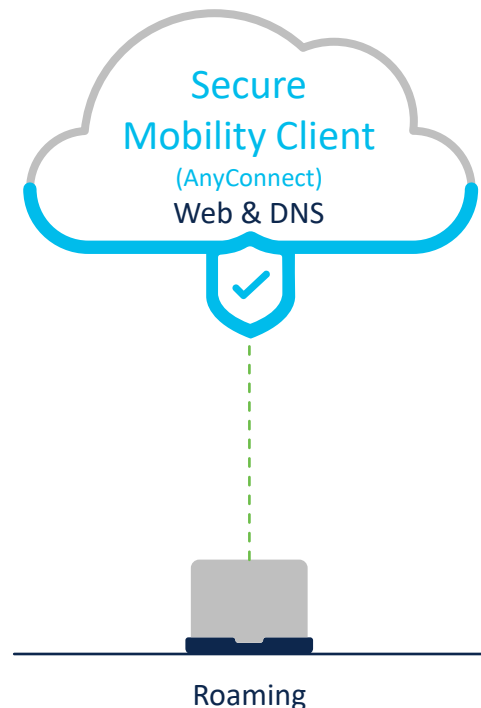
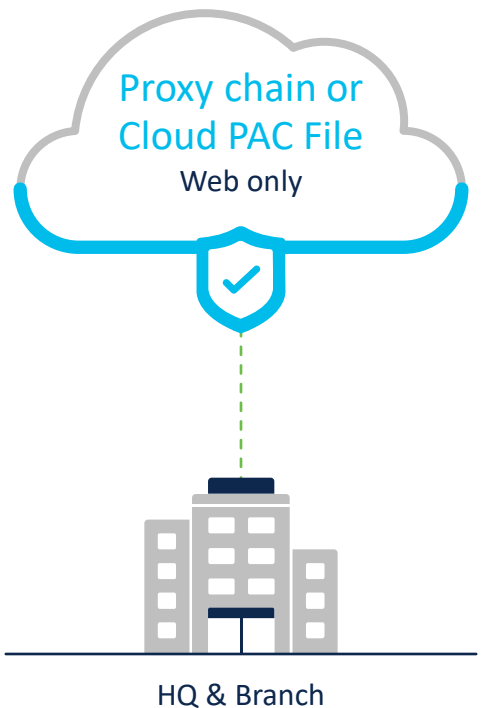
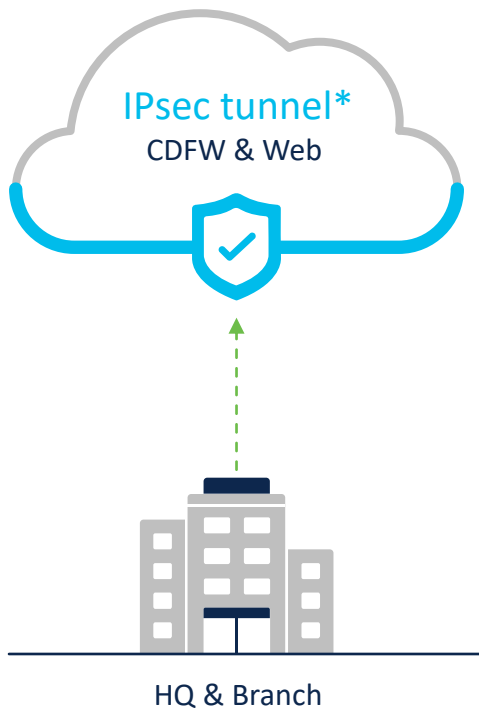
# SIG policy outcome summary



# Connections, integrations and logging

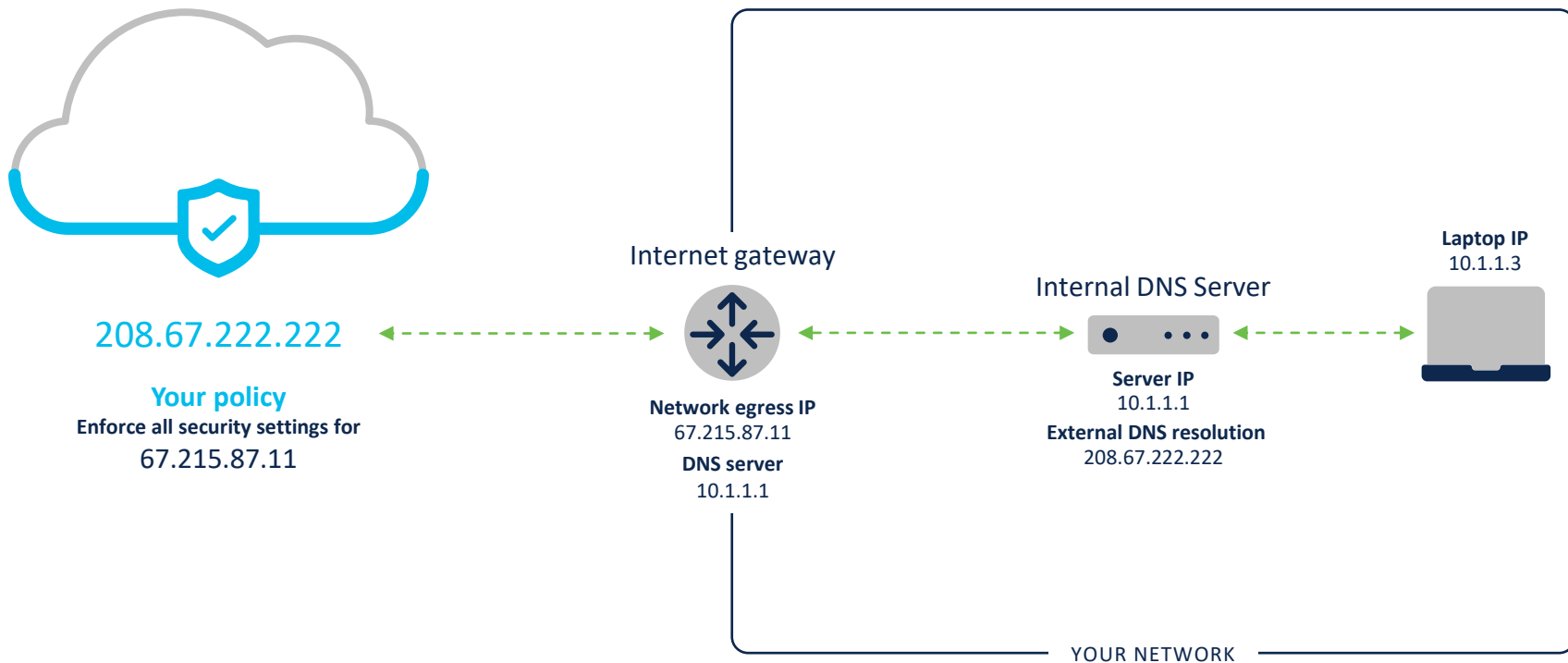


# Flexible connection methods



\*Optional customer hosted PAC file

# Protect on-network devices via DNS server



# Tunnel capabilities

## IPsec capacity

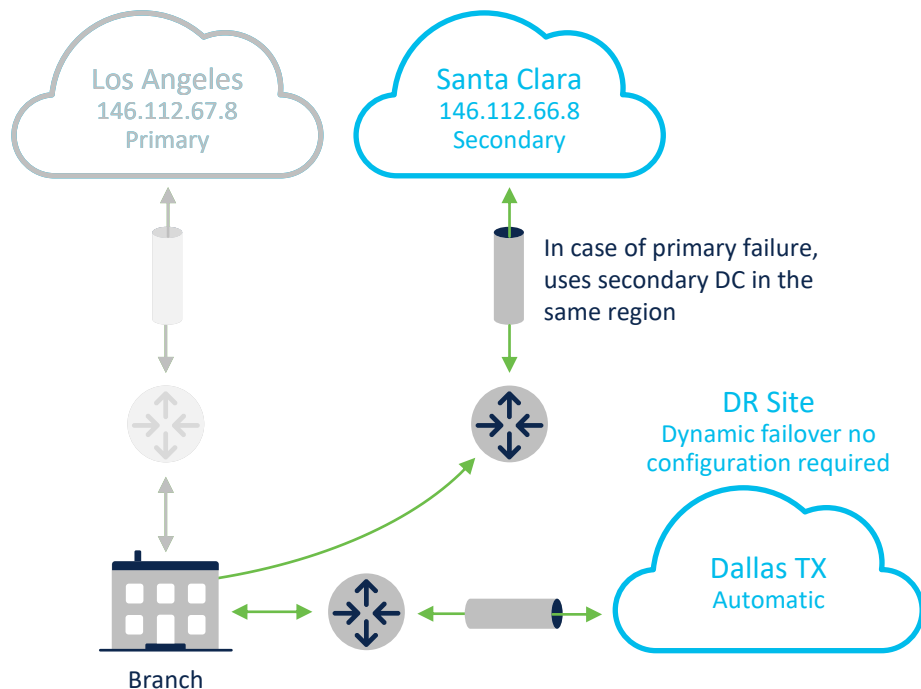
- 500 Mbps by default, with ongoing development to increase capacity
- Multiple tunnels can be deployed to support higher capacity

## Availability

- Hard code primary, secondary (optional)
- Failover to secondary data center and disaster recovery is handled by anycast
- Failure detection uses IKE dead peer detection

## Example

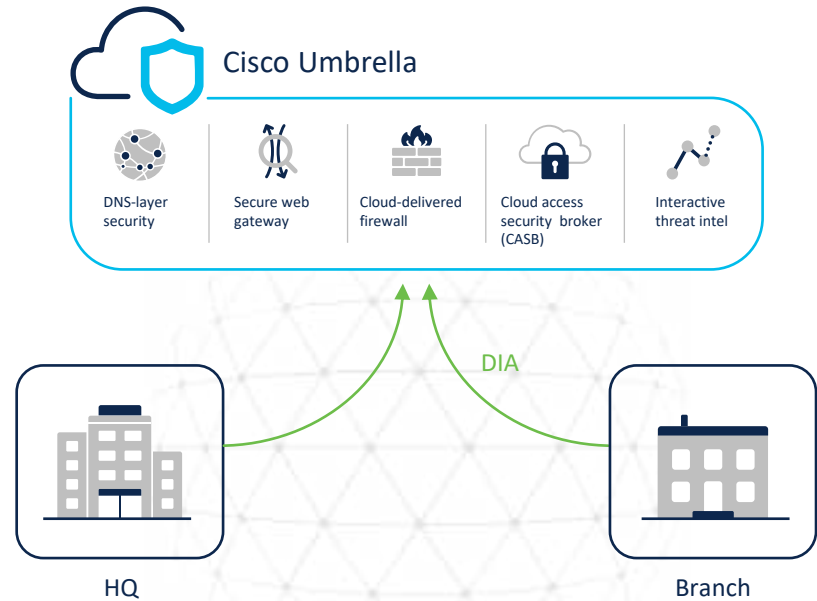
Data center region code US-1



# Umbrella for Cisco SD-WAN

## Fast forward time to value with automated security

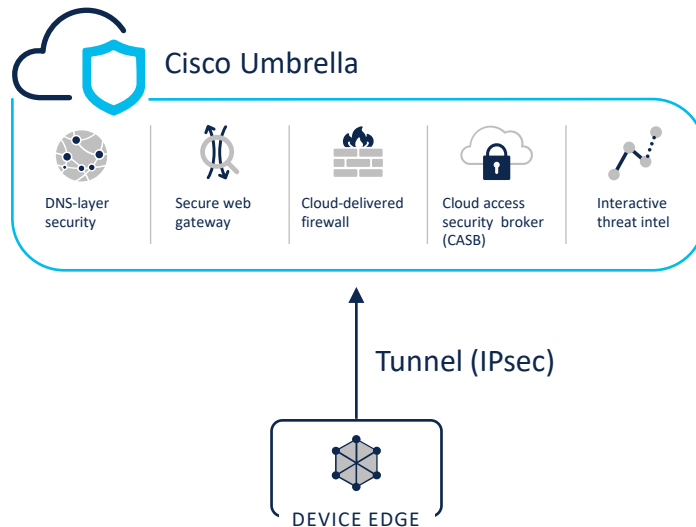
- **Hands-off automation:** deploy IPsec tunnels across thousands of branches in minutes
- **Top notch protection:** defend against threats with the leader in security efficacy
- **Simplified management:** single pane of glass across all offices, users and roaming clients
- **Deeper inspection & controls:** SWG, CASB, and cloud-delivered firewall layer 3, 4, and 7



# Automated IPsec tunnel creation

## Umbrella for Cisco SD-WAN

- By pushing the SIG feature template, a customer can now setup an IPsec tunnel to Umbrella SIG
- Without this solution, a customer would need to manually establish the tunnel for each WAN Edge device at branch



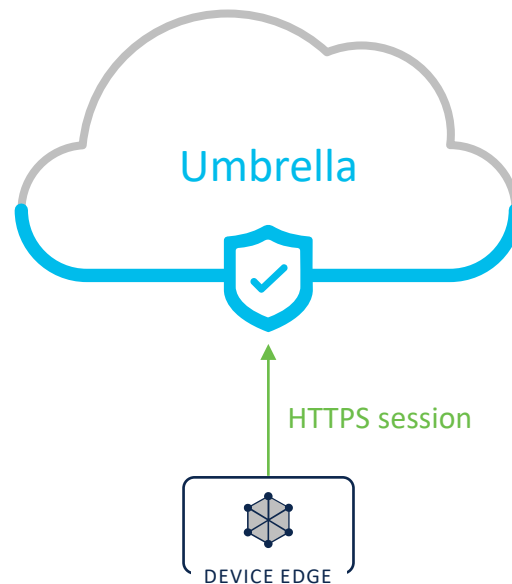
With this feature, SD-WAN will have much deeper integration with Umbrella

# Rapid onboarding: accelerates security and ROI

## Umbrella for Cisco SD-WAN

Deploying Secure SD-WAN now takes minutes not months:

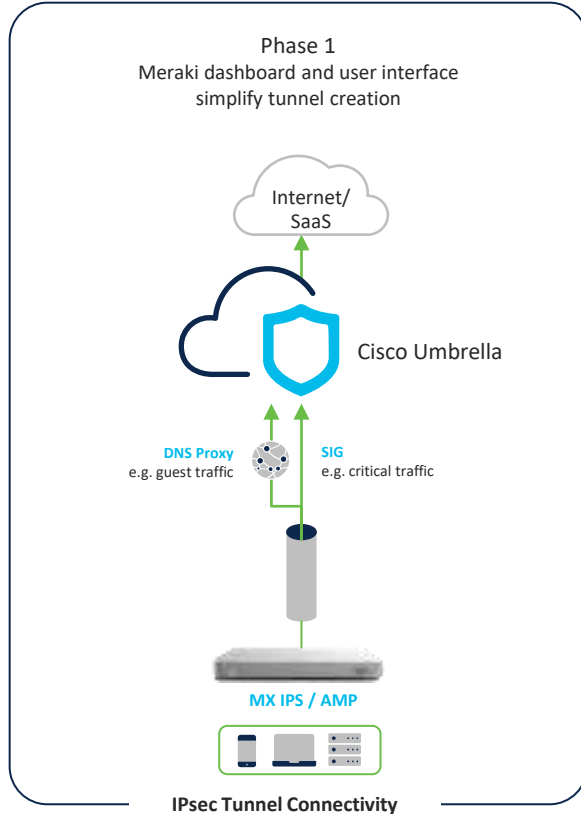
- SD-WAN Edge devices are automatically registered to Umbrella
- No need to manually enter API keys
- Secure API key is automatically provisioned on the edge device via an HTTPS session



New DNA-Premier package



# Meraki MX and Umbrella Integration Options

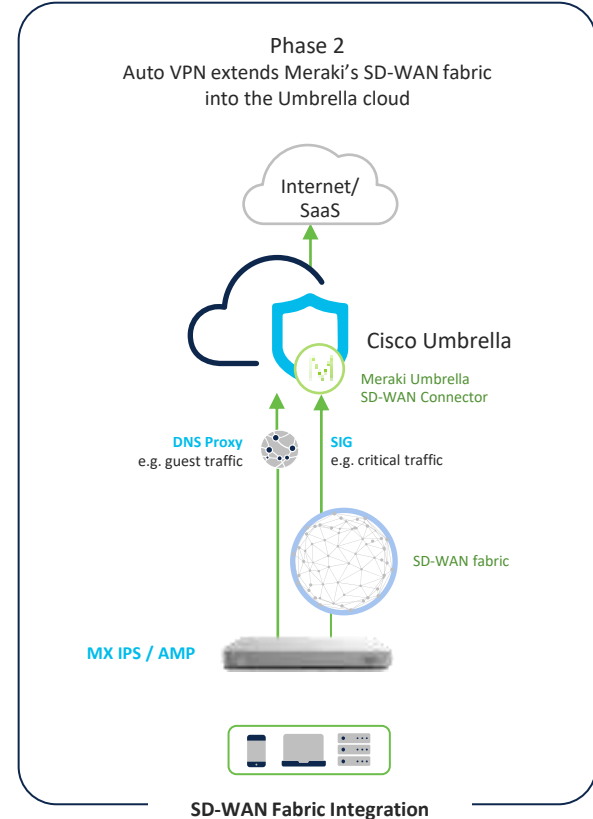


Choose per site

Flexible security  
options

Automated SD-  
WAN fabric  
integration

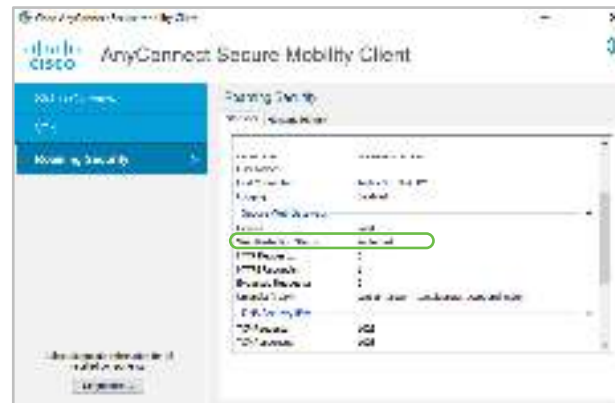
Competitive  
Differentiator



# Cisco AnyConnect Security Mobility Client

Entitlement for Mobility Client is included (excludes VPN functionality)

- AnyConnect can be used across an entire enterprise
- Both Umbrella DNS and Secure Web Gateway services can co-exist
- Protect assets on or off network
- Simple and consistent user attribution
- Choice of fail open or fail closed



Supports Windows and Mac desktops

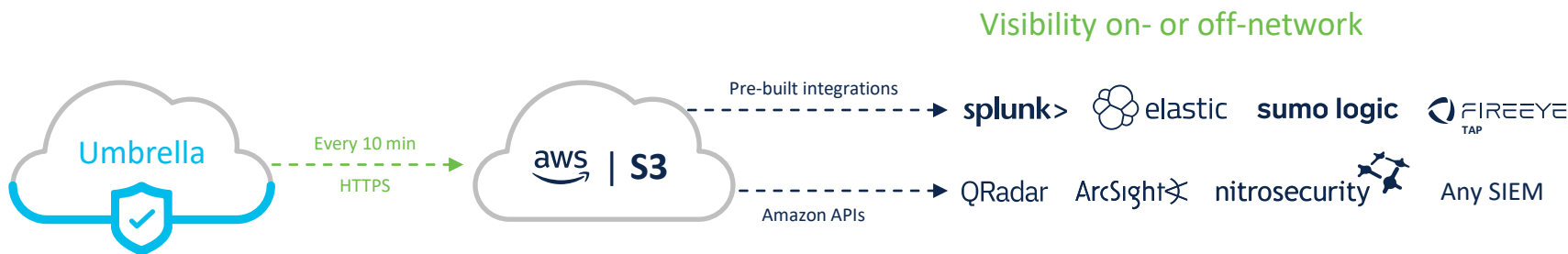
# Log storage with Amazon S3

## S3 benefits

- Triple redundant and encrypted storage
- Pre-built SIEM/log analytic integrations
- Use self-managed or Cisco-managed bucket
- Centrally managed S3 logs

## EU data warehouse available

- Ease data security concerns
- Store data in EU facility
- Use multi-org console for different storage settings for different locations



# DNS security



# Proven leader in cloud-native security



620B

requests per day



500M

authentication events every month



500K

global customers



96%

Highest threat detection rate in the industry \*

# Unique protections from DNS-layer security

Add New Security Setting

Setting Name  
New Security Setting

This security list is applied to:  
DNS Policies

Copy From Existing  
None

- Malware  
Websites and other services that host malicious software, drive-by downloads, exploits, mobile threats and more.
- Newly Seen Domains  
Domains that have become active very recently. These are often used in new attacks.
- Geolocation and Control Callbacks  
Prevent compromised devices from communicating with attacker's infrastructure.
- Phishing Attacks  
Fraudulent websites that aim to trick users into handing over personal or financial information.
- Dynamic DNS  
Bad actors that use hosting dynamic DNS content.
- Potentially Harmful Domains  
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN  
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
- Cryptomining  
Cryptomining allows organizations to control cryptocurrency access to mining pools and web miners.

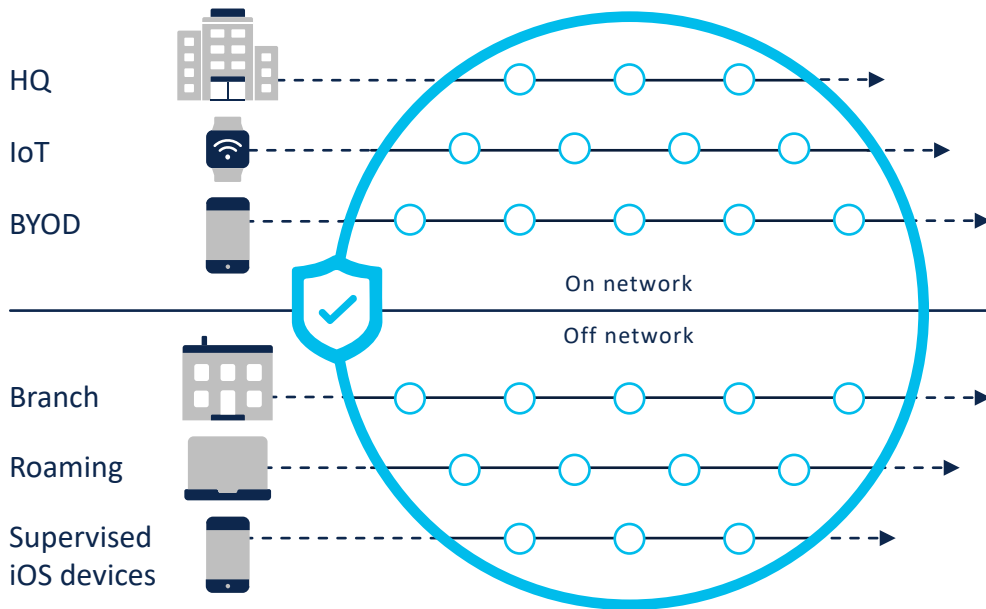
RELATED

CANCEL SAVE

- **Good:** Umbrella DNS-layer security
  - **Better:** Umbrella cloud-security service using secure web gateway (full proxy) and firewall.
  - **Best:** Both
- DNS-layer security provides unique protection

# DNS security

Visibility and protection for all activity, anywhere

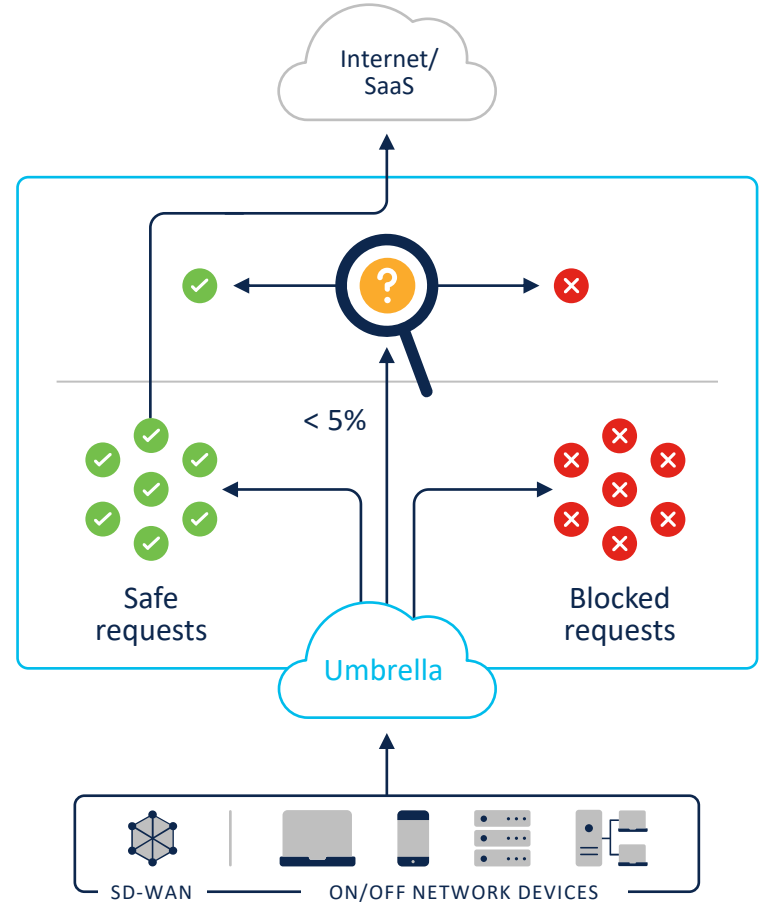


- All office locations
- Any device on your network
- Roaming laptops
- Mobile devices - IOS and Android
- Every port and protocol

# DNS-layer security

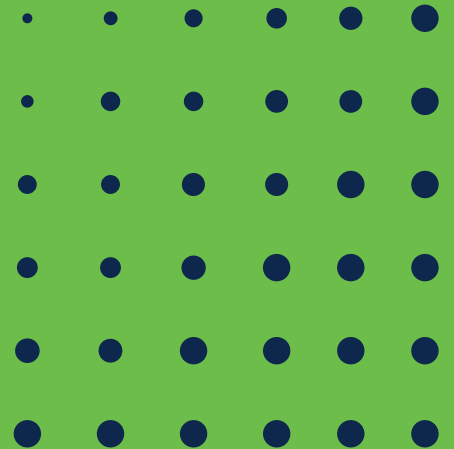
## First line of defense

- 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
- Accelerate threat response with an integrated security platform
- Amazing user experience — faster internet access; only proxy risky domains





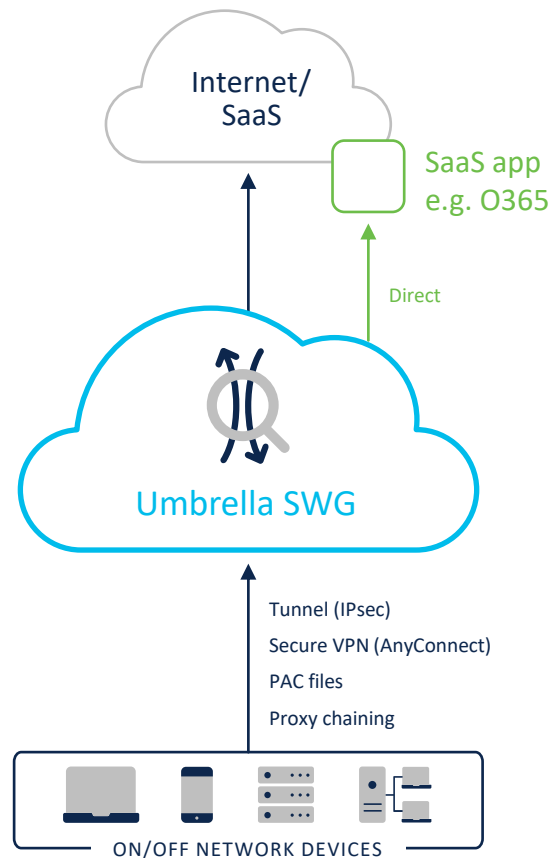
# Secure web gateway



# Umbrella SWG

## Multiple functions and aggregated reporting in one cloud console

- Malware scanning includes two anti-virus engines and Secure Endpoint (AMP) lookup
- File type controls
- Full or selective SSL decryption
- Category or URL filtering for content control
- Secure Malware Analytics (Threat Grid) file sandboxing
- App visibility and granular controls
- Full URL level reporting

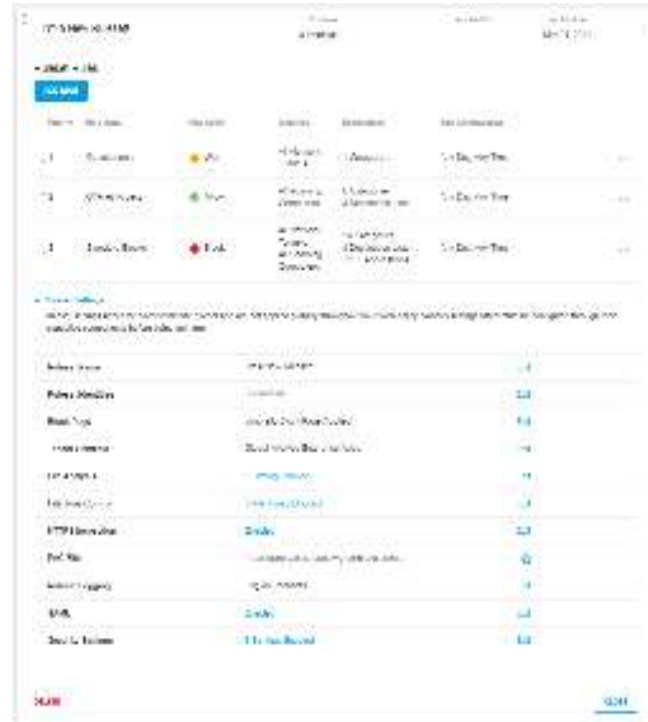


# Umbrella rules-based policies

**Overview:** Umbrella rules-based policies wizard gives granular controls and enabling the creation of more sophisticated policies.

## Features

- Create specific rules for placing allow, block, or warn actions on destinations
- Match rules on identity and destination
- Gain more flexibility when creating web policies
- Create in-policy exceptions



# Categories

- Apply policy to a large number of sites
  - Content categories are used for “acceptable use policies”
  - Security categories are used for security policies
- Umbrella SWG uses Talos categories for both content and security
- Over 100+ categories
- Dynamic Cloud updates (full dataset)

Limit Content Access

Access to these sites will be restricted based on the type of content served by the pages

Select Setting

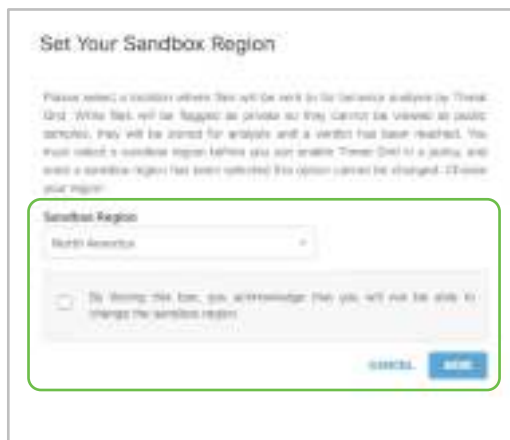
Base Content

CATEGORIES TO BLOCK [SELECT ALL](#)

<input type="checkbox"/> Academic Fraud	<input type="checkbox"/> Nature
<input checked="" type="checkbox"/> Adult	<input type="checkbox"/> News/Media
<input type="checkbox"/> Adult Themes	<input type="checkbox"/> Non-Profits
<input type="checkbox"/> Piracy	<input type="checkbox"/> Nudity
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Online Communities
<input type="checkbox"/> Arms	<input type="checkbox"/> Online Meetings
<input type="checkbox"/> Arsenology	<input type="checkbox"/> Online Trading
<input type="checkbox"/> Auctions	<input type="checkbox"/> Organizational Email

# Cisco Secure Malware Analytics (Threat Grid) sandboxing

- Ability to detect hidden threats in files that are being downloaded
- A set of new or higher risk files are placed in a sandbox environment and checked for malicious activity/content
  - Alerts posted on files that do show bad activity
  - Umbrella threat intelligence is updated for that file



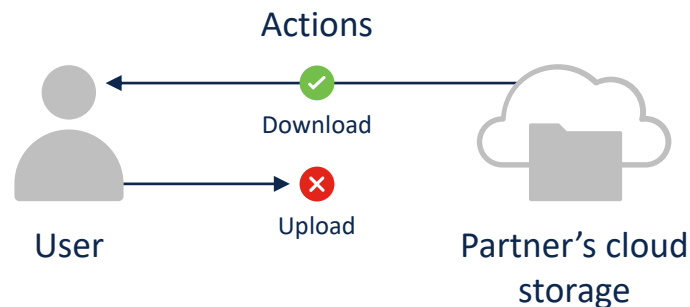
Regions:  
Europe  
or North  
America

SIG Essentials now has a Cisco Secure Malware Analytics limit of 500 files per day

SIG Advantage includes unlimited submissions and access to the full sandbox console for 3 users

# Granular controls for popular SaaS apps

- Block posts/shares to social media apps
- Block attachments to webmail apps
- Block uploads to cloud storage, collaboration, office productivity, content management, and media apps



# File type control – categories and file types

Edit File Control

Search for and apply policy controls for downloaded file types.

Search file types

**All Groups**

<input type="checkbox"/>	Audio	7
<input type="checkbox"/>	Compressed files	13
<input type="checkbox"/>	Data and database	10
<input type="checkbox"/>	Disc and media files	4
<input type="checkbox"/>	Documents	10
<input type="checkbox"/>	Executables	15
<input type="checkbox"/>	Images	12
<input type="checkbox"/>	System-related files	9
<input type="checkbox"/>	Videos	23



Edit File Control

Search for and apply policy controls for downloaded file types.

Search file types

**All Groups / Audio**

<input type="checkbox"/>	aif
<input type="checkbox"/>	cda
<input type="checkbox"/>	mid
<input type="checkbox"/>	mp3
<input type="checkbox"/>	wav
<input type="checkbox"/>	wma
<input type="checkbox"/>	wpl

# SSL/HTTPS decryption in the cloud

- Visibility and set of security measures for the increased amount of encrypted web traffic
- Decryption, reporting and inspection for encrypted web traffic and files
  - No hardware expense
  - No scaling issues as encrypted Internet traffic increases
  - Ability to selectively decrypt





# Microsoft compatibility mode



Organizations rely on M365 to run daily business and require high performance



Microsoft doesn't recommend traffic inspection for M365

- ✓ Compatibility Mode ensures that M365 traffic transparently passes thru Umbrella - yet gains native Umbrella backbone performance improvements
- ✓ Uses Microsoft APIs to determine the domains recommended to be bypassed, saving work for the customers trying to keep their devices up to date
- ✓ No policies can be applied to M365 traffic when enabled, (e.g. no tenant controls)
- ✓ Umbrella will log all traffic sent to these domains

# User attribution and authentication

- Security Assertion Markup Language (SAML 2.0)
  - Service Provider (SP) – Umbrella
  - Identity Provider (IdP) –PingID, Okta, Azure, Duo, OpenAM, ADFS, and others via generic support
- Surrogate support options
  - Cookie surrogate-requires HTTP/HTTPS inspection, can specify timeframe expiry
  - IP surrogate-HTTPS inspection not required, more consistent userID auths
- Intended support for browsers, may not work for “desktop apps”



# SWG users and groups

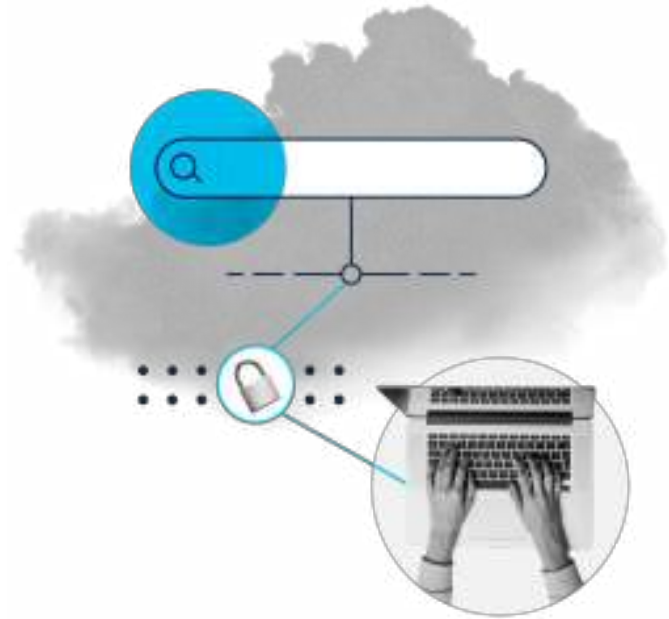
- CSV upload
  - Recommend CSVDE tool on Windows Domain Controller
- AD connector Active Directory sync
  - Group filtering supported with data file
  - Standard AD connector install version 1.3.8+
  - Only one Domain Controller required, no VA required



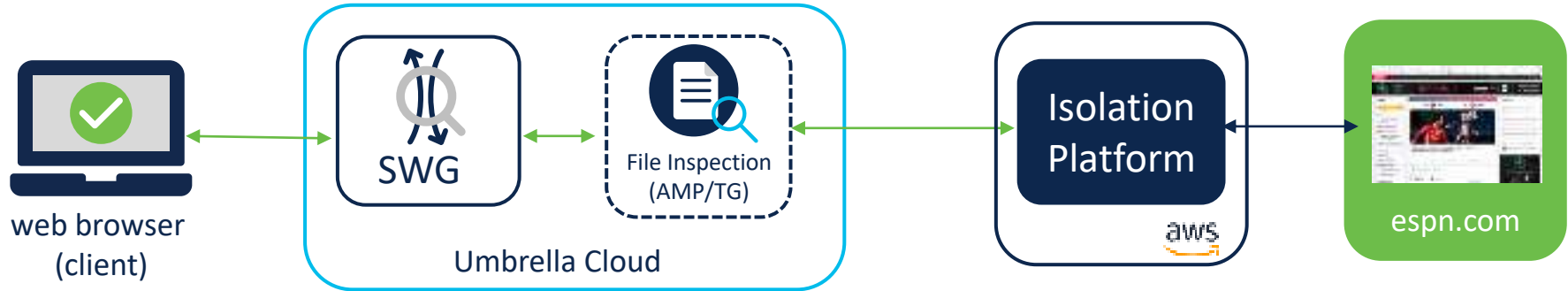
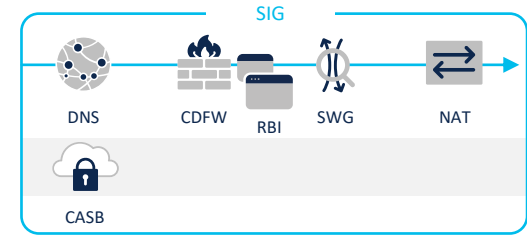
# New Umbrella remote browser isolation (RBI)

## Added layer of protection for risky destinations and users

- Provide air gap between user device and browser-based threats
- Deploy rapidly without changing existing configuration
- Deliver a secure browsing experience with protection from zero-day threats



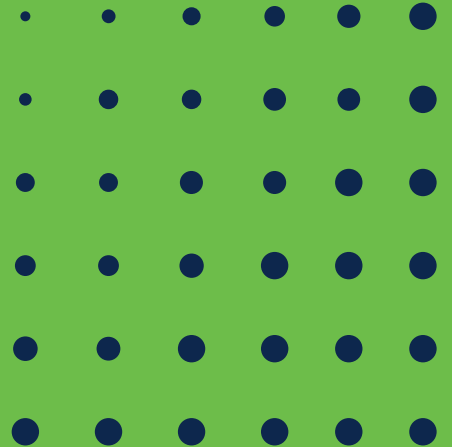
# RBI traffic flow overview



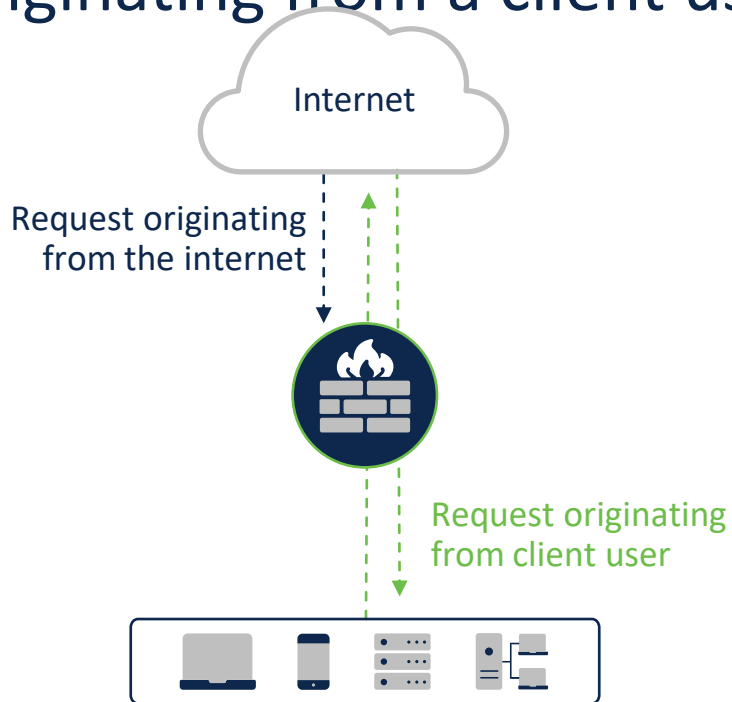
# Three RBI package options

- **Isolate Risky**
  - Isolate uncategorized websites
  - Isolate security categories (including Potentially Harmful)
- **Isolate Web Apps**
  - Isolate popular communication and collaboration applications like Box, Slack, Gmail
  - Content categories: Chat/IM, Social/Personal Networking, File Storage/Transfer, Webmail/Organization Email
- **Isolate Any**
  - Isolate any chosen destination, including content categories, security categories, destination lists, applications, uncategorized, etc.

Cloud-delivered firewall



# Umbrella firewall protects traffic from requests originating from a client user



Firewall use cases that protect traffic from requests **originating from a client user** are **essential to securing access** to the internet and controlling cloud app usage





Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view [Manage Firewall](#).

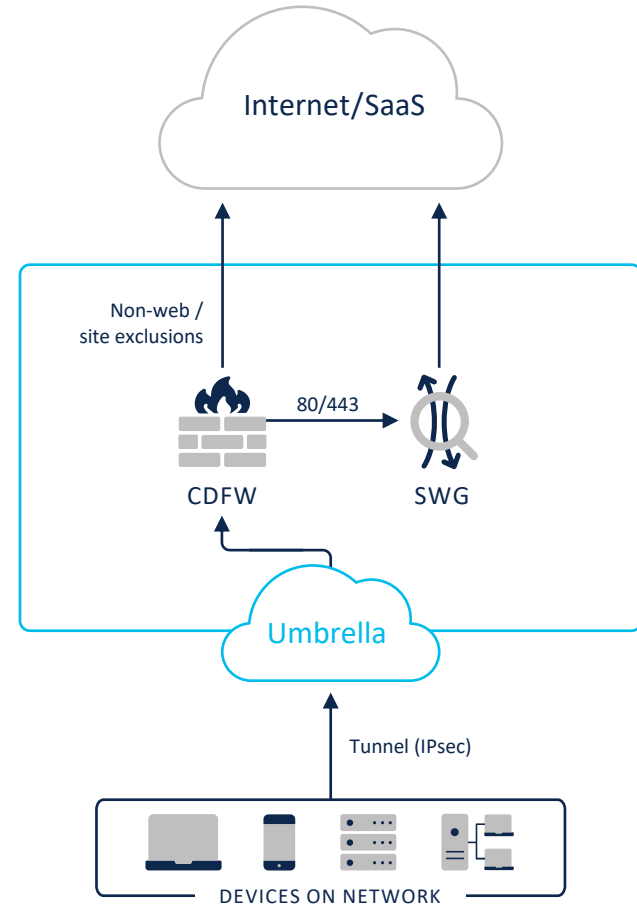
FILTERS

3 Total

<input type="checkbox"/>	Priority	Name	Status	Action	Applications	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit	
<input type="checkbox"/>	1	Block SSH	<span style="color: green;">●</span> Enabled	<span style="color: red;">●</span> Block	ssh	Any	Any IPs Any Ports	Any IPs 1 Port	<span style="background-color: black; color: white; border-radius: 10px; padding: 2px 5px;">▲ 0/24hrs</span>	<span style="color: red;">▲</span> No Hits	...
<input type="checkbox"/>	2	p2p rule	<span style="color: green;">●</span> Enabled	<span style="color: red;">●</span> Block	Any P2P ftp	Any	Any IPs Any Ports	Any IPs Any Ports	<span style="border: 1px solid gray; border-radius: 10px; padding: 2px 5px;">25.0 /24hrs</span>	Aug 24, 2020 - 08:33am	...
<input type="checkbox"/>	3	Default Rule	<span style="color: green;">●</span> Enabled	<span style="color: green;">✓</span> Allow	Any Application	Any	Any IPs Any Ports	Any IPs Any Ports	<span style="border: 1px solid gray; border-radius: 10px; padding: 2px 5px;">58.1 k/24hrs</span>	Aug 24, 2020 - 03:15pm	...

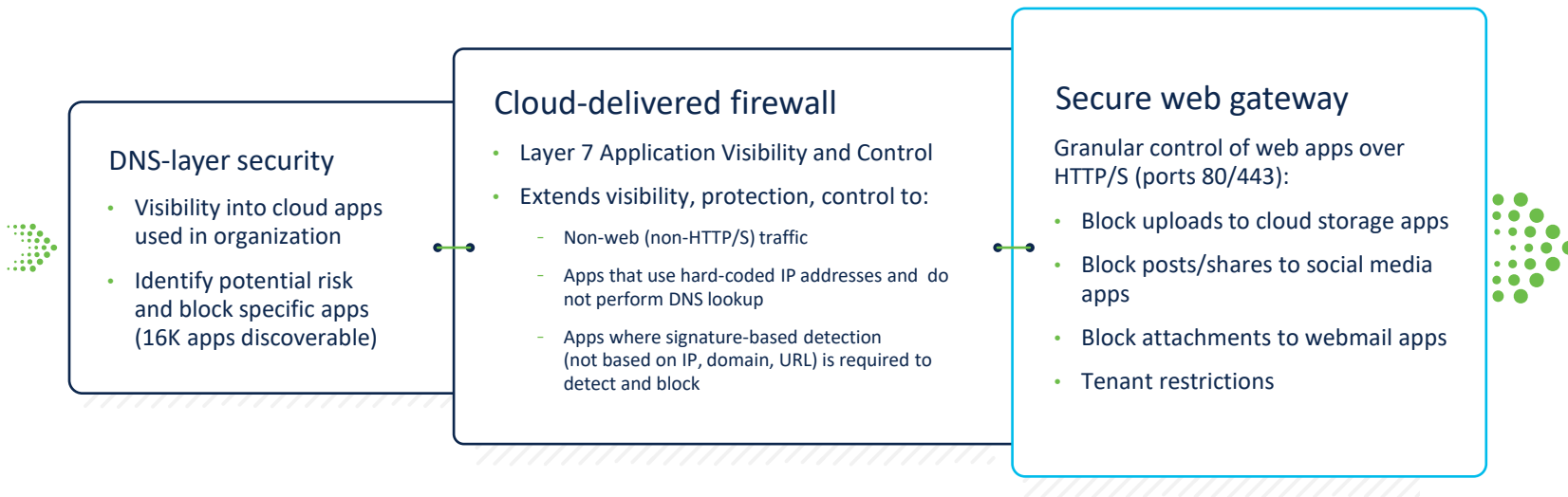
# Layer 7 application visibility and control

- Tunnel all client-driven traffic to Umbrella
- Block high risk applications and protocols (layer 7 application visibility & control)
- Centrally manage IP, port, protocol and application rules (layer 3, 4 and 7)
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination required



# Application visibility and control

## Extends across enforcement points



# Key use cases

## Layer 7 application visibility and control

### Block shadow IT over non-web ports

Example: Stop use of unapproved SaaS apps

- WebEx allowed
- MS Teams video not allowed
- Google Hangouts not allowed

### Block insecure applications on non-standard ports

Example: Stop remote virtual terminal connection into other networks

- Such as telnet via non-standard port 8080

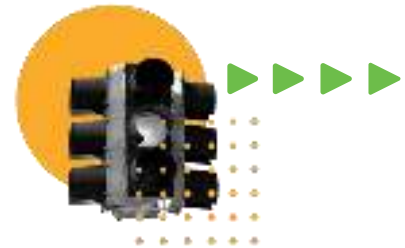
Example: Stop file transfer

- Such as FTP via non-standard port 1003

### Block unsanctioned traffic over non-web ports

Example: Stop use of unapproved traffic

- Block all peer-to-peer traffic (e.g. TOR or BitTorrent)



# Umbrella Intrusion Prevention System (IPS)

Available from November 2021

## Capabilities

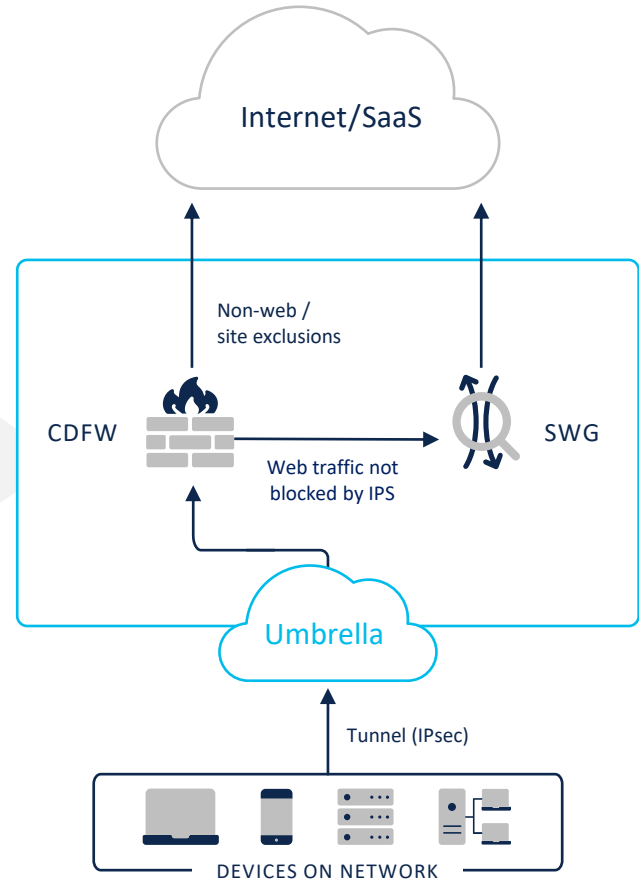
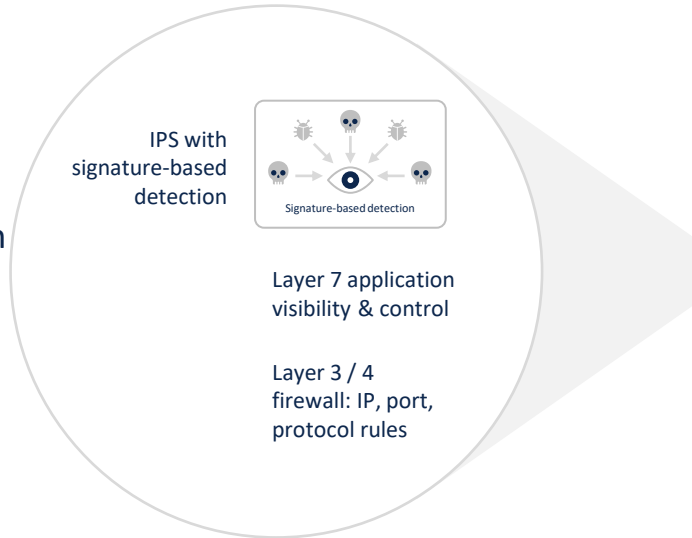
- Deepen Umbrella cloud firewall protection for client-driven traffic
- Use signature-based detection (Snort 3) to examine network traffic flows & prevent vulnerability exploits
- Add layer of detection/blocking for malware, botnets, phishing, and more
- Leverage Cisco Talos' 40K+ signatures (and growing) to detect and correlate threats in real-time

## Results

- ✓ Simplify management via Umbrella's single, unified dashboard
- ✓ Remove capacity concerns of appliances by using scalable cloud compute resources
- ✓ Stop more threats with the industry's most effective threat intelligence
- ✓ Detect/block exploitations of vulnerabilities

# Umbrella Intrusion Prevention System (IPS)

Layers of security for high security efficacy



# Umbrella key IPS differentiators

## Simplicity

IPS rules can be complex

- Single, unified dashboard simplifies management
- Simple, global ruleset, configured in seconds
- Cisco-unique metadata will foster easy ruleset management and configuration

## Performance

Security at stable cost

- IPS may degrade on-premise firewall performance
- Cloud-native IPS means no tradeoff between performance and security

## Efficacy

Threat landscape constantly evolves

- Powered by Cisco Talos threat feed (40K+ signatures)
- Easily gain latest Snort 3 technology for effective security
- Automatically get future Snort 3 updates

## Reliability

Designed for reliability

- Global footprint of world-class data centers
- High availability with Umbrella's innovative use of Anycast with automated failover

# Umbrella IPS use cases



## Meet compliance requirements

- Serve customers with compliance mandates that specify IDS/IPS
- Help address customer requirements through proposals (RFPs)



## Deepen security protection

- Provide added layer of detection and blocking for malware, botnets, phishing, command and control call backs

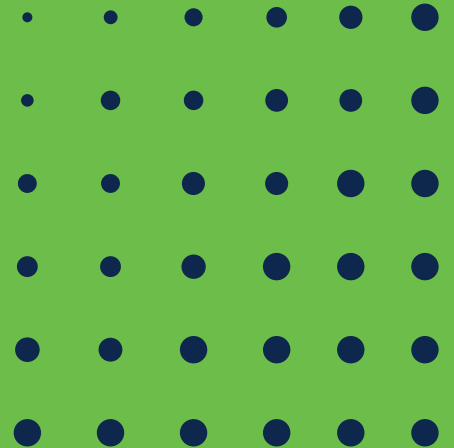


## Extend security protection

- Extend detection and blocking of vulnerabilities to outbound traffic from user-initiated request and inbound traffic associated with that original request



# CASB functionality



# CASB types

## Inline/proxy

### Umbrella

- App visibility & blocking
- Advanced app control
  - Block uploads (i.e. Dropbox/Box)
  - Block attachments (i.e. webmail)
- Tenant controls
- Inline DLP

## Out of band/API

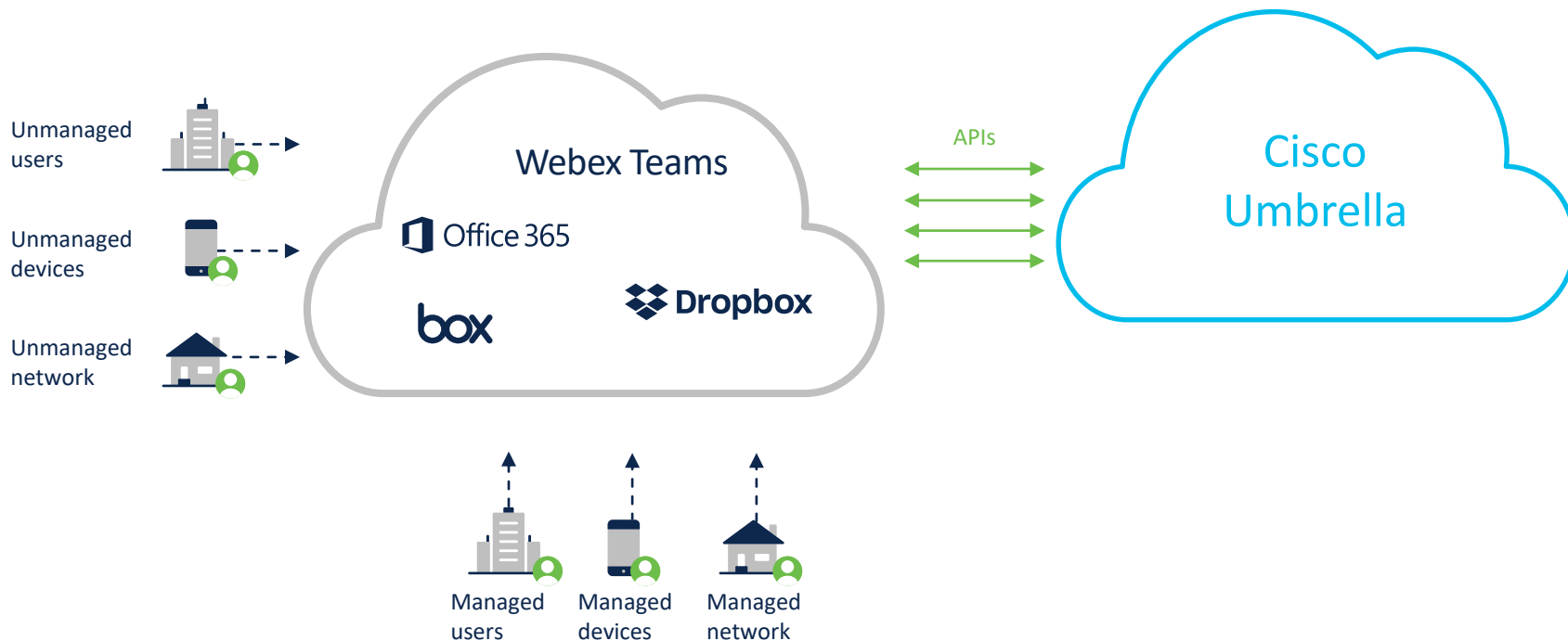
### Umbrella

- Data-at-rest cloud malware detection

### Cloudlock

- User behavior monitoring/alerts
- Cloud storage policy enforcement
- DLP quarantine and revocation actions (out of band)
- OAuth apps: visibility & control

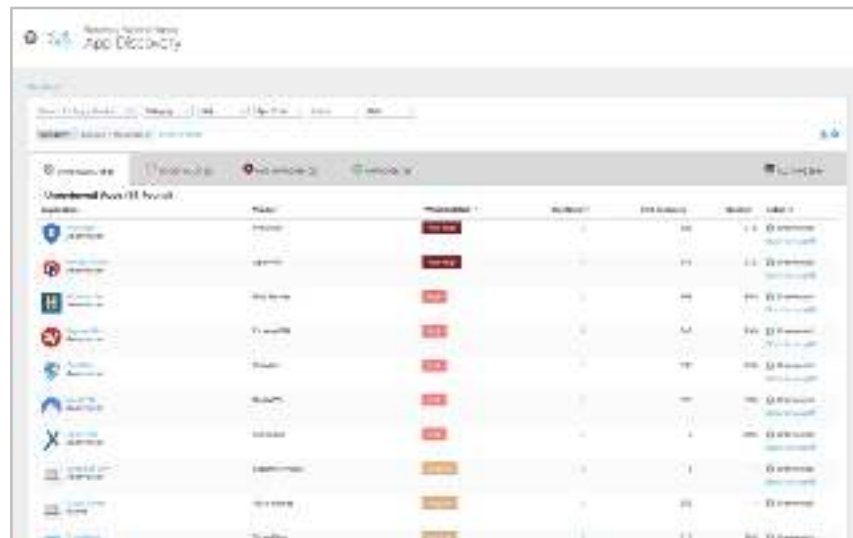
# Malware scanning is API-based, cloud to cloud



# App discovery and controls

## Visibility into shadow IT and control of cloud apps

- Full list of cloud apps in use
- Reports by category and risk level
- Number of users and amount of incoming and outgoing traffic
- Blocking of high-risk categories or individual apps



The screenshot displays the Cisco Secure Network Visibility App Discovery interface. It features a navigation bar with tabs for 'Overview', 'Reports', 'Settings', and 'Help'. Below the navigation bar, there are filters for 'All Applications', 'Risk Level', and 'Category'. The main content area shows a table of cloud applications with columns for 'Application', 'Risk Level', 'Users', 'Inbound Traffic', 'Outbound Traffic', and 'Actions'. The table lists various applications such as Facebook, LinkedIn, and Microsoft Office 365, each with a corresponding risk level indicator (e.g., High, Medium, Low) and user count.

Application	Risk Level	Users	Inbound Traffic	Outbound Traffic	Actions
Facebook	High	100	100	100	Block, Allow, Whitelist
LinkedIn	Medium	50	50	50	Block, Allow, Whitelist
Microsoft Office 365	Low	100	100	100	Block, Allow, Whitelist
Zoom	Medium	50	50	50	Block, Allow, Whitelist
Slack	Medium	50	50	50	Block, Allow, Whitelist
Dropbox	Medium	50	50	50	Block, Allow, Whitelist
Google Drive	Medium	50	50	50	Block, Allow, Whitelist
OneDrive	Medium	50	50	50	Block, Allow, Whitelist
Zoom	Medium	50	50	50	Block, Allow, Whitelist
Slack	Medium	50	50	50	Block, Allow, Whitelist
Dropbox	Medium	50	50	50	Block, Allow, Whitelist
Google Drive	Medium	50	50	50	Block, Allow, Whitelist
OneDrive	Medium	50	50	50	Block, Allow, Whitelist

# Granular app controls

The screenshot displays the Cisco App Discovery interface. A modal window titled "Control Dropbox" is open, allowing for granular control of application settings. The modal contains three application settings, each with a checkbox and a dropdown menu:

- Default Settings**  
Applied in: Global Branch Policy; Security Only ...  
Block
- HR App Restrictive**  
Applied in: High Restrict Group  
Block Uploads
- Global App Allow**  
Applied in: Global Allow Policy  
Allow

Below these settings, there is a checkbox for "Label application as" with a dropdown menu set to "Not Approved".

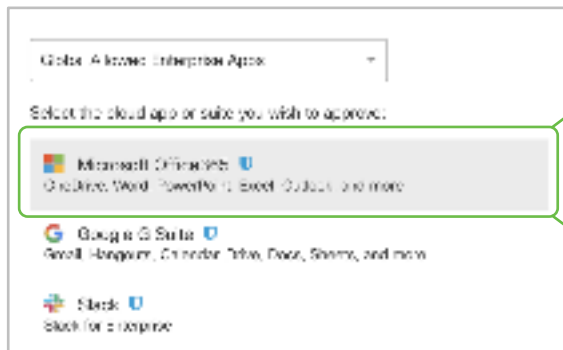
At the bottom of the modal, there are "CANCEL" and "SAVE" buttons.

In the background, the main interface shows a list of applications. The "ALL APPS (3287)" section is visible, with a table of application details. The "Edit app controls" link for the "Under Audit" application is highlighted with a green box.

Total Traffic	Outbound Traffic	Inbound Traffic	Label
51 MB total traffic 4 MB 48 MB	48 MB	4 MB	Under Audit Edit app controls
3 MB total traffic 89 KB 3 MB	3 MB	89 KB	Unreviewed Edit app controls
157 KB total traffic 86 KB 71 KB	71 KB	86 KB	Unreviewed

# Tenant controls

Select the instance(s) of Core SaaS applications that can be accessed by all users or by specific groups/individuals



- ✓ cisco.com (Corp. instance)
- ✗ Deb Smith (Personal instance)
- ✗ Bob Jones (Personal instance)

## Key Use Cases

### Security

Ensure, sensitive data is created and stored in approved instances of cloud apps

### Productivity

Only provide access to corporate instances of core SaaS apps



# Data-at-rest, cloud malware detection (API-based)

Files that contain malware in cloud repositories can do damage

Malware enters/exits via:

- Endpoints that aren't covered by Cisco Secure Endpoint (AMP)
- Unmanaged devices
- External sharing- sharing files with other companies

Solution:

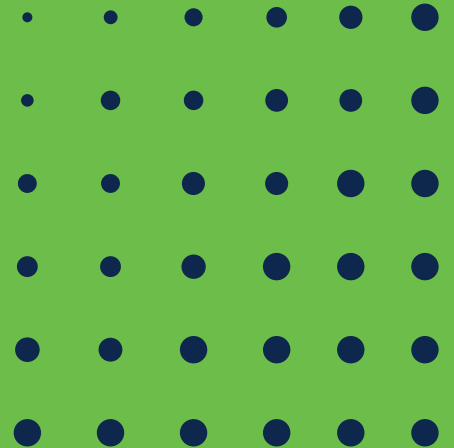
- Scan repositories and ongoing save events for cloud storage



Prevent the malware from spreading to additional endpoints and users

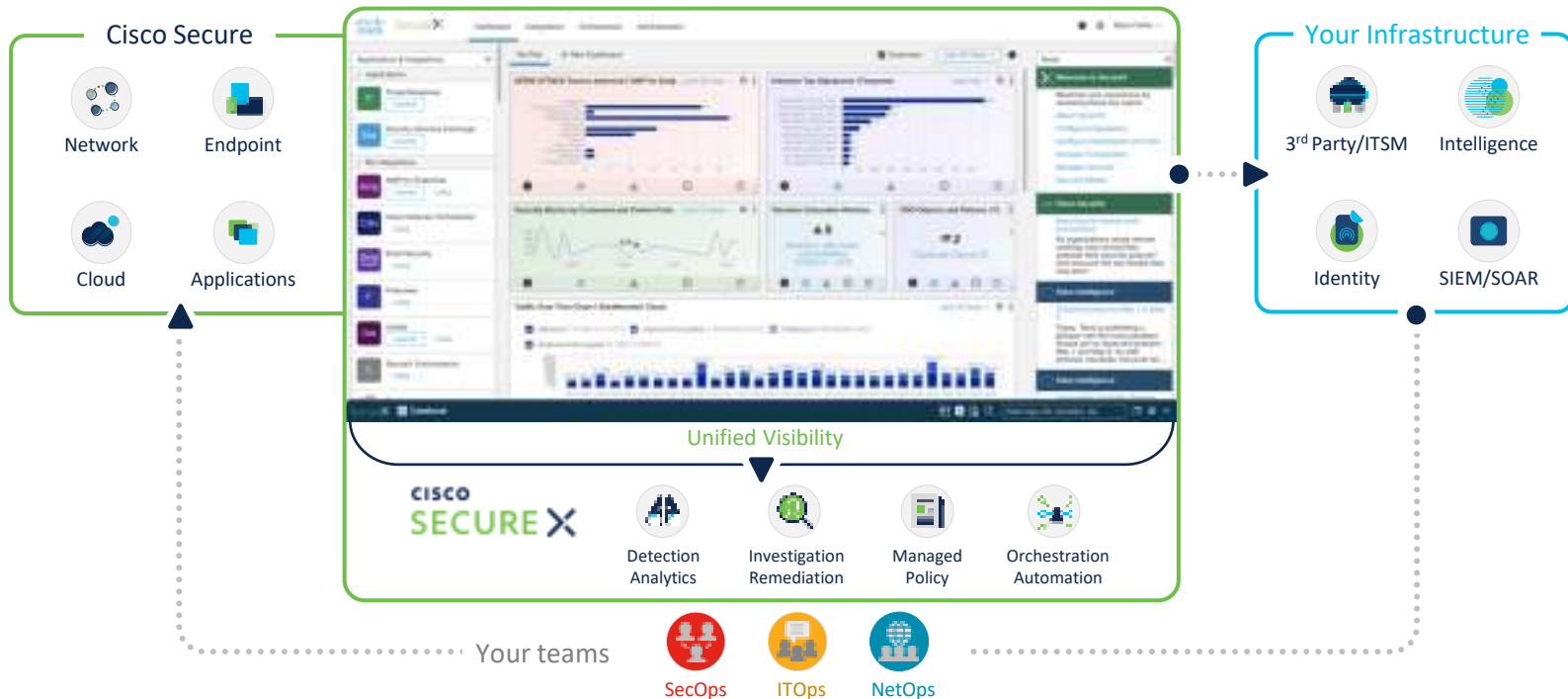


Cisco SecureX

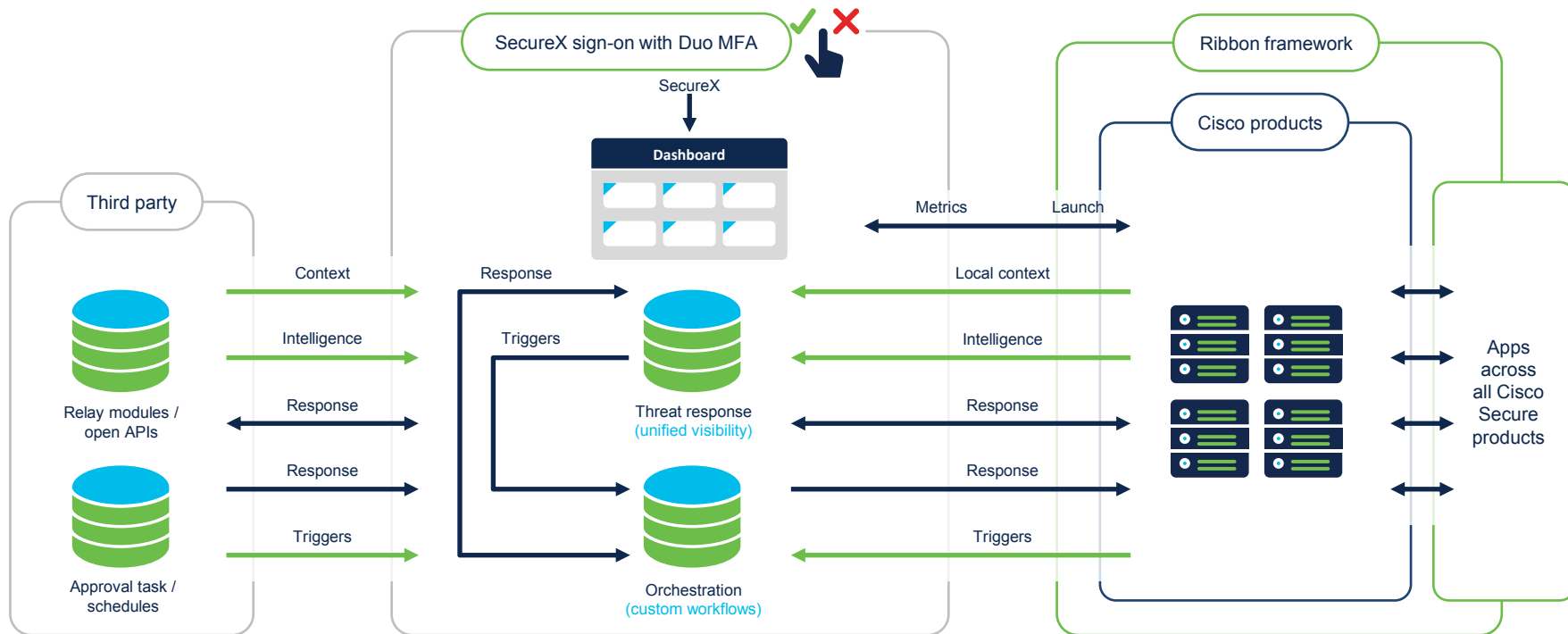


# Introducing SecureX

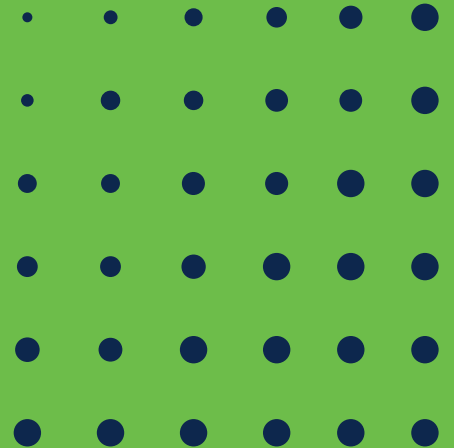
A cloud-native, built-in platform experience within our portfolio



# SecureX architecture



# Appendix



# Umbrella Data Center Availability

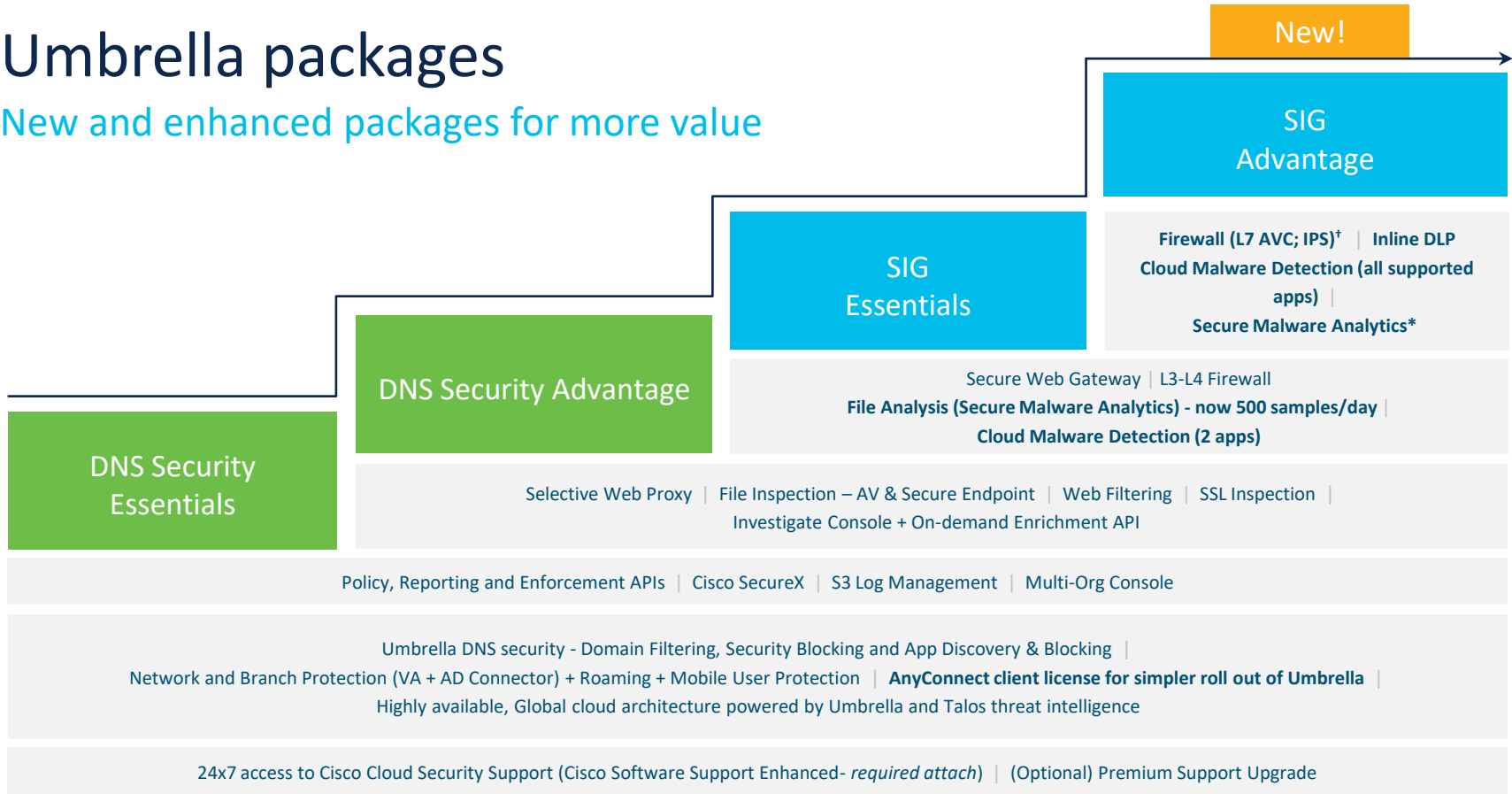
Country	Title	DNS Availability	SWG Availability	Full SIG (SWG + CDFW + IPsec) Availability
Australia	Melbourne	Available	Available	Available
Australia	Sydney	Available	Available	Available
Brazil	Rio De Janeiro	Available	Available	Available
Brazil	Sao Paulo	Available	Available	Available
Canada	Toronto, ON	Available	Available	Available
Canada	Vancouver, BC	Available	Available	Available
China	Hong Kong	Available	Available	TBD
Czech Republic	Prague	Available	Available	Available
Denmark	Copenhagen	Available	Available	Available
France	Paris	Available	Available	Available
Germany	Frankfurt	Available	Available	Available
India	Mumbai (1)	Available	Available	FY21 - Q4
Ireland	Dublin	Available	TBD	TBD
Italy	Milan	Available	Available	Available
Japan	Osaka	Available	Available	FY21 - Q4
Japan	Tokyo	Available	Available	Available
Netherlands	Amsterdam	Available	Available	TBD

# Umbrella Data Center Availability

Country	Title	DNS Availability	SWG Availability	Full SIG (SWG + CDFW + IPsec) Availability
Poland	Warsaw	Available	TBD	TBD
Romania	Bucharest	Available	TBD	TBD
Singapore	Singapore	Available	Available	Available
South Africa	Johannesburg	Available	Available	FY22 - Q1
Spain	Madrid	Available	Available	Available
Sweden	Stockholm	Available	Available	Available
United Arab Emirates	Dubai (1)	Available	Available	FY21 - Q4
United Kingdom	London	Available	Available	Available
United States	Ashburn, VA	Available	Available	Available
United States	Atlanta, GA	Available	Available	Available
United States	Chicago, IL	Available	Available	FY21 - Q4
United States	Dallas, TX	Available	Available	FY21 - Q4
United States	Denver, CO	Available	Available	FY21 - Q4
United States	Los Angeles, CA	Available	Available	Available
United States	Miami, FL	Available	Available	Available
United States	New York, NY	Available	Available	Available
United States	Santa Clara, CA	Available	Available	Available
United States	Seattle, WA	Available	FY22 - Q1	FY22 - Q1

# Umbrella packages

New and enhanced packages for more value



# Summary of Software Support deliverables

## For Umbrella packages

### Software Support For Cisco Umbrella

	Enhanced Required for Cisco Umbrella packages*	Premium Optional upgrade
Software technical support (24x7 access to Cisco Cloud Security Support–phone/online)	•	•
Initial response target (Severity 1 and Severity 2)	30 minutes	15 minutes
Software updates	•	•
Prioritized case handling	Prioritized over Basic option	Prioritized over Enhanced option
Primary point of contact with software expertise	•	•
Onboarding guidance for Smart Accounts, configuration, migration, and IT software integration	•	•
Learning and training**	•	•
Guidance for software usage	•	•
Support case analytics		•
Designated service management: assigned expert who provides incident, case, and change management plus proactive consultation and recommendations		•

Note, required attach for Cisco Umbrella packages DNS Essentials, DNS Advantage, and SIG Essentials

\*\*Feature is dependent upon support contract amount





# Děkuji za pozornost

<https://umbrella.cisco.com/info/cisco-umbrella-studio>

- March 22, 9:00am – 2:00pm CET
- April 5, 9:00am – 2:00pm CET
- April 19, 9:00am – 2:00pm CET

