# Cisco Umbrella

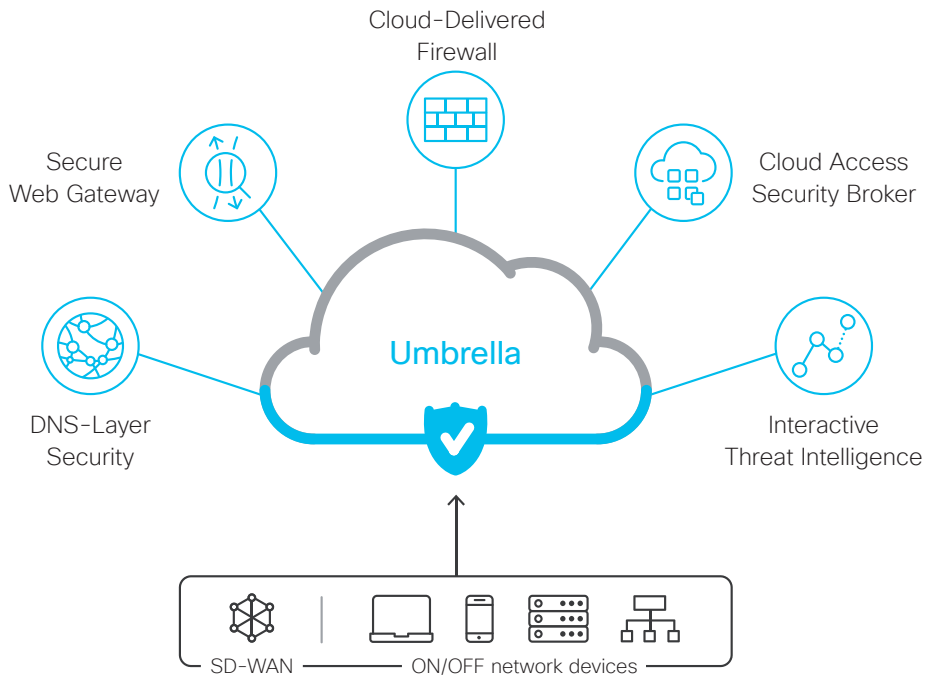
Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED



## Cisco Umbrella. Cloud Security Made Simple.

Cisco Umbrella uses the Internet's infrastructure to enforce security and block malicious activity before a connection is ever established. With this cloud-delivered service, there is no hardware to install and no software to update manually. You save time, reduce overhead, and get effective security that has a history of 100% uptime since 2006. Security doesn't have to be hard.
As a leading provider of recursive DNS service, we've helped businesses of all sizes and industries connect to the Internet with confidence. We've built our reputation on easy deployment and powerful protection anywhere users work.
To help organizations embrace direct internet access (DIA), in addition to DNS-layer security and interactive threat intelligence, Cisco Umbrella now includes secure web gateway, cloud-delivered firewall, and cloud access security broker (CASB) functionality, plus integration with Cisco SD-WAN, delivered from a single cloud security service.




## Highlights

- **DNS-Layer Security**
  Umbrella's DNS-layer security provides the fastest, easiest way to improve your security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.
- **Secure Web Gateway (SWG)**
  Umbrella's secure web gateway logs and inspects web traffic for full visibility, URL and application controls, and protection against malware. Use IPsec tunnels, PAC files, AnyConnect, or proxy chaining to forward traffic to our cloud-based proxy servers to enforce acceptable use policies and block advanced threats.
- **Cloud-Delivered Firewall**
  Umbrella's firewall logs all activity and blocks unwanted traffic using IP, port, and protocol rules. To forward traffic, simply configure an IPsec tunnel from any network device. As new tunnels are created, policies are automatically applied for easy setup and consistent enforcement everywhere.
- **Cloud Access Security Broker (CASB)**
  Umbrella exposes shadow IT by providing the ability to detect and report on cloud applications in use across your organization. For discovered apps, you will be able to view details on vendor, category, and activity volume to better manage cloud adoption and reduce risk. Risky apps can be blocked completely, or for a set of popular SaaS apps, you can apply granular activity controls to stop posts, shares, attachments, or uploads.
- **Interactive Threat Intelligence**
  Our unique view of the internet gives us unprecedented insight into malicious domains, IPs, and URLs. Available via a console and API, Umbrella Investigate provides real-time context on malware, phishing, botnets, trojans, and other threats enabling faster incident investigation and response.

© 2020 Cisco and/or its affiliates. All rights reserved.

# Cisco Umbrella

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED



## Cisco Umbrella Package Comparison

| | | DNS Security Essentials | DNS Security Advantage | Secure Internet Gateway Essentials |
|---|---|---|---|---|
| DNS-Layer Security | Block domains associated with phishing, malware, botnets, and other high risk categories (cryptomining, newly seen domains, etc.) | ✓ | ✓ | ✓ |
| | Block domains based on partner integrations (Splunk, Anomali, and others) and custom lists using our enforcement API | ✓ | ✓ | ✓ |
| | Block direct-to-IP traffic for C2 callbacks that bypass DNS*1 | | ✓ | ✓ |
| Secure Web Gateway | Proxy web traffic for inspection | | Risky domains via selective proxy | All web traffic |
| | Decrypt and inspect SSL (HTTPS) traffic | | Risky domains via selective proxy | ✓ |
| | Enable web filtering | By domain or domain category | By domain or domain category | By domain, URL, or category |
| | Create custom block/allow lists | Of domains | Of domains | Of URLs |
| | Block URLs based on Cisco Talos and third party feeds, and block files based on AV engine and Cisco Advanced Malware Protection (AMP) data | | Risky domains via selective proxy | ✓ |
| | Use Cisco Threat Grid cloud sandbox environment to analyze suspicious files (200 files/day) | | | ✓ |
| | Use retrospective security to identify previously-benign files that became malicious | | | ✓ |
| Cloud-Delivered Firewall | Create layer 3/layer 4 policies to block specific IPs, ports, and protocols | | | ✓ |
| | Use IPsec tunnel termination | | | ✓ |
| Cloud Access Security Broker | Discover and block shadow IT (based on domains) with our App Discovery report | ✓ | ✓ | ✓ |
| | Discover and block shadow IT (based on URLs) with App Discovery report | | | ✓ |
| | Create policies with granular controls (block uploads, attachments, and posts) for select apps | | | ✓ |
| Umbrella Investigate | Access Investigate's web console for interactive threat intelligence (5 logins) | | ✓ | ✓ |
| | Use the Investigate on-demand enrichment API to enrich other tools/systems with domain, URL, IP, and file threat intelligence (2,000 requests per day) | | ✓ | ✓ |
| | Integrate with Cisco Threat Response to aggregate threat activity across Cisco AMP, Threat Grid, Email Security, NGFW, and Umbrella | With enforcement API only | ✓ | ✓ |

*1 Endpoint footprint (Umbrella Roaming Client, Umbrella Chromebook Client, or Umbrella Roaming Security Module for AnyConnect) is required.

© 2020 Cisco and/or its affiliates. All rights reserved.

# Cisco Umbrella

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED



## Cisco Umbrella DNS Security Essentials License NEW

| Product SKU*1 | Description |
|---|---|
| UMB-DNS-ESS-K9 | Umbrella DNS Security Essentials per User License (1 ~ Users) |

*1 UMB-SEC-SUB is required in CCW. See Ordering Guide for details.

## Cisco Umbrella DNS Security Advantage License NEW

| Product SKU*1 | Description |
|---|---|
| UMB-DNS-ADV-K9 | Umbrella DNS Security Advantage per User License (1 ~ Users) |

*1 UMB-SEC-SUB is required in CCW. See Ordering Guide for details.

## Cisco Umbrella Secure Internet Gateway Essentials License NEW

| Product SKU*1 | Description |
|---|---|
| UMB-SIG-ESS-K9 | Umbrella Secure Internet Gateway Essentials per User License (1 ~ Users) |

*1 UMB-SEC-SUB is required in CCW. See Ordering Guide for details.

### Ordering and Licensing Guide

Cisco Umbrella is licensed on a subscription basis. Each customer has only one subscription, though each subscription may comprise multiple products (Umbrella, Investigate, and others). Subscriptions are available for standard term lengths of 12, 36, and 60 months. Following the completion of the term, the subscription will be renewed automatically for an additional 12-month term unless the renewal is canceled or auto-renewal was deselected at the time of the initial order. Subscriptions can be changed mid-term or manually renewed.

### Seat-based Licensing

Cisco Umbrella DNS Security and Secure Internet Gateway are licensed per seat. A seat is defined as an Internet-connected user who may have access to the service. Seat counts are independent of the number of devices or endpoints protected.
Minimum one seat is required to purchase.

## Cisco Umbrella Roaming License

| Product SKU*1 | Description |
|---|---|
| UMB-ROAM | Umbrella Roaming per User License |

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

## Cisco Umbrella Branch Licenses

| Product SKU*1 | Description |
|---|---|
| UMB-BRAN-RV | Umbrella Branch License for Cisco RV 340 Series |
| UMB-BRAN-1100 | Umbrella Branch License for Cisco ISR 1100 Series |
| UMB-BRAN-4221 | Umbrella Branch License for Cisco ISR 4321 |
| UMB-BRAN-4321 | Umbrella Branch License for Cisco ISR 4321 |
| UMB-BRAN-4331 | Umbrella Branch License for Cisco ISR 4331 |
| UMB-BRAN-4351 | Umbrella Branch License for Cisco ISR 4351 |
| UMB-BRAN-4431 | Umbrella Branch License for Cisco ISR 4431 |
| UMB-BRAN-4451 | Umbrella Branch License for Cisco ISR 4451 |

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

## Cisco Umbrella WLAN License

| Product SKU*1 | Description |
|---|---|
| UMB-WLAN | Umbrella WLAN per Access Point License (5 ~ APs) |

*1 UMB-SEC-SUB is required in CCW. See Ordering Guide for details.

© 2020 Cisco and/or its affiliates. All rights reserved.

# Cisco Umbrella

Expansion of Free Security Offerings
bit.ly/2UqY86W

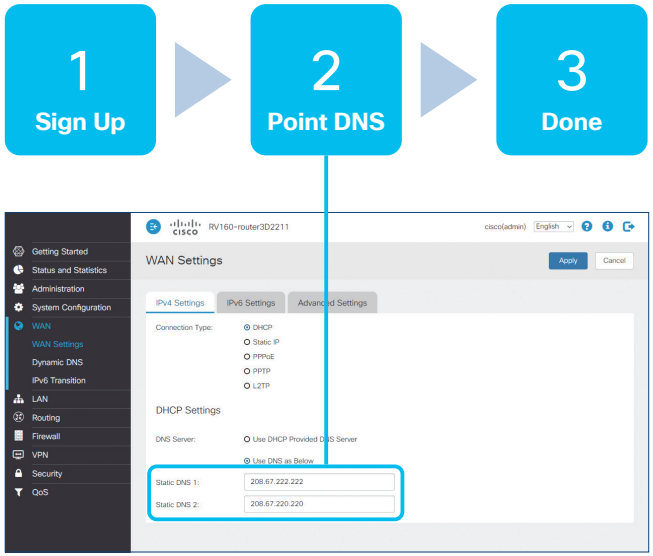
CISCO DESIGNED

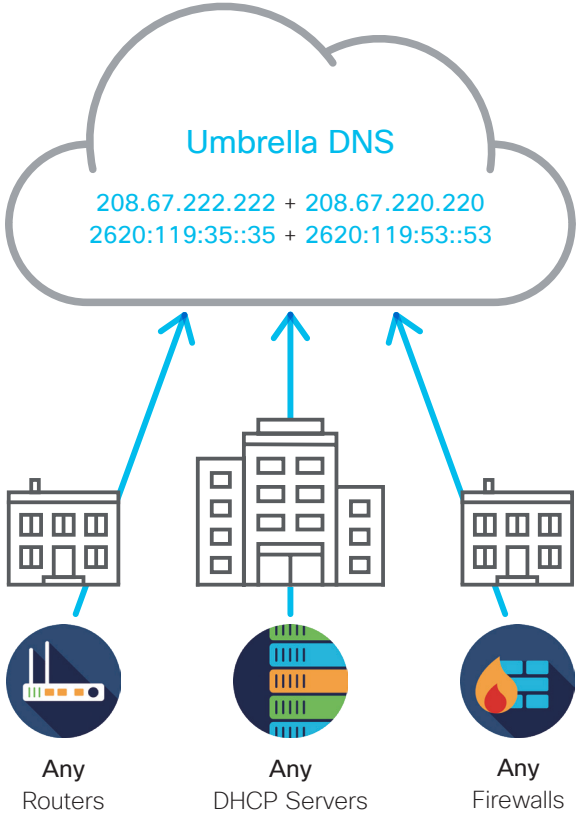


## Enterprise-wide Deployment in Minutes

Cisco Umbrella is the fastest and easiest way to protect all of your users in minutes. Because it is delivered from the cloud, there is no hardware to install or software to manually update. You can provision all on-network devices — including BYOD and IoT — in minutes and use your existing Cisco footprint to quickly provision thousands of network egresses and roaming laptops.
Additionally, with the Cisco Security Connector app, you can use the Umbrella extension to protect supervised iOS 11.3 or higher devices.

### How Easy Is It to Deploy Umbrella?




© 2020 Cisco and/or its affiliates. All rights reserved.

# Cisco Umbrella

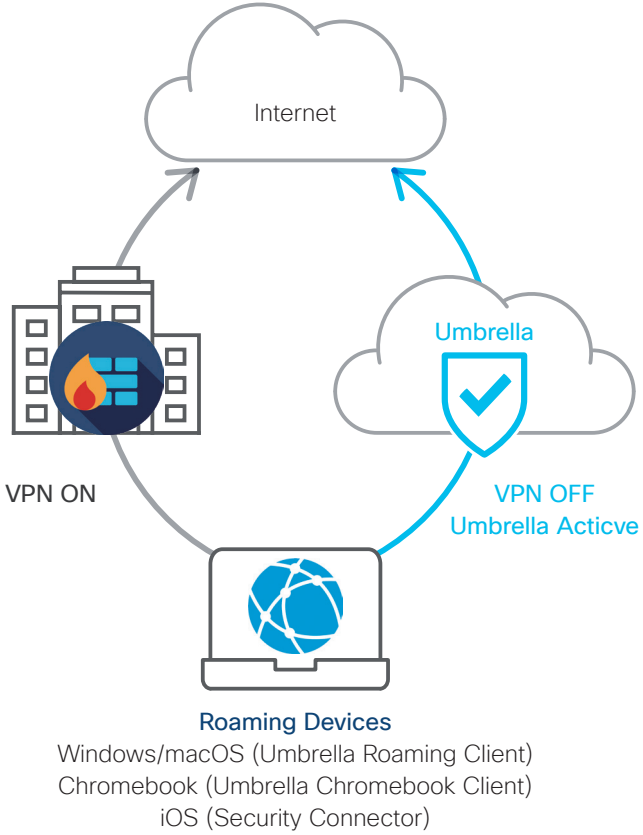
Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED



## Off-Network Security without VPN

Cisco Umbrella protects employees when they are off the VPN by blocking malicious domain requests and IP responses as DNS queries are resolved. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. This protects against malware, command & control (C2) callbacks, and phishing attacks and helps detect the exfiltration of data over any port.




### The Way Your Employees Work Has Changed

82% of your workers admit to not always using the VPN*1
Employees are using more cloud apps for work and leveraging their work laptops for personal use—the reality is that not every connection goes through the VPN. Your network extends beyond the perimeter, and your security must too.

49% of your workforce is mobile and under defended*2
Zero-day malware spikes at night and on weekends when we're roaming and attackers know we're vulnerable. In fact, 22% of malicious email links are clicked when roaming.*3 While security may never stop 100% of the threats, it must work 100% of the time.

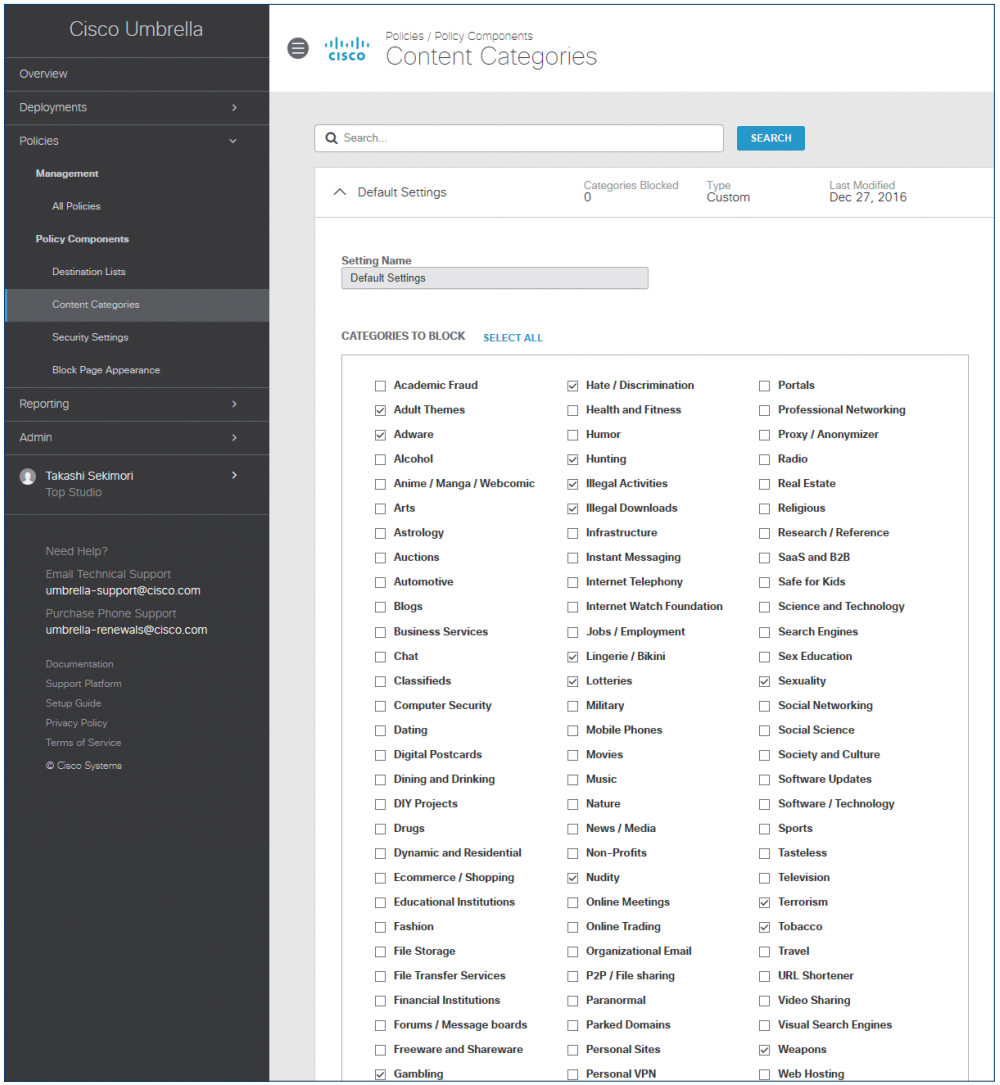
*1 cs.co/IDG-survey *2 cs.co/sans-survey *3 cs.co/proofpoint-report

© 2020 Cisco and/or its affiliates. All rights reserved.

## Manage Flexible, Location-aware Policies

Cisco Umbrella's 80+ content categories cover millions of domains (and billions of web pages) to give you control over which sites can be accessed by users on your network and by roaming users. The easy-to-use, cloud-delivered administration console enables you to quickly set up, manage, and test different acceptable use policies per network, group, user, device, or IP address, giving you greater control of your organization's internet usage. You even have the flexibility to set up different policies depending on whether users are on or off the corporate network.

Umbrella enables you to customize our category-based filtering to meet each network's unique needs to enable you to meet specific compliance requirements. Quickly create exceptions to allow or block specific domains, regardless of whether it is in a category that is allowed or blocked. Our 80+ content categories empower you to enforce acceptable web use to comply with internal policies or external regulations such as CIPA. We are also a member of the Internet Watch Foundation (IWF), enabling you to block their list of child sexual abuse sites.

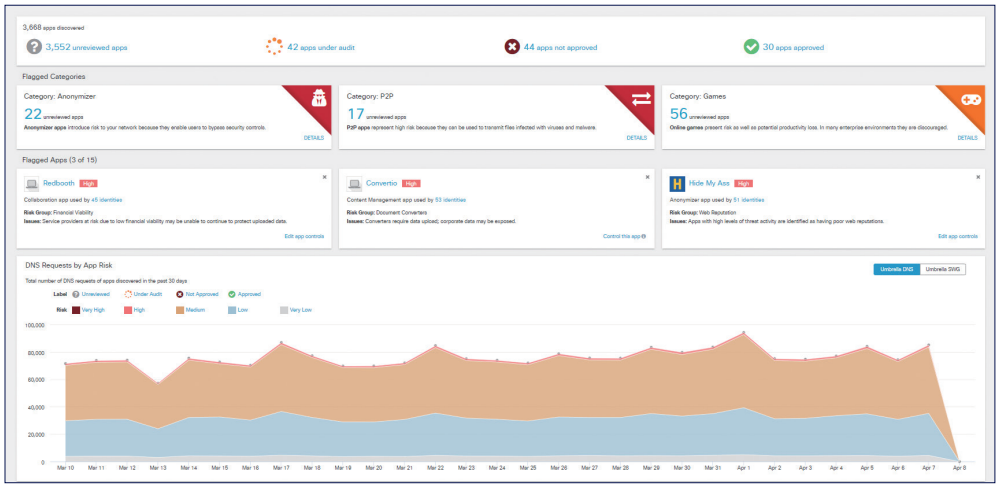



© 2020 Cisco and/or its affiliates. All rights reserved.

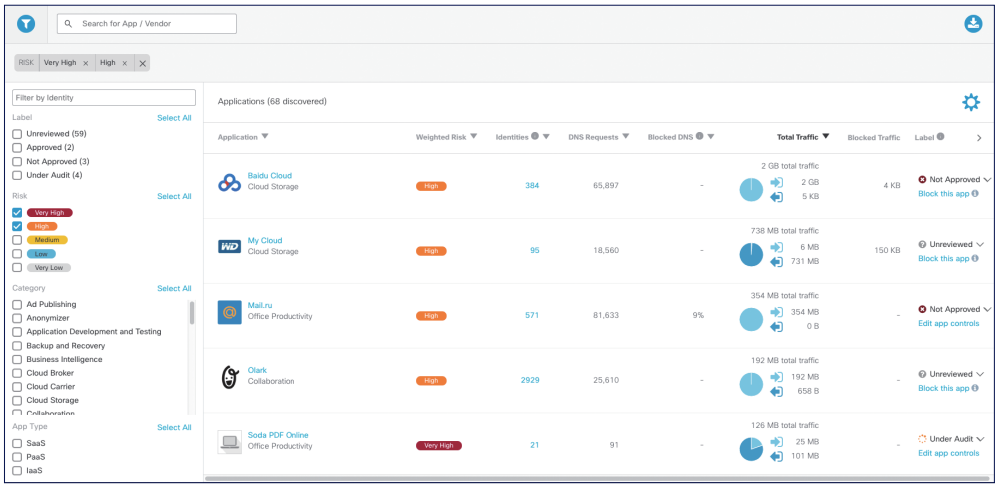
## Expose Shadow IT and Manage Cloud Adoption

Cloud usage is continuing to expand as end-users and departments become more comfortable acquiring cloud services. The typical organization is only aware of a small fraction of its overall cloud activity. The lack of a coordinated cloud enablement strategy leads to a broad set of productivity, expense, security, and support issues.

The **App Discovery** report included in Cisco Umbrella provides full visibility and risk information to manage cloud adoption in a secure and organized fashion. Once decisions are made about specific apps, you can block access to applications that are not approved to reduce the risk of sensitive data loss, account compromise, and malware infection.




The App Discovery dashboard provides an overview of the number of app requests by date and risk level to show patterns and changes over time. The most recent set of discovered and unreviewed apps are highlighted for easy access and a chart showing the number of apps in each major category is provided with a breakdown by risk level. These summary charts allow point and click access to more detailed information on the category or individual application to simplify common administrator tasks.




The Apps Grid report provides key details on all applications that have been discovered, including the app and vendor name, category, weighted risk level, number of users, number of requests, and current status. This report can be segmented and filtered into groups for deeper analysis by category, risk level, or number of users to provide views that assist with the organization and management of cloud adoption.

© 2020 Cisco and/or its affiliates. All rights reserved.

# Cisco Umbrella

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED



## Simple and Effective Protection for Corporate and Guest Wi-Fi

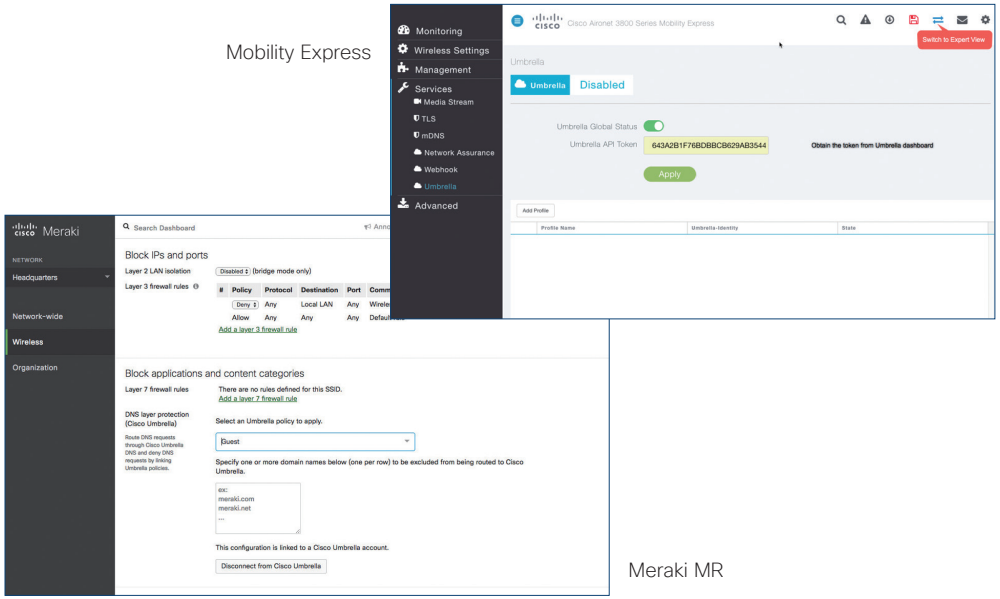
The Cisco Umbrella Wireless LAN (WLAN) package provides the first line of defense against threats for Wi-Fi connections. It offers the simplest, fastest way to protect every user on your Wi-Fi network.

Umbrella WLAN protects employees and guests who are accessing the internet from wireless access points. By enforcing security at the DNS layer, connections to unsafe sites are never established and malicious files are never downloaded. This prevents malware from infecting devices and stops attacks from exfiltrating data over any port and protocol. Umbrella WLAN also brings a simple-to-use content filtering solution to your Wi-Fi network. It stops guests and corporate users from accessing inappropriate content, based on company policy. This keeps users happy with safe internet access, while also protecting your business.

Umbrella WLAN is the simplest way to protect any device accessing your wireless network — there's no action required from end-users for protection. Whether it's a corporate device, employee-owned, or customer-owned device, Umbrella WLAN adds an easy, but very effective layer of protection.

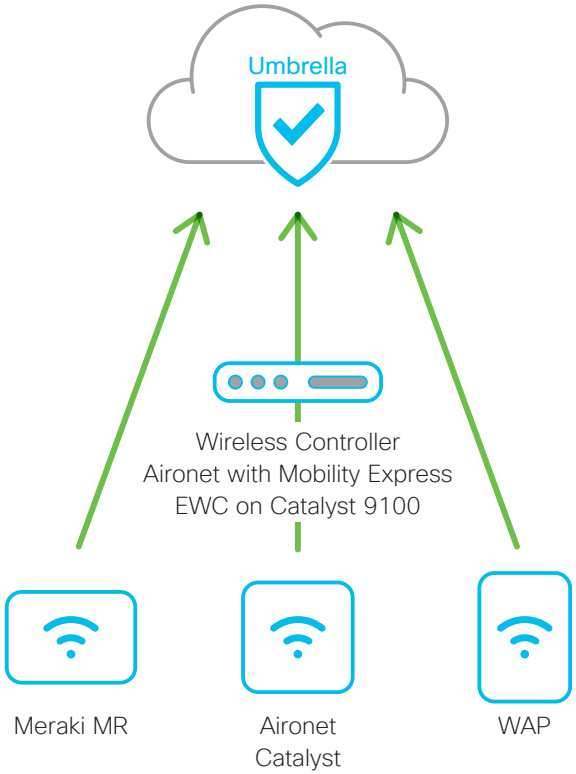
Umbrella WLAN works across a broad portfolio of wireless controllers and access points. Built-in integrations with the Cisco WAP125/WAP581, Cisco Aironet Access Points with Mobility Express, Cisco Embedded Wireless Controller (EWC) on Catalyst 9100 Access Points, Cisco Wireless Controllers, and Cisco Meraki MR Cloud Managed Access Points provides additional ease of use and granularity.

Mobility Express




Meraki MR

You can deploy Umbrella in minutes across your access points.
Simply input the API key and secret from Umbrella into the AP's GUI.




© 2020 Cisco and/or its affiliates. All rights reserved.

# Cisco Umbrella

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED

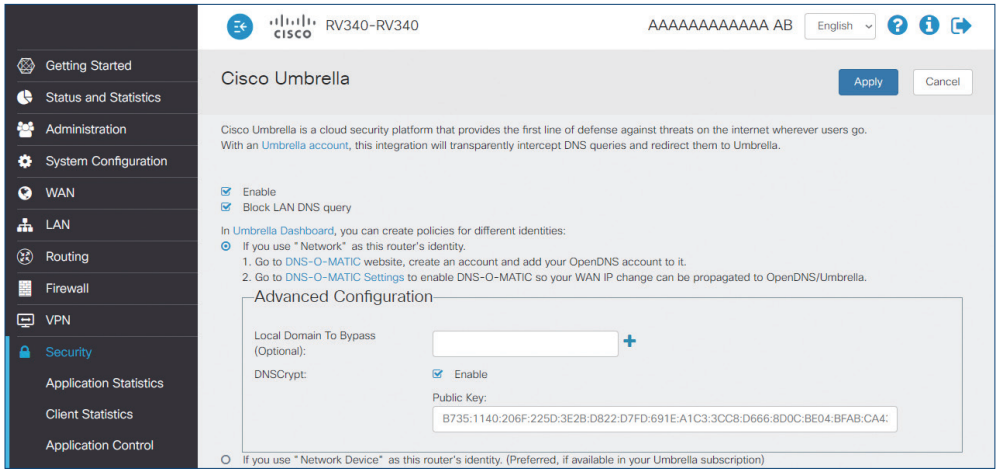


## The Simplest Way to Provide DNS Security for Direct Internet Access (DIA) from Branch Offices from Branch

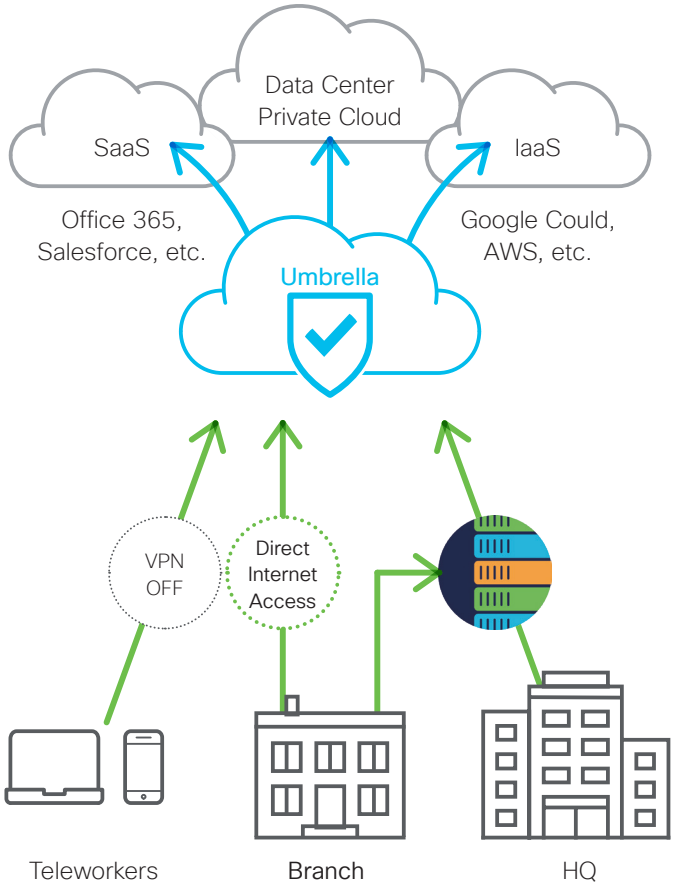
The traditional WAN was built to give branch offices and roaming users access to IT resources within private data centers. But today, as networks become more decentralized and users connect directly to SaaS applications, backhauling traffic to apply security policies just isn't efficient. And that's not the only problem. Backhauling internet-bound traffic is expensive, and it adds latency. So users get frustrated — and thwarted — in their attempt to get work done. That's why so many branch offices are migrating to DIA.

The **Cisco Umbrella Branch** package is a cloud-delivered security service for the **Cisco RV 340 Series** and **Cisco ISR 1100/4000 Series** routers. It provides the first layer of defense against threats at branch offices. And it offers the simplest, fastest way to protect every device on your branch network. You gain visibility and enforcement at the DNS-layer, so you can block requests to malicious domains and IPs before a connection is ever made.

Umbrella Branch protects employees and guests in distributed branch offices — like those in retail, finance, hospitality, and education. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. This prevents malware from infecting devices and stops attacks from exfiltrating data over any port.




You can deploy Umbrella in minutes on your RV 340 series router.
Simply input the API key and secret from Umbrella into the router's GUI.

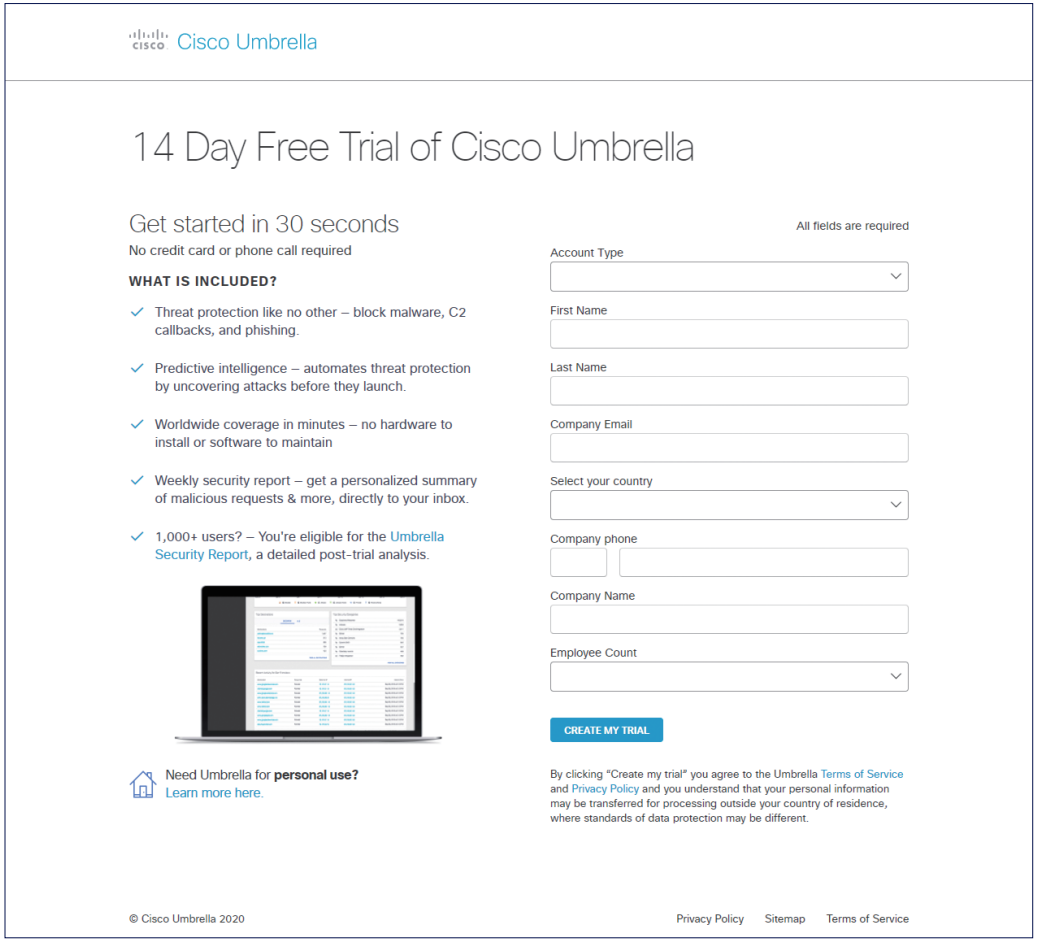



© 2020 Cisco and/or its affiliates. All rights reserved.

## Free Umbrella 14-Day Trial

If you want to add an additional layer of DNS security to your router or firewall, try our free trial. You can set it up yourself in less than five minutes, no credit card or phone call required.

WEB signup.umbrella.com




## Expansion of Free Security Offerings

With this offer, existing customers can exceed their user limit to support an increase in remote workers, and new customers can access a free license that can be extended from the initial 14-day period to 90 days.

WEB bit.ly/2UqY86W

| | Existing Customers | New Customers |
|---|---|---|
| Offer Details | Can exceed purchased user limit until end of offer period (1 July 2020) | Can extend trial period of Umbrella from 14 to 90 days |
| Offer Period | Through 1 July 2020 | 90 days from activation |
| Country/Region Availability | All regions where Umbrella is available for sale today. | |
| Seller Action | No action is required for the seller. Email can be sent to customers impacted by COVID-19 and require support from Cisco. | Direct request via signup.umbrella.com (14-day trial), which means Umbrella BDR team will respond per existing process.<br>To extend the trial duration beyond 14 days to 90 days, the Cisco seller must request trial duration to be 90 days. |
| Post-Offer Sales Engagement | At the end of the offer period, customers will need to purchase the additional user licenses or reduce their usage to purchased user limits. | At the end of the trial, customers must purchase the required licenses or have their service automatically converted to DNS monitoring. |
| Technical On-boarding | None, customers are already deployed. The configuration of additional users is an existing process for the customer. | Customers can easily self-implement using documentation here.<br>Assistance can be provided via sales team and technical support. |
| Support Details | Customers will be entitled to the same technical support they have purchased. | Technical support will continue to provide assistance during trial as part of normal process. |

© 2020 Cisco and/or its affiliates. All rights reserved.