In order to make sure you have all the information you need about 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: www.opendns.com/enterprise-security/resources/#filter=.techdocs

Packaging & Pricing

How do you license your products?

We license by the total # 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 never license by the # of devices used/provisioned, networks provisioned, AD components deployed, or DNS and Web traffic volume. However, the # of concurrent or active (vs. total) users is not used 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 OpenDNS 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 your products?

We offer three product packages.

- Umbrella Professional is priced lowest, but delivers the fewest capabilities.
- Umbrella Insights balances the price with the capabilities delivered to suit most organizations.
- Umbrella Platform is priced highest, and delivers the most capabilities.
- 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 ➔ OpenDNS 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 OpenDNS Global Network.
- We started building the OpenDNS 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 (https://www.opendns.com/data-center-locations/). And refer to our technical documentation 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 on or off our corporate networks?

Roaming Client ➔ OpenDNS Global Network.
- Our Roaming Client tags, encrypts and forwards DNS queries bound for the Internet to the OpenDNS Global Network so per-device security policies can be enforced everywhere without latency or complexity.
- Our 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 secure mobile devices on or off corporate networks, and even carrier 3/4G connections?

Mobile App ➔ OpenDNS Global Network.
- Our Mobile App encrypts and forwards all TCP/IP traffic to the OpenDNS Global Network over WiFi and 3/4G connections. It keeps traffic safe from rogue access points, and enforces per-device security policies.
- Our Mobile App for iOS can be provisioned by emailing a profile configuration to the end user, pushing the profile configuration transparently via a third-party or Apple MDM (mobile device management) solution, or by downloading the Umbrella Mobile App via the iTunes store.

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

Clientless DHCP ➔ Virtual Appliance ➔ OpenDNS 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.
- Our Virtual Appliance tags and forwards DNS queries bound for the Internet to the OpenDNS 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?

Umbrella Connector ➔ 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.
## Technical Requirements

<table>
<thead>
<tr>
<th>PROVISION...</th>
<th>Supported Platforms</th>
<th>Non-Supported Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming Client</td>
<td>• Windows XP, Vista, 7, 8 or 10&lt;br&gt;• OSX 10.7 or later</td>
<td>• Windows 2000 or earlier&lt;br&gt;• OSX 10.6 or earlier</td>
</tr>
<tr>
<td>Mobile App</td>
<td>• iOS 5.1.1 or later&lt;br&gt;• iPhones, iPads, iPods</td>
<td>• iOS 5.1.0 or earlier&lt;br&gt;• Android, Blackberry, Windows 8 RT, others&lt;br&gt;• Concurrent VPN used to access corporate intranet</td>
</tr>
<tr>
<td>Virtual Appliance</td>
<td>• VMware ESXi v4.1 update 2 or later&lt;br&gt;• Hyper-V for Windows Server 2008R2, 2012SP1, 2012R2&lt;br&gt;• Multiple sites with separate virtual host servers, or multiple locations linked to same virtual host server</td>
<td>• Hyper-V for Windows Server 2008&lt;br&gt;• Other VMware (Player, Workstation, Fusion)&lt;br&gt;• Others (Citrix Xen, VirtualBox, Parallels)&lt;br&gt;• NAT/proxy between devices and virtual host server&lt;br&gt;• Contact support for non-Microsoft DNS/DHCP</td>
</tr>
<tr>
<td>Connector</td>
<td>• Domain controllers on Windows Server 2012, 2008, 2003 R2 or SBS 2011&lt;br&gt;• Multiple domain controllers per AD site&lt;br&gt;• Single domain</td>
<td>• Domain controllers on Windows Server 2003 (non-R2) or 2000&lt;br&gt;• Multiple domains (or forests)</td>
</tr>
</tbody>
</table>

## Service Performance

### Will this service introduce any latency?

**Umbrella adds no net new latency.**

- Because with OpenDNS there is no need to reroute all connections through proxies or over VPNs to secure mobile users or remote offices.
- Today, your external DNS traffic by default is pointed to your ISP’s cloud-delivered recursive DNS service. Now, your external DNS traffic points to the OpenDNS 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/](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 OpenDNS Global Network has maintained 100% uptime since OpenDNS launched as an infrastructure company in 2006.
- We publicly display our operational system status and stats. [http://system.opendns.com/](http://system.opendns.com/)
- 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. providers.
How scalable are your Virtual Appliances?

Each Virtual Appliance (VA) instance can easily support 10,000s of concurrent users.

- Only one CPU core and 512MB or RAM 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 70+ 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 other cyber attacks?

Absolutely!

- By pointing only your external DNS traffic to OpenDNS, we allow users to connect to the Internet with confidence on any device, anywhere, every time.
- 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.

- OpenDNS doesn’t host DNS records or protect your publicly accessible infrastructure that rely on DNS name servers being available.
- We recommend that you use a complementary service such as CloudFlare (we’re not affiliated).

If OpenDNS 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.
- OpenDNS provides a recursive DNS service for just your users and devices, which is likely provided by your ISP(s) today, but only OpenDNS 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-delivered, DNS-based solution 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 does 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 antimalware solutions. Unlike these reactive signature-based solutions, Umbrella leverages our predictive signature-less security that blocks where malware is delivered from, or callbacks to, via Internet connections.
- 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 content 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 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 OpenDNS 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.

Does Umbrella provide mobile device management?

No. MDM solutions main focus is enforcing device security, not mobile network security.

- Umbrella uses a VPN tunnel for all TCP/IP traffic to secure communications over unsafe public networks and prevent access to mobile threats or phishing sites via any app, port or protocol.
- If you already have an MDM solution, just layer Umbrella on top. Gartner recommends that Secure Web Gateway/Filtering and MDM solutions need to coexist.
- **MDM Use Case**: On-device data security, such as enforcing minimum password, remote data wipe or restricting apps.
- **Umbrella Use Case**: Network security, which reduces the risk of login credential theft or data breach via rogue Wi-Fi access points, phishing sites and mobile threats.