Cisco Umbrella

FREQUENTLY ASKED QUESTIONS

# Cisco Umbrella

In order to make sure you have all the information you need about Cisco Umbrella, we've compiled answers to the most common questions we hear. If we didn't answer your question, you can get in touch with our Sales team at 1-877-811-2367.

If you have technical product questions, please visit: http://cs.co/umbrellatechdocs

## Packaging & Pricing

### How do you license Cisco Umbrella?

**For most Umbrella packages, we license by the total number of users with internet access.**

- Count employees that connect IT-provisioned or user-owned devices to local or remote networks.
- For organizations with guest Wi-Fi networks, include the average # of guest users connecting to your access points daily. However, if you are a guest Wi-Fi provider or providing internet access to only guests, our sales team can discuss special licensing packages available.
- We do not use the number of concurrent or active (vs. total) users in our licensing. Unlike appliance-based solutions with performance constraints based on the # of concurrent or active users, Umbrella is infinitely scalable.

### Will I need to contact Cisco each time my total # of users exceeds my licensed # of users?

**No, but you may contact us anytime you need to increase your license count.**

- We advise organizations to purchase a license count to accommodate expected user growth over a 1-or 3-year term subscription, but protection is never ceased for exceeding license count.
- We monitor network-level DNS traffic volume only to identify account issues or abuse. You may receive a courtesy email or call from a sales representative before your renewal date if your account appears to significantly exceed the license count.

### How do you package and price Cisco Umbrella?

**We offer five packages of Umbrella to best suit your needs.**

- Umbrella Platform is our high-end package, providing all of the product features and functionality, including access to our threat intelligence console and our enforcement API for integration with your existing systems.
- Umbrella Insights balances the price with the capabilities delivered to suit most organizations. In addition to the features in Professional, it offers user-based policies, the ability to retain DNS logs forever, and more reporting options.
- Umbrella Professional protects users on & off the corporate against malware & phishing attacks, contains C2 callbacks from already infected devices, and offers web filtering, along with basic reporting.
- Umbrella Roaming is an entry-level package that provides protection only when users are off the VPN. This package is best suited for organizations who have Cisco firewalls or next-generation firewalls and Cisco AnyConnect clients.
- Umbrella Branch is an entry-level package that can be used alongside the Cisco Integrated Services Router (ISR) 4000 Series devices for protection of corporate and guest users at branch offices.
- Tiered discounts are built into the price depending on the number of users licensed.
- An annual discount is available for paying upfront for a 3-year subscription.
- Standard online and email support is included in all of our packages.

# Protecting Sites, Devices & Users

## How do I secure any device on our corporate networks?

**Clientless DHCP → Cisco Umbrella global network.**

- Change one setting native to all internet gateways (e.g. routers, APs) and DHCP seamlessly provisions devices—even those you don't own—to forward DNS traffic to the Umbrella global network.
- We started building the Umbrella global network in 2006, and we're continuously adding new data centers. Please check the network map on our Website for the most up-to-date locations (http://cs.co/umbrelladatacenters). And refer to our technical documentation (http://cs.co/umbrellatechdocs) to understand how our Anycast infrastructure works, such that no matter where each site is physically located, your DNS traffic is routed to the fastest location.

## How do I secure laptops off our corporate network

**The Cisco Umbrella roaming client or Cisco AnyConnect roaming security module can be used to protect laptops off the corporate network.**

- If you currently use the Cisco AnyConnect client, you have the option to enable the roaming security module, which provides seamless protection when the VPN is turned off – without requiring an additional agent!
- Alternatively, you can deploy the Umbrella roaming client. It tags, encrypts, and forwards DNS queries bound for the internet to the Umbrella global network so per-device security policies can be enforced everywhere without latency or complexity.
- The roaming client for Windows or Mac OSX is extremely lightweight with near-zero CPU or RAM usage. Deployment can be distributed by third-party solutions using our command line installation. It can run in "head" or "headless" mode, and is updated automatically without user intervention.

## How do I manage policies and pinpoint activity per internal subnets or IP addresses?

**Clientless DHCP → the Umbrella virtual appliance → the Umbrella global network.**

- Change one setting native to all internet gateways (e.g. routers, access points) and DHCP seamlessly provisions devices – even those you don't own – to forward DNS traffic to our virtual appliance.
- The virtual appliance tags and forwards DNS queries bound for the internet to the Umbrella global network so more granular security policies can be enforced without latency or complexity.
- Our virtual appliance for VMware or HyperV requires minimal CPU or RAM resources to run, and we support an unlimited number of instances, which are updated automatically without user intervention.

## How do I manage policies and pinpoint activity per device or user without touching devices or reauthenticating users?

**The Umbrella connector → the Umbrella virtual appliance.**

- Deploy our connector in your Active Directory (AD) environment along with the Umbrella virtual appliance, and you can use your AD group, user, and computer identities for more granular policy enforcement and threat visibility.
- Our connector is updated automatically without user intervention.

## Service Performance

### Will this service introduce any latency?

**Umbrella adds no additional latency.**

- That's because with Umbrella there is no need to reroute all connections through proxies or over VPNs to secure roaming users or remote offices.
- Today, your external DNS traffic by default is probably pointed to your ISP's cloud-delivered recursive DNS service. Now, your external DNS traffic points to the Umbrella global network, which is built using our more reliable, faster, safer, and smarter DNS resolvers.
- Our infrastructure is extensively peered at major Internet exchanges to minimize routing latency no matter where in the world you're located. And we are the key participant of the http://www.afasterinternet.com/ project along with all leading CDN (content distribution network) providers.

### What happens when the service goes down; will I lose all internet connectivity?

**No, and it's never happened.**

- The Umbrella global network has maintained 100% uptime since it launched in 2006.
- We publicly display our operational system status and stats: http://cs.co/umbrellasystems
- If one or more of our global data centers has scheduled maintenance or an unanticipated issue, our Anycast infrastructure instantly re-routes your DNS requests to the next closest datacenter without any disruption in service.

### How scalable are your virtual appliances?

**Each virtual appliance (VA) instance can easily support 10,000s of concurrent users.**

- Only one CPU core, 512MB of RAM, and 7GB of disk space is required per VA instance. (NOTE: We do require two instances per site for high-availability and to support automatic updates.)
- You may provision additional resources per VA instance or add VA instances in large network environments, at any time, with no extra fees.

### What happens if one of your virtual appliances goes down; will I lose all internet connectivity?

**No, because our high-availability virtual appliance (VA) pair includes native redundancy and load balancing.**

- VAs are built on the same code base as our cloud-delivered service, which handles 80+ billion DNS requests daily. And if one VA restarts due to technical issues or upgrades, all devices will automatically use the second (or even third) VA deployed.
- VAs do not store data persistently. So even if the VMware or HyperV hosts running the VAs suffered a catastrophe, no loss of unrecoverable data would occur.

## Security Enforcement

### Do you protect my data, apps, and users from most cyber attacks?

**Absolutely!**

- Umbrella is built into the foundation of the internet and blocks requests to malicious and unwanted destinations before a connection is even established. So you can stop threats from ever reaching your network or endpoints, and you can contain command & control callbacks from already infected devices to prevent data exfiltration.
- The data and apps that your users and devices access are protected by extension.

### Do you protect my Website or DNS infrastructure from DDoS attacks

**No.**

- Umbrella doesn't host DNS records or protect your publicly accessible infrastructure that rely on DNS name servers being available.

### If Umbrella enforces security policies at the DNS and IP layers, why don't you protect me from all types of attacks?

**There are authoritative and recursive DNS services, which are different, but complementary.**

- Authoritative name servers host the information (i.e. domain name maps to IP address) that recursive DNS services resolve and send back for everything on the internet.
- Umbrella provides a recursive DNS service for just your users and devices, which is likely provided by your ISP(s) today, but only Umbrella delivers secure connectivity.

### Does Umbrella replace or layer on to existing network or endpoint security products?

**It depends on your use case.**

- Most customers do replace some existing appliance-based or proxy-based solutions with Umbrella. Our cloud security platform provides more effective security for the way the world works today without sacrificing performance or manageability.
- Umbrella is not intended to completely replace a firewall, which is designed to secure both internal and external network connections, whereas Umbrella is designed to secure external connections from any network. But it can eliminate the need for firewall threat feed add-ons, which rely on reactive technologies and reduce the appliance-based firewall's performance and manageability.
- We complement, rather than replace, endpoint security solutions (antivirus, endpoint threat detection, etc.). Umbrella acts as the first line of defense against threats on the internet and often stops malware before it ever reaches the endpoint.
- While customers often keep such products, Umbrella becomes their first line of defense inside and outside the network perimeter to add advanced threat protection.

### Does Umbrella provide web filtering and application controls?

**Yes, but it also depends on your use case.**

- The primary solutions that Umbrella delivers are network security, threat intelligence, and web filtering.
- Umbrella enforces filtering policies using 60 content categories that prevent connections to either web or non-web servers hosting pre-defined content or applications over any port or protocol.
- However, Umbrella is not intended to enforce data loss prevention policies, which address compliance concerns due to accidental disclosure of company or customer data. Such DLP solutions require proxying every web connection, which often adds significant latency and complexity.
- Also, Umbrella is not intended to enforce WAN optimization policies, which address bandwidth concerns due to applications or users that consume too much data.

### Can Umbrella block direct (non-DNS) IP connections?

**Yes, but there are differences between threat protection and content filtering.**

- Threat protection
  We can prevent data exfiltration as a result of command & control callbacks initiated by direct (non-DNS) IP connections. While less common, if a system is compromised with malware with hard-coded IP addresses, the Umbrella roaming client (for Windows or Mac OSX devices) will tunnel suspect IP connections to our cloud service and block malicious destinations.
- Content Filtering
  Due to the way that today's web servers and browsers work, users cannot simply circumvent acceptable use policies by entering IP addresses. Servers silently instruct browsers to download its Web content from one or more different domains. After the initial connection is established, several additional DNS requests are sent via the user's browser on the server's behalf, which are enforced as normal.