



Cisco SASE Lösung mit Meraki SD-WAN Integration

Virtual Espresso Webinar

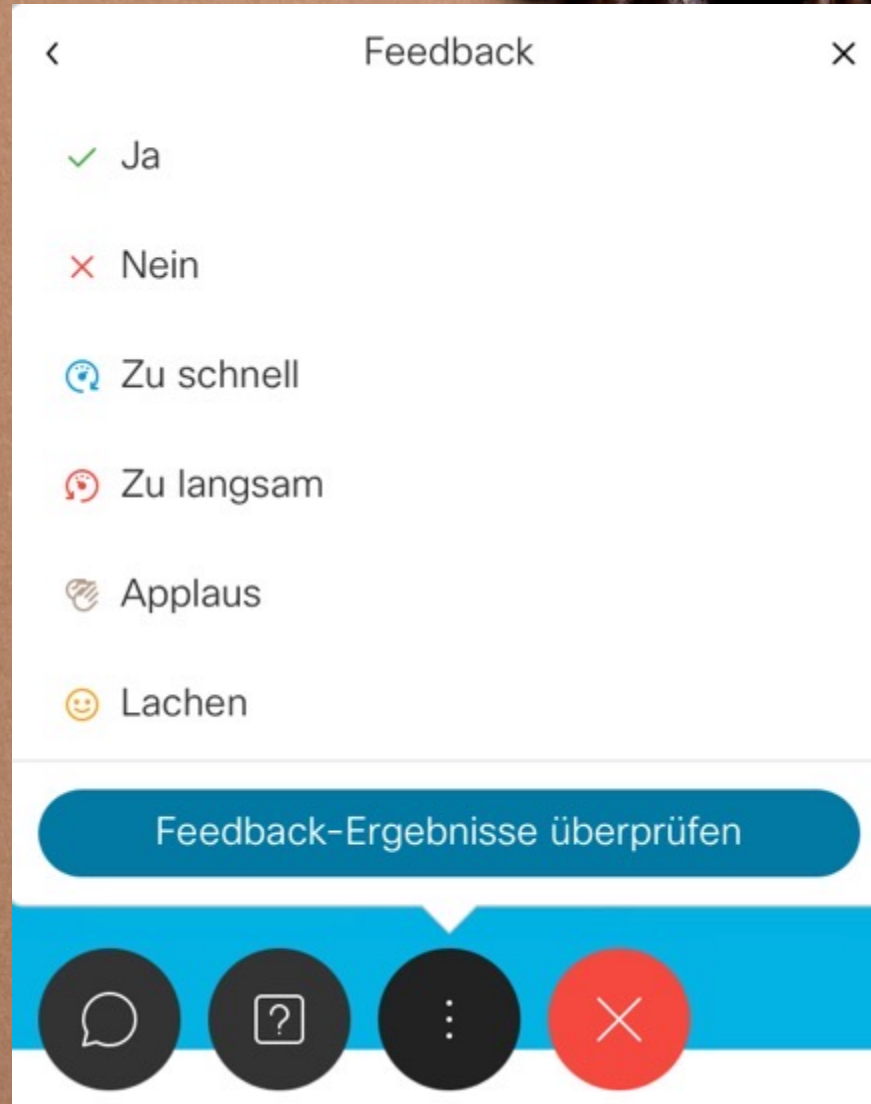
Mittwoch, 8. Dezember 2021, 15:00 Uhr



👉 please utilise the Q&A function to get your question answered

The image shows a Zoom interface with a Q&A menu and a Q&A panel. The menu on the left includes options like 'Q&A', 'Lock event', 'Invite and remind', 'Copy event link', 'Audio connection', and 'nfoersteOfficeDX80'. The Q&A panel on the right is titled 'Q&A' and shows 'All (0)' questions. A blue arrow points from the 'Q&A' menu item to the Q&A panel. A yellow box highlights the 'Q&A' menu item and the 'More options' button (three dots) in the bottom toolbar. Another yellow box highlights the Q&A input area, which contains the text: 'Select a question and then type your answer here, There's a 256-character limit.' Below the input area are 'Send' and 'Send Privately...' buttons.

👉 and use feedback button for answering polling questions



👉 and stay focused during the session...

There will be a Quiz at the end with a Chance to win nice Prices!



3rd Price
Coffee Cup



1st Price
Cisco Headset HS730



2nd Price
Thermo Bottle

Cisco SASE Lösung

Meraki SD-WAN Integration

Cyrill Meier
Security Architect
Dezember 2021



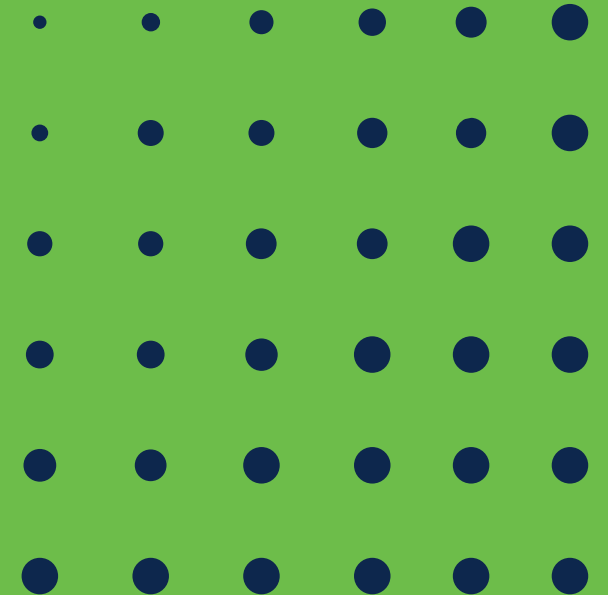


Agenda



- ▶ Was ist SASE?
- ▶ SASE Use-Case
- ▶ Global cloud architecture
- ▶ Umbrella Übersicht
- ▶ Testresultate
- ▶ Demo

Was ist SASE?



Gartner: Secure Access Service Edge (SASE)

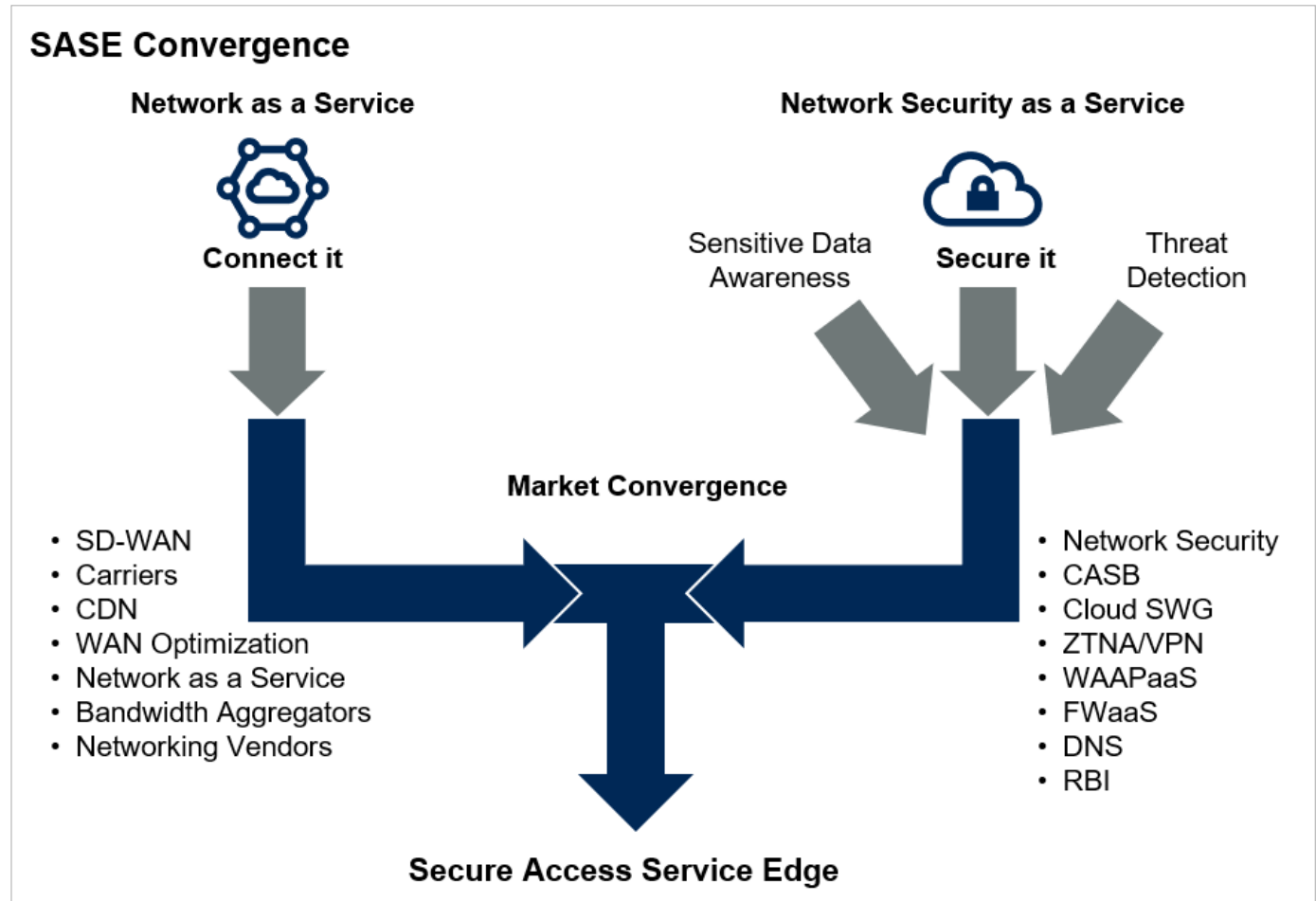
Convergence of networking and security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

Benefit rating:
Transformational

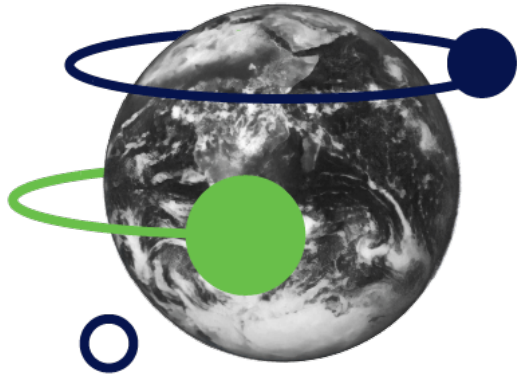
Market penetration:
Less than 1% of target audience

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

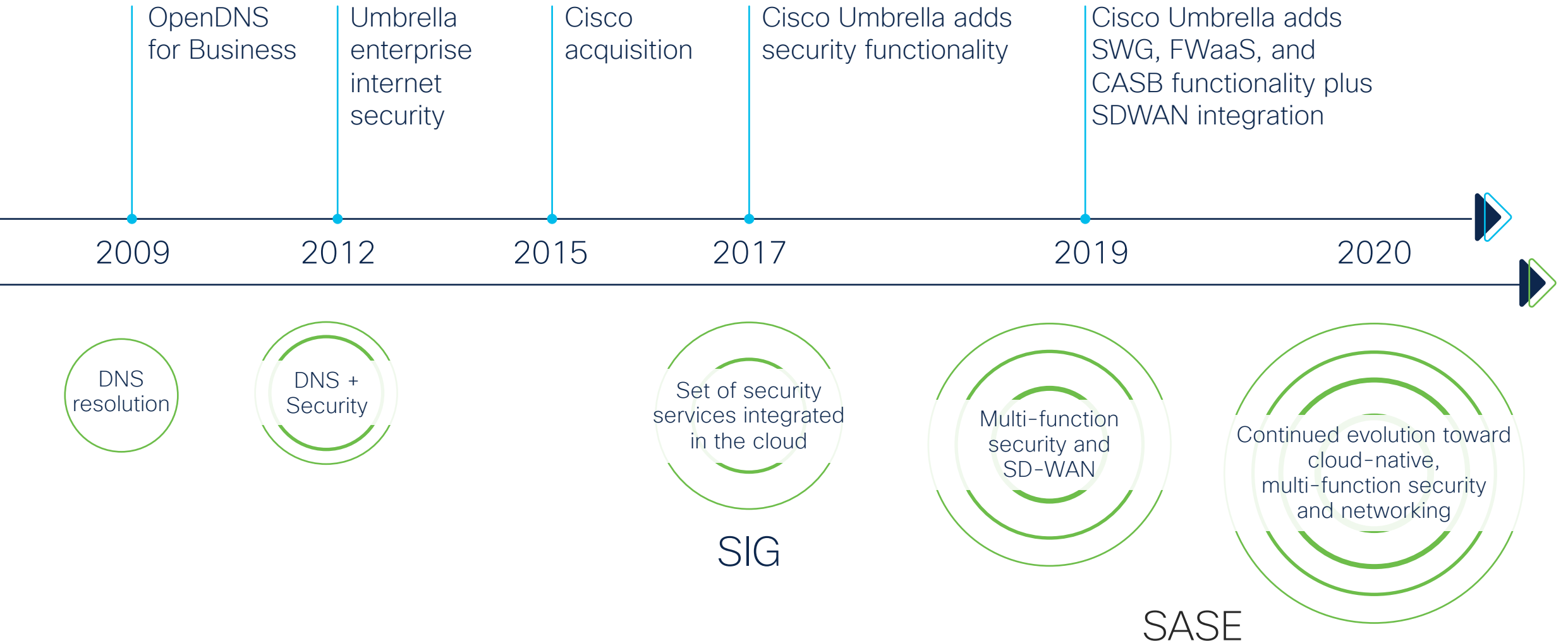
Defending 100% of the Fortune 100



Zero Trust

Leader in Zero Trust two years running

Cisco Umbrella evolution



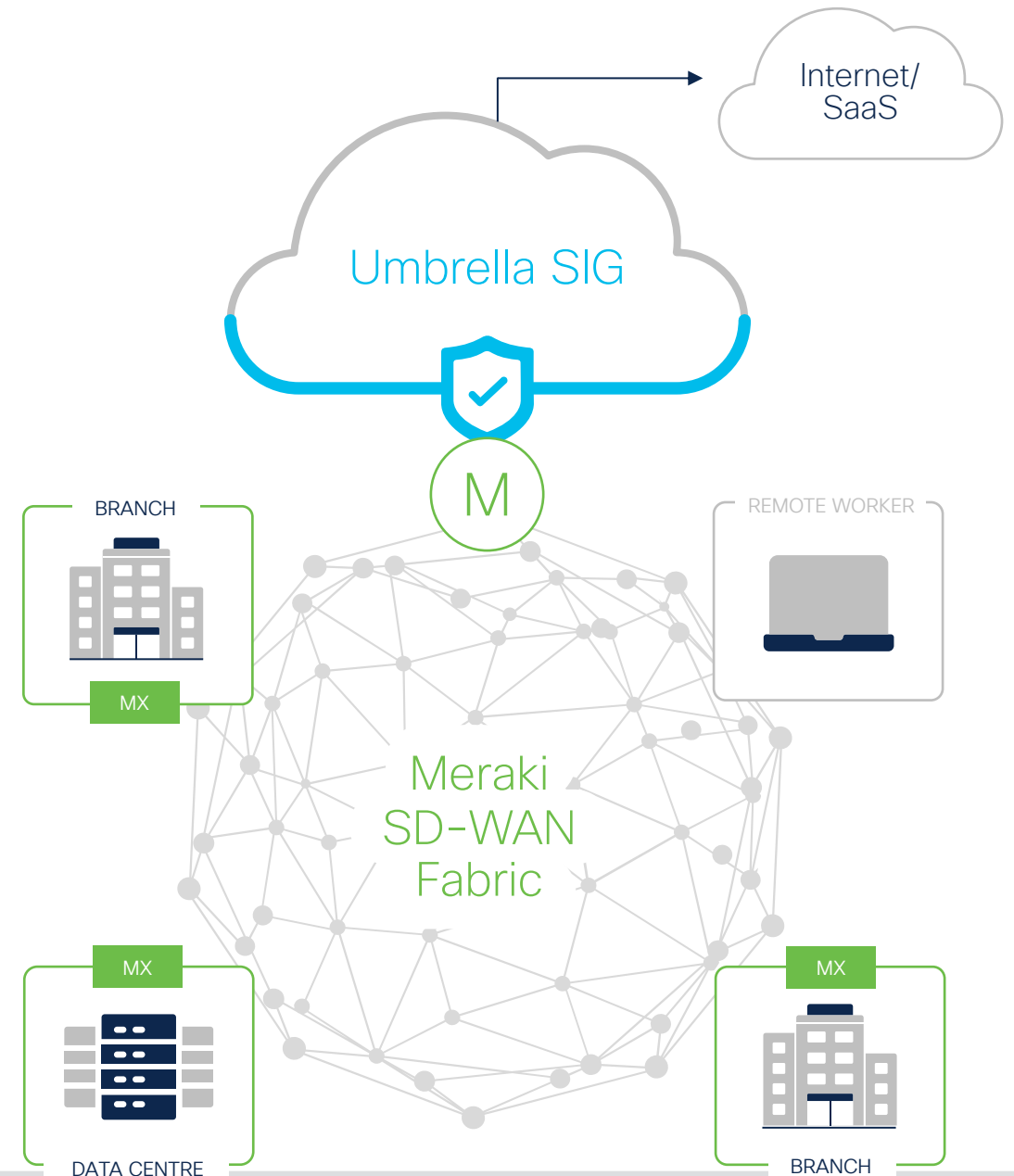
SASE Use-Case



Major use cases

Secure, optimized edge

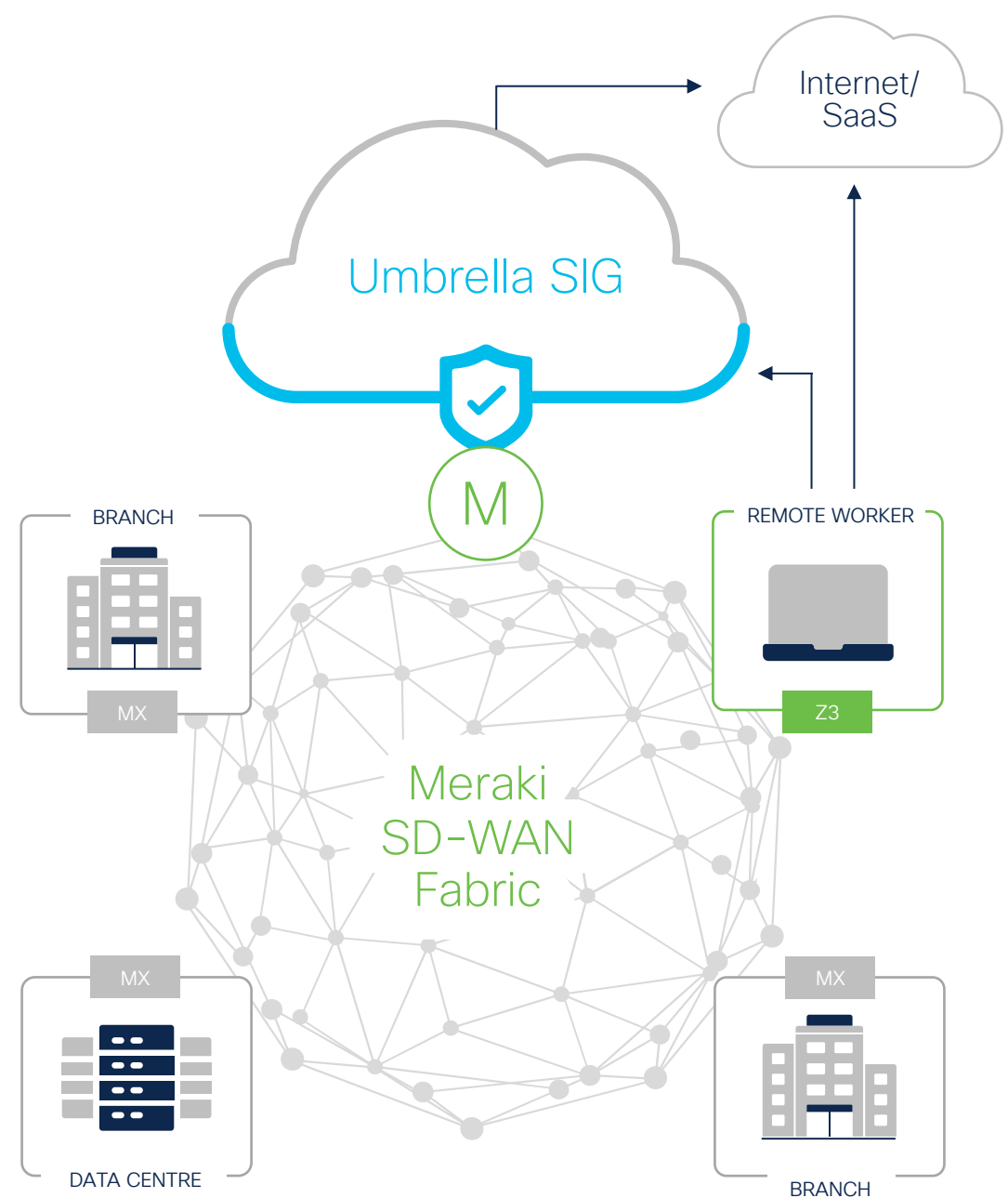
- Streamline connectivity to public and private apps across all office locations
- Secure branch-to-branch (east/west) traffic
- Provision SD-WAN fabric across thousands of users and locations
- Secure access to apps and direct internet access



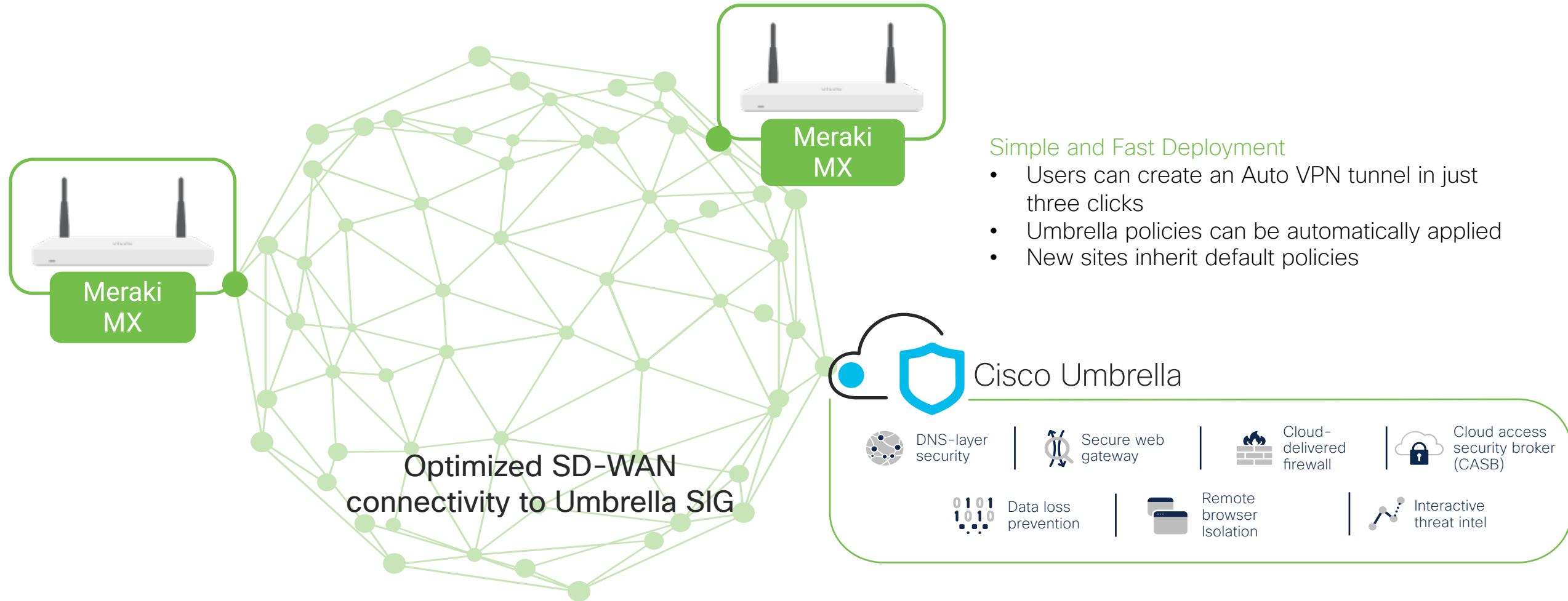
Major use cases

Secure remote worker

- Seamless connection to apps and data anywhere users work
- Secure access to internet and cloud apps
- Authenticate users and ensure device health before establishing connection



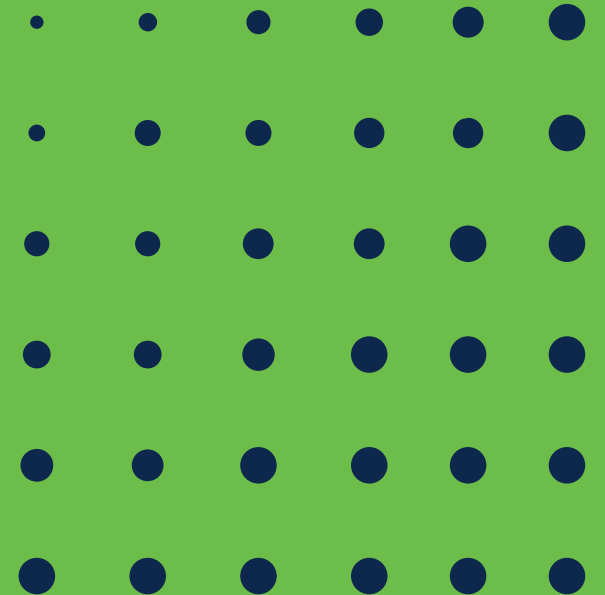
Best-in-Class & Seamless SASE Security



Simple and Fast Deployment

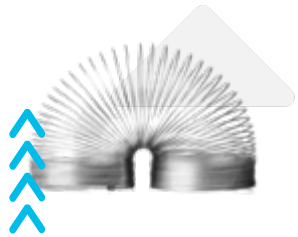
- Users can create an Auto VPN tunnel in just three clicks
- Umbrella policies can be automatically applied
- New sites inherit default policies

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

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

Cisco Umbrella earns SOC 2 Type II Compliance



What is SOC 2?



SOC 2 is a compliance framework that covers Security, Availability and Confidentiality trust services criteria.



SOC 2 requires an independent audit and provides our customers and prospects with assurance that controls are implemented.

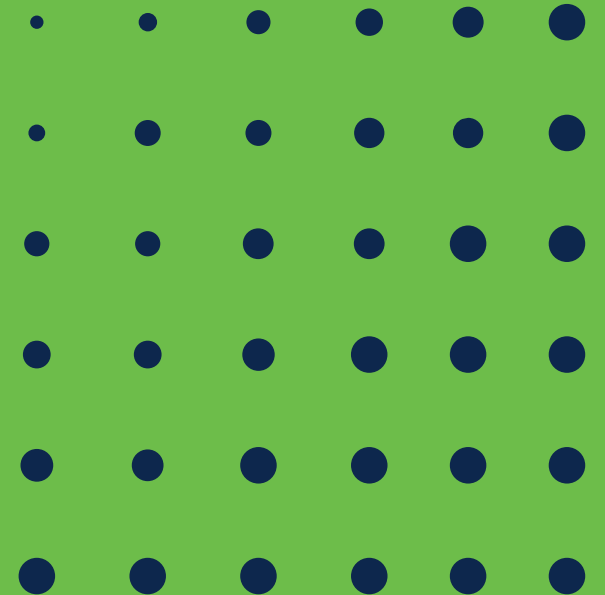


SOC 2 Type II requires that controls are tested for design & operating effectiveness over a minimum of 3-month assessment period, typically annually thereafter.



After the audit, the SOC 2 Type II report is received and can be shared with customers and prospects under NDA.

Umbrella Übersicht



Cisco Umbrella



Cisco Umbrella



DNS-layer security



Secure web gateway



Cloud-delivered firewall (w/ IPS)



Cloud access security broker



Interactive threat intelligence



Remote browser Isolation



Data loss prevention



Cloud malware detection



SecureX
Integrated security platform



SD-WAN
Meraki MX
Viptela

ON/OFF NETWORK DEVICES

► Visit our website to learn more
www.umbrella.cisco.com/products

Enforcement that works together

Improved responsiveness and performance

1. DNS-layer security

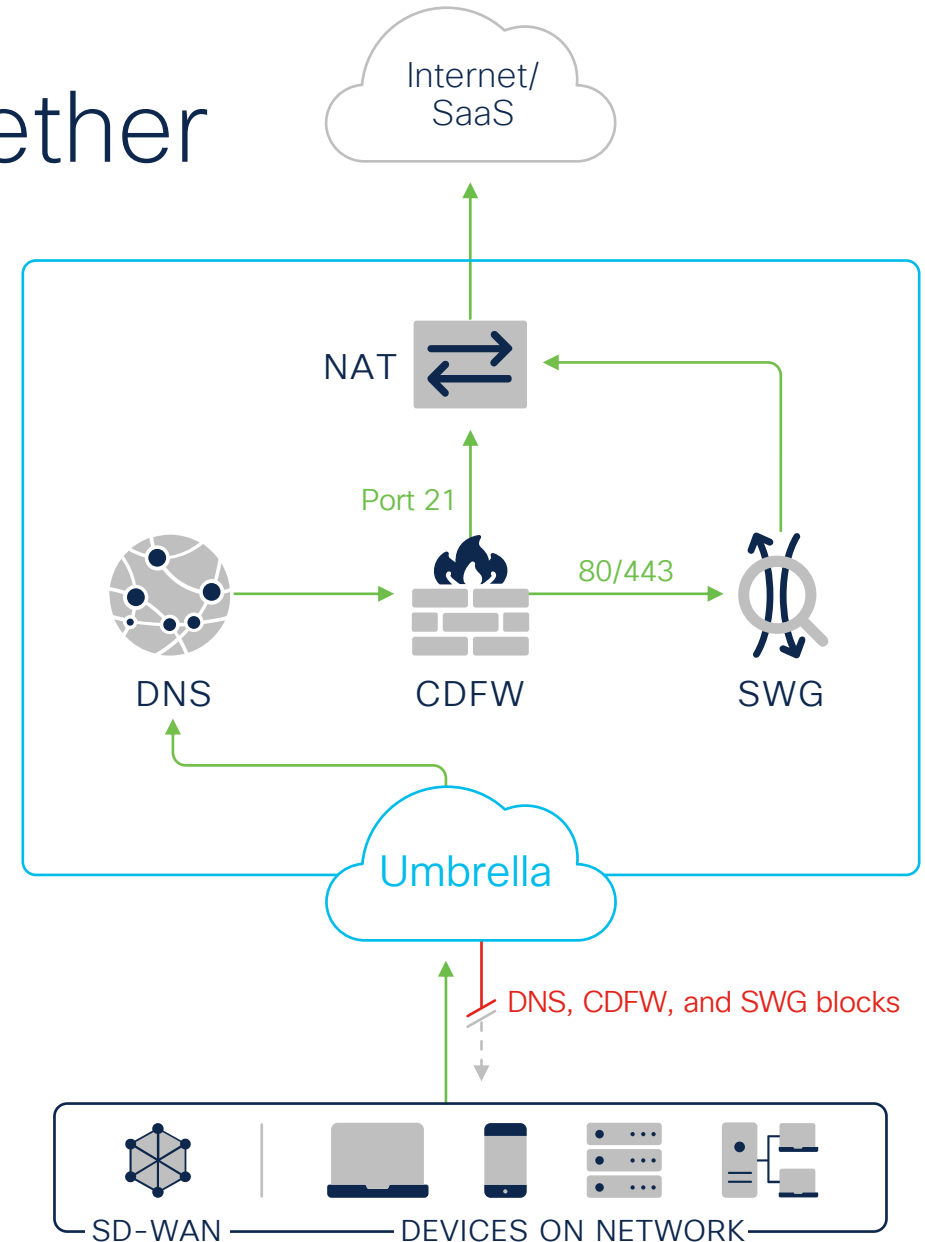
First check for domains associated with malware

2. Cloud-delivered firewall (CDFW)

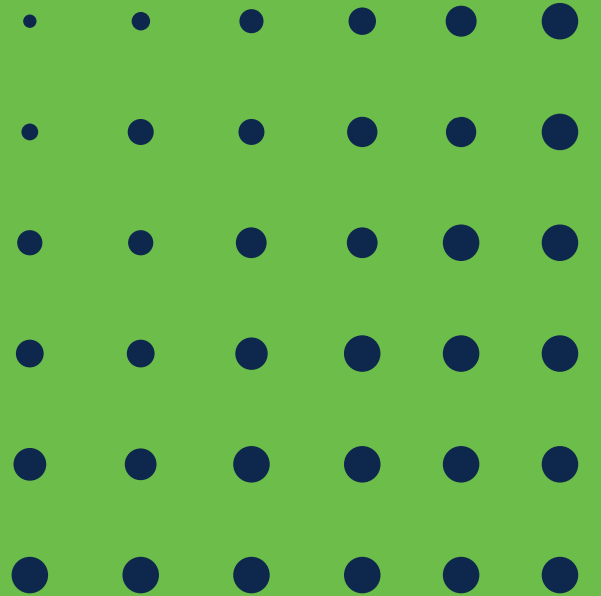
Next check for IP, port, protocol and application rules

3. Secure web gateway (SWG)

Final check of all web traffic for malware and policy violations



Connecting to Umbrella



Tunnel internet connections

Example

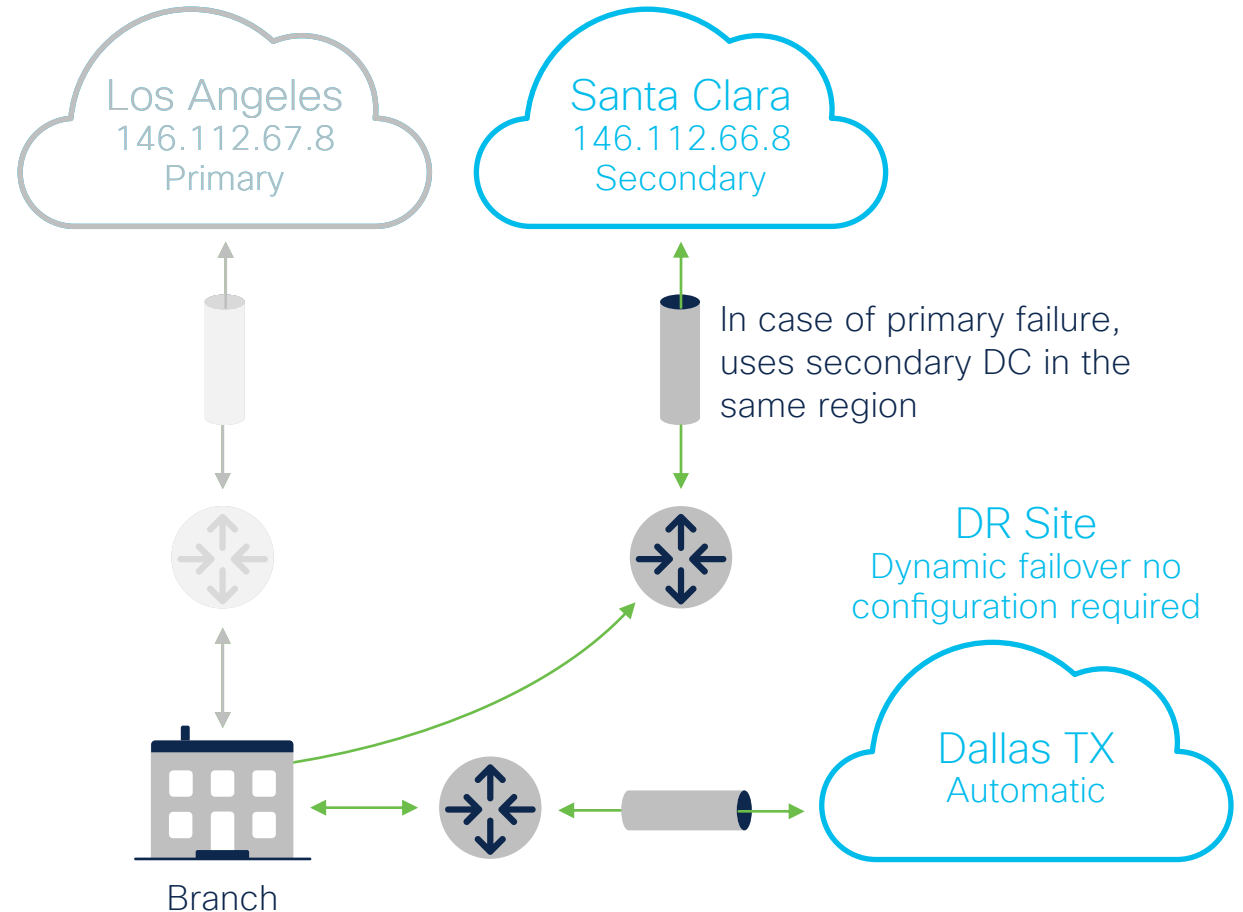
Data center region code US-1

IPsec capacity

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

Availability

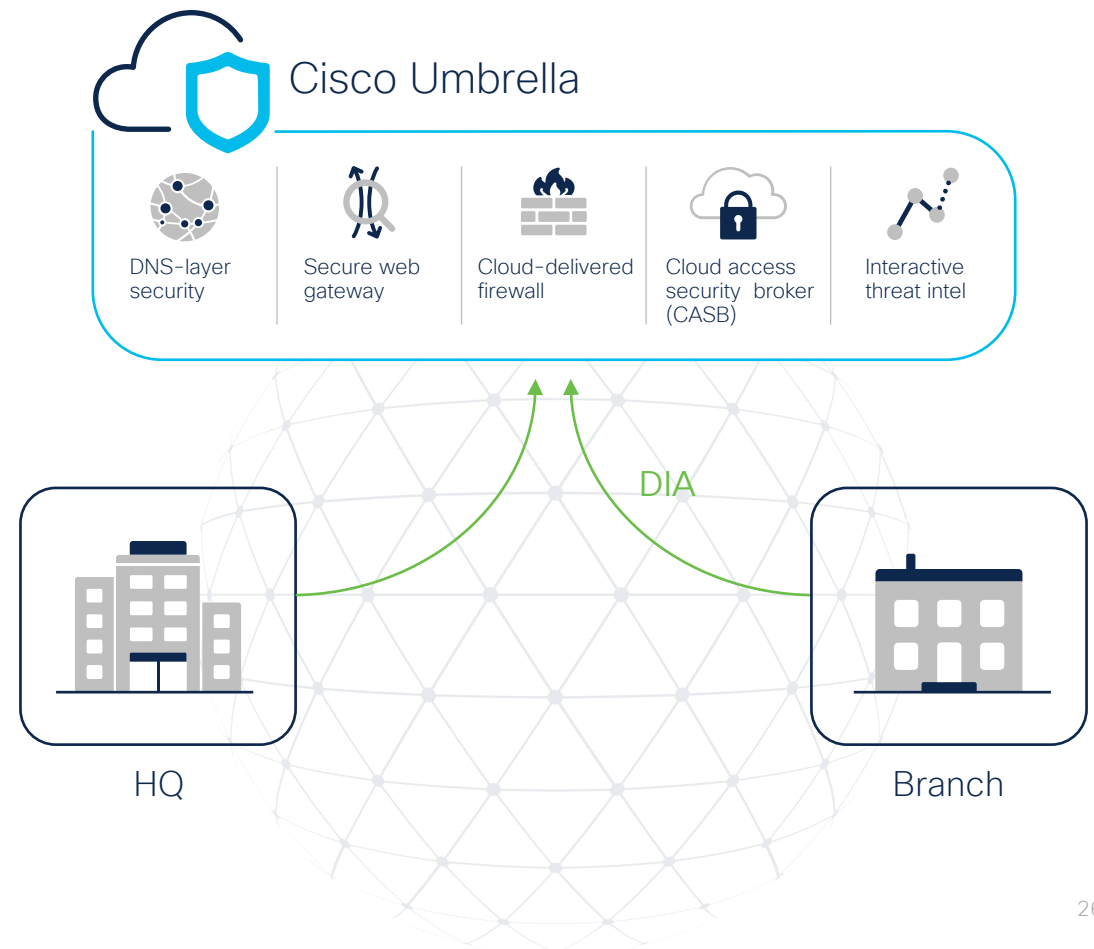
- Hard code primary, secondary (optional)
- Failover to secondary data center and disaster recovery is handled by anycast
- Failure detection uses IKE dead peer detection



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



Meraki SD-WAN Connector Capabilities

UMB-SIG SD-WAN Connector

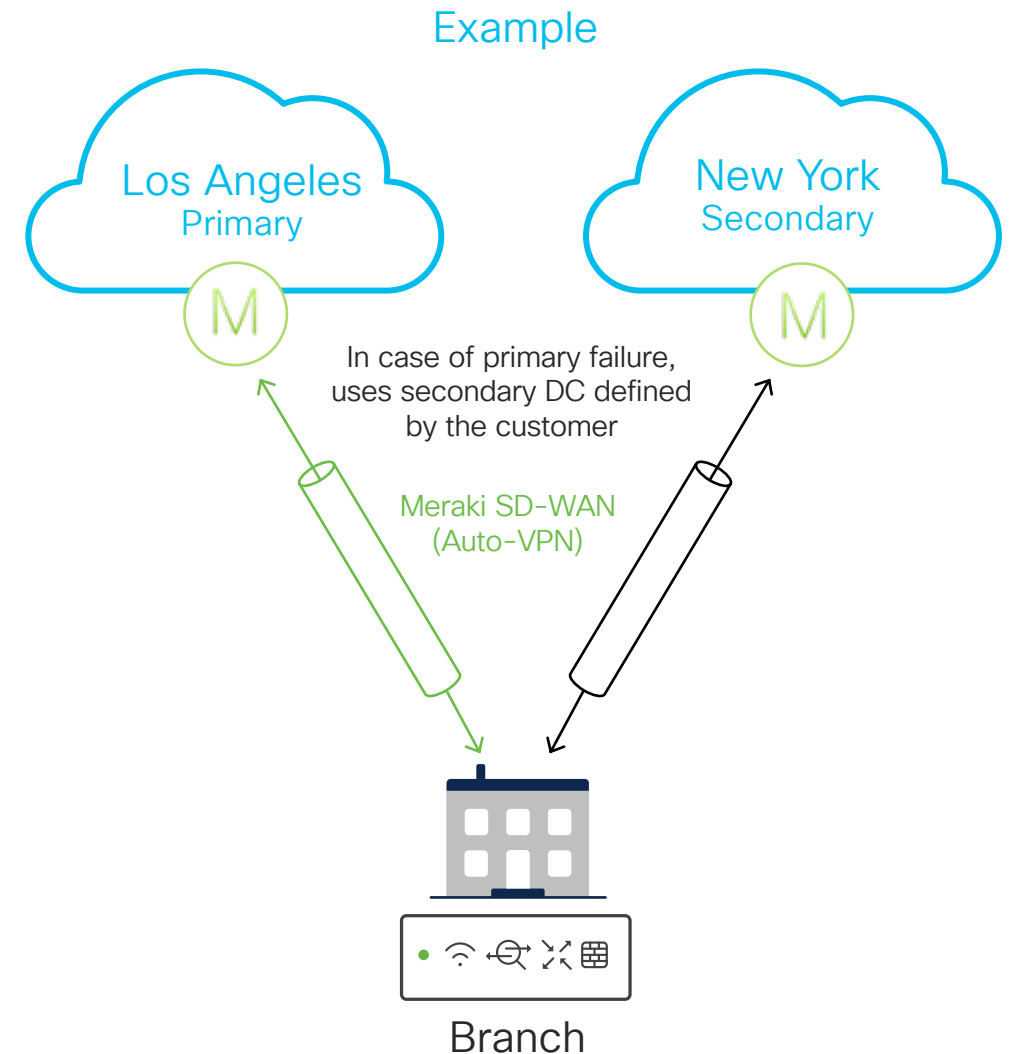
- 250 Mbps per UMB-SIG connector, ongoing development to increase capacity
- Multiple UMB-SIG connectors can be deployed to support higher capacity
- Supports VPN exclusions for DIA

Availability/HA

- Customer-defined primary and secondary DC
- Failover to secondary DC is handled by the Meraki SD-WAN fabric
- Initially available in select SIG DC's globally

Licensing

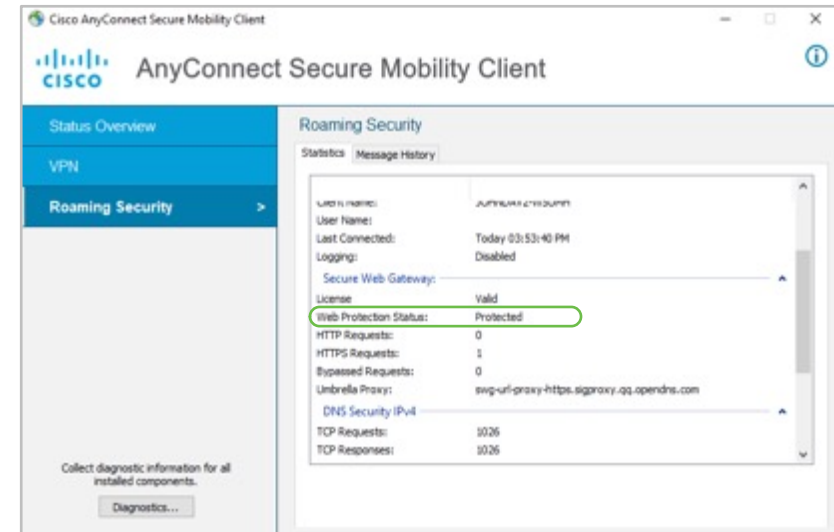
- Requires Umbrella SIG licensing + any MX license tier



Cisco AnyConnect Security Mobility Client

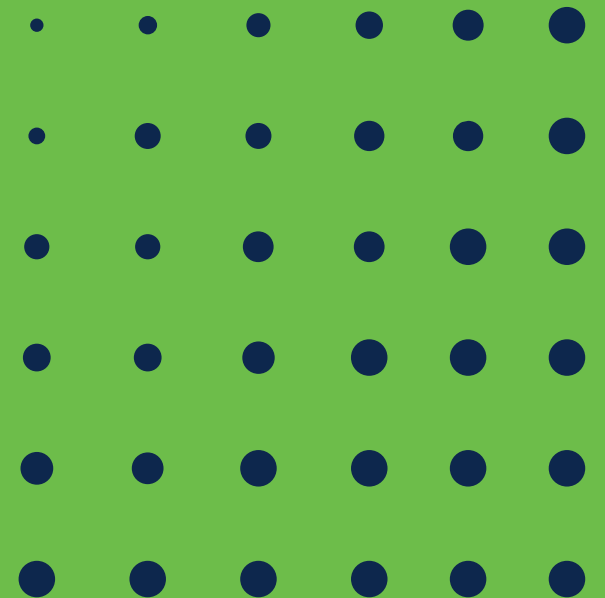
Entitlement for Mobility Client is included (excludes VPN functionality)

- 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

DNS security



Proven leader in cloud-native security



620B
requests per day



500M
authentication events
every month



500K
global customers

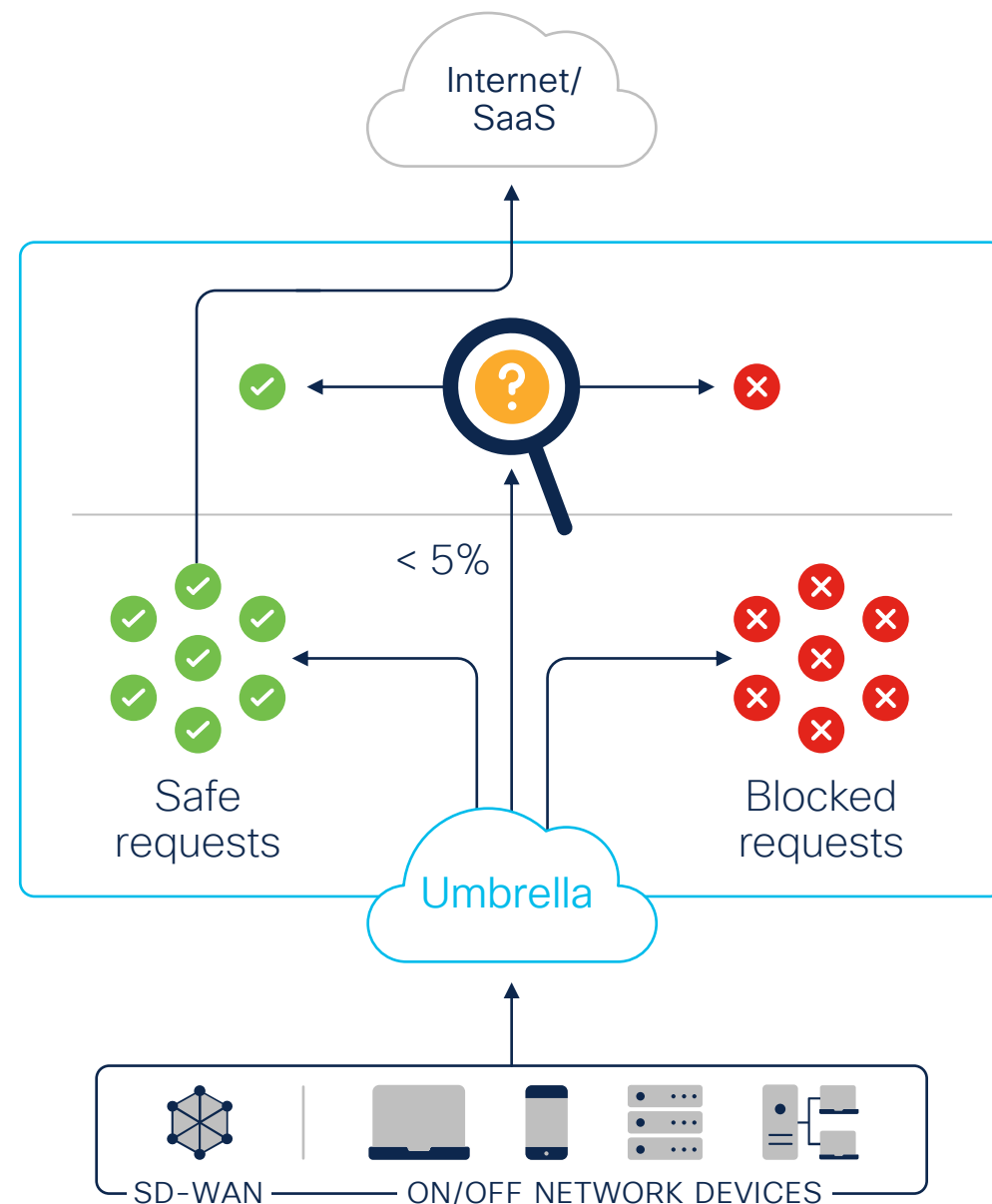


96%
Highest threat detection
rate in the industry *

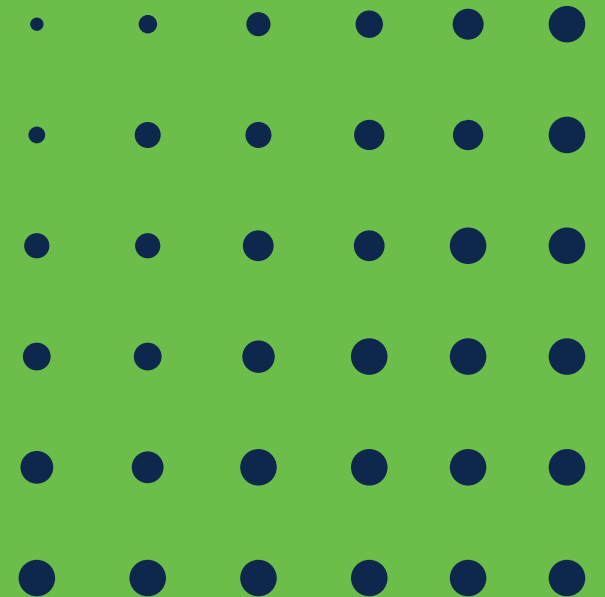
DNS-layer security

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



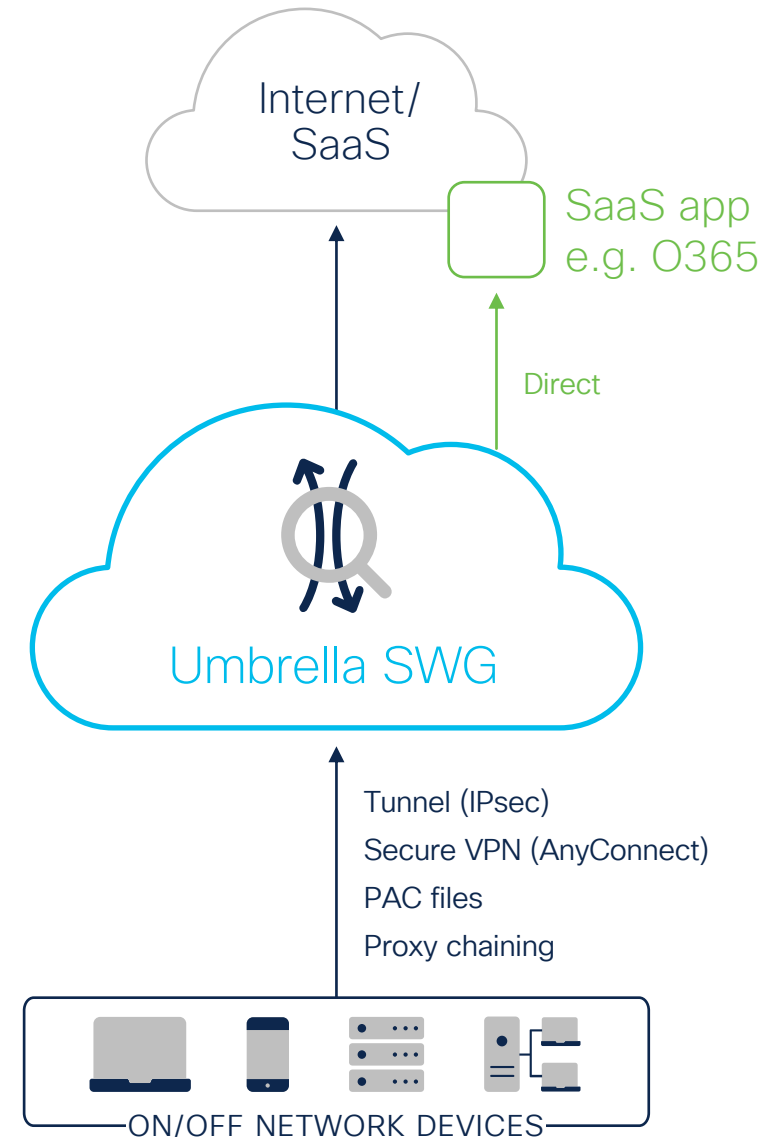
Secure web gateway



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



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

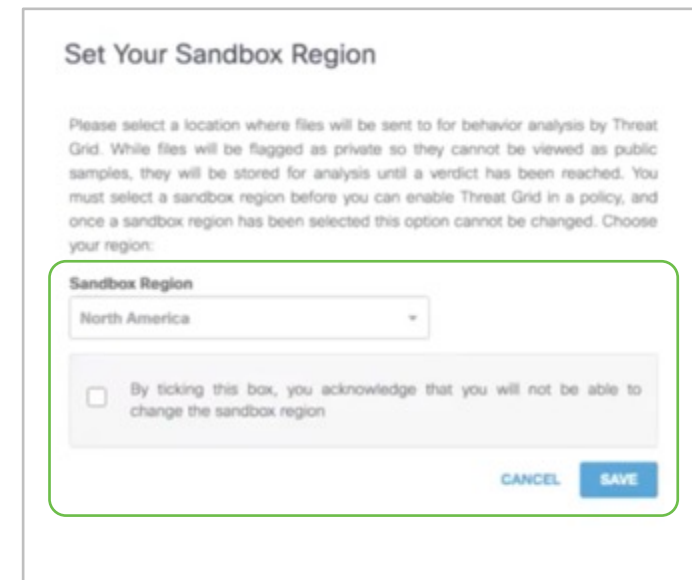
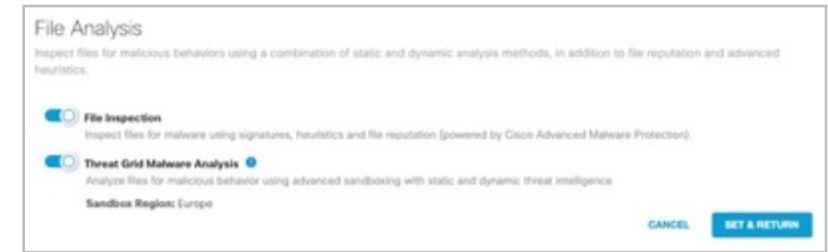
Base Content

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

Secure Malware Analytics (Threat Grid)

Sandbox inspection

- Files that make it through the anti-virus and malware scan by Cisco SecureX Malware Analytics and third-party tools (less than 50 Mb in size)
- Files that haven't been seen before by Cisco Secure Malware Analytics and have attributes that the Cisco Secure Malware Analytics model targets
- We are using libmagic for file type detection as well as listed file extension

File Retrospective ⓘ

Recent Retrospective Events

SHA256	Threat Score	Malware Name	Date Detected	
7638f6d4a9cd3ea5fa88f9958da6e6e745b2931b96ecea...	100	W32.7638F6D4A9-100.SBX.TG	Jul 30, 2019 at 3:22 AM	...
526b2cad716f7dc1e568d5e68b8a251d19e129308806b...	100	W32.526B2CAD71-100.SBX.TG	Jul 27, 2019 at 3:23 AM	...
1a27fdf68d61964ddc13a62a75b15b7c94978def0b014...	100	W32.1A27FDF68D-100.SBX.TG	Jul 26, 2019 at 3:24 AM	...
49ade947bb9de7ce36f9735f90758d8425f939c2ce84b6...	100	W32.49ADE947BB-100.SBX.TG	Jul 25, 2019 at 4:31 AM	...
f9f23288188bc1a959e890084cc685db4ff9c50b95a52a...	100	W32.F9F2328818-100.SBX.TG	Jul 24, 2019 at 3:26 AM	...

1 - 5 of 32 < >










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

SWG users and groups

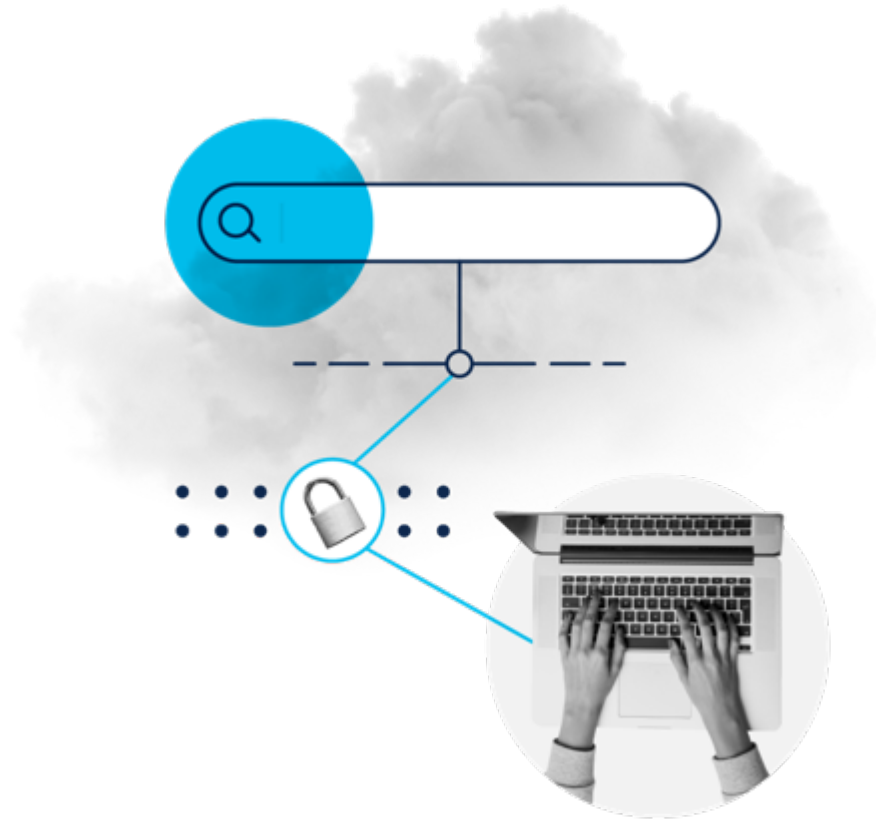
- CSV upload
 - Recommend CSVDE tool on Windows Domain Controller
- AD connector Active Directory sync
 - Group filtering supported with data file
 - Standard AD connector install version 1.3.8+
 - Only one Domain Controller required, no VA required



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 integrated in a very simple and SASE way

Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
	Isolate	Block	No Selections Add Identity	No Selections Add Destination	Any Day, Any Time Change Schedule No additional configuration applied

- Allow - Security Enforced**
Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.
- Warn**
Warns selected ruleset identities before allowing access to destinations.
- Block**
Blocks selected ruleset identities from accessing destinations.
- Isolate**
Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

Ruleset Settings

Ruleset settings affect the rules within the ruleset and must be configured through their respective components before being set here.

Ruleset Name	Edit
Ruleset Identities	Edit
Block Page	Edit
Tenant Controls	Edit
File Analysis	Edit
File Type Control	Edit

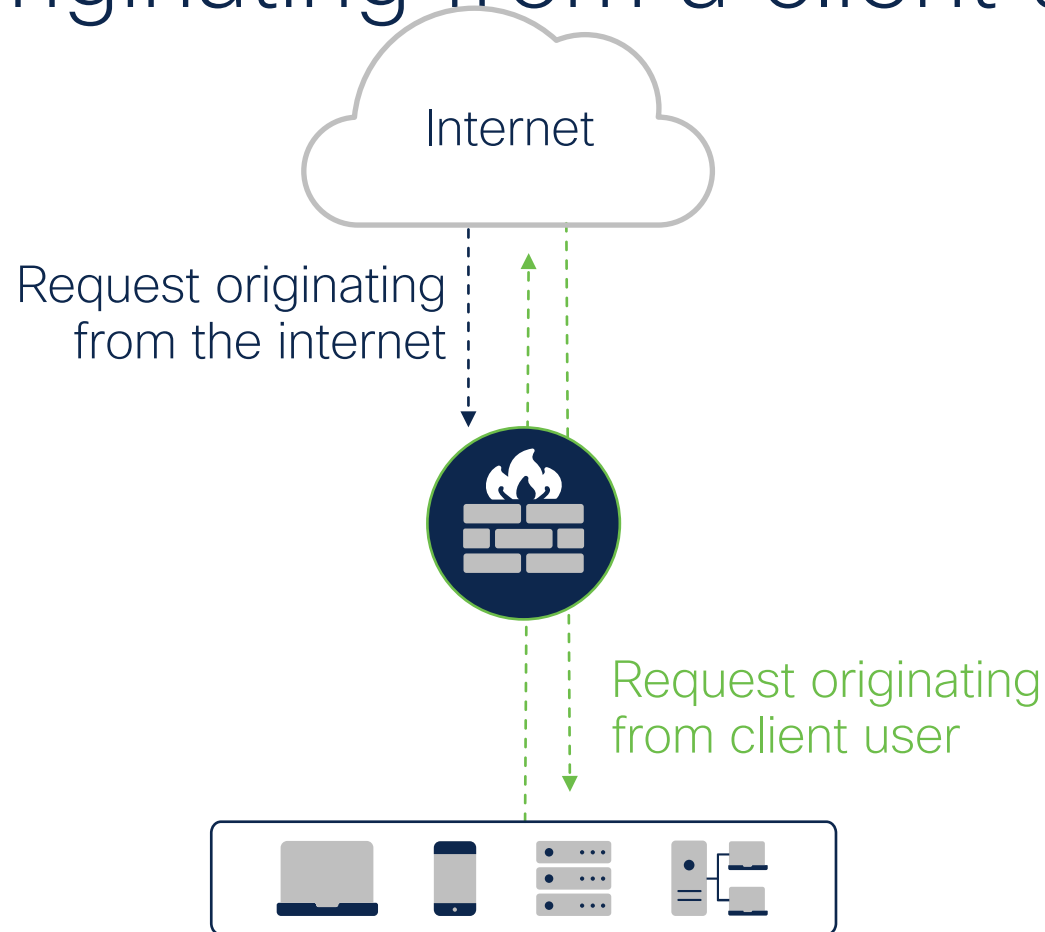
RBI traffic flow overview



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

🔍 Search Firewall Rule names or descriptions

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	...

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

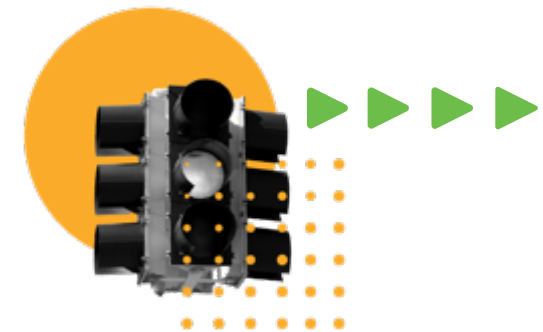
Example: Stop file transfer

- 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)

Capabilities

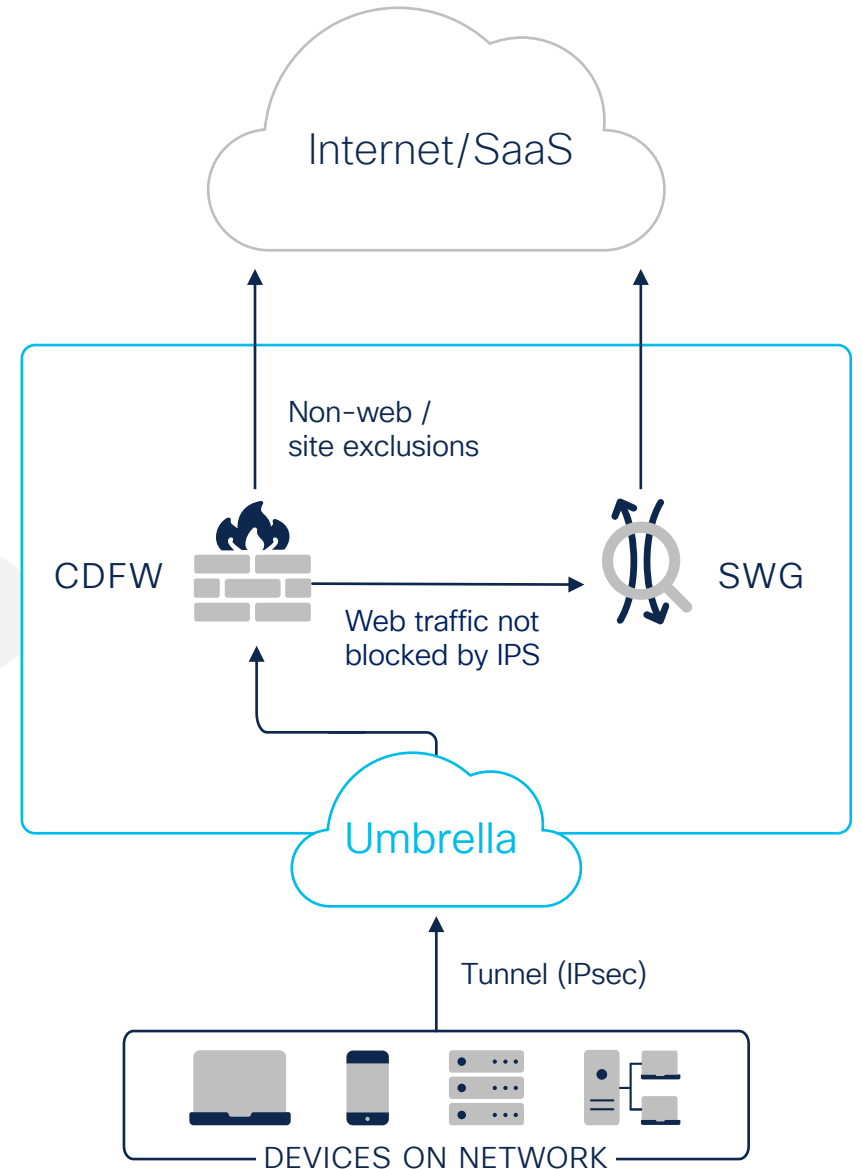
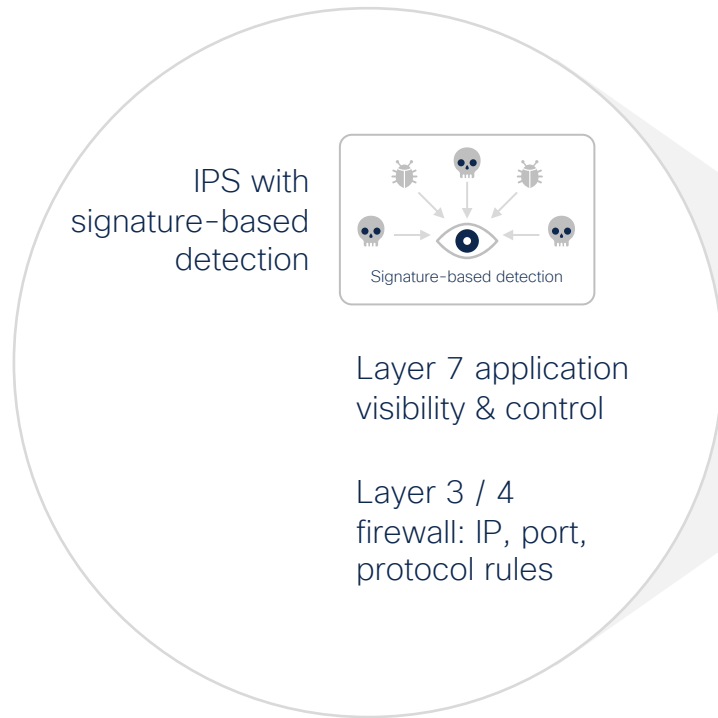
- Deepen Umbrella cloud firewall protection for client-driven traffic
- Use signature-based detection (Snort 3) to examine network traffic flows & prevent vulnerability exploits
- Add layer of detection/blocking for malware, botnets, phishing, and more
- Leverage Cisco Talos' 40K+ signatures (and growing)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

Results

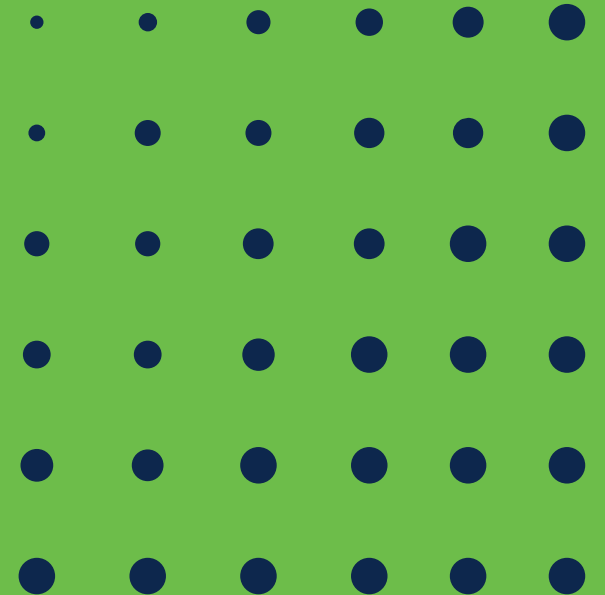
- ✓ Simplify management via Umbrella's single, unified dashboard
- ✓ Remove capacity concerns of appliances by using scalable cloud compute resources
- ✓ Stop more threats with the industry's most effective threat intelligence
- ✓ Detect/block exploitations of vulnerabilities

Umbrella Intrusion Prevention System (IPS)

Layers of security for high security efficacy



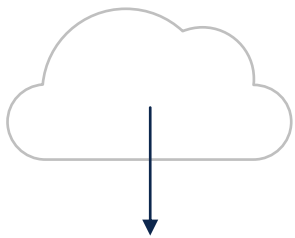
CASB functionality



General CASB types (multimode)

Inline/proxy

- High impact deployment
- Agent or traffic redirection
- No API to app protecting
- Limited retrospective
- Real-time enforcement inline
- Limited east-west & cloud-to-cloud
- All application coverage



Out of band/API

- Low impact deployment
- Agentless no user experience impact
- Relies on API of cloud apps
- Retrospective
- Near real-time enforcement
- Universal coverage
- Sanctioned app coverage



CASB types continued

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

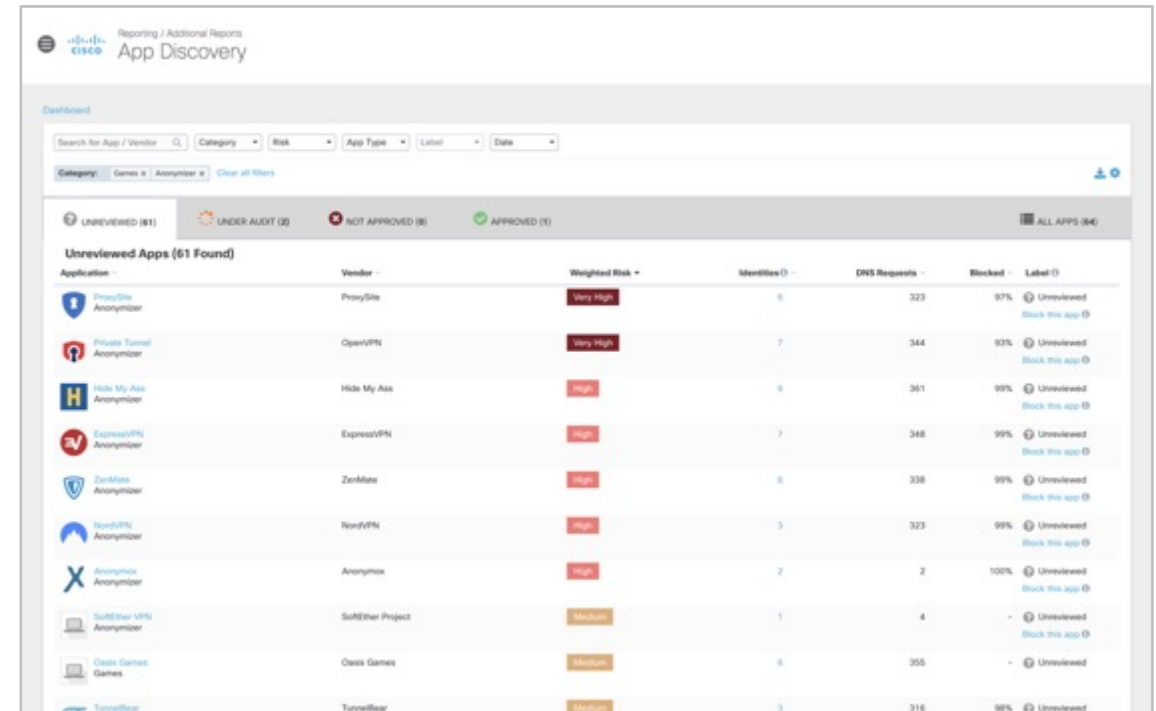
Cloudlock

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

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
Cisco App Discovery

Dashboard

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

Category: Games | Anonymizer | Clear all filters

UNREVIEWED (61) | UNDER AUDIT (0) | NOT APPROVED (0) | APPROVED (1) | ALL APPS (64)

Unreviewed Apps (61 Found)

Application	Vendor	Weighted Risk	Identifies	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
Anonymix Anonymizer	Anonymix	High	2	2	100%	Unreviewed Block this app
SurfEater VPN Anonymizer	SurfEater Project	Medium	1	4	-	Unreviewed Block this app
Class Games	Class Games	Medium	6	355	-	Unreviewed
TunnelBear	TunnelBear	Medium	3	316	98%	Unreviewed

Granular app controls


Dashboard

Search for App / Vendor Filter by Identity


UNREVIEWED (3197) UNDER AUDIT (12)

All Apps (3,287 Found)

Application

 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)

<input checked="" type="checkbox"/>	Default Settings Applied in: Global Branch Policy, Security Only ...	Block
<input checked="" type="checkbox"/>	HR App Restrictive Applied in: High Restrict Group	Block Uploads
<input checked="" type="checkbox"/>	Global App Allow Applied in: Global Allow Policy	Allow

Label application as

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

CANCEL

SAVE

ALL APPS (3287)

Total Traffic Outbound Traffic Inbound Traffic Label

51 MB total traffic 48 MB 4 MB Under Audit
4 MB 48 MB Edit app controls

3 MB total traffic 3 MB 88 KB Unreviewed
88 KB 3 MB Edit app controls

157 KB total traffic 71 KB 86 KB Unreviewed
86 KB 71 KB

6 MB total traffic 6 MB 72 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

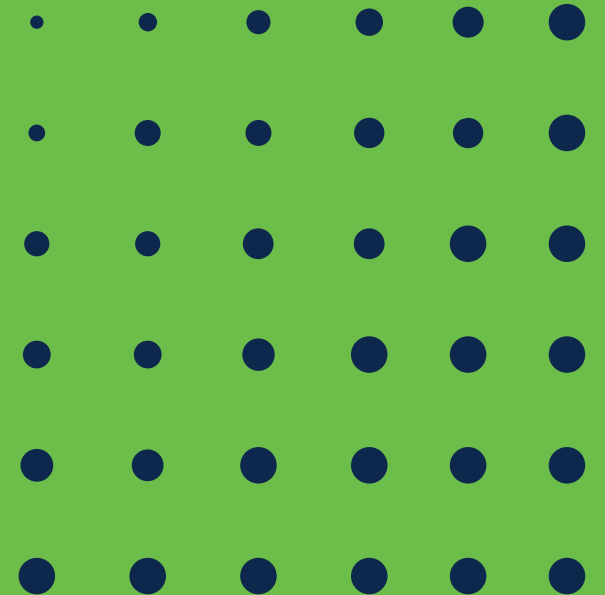
Robust Reporting

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

The image shows three overlapping screenshots of the Cisco DLP management console. The top screenshot is titled 'DLP Data Classification', the middle one 'DLP Rules', and the bottom one 'DLP Report'. The 'DLP Report' screenshot displays a table with the following data:

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

Security Efficacy



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 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)

Better Together

Layer 7 firewall	
IDS/IPS	
Content filtering	
Malware protection	
Sandboxing	
AnyConnect remote VPN access	
Centralized enforcement, policy & reporting	
Site-to-site Auto VPN	
East-west security filtering	
URL filtering	
SSL decryption/inspection	
Data loss prevention (DLP)	
Remote Browser Isolation (RBI)	
Granular app control	
File type control	
SaaS Tenant Restrictions	
CASB	



Meraki

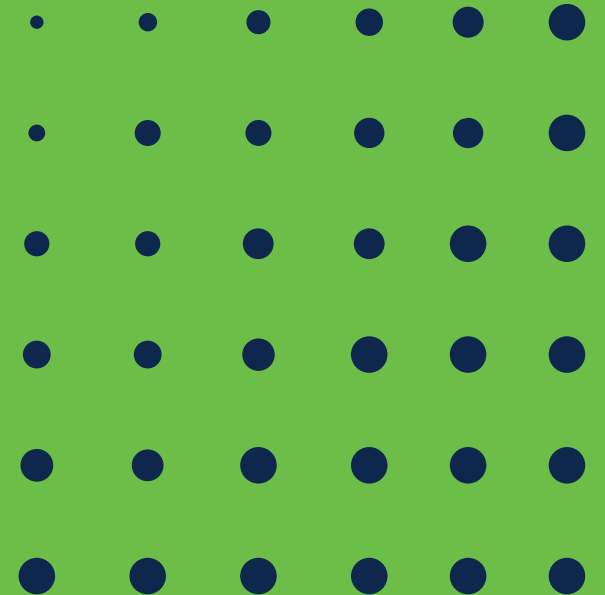


Umbrella



Umbrella + Meraki

DEMO



Fragen?



👉 Now it's time to play the game!

Please use a real name as nickname. Win nice Prices!

Join at www.kahoot.it
or with the Kahoot! app
Game Pin: 554718



3rd Price
Coffee Cup



1st Price
Cisco Headset HS730



2nd Price
Thermo Bottle

OUTLOOK Upcoming Virtual Espresso

- Blog:
<https://gblogs.cisco.com/ch-de/tag/virtual-espresso/>
- Topics:
 - 22. Dezember 2021: Cisco SD-Access Migrationsszenarien

Join the game at www.kahoot.it
or with the **Kahoot! app**
Game Pin: 554718

...so then - let the games begin...

Get ready to join

Game Pin: 554718

Join at www.kahoot.it
or with the **Kahoot! app**

Game PIN:

Loading Game PIN...



dankä villmal
grazie mille
merci beaucoup
grazia fitg
thank you

