Enterprise-Grade Threat Protection Like No Other.

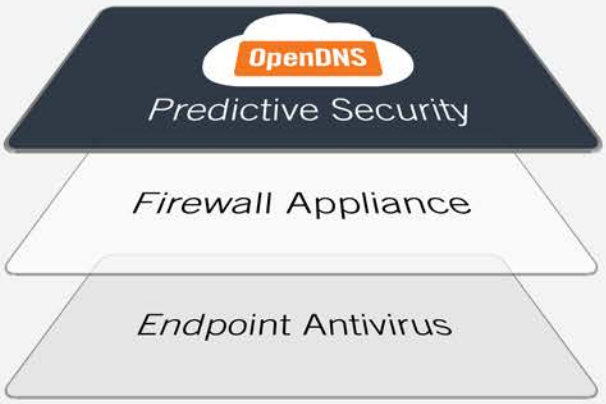
Cloud-delivered network security and Web filtering that protects any device, anywhere.

Umbrella not only blocks malware, botnets and phishing over any port, protocol or app, but also detects and contains advanced attacks before they can cause damage. It uses big-data analytics and machine learning to automate protection against both known and unknown threats. Umbrella stays always up-to-date with no hardware to install, no software to maintain and no admin intervention required.

Unlike security products that react to known threats and add latency by re-routing every Internet connection through proxy or VPN gateways, OpenDNS uses predictive intelligence to discover unknown threats and adds no latency. OpenDNS Global Network handles more than two percent of the world's Internet requests daily with 100 percent uptime.

Security for the way the world works today

- The move to cloud applications and mobile users results in erosion of the network perimeter.
- Cybercriminals, nation states, and hacktivists are sharing infrastructure and code to stage advanced targeted attacks designed to manipulate or steal data.
- Umbrella provides security against Internet threats, advanced attacks, and security breaches everywhere.



Comprehensive Threat Protection

OpenDNS not only blocks malware, botnets and phishing over any port, protocol or app, but also detects and contains advanced attacks before they can cause damage.

Pinpoint devices infected or users targeted by advanced attacks to reduce the time to remediation.
Not all attacks are equally dangerous. OpenDNS compares your blocked threat requests to our global visibility—so you can prioritize and reduce response times to sophisticated or targeted attacks.

View new network security activity in real time with globally aggregated reports.
Other solutions limit and fragment your visibility by the activity detected per appliance deployed or per port proxied. OpenDNS restores loss visibility and control because we aggregate and display global activity in under one minute.

Apply consistent network security and acceptable use policies everywhere based on your needs.
Centralized location-based policy configuration per network, device or user reduces administrative burdens. And customizable block lists and pages with flexible bypass options enable you to tailor policies to your requirements. Optionally, filter up to 60 content categories to maintain compliance.

Cloud infrastructure trusted by enterprises and SMBs worldwide

- In 2006, our mission was to build the most reliable DNS service on the planet, and unlike others, we have always provided operational visibility. Just visit http://system.opendns.com
- Today, our security uses the same foundation trusted by over 50 million daily-active users across 160 countries, including 10,000 businesses and ISPs.

Worldwide Coverage in Minutes

OpenDNS protects devices anywhere and stays always up-to-date with no hardware to install, no software to maintain and no admin intervention required.

Instantly secure devices–even those you don't own–across all decentralized networks via clientless DHCP.
Change one setting native to all Internet gateways (e.g. routers, access points) and DHCP does the rest. Optionally, our Virtual Appliance and Connector components enable you to identify internal networks or Active Directory users infected or targeted by attacks, without touching devices or re-authenticating users. Both components are updated automatically without admin intervention or service interruption as soon as a new version is available.

Easily secure devices inside or outside the network perimeter via auto-updated lightweight agents.
Our Roaming Client and Mobile App can be deployed to devices in minutes using Windows GPO, Apple Remote Desktop or an MDM solution. The client offers command-line installations, and can be run in "head" or "headless" mode. Both agents are updated automatically without user intervention or reboots as soon as a new version is available.

Proven Reliability

The OpenDNS Global Network handles more than two percent of the world's Internet requests daily with 100 percent uptime.

To be more precise, over 65,000,000,000,000 requests have been resolved with zero down time.
Every HTTPS Web post, FTP upload, RTSP video stream and P2P file share is preceded by a DNS request. With Umbrella, infrastructures hosting malware, botnet or phishing threats are blocked from resolving such requests, keeping attacks from ever reaching OpenDNS customers.

Our cloud infrastructure uses Anycast routing that is extensively peered at major Internet exchanges.

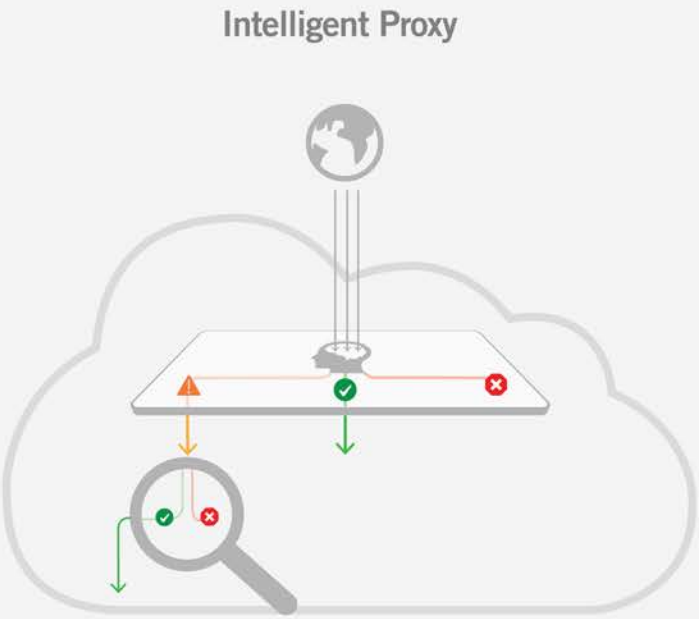
(1) It allows OpenDNS to easily scale our service globally for customers by just adding more servers and data centers, all with the same IP address. So users never experience degraded performance.

(2) It makes a failover event within a data center or globally between data centers transparent to customers. There is no need for making changes to load balancers, proxy servers or DNS servers because the IP address will not change.

(3) It reduces the DNS resolution round trip time for customers because we have the shortest possible routes to all users. Building direct peered connections with other networks increases the number of available paths to our users and content providers or ISPs.

The world's first Intelligent Proxy

- Traditional security solutions reroute every Web connection through a proxy, which slows traffic, invades privacy, and can break some sites. Yet the vast majority of malware, botnet and phishing threats are hosted at domains or IPs that are entirely malicious. No proxy is required to block them.
- OpenDNS built a faster, easier and smarter proxy. One that achieves the security benefits of pure-proxy solutions without degrading the performance and availability of corporate networks by leveraging our DNS layer.
- And unlike Web-only solutions, Umbrella secures every Web and non-Web connection to detect infected devices that use multi-protocol callbacks to botnet command and control infrastructures.



Predictive Intelligence

OpenDNS uses Big Data analytics and machine learning to automate protection against both known and unknown threats.

Layer predictive security to complement reactive signature-based or real-time behavior-based security.
Traditional and even "next-generation" security solutions are reactive in nature. They rely on attack data, malware samples, and Web or email traffic collection to identify new threats. They also depend on researchers to facilitate the process. And many advanced attacks continue to evade behavioral sandboxes and reputation systems. In short, collect-and-react technologies simply aren't scalable. What makes OpenDNS unique is acquiring data unrivaled in scale and scope, and pioneering security automation. So our researchers do not become a bottleneck to keep our customers protected.

Identifies the infrastructures that deliver attacks by observing the 'threatcrumbs' they leave behind.
The OpenDNS processes over one million malicious and non-malicious Internet events per second. Using graph theory and machine learning it observes relationships forming between domains, IPs and known bad infrastructures. Ultimately, it automates discovering and predicting when and where on the Internet new attacks are being staged. Thereby, protecting against known and unknown threats.

No Added Latency

With OpenDNS there is no need to reroute every connection through proxy or VPN gateways to secure mobile users or remote offices.

No extra "hops" because DNS traffic is resolved in the cloud by OpenDNS rather than the ISP.
Mobile users or remote offices no longer need to route connections over VPN back to the perimeter for network security. And devices inside the perimeter no longer need to route every connection through another appliance and/or proxy-based enforcement point.

Only a few connections are routed through our proxy when we must inspect below the DNS layer.
Proxying every Web connection slows traffic, invades privacy, and can break some sites. Based on intelligence for which domains are partially malicious or suspicious, OpenDNS transparently routes and proxies these connections that require deeper inspection below the domain- or IP-level.

Resolve DNS requests faster than ever before.
Our world-class infrastructure team is obsessed with inventing new technologies not only to use DNS to intelligently route our users around Internet threats but also to speed up the Internet and move the state of the art for the Domain Name System forward. We have pioneered some of the foremost innovations the DNS has seen in its lifetime. The result is not only secure connectivity, but also a faster connectivity.

Contact Us

Have a question?

877.942.2568

sales@trapptechnology.com

www.trapptechnology.com

trapp TECHNOLOGY