

Cisco Secure Service Edge

Bezpečnost přichází z cloudu

Milan Habrcetl

Cisco Cyber Security Specialist, mhabrcet@cisco.com

28.3.2023



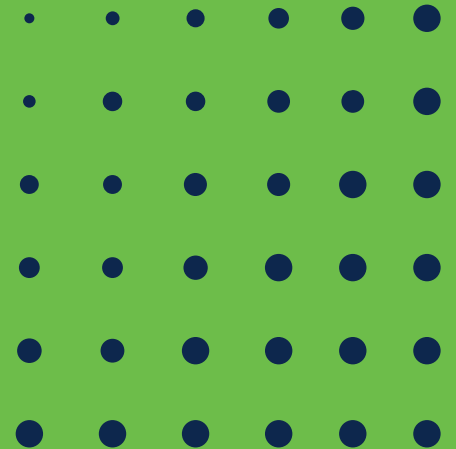


Agenda



- ▶ 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



Gartner: Secure Access Service Edge (SASE)

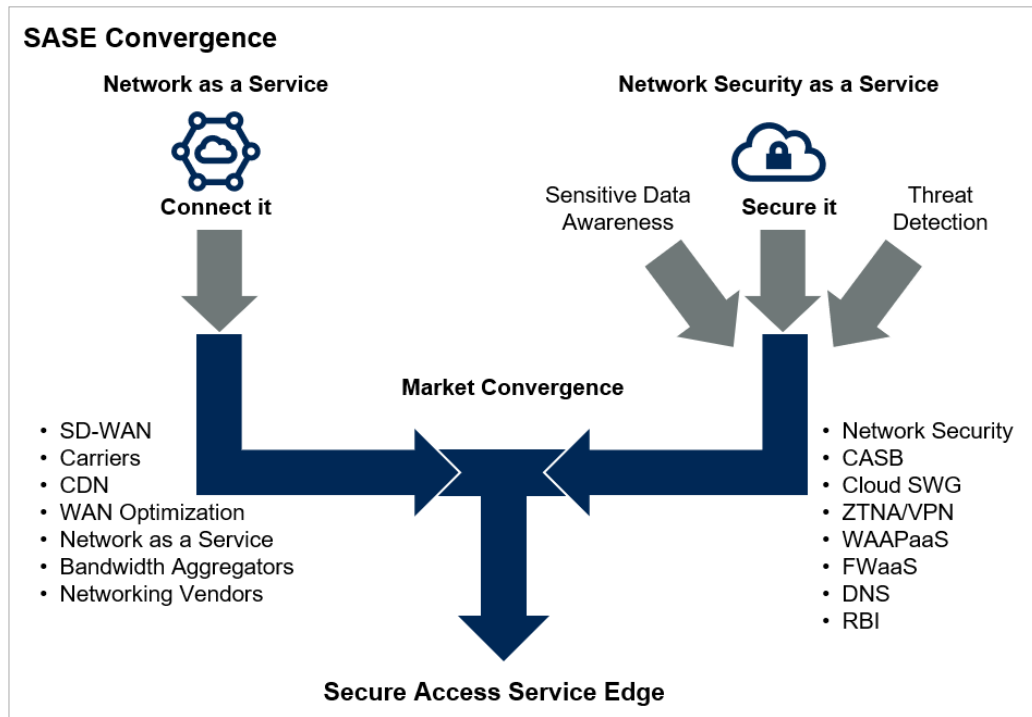
Convergence of networking and security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

Benefit rating:
Transformational

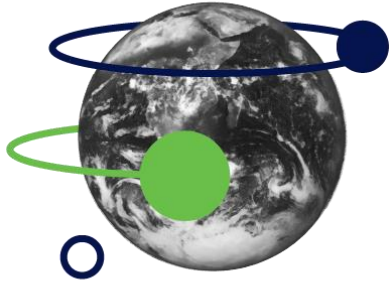
Market penetration:
Less than 1% of target audience

Maturity:
Emerging

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



At Cisco, we're uniquely positioned to help



Networking

Largest SD-WAN solution provider



Security

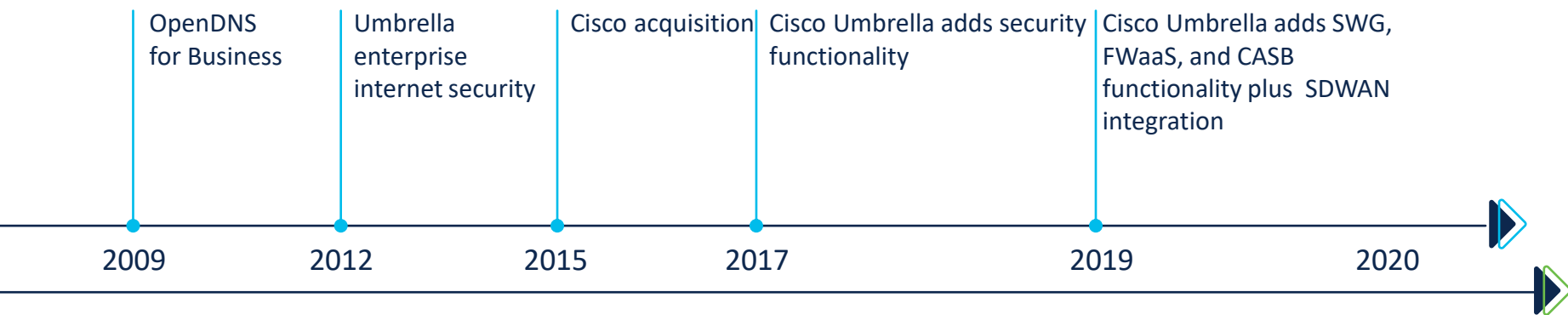
Defending 100% of the Fortune 100



Zero Trust

Leader in Zero Trust two years running

Cisco Umbrella evolution



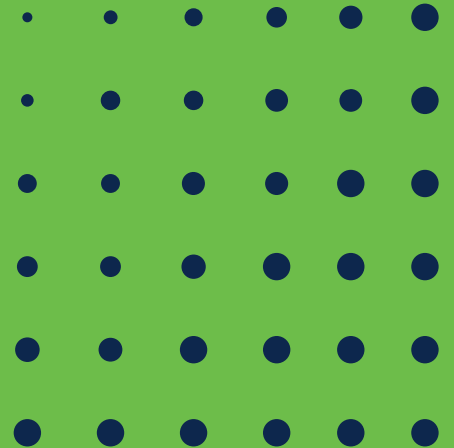
SIG



SASE

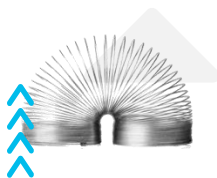


Global cloud architecture



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



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

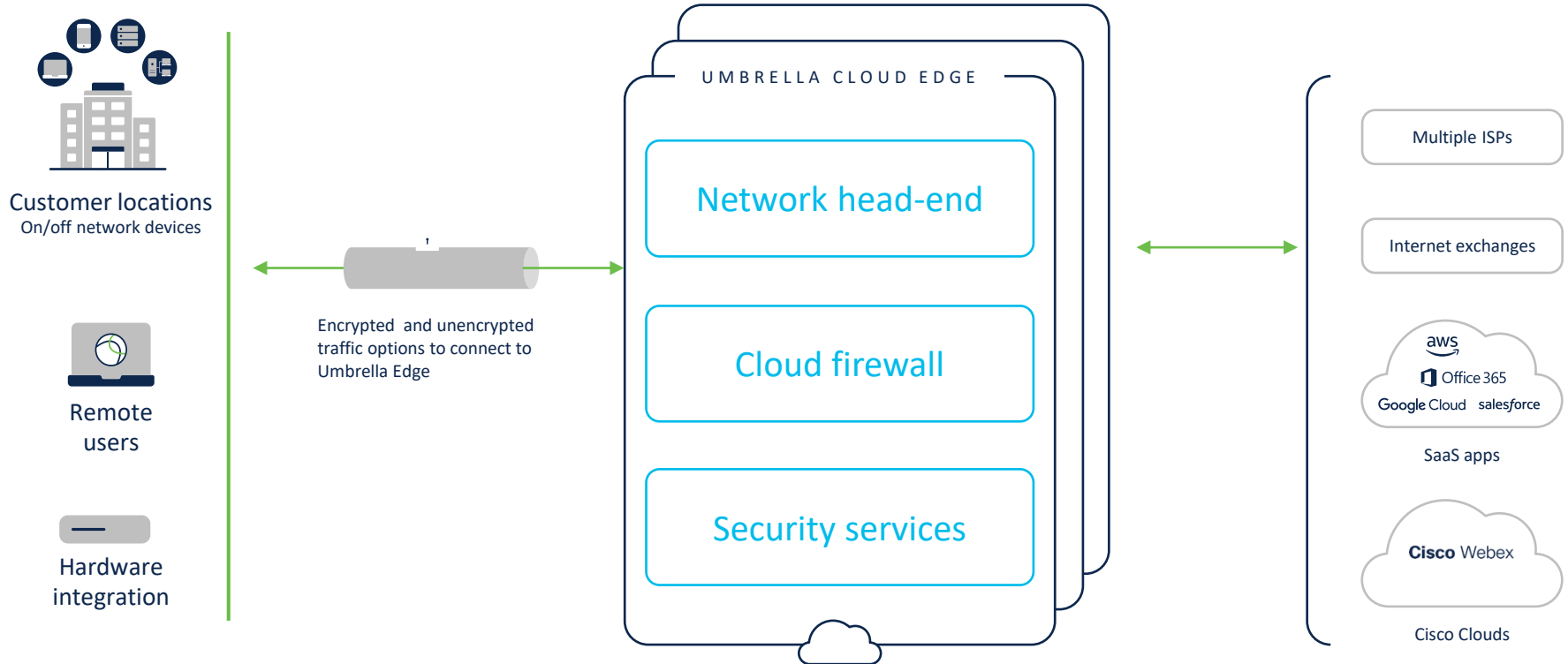
- Connection to seven popular SaaS applications (table below is BOX)
- Compared direct-to-internet vs. through Umbrella with secure web gateway (with decryption) and cloud firewall policies set

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

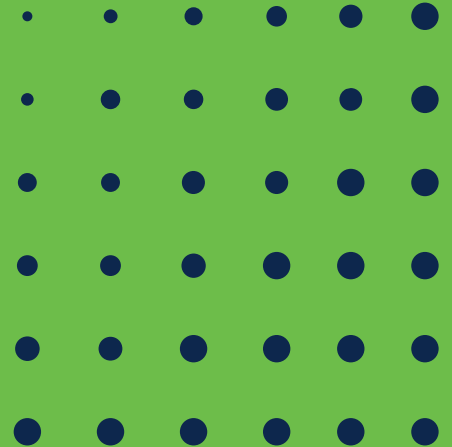
Global cloud architecture: top-line



Cisco Umbrella earns SOC 2 Type II Compliance



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.



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>

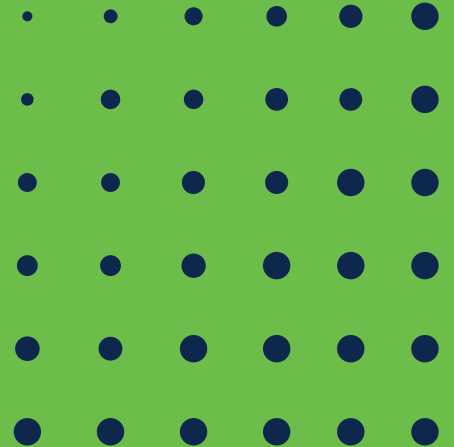
Efficacy testing: SWG

- 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

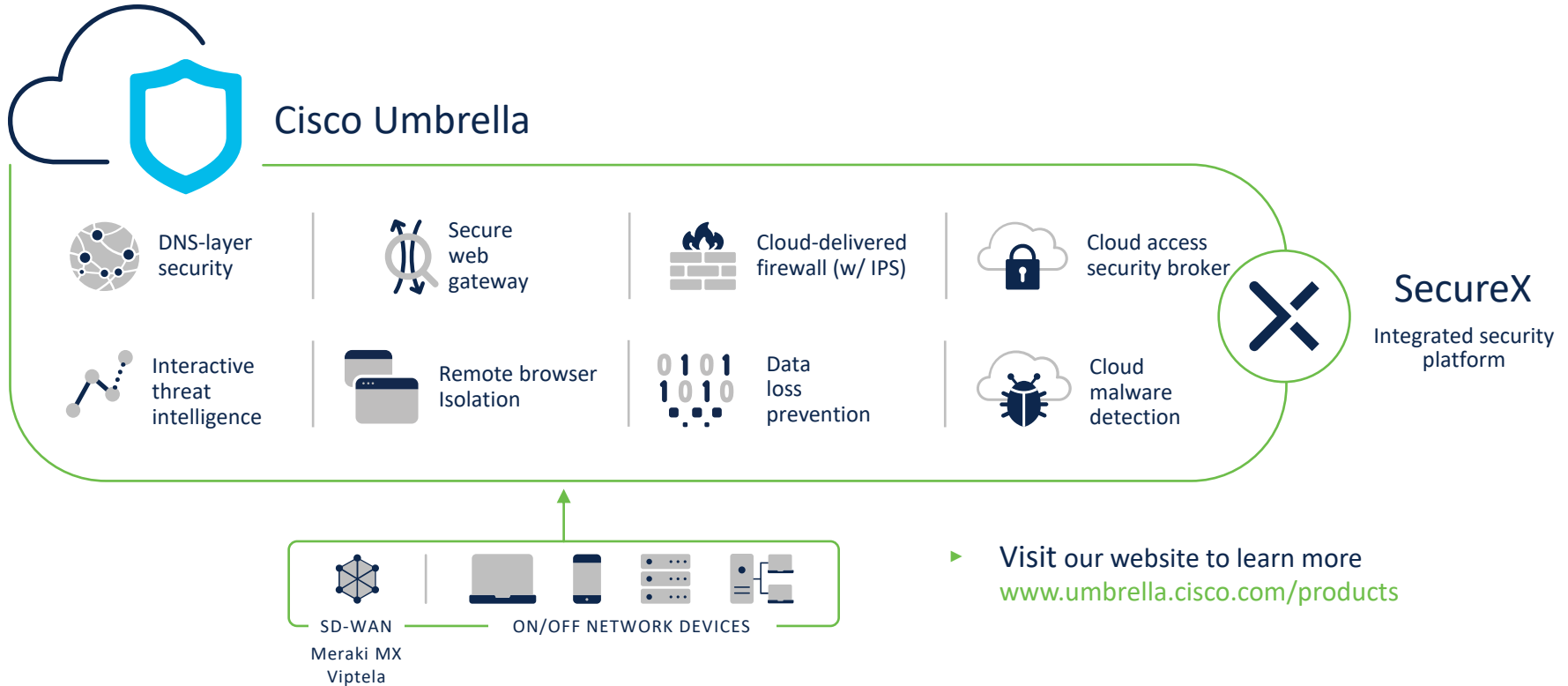
Type of test	Umbrella	Zscaler	Palo Alto	Netskope	Akamai
Malicious PE files (Portable executables)	93.65	87.29	83.88	82.12	61.41
Malicious destinations	99.15	93.28	57.68	55.52	48.35
Phishing links	93.79	85.20	91.51	48.35	74.12
Total detection rate	96.39	89.67	73.15	61.90	58.43

% Detected (higher is better)

Product overview



Cisco Umbrella



► Visit our website to learn more
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

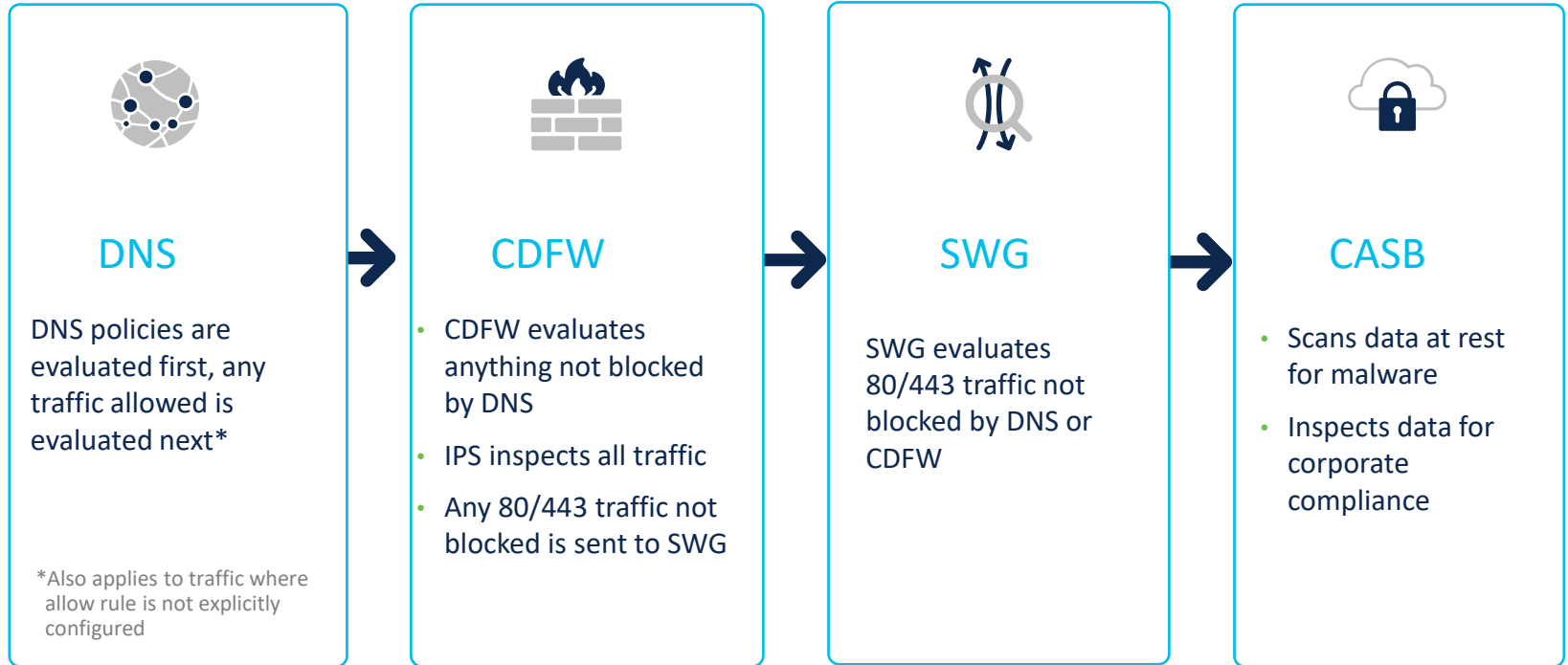


Control

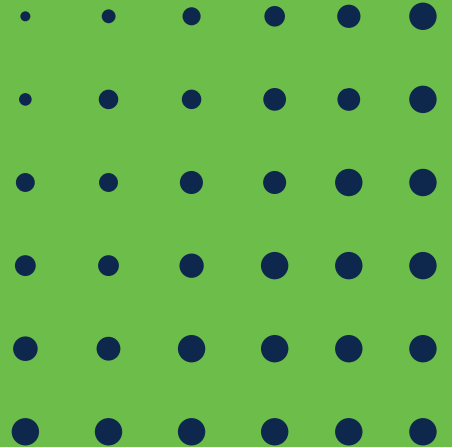
- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls

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

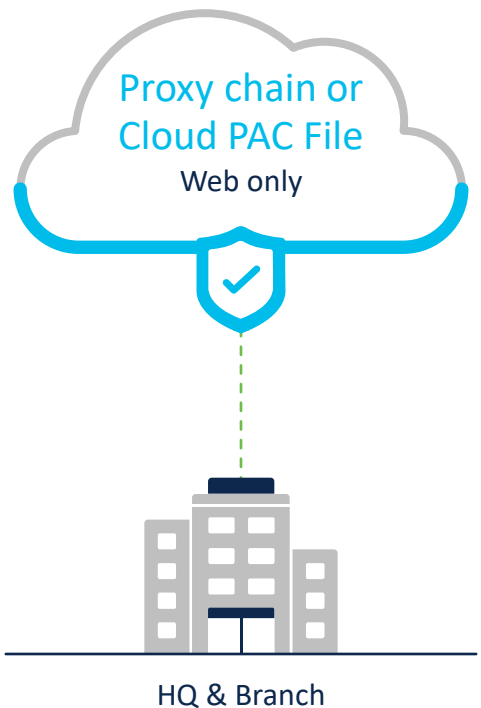
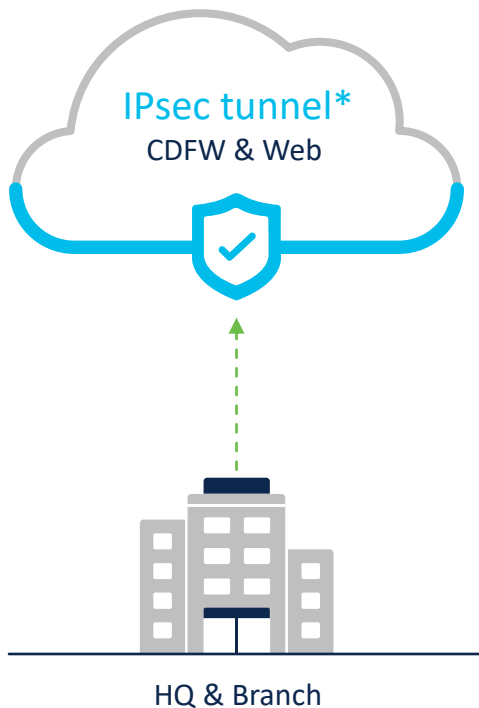
SIG policy outcome summary



Connections, integrations and logging

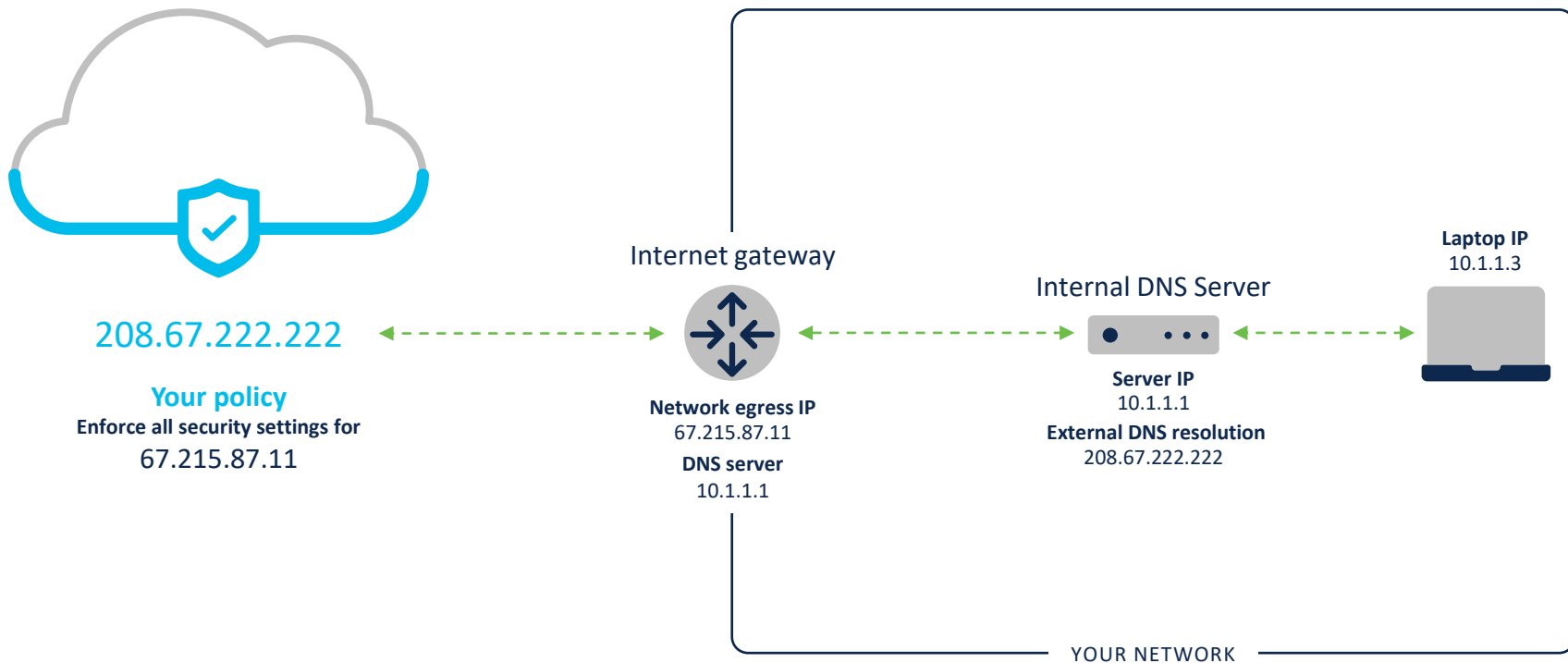


Flexible connection methods



*Optional customer hosted PAC file

Protect on-network devices via DNS server



Tunnel capabilities

IPsec capacity

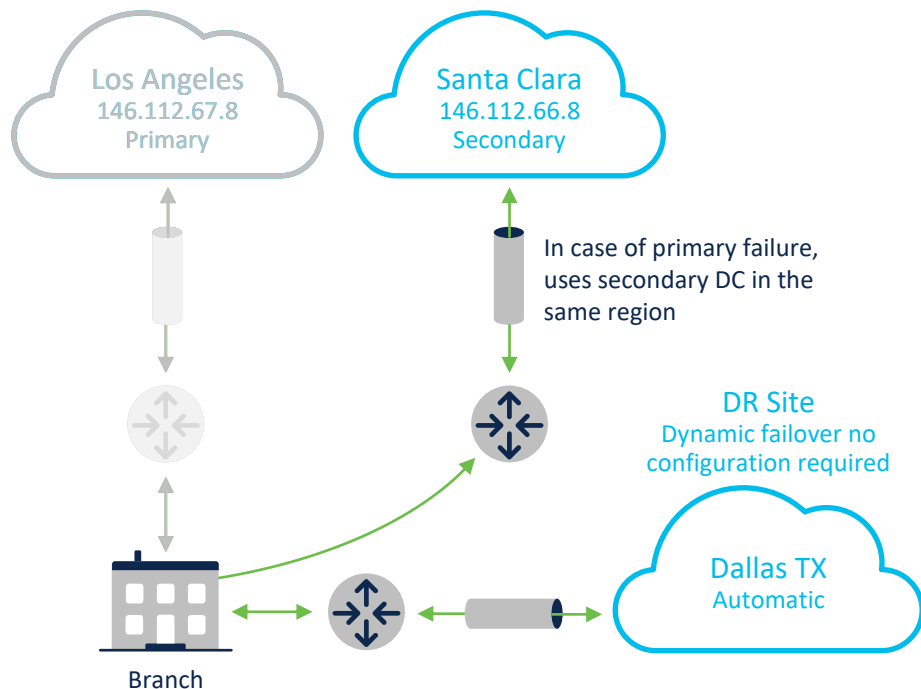
- 500 Mbps by default, with ongoing development to increase capacity
- Multiple tunnels can be deployed to support higher capacity

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

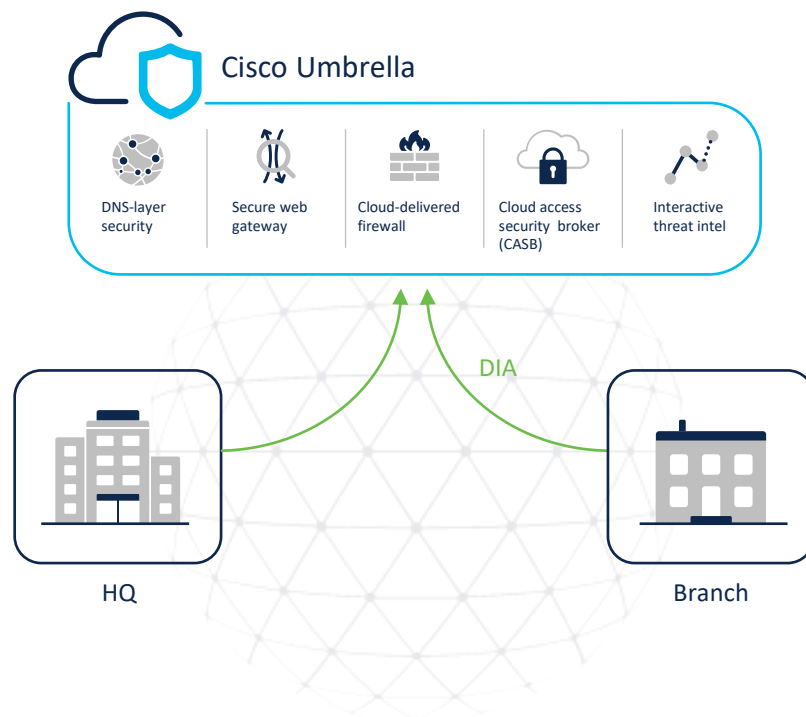
Data center region code US-1



Umbrella for Cisco SD-WAN

Fast forward time to value with automated security

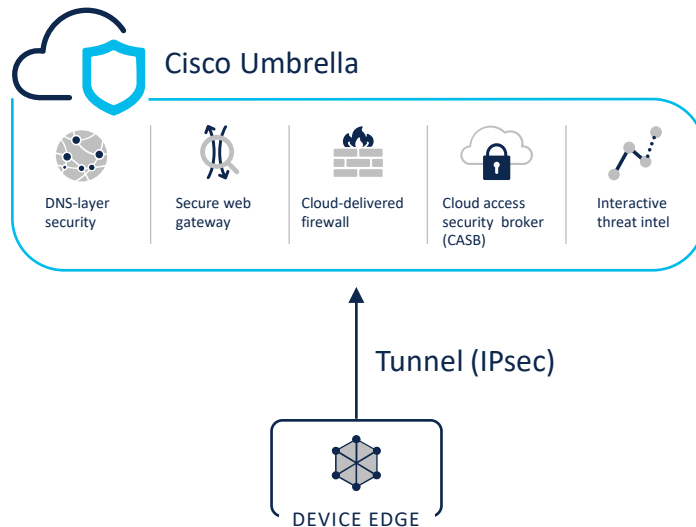
- **Hands-off automation:** deploy IPsec tunnels across thousands of branches in minutes
- **Top notch protection:** defend against threats with the leader in security efficacy
- **Simplified management:** single pane of glass across all offices, users and roaming clients
- **Deeper inspection & controls:**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



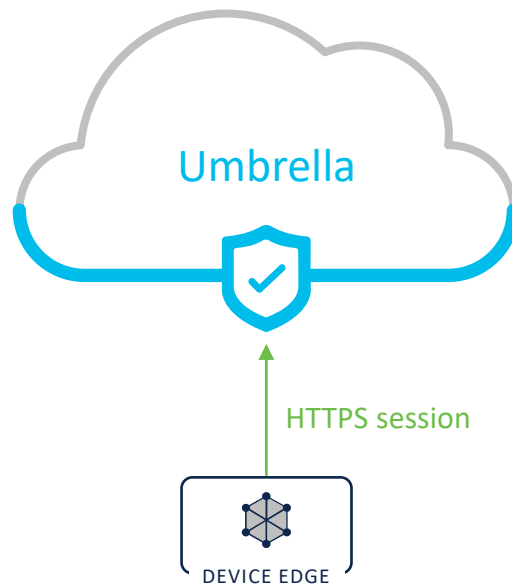
With this feature, SD-WAN will have much deeper integration with Umbrella

Rapid onboarding: accelerates security and ROI

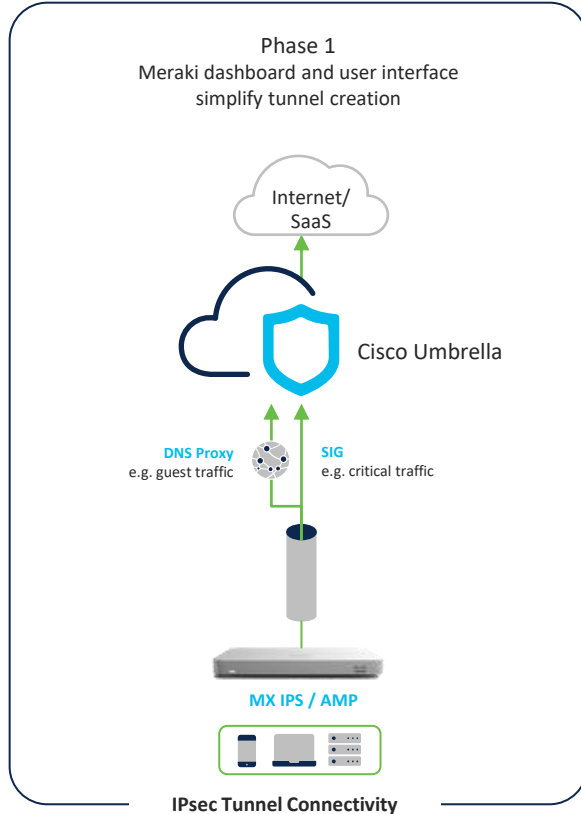
Umbrella for Cisco SD-WAN

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



Meraki MX and Umbrella Integration Options

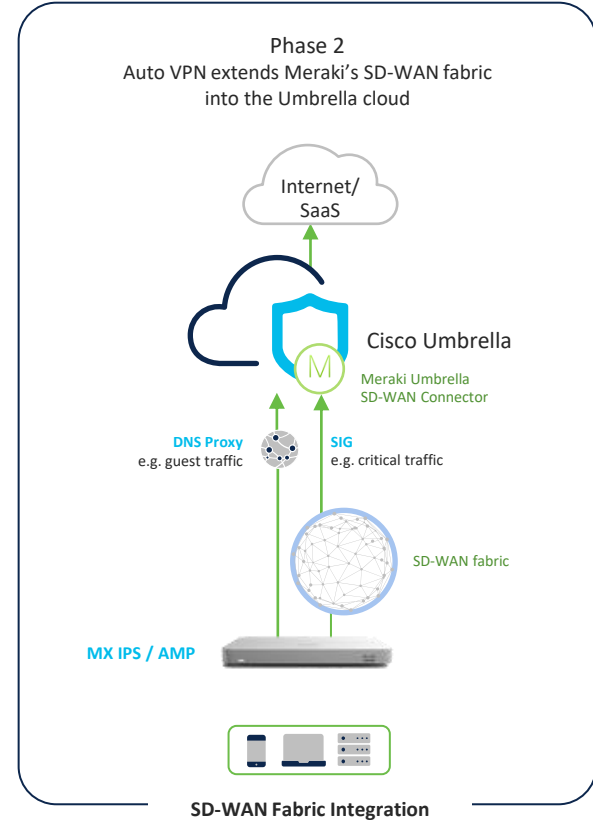


Choose per site

Flexible security
options

Automated SD-
WAN fabric
integration

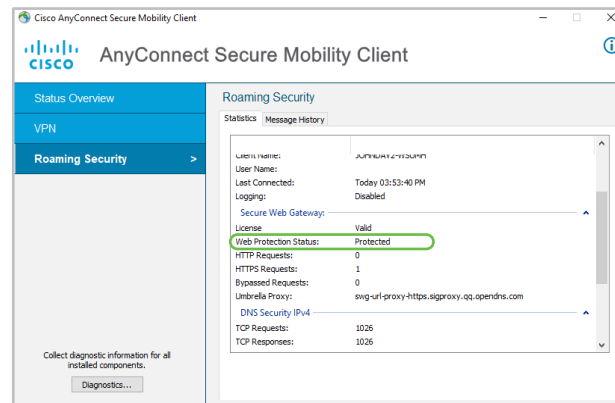
Competitive
Differentiator



Cisco Secure Client

Entitlement for Umbrella Mobility Client is included Umbrella subscription (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

DNS security



Proven leader in cloud-native security



620B

requests per day



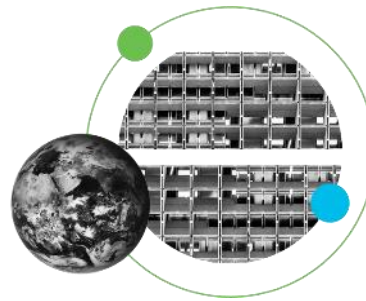
500M

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 servers 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.

Command and Control Callbacks
Prevent compromised devices from communicating with attackers' infrastructure.

Phishing Attacks
Fraudulent websites that aim to trick users into handing over personal or financial information.

Dynamic DNS
Block sites that are 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 cryptominer access to mining pools and web miners.

› INTEGRATIONS

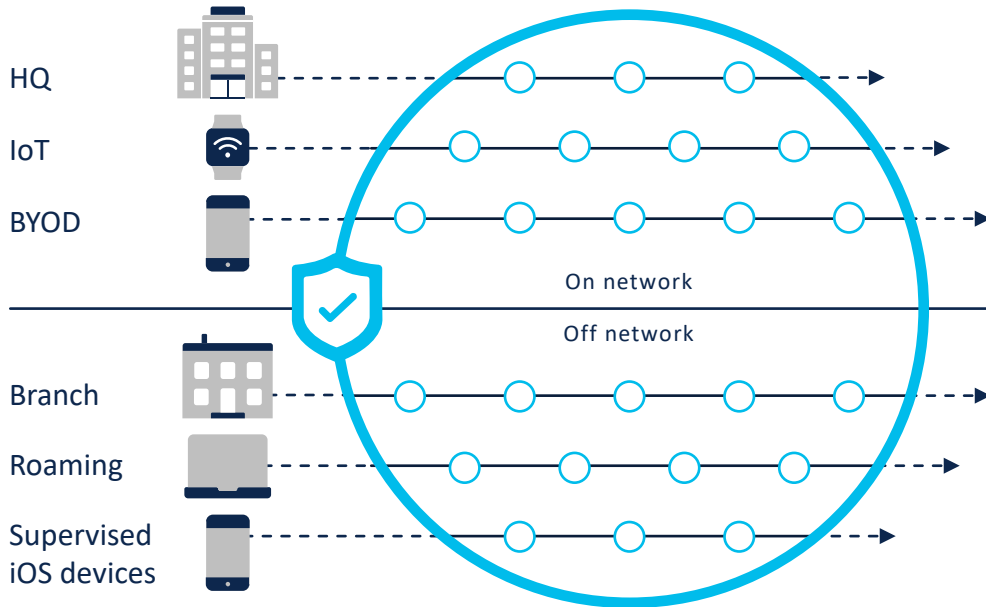
CANCEL SAVE

- **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

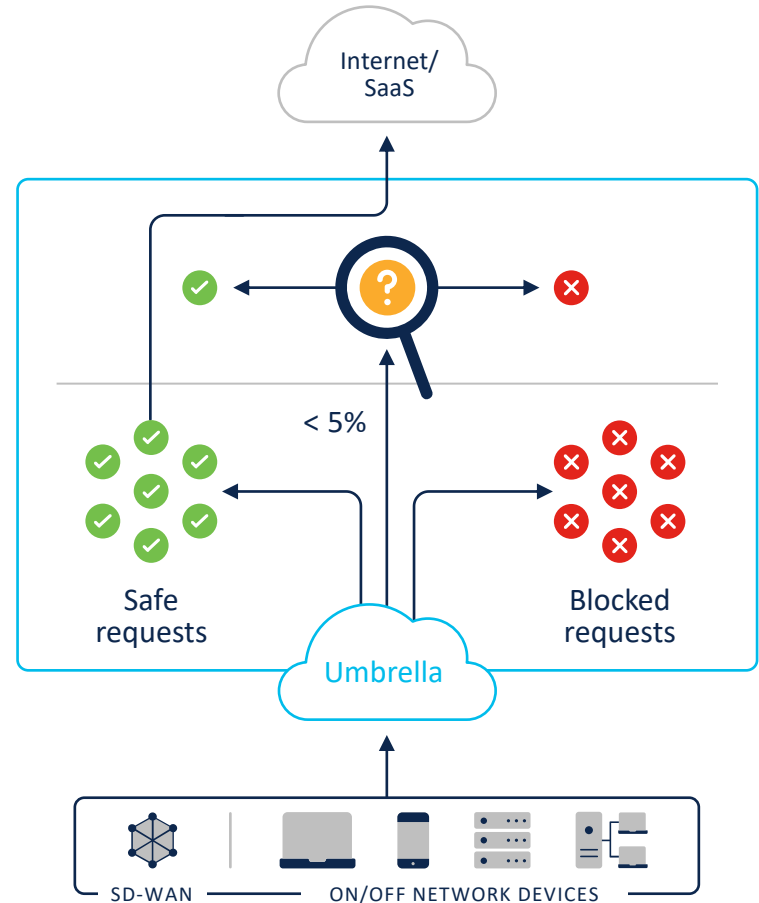


- All office locations
- Any device on your network
- Roaming laptops
- Mobile devices - IOS and Android
- Every port and protocol

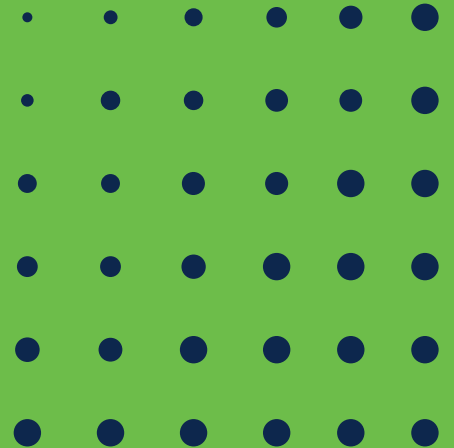
DNS-layer security

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



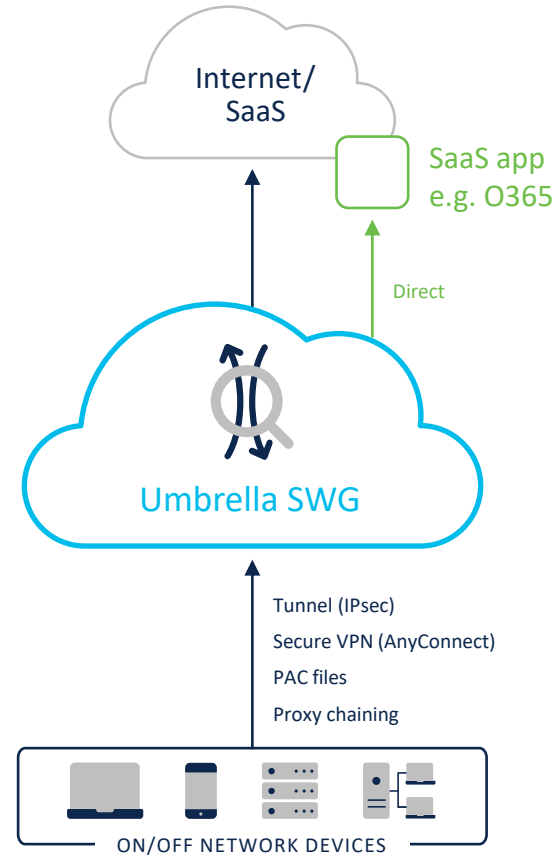
Secure web gateway



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

I'm a New Ruleset

Contains 3 Identities Applied To Last Modified Mar 24, 2021

Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
1	Questionable	Warn	All Network Tunnels	1 Category ...	Any Day, Any Time
2	Off-net Access	Allow	All Roaming Computers	5 Categories 3 Destination Lists ...	Any Day, Any Time
3	Standard Blocks	Block	All Network Tunnels All Roaming Computers	24 Categories 4 Destination Lists ... 1211 Applications ...	Any Day, Any Time

Ruleset Settings

Ruleset settings affect the rules within the ruleset and are not applied globally throughout your Web policy. Various settings listed must be configured through their respective components before being set here.

Ruleset Name	I'm a New Ruleset	Edit
Ruleset Identities	3 Identities	Edit
Block Page	Umbrella Block Page Applied	Edit
Tenant Controls	Global Allowed Enterprise Apps	Edit
File Analysis	1 Setting Enabled	Edit
File Type Control	3 File Types Blocked	Edit
HTTPS Inspection	Enabled	Edit
PAC File	https://brony.prod.pac.svg.umbrella.com/...	Edit
Ruleset Logging	Log All Requests	Edit
SAML	Enabled	Edit
Security Settings	3 Settings Enabled	Edit

DELETE CLOSE

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

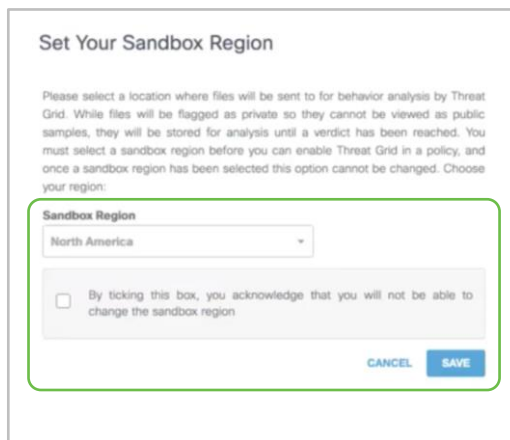
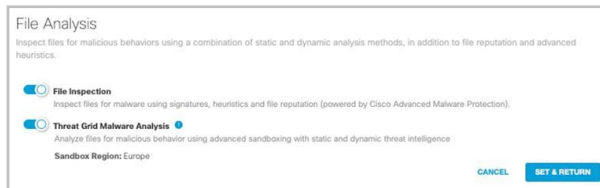
Base Content

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 checked="" type="checkbox"/> Adult Themes	<input type="checkbox"/> Non-Profits
<input checked="" type="checkbox"/> Sexuality	<input type="checkbox"/> Nudity
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Online Communities
<input type="checkbox"/> Arts	<input type="checkbox"/> Online Meetings
<input type="checkbox"/> Astrology	<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



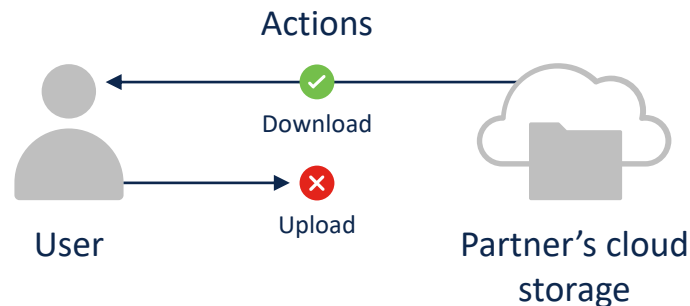
Regions:
Europe
or North
America

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	19 >
<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

HTTPS Inspection

Configure how Umbrella should handle HTTPS traffic. [See HTTPS Inspection](#)

Enable HTTPS Inspection

HTTPS traffic is intercepted and decrypted to provide security and policy enforcement at the URL layer, and visibility into the URL path. By default, HTTPS inspection attempts to decrypt all HTTPS traffic. For any HTTPS traffic that should not be decrypted, create a bypass inspection group.

Add domains and select categories you want to exempt from HTTPS inspection:

Privacy categories ▾

4 Categories Selected ADD	0 Domains ADD
Financial Institutions	
Health and Fitness	
Social Networking	
Webmail	
	No Domains

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

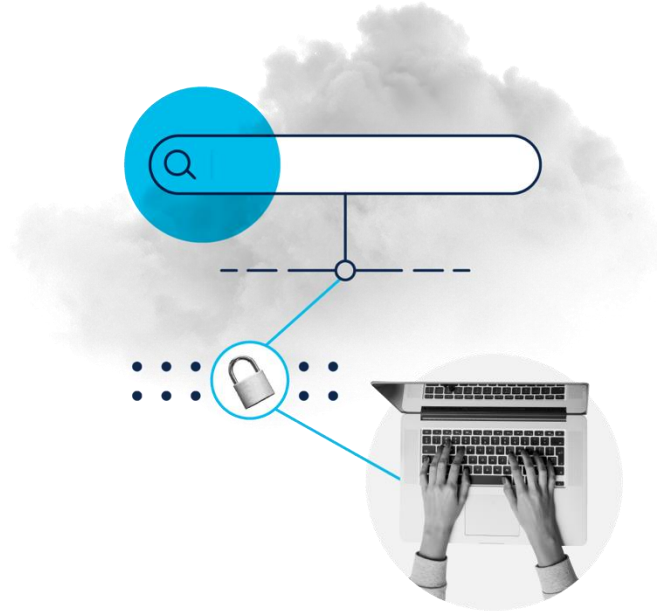
- CSV upload
 - Recommend CSVDE tool on Windows Domain Controller
- AD connector Active Directory sync
 - Group filtering supported with data file
 - Standard AD connector install version 1.3.8+
 - Only one Domain Controller required, no VA required



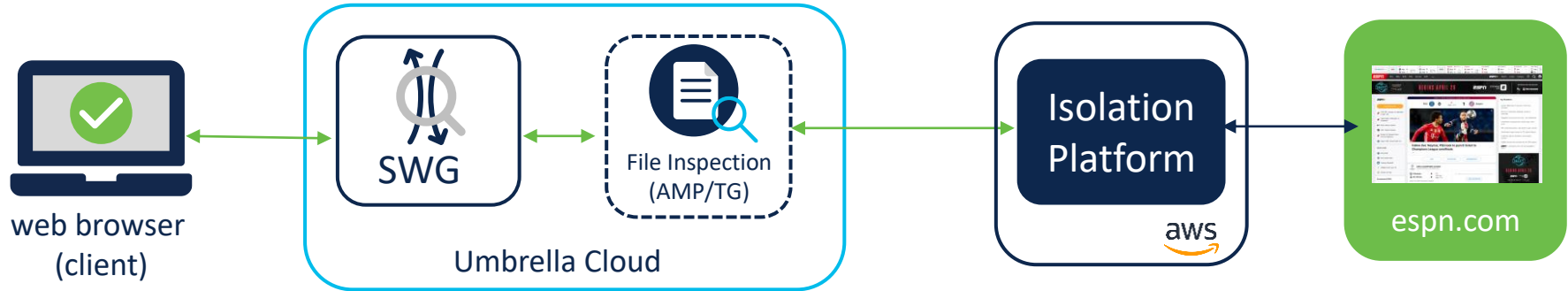
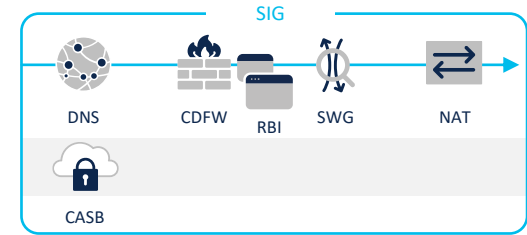
New Umbrella remote browser isolation (RBI)

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



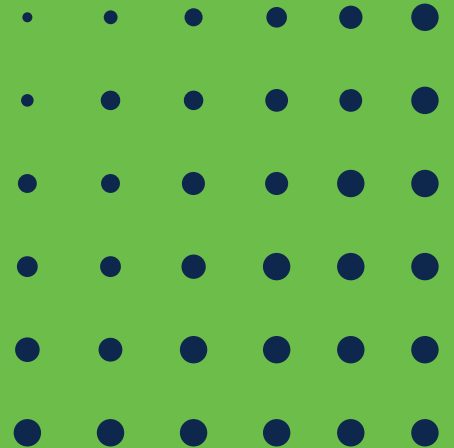
RBI traffic flow overview



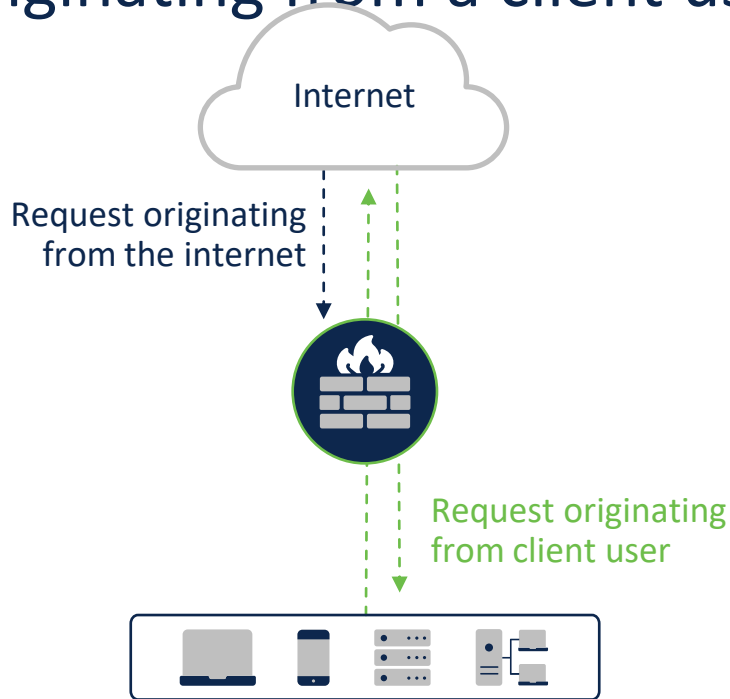
Three RBI package options

- **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](#).

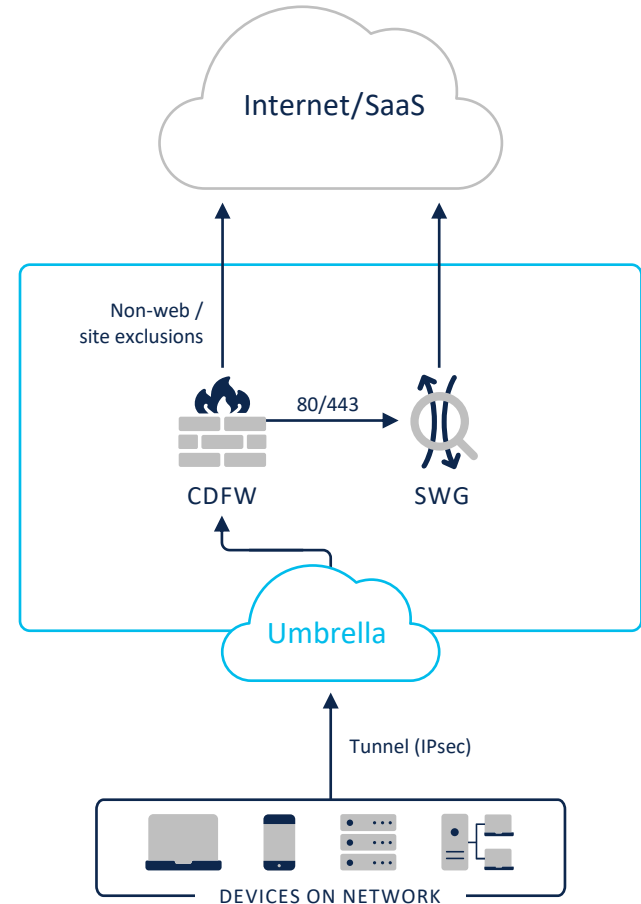
FILTERS

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	● Enabled	● Block	ssh	Any	Any IPs Any Ports	Any IPs 1 Port	▲ 0/24hrs	▲ No Hits	...
<input type="checkbox"/>	2	p2p rule	● Enabled	● Block	Any P2P ftp	Any	Any IPs Any Ports	Any IPs Any Ports	25.0 /24hrs	Aug 24, 2020 - 09:33am	...
<input type="checkbox"/>	3	Default Rule	● Enabled	✓ Allow	Any Application	Any	Any IPs Any Ports	Any IPs Any Ports	69.1 k/24hrs	Aug 24, 2020 - 03:15pm	...

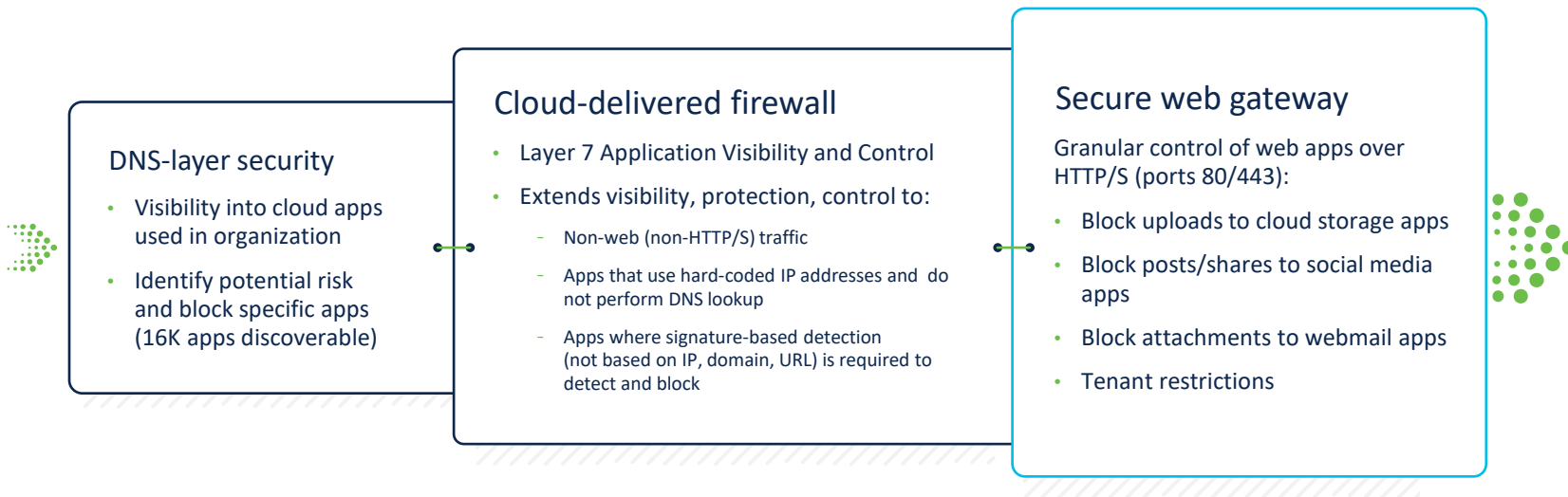
Layer 7 application visibility and control

- 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



Umbrella Intrusion Prevention System (IPS)

Capabilities

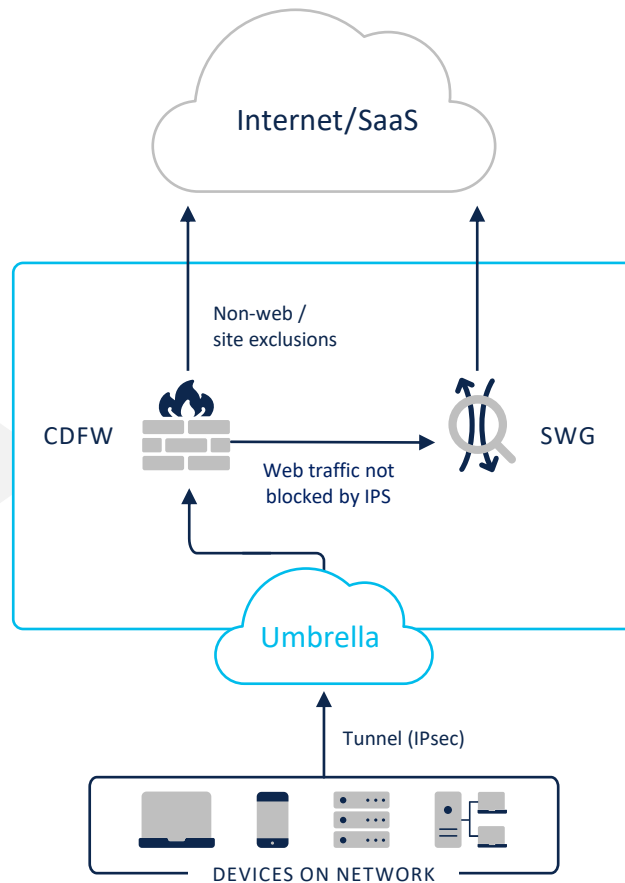
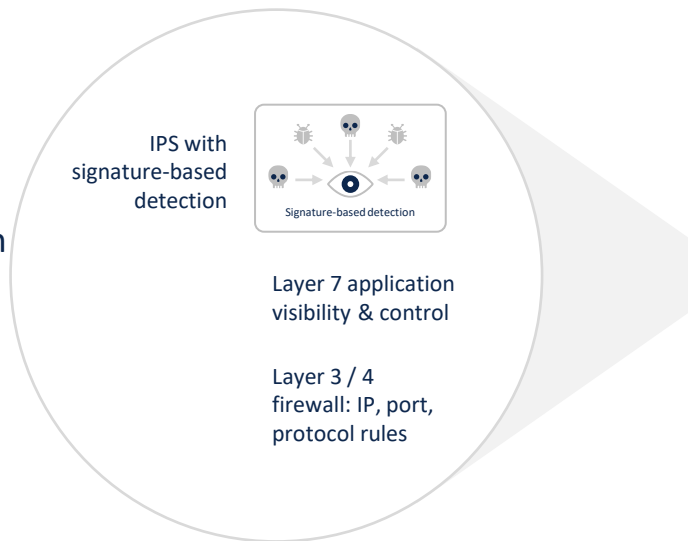
- Deepen Umbrella cloud firewall protection for client-driven traffic
- Use signature-based detection (Snort 3) to examine network traffic flows & prevent vulnerability exploits
- Add layer of detection/blocking for malware, botnets, phishing, and more
- Leverage Cisco Talos' 40K+ signatures (and growing)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

Results

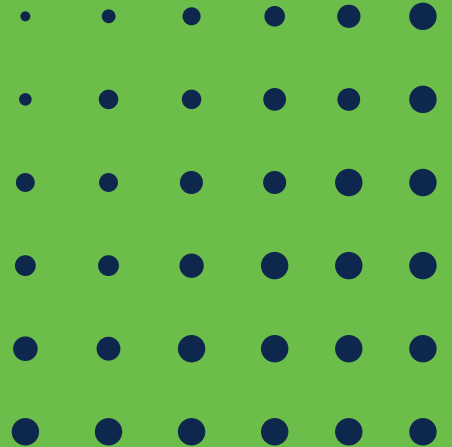
- ✓ Simplify management via Umbrella's single, unified dashboard
- ✓ Remove capacity concerns of appliances by using scalable cloud compute resources
- ✓ Stop more threats with the industry's most effective threat intelligence
- ✓ Detect/block exploitations of vulnerabilities

Umbrella Intrusion Prevention System (IPS)

Layers of security for high security efficacy



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

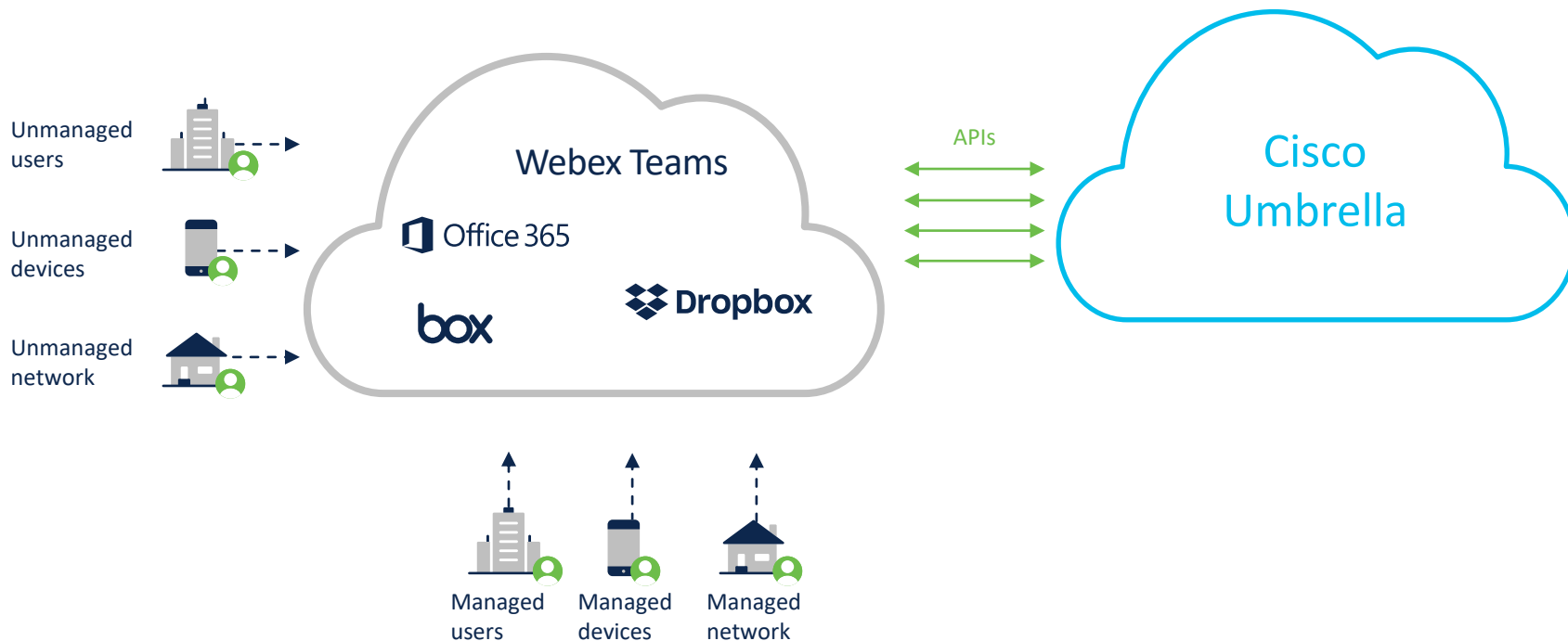
Umbrella

- 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

Reporting / Additional Reports
App Discovery

Dashboard

Search for App / Vendor | Category | Risk | App Type | Label | Date

Category: Games (x) | Anonymizer (x) | Clear all filters

UNREVIEWED (81) | UNDER AUDIT (2) | NOT APPROVED (8) | APPROVED (1) | ALL APPS (84)

Application	Vendor	Weighted Risk	Identities	DNS Requests	Blocked	Label
ProxySite Anonymizer	ProxySite	Very High	6	323	97%	Unreviewed Block this app
Private Tunnel Anonymizer	OpenVPN	Very High	7	344	93%	Unreviewed Block this app
Hide My Ass Anonymizer	Hide My Ass	High	6	361	99%	Unreviewed Block this app
ExpressVPN Anonymizer	ExpressVPN	High	7	348	99%	Unreviewed Block this app
ZenMate Anonymizer	ZenMate	High	6	338	99%	Unreviewed Block this app
NordVPN Anonymizer	NordVPN	High	3	323	99%	Unreviewed Block this app
Anonymous Anonymizer	Anonymous	High	2	2	100%	Unreviewed Block this app
SoftEther VPN Anonymizer	SoftEther Project	Medium	1	4	-	Unreviewed Block this app
Ceas Games	Ceas Games	Medium	6	395	-	Unreviewed
TunnelBear	TunnelBear	Medium	3	316	88%	Unreviewed

Granular app controls

Search for App / Vendor Filter by Identity

UNREVIEWED (3197) UNDER AUDIT (12)

All Apps (3,287 Found)

- Dropbox Cloud Storage
- Netflix Media
- Amplitude Business Intelligence

Control Dropbox

Select which settings should block or allow this application

Application Settings (3 selected of 3 total)

- 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

Label application as Not Approved

For more configuration options, go to [Application Settings](#) in the policy section.

ALL APPS (3287)







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 88 KB 3 MB	3 MB	88 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

Global Allowed Enterprise Apps

Select the cloud app or suite you wish to approve:

-  Microsoft Office365 
OneDrive, Word, PowerPoint, Excel, Outlook, and more
-  Google G Suite 
Gmail, Hangouts, Calendar, Drive, Docs, Sheets, and more
-  Slack 
Slack for Enterprise

- ✓ 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

Inline DLP

Cloud-native proxy DLP

Leverages SWG for connectivity, routing and SSL decryption

Robust DLP classification

- 80+ built-in data classifiers
- Custom keywords

Flexible DLP policy

- Apply to specific identities and destinations with defined data classifications

Robust Reporting

- Includes identity, file name, destination, classification, pattern match, excerpt, triggered rule and more
- Native Umbrella Ux

887 Total

Detected	Identity	Name	Destination	Classification	Action
Aug 13, 2020 at 3:31 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:22 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:22 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	test.pdf	files.slack.com	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	test.pdf	files.slack.com	1 Match Confidential Classification	Block

Currently LA. GA target July 2021

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

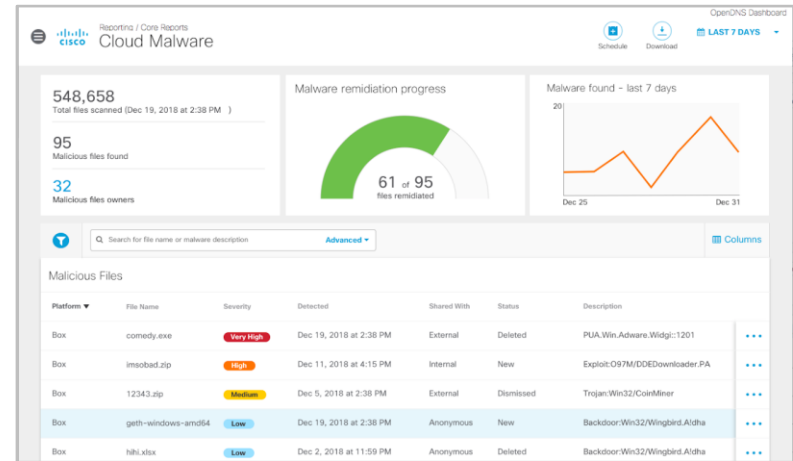
Files that contain malware in cloud repositories can do damage

Malware enters/exits via:

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

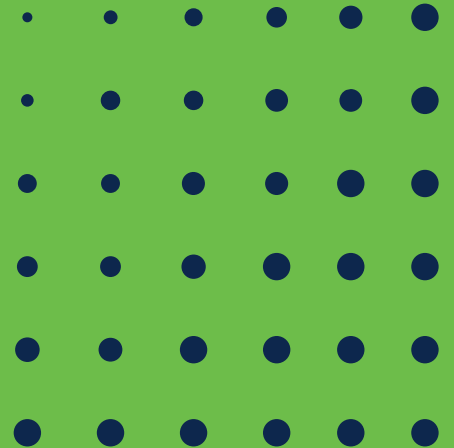
Solution:

- Scan repositories and ongoing save events for cloud storage



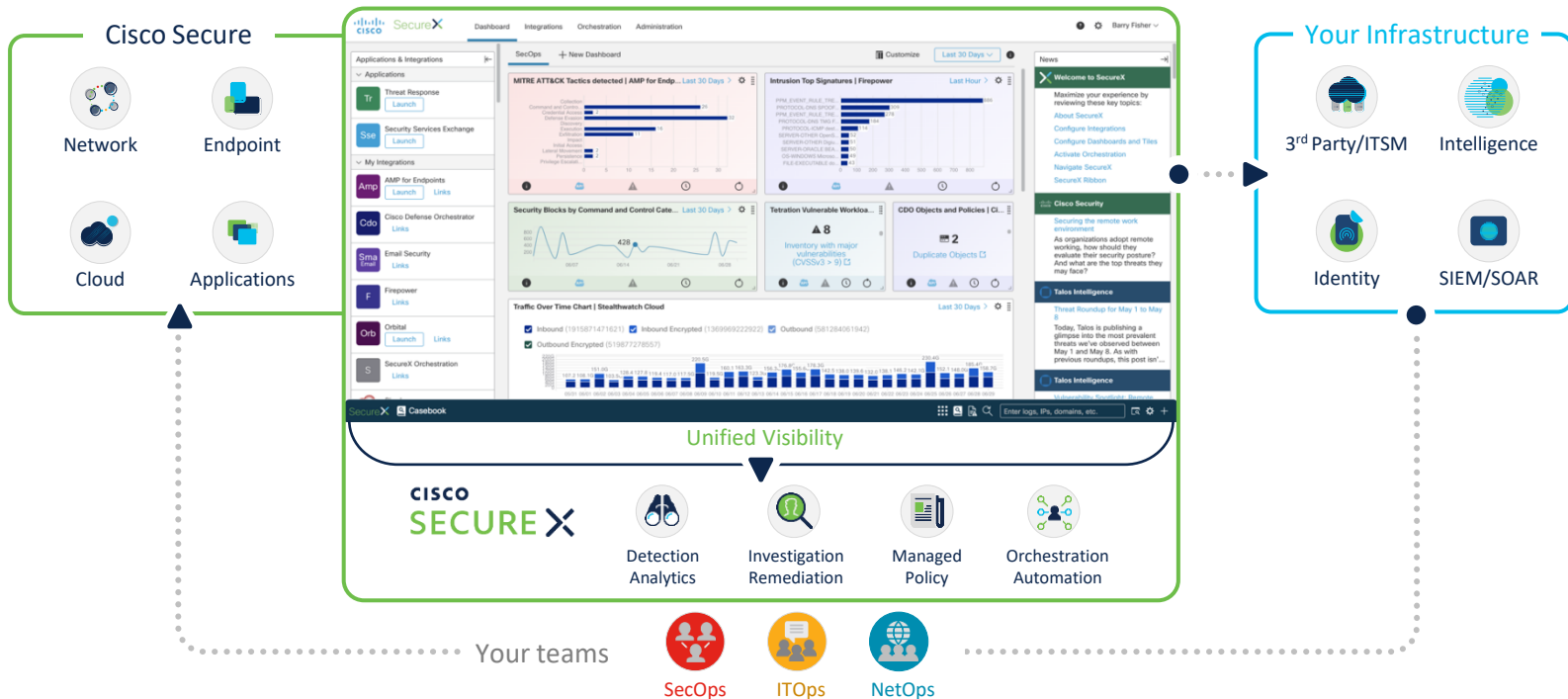
Prevent the malware from spreading to additional endpoints and users

Cisco SecureX

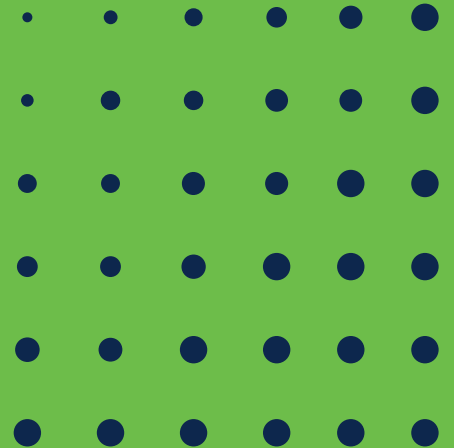


Introducing SecureX

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



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



Děkuji za pozornost

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

