

Does OpenDNS replace antivirus clients or firewalls?

OpenDNS is a new layer of Internet security that complements your existing endpoint and network security solutions to provide dramatically stronger protection from malware, botnets and other Internet-based threats. We recommend you keep your antivirus clients installed since data is run and retained on the endpoint, not in transit between hosts. We also recommend you keep your firewalls to control internal and external network access permissions and traffic. OpenDNS transparently makes your users, devices and networks more secure by providing deep inspection of DNS traffic to let in the good DNS and block the bad DNS (malware drop sites, botnet command and control servers, phishing sites, etc.) without adding latency or complexity. Unlike proxy-based solutions that slow down your network and add single points of failure, OpenDNS doesn't increase overhead.

How is OpenDNS different than any other security software or appliances on the market?

Unlike traditional security software or appliances, OpenDNS is the only vendor securing the network perimeter at the DNS layer. Essentially, you're adding a hardened outer shell, proactively sinkholing (aka. blocking) bi-directional Internet connections to servers that host threats such as inbound malware or phishing attacks and outbound botnet data leaks without the traffic ever crossing your network perimeter; yet, still allowing your network to communicate with safe servers hosting applications and web content. DNS is the "choke-point" for nearly every network service on the Internet, good or bad, and without OpenDNS most organizations simply allow all DNS in and out of their network like a fire hose.

Does OpenDNS only screen Web traffic?

OpenDNS can block all bi-directional traffic between all malicious applications that rely on DNS, not just inbound traffic from malicious Websites to the web browser as proxy services do. **This includes malware that uses DNS to "phone home" over hundreds of non-HTTP/S protocols (i.e. IRC) and thousands of non-80/443 ports, a major point of differentiation from other security vendors.** Any applications that connect to your network and use DNS (which is nearly all of them) – file transfer apps, Web browsers, IM apps, and more – are protected.

Doesn't a UTM (Unified Threat Management) or NGFW (Next Generation Firewall) solution provide all the protection I need?

Firewalls already have a lot of settings to enforce within the network perimeter, and even the best are quite complex to manage requiring significant training. Adding multiple security features increases this complexity further, often compromises the user experience to adequately scale, and usually each added commodity feature adds relatively little efficacy to securing your users and devices. We are not aware of any solution in the market that dives deep into DNS traffic and provides anything like the protection offered by OpenDNS.

Can you substantiate your claims to block botnets and malware?

OpenDNS blocked over 750 million DNS queries to servers hosting security threats just in September 2011, which increases every month. To take this staggering number down to a per-customer level, on average, we block 4 DNS queries to known security threats every hour for each Enterprise network, or 1,500 over the span of a month. Some customers manage only a few networks whereas other customers use us to protect 1000s.

The leading institutions worldwide researching new methods for the discovery, detection, mitigation and prevention of botnets, polymorphic malware, and advanced persistent threats have produced over 30 publications over the last 2 years focused on inspecting DNS traffic. In fact, read most any security vendors' whitepaper or blog about the latest botnet or malware attack and you'll see they describe how the hackers try and use DNS to stay one step ahead of web proxies, URL filters, antivirus clients and firewalls.

Does OpenDNS allow me to filter by user?

You can grant granular time-based bypass permissions for individual users, or adjust settings on an IP by IP basis, that allow them to bypass your content filtering settings (either for a particular blocked domain or for all domains). Granular per-user Active Directory integration is in development.

Most security solutions require training to deploy, configure and maintain. How difficult is it to get started with OpenDNS?

It is extremely simple and takes less than 30 minutes to get started with OpenDNS. Since there is no software to install, IT Managers simply point their external DNS at each of their locations to OpenDNS' IP addresses and are ready to go. Some of the

largest companies in the world with hundreds or thousands of locations and networks have deployed OpenDNS quickly and effortlessly. Because we're cloud-based, you receive the benefits of product updates automatically, and because only DNS-based traffic is redirected, non-standard web-based authentications or encryptions do not require on-going exceptions created nor do they require re-routing through our global network.

Does OpenDNS secure mobile devices?

OpenDNS secures *any* device while it's connected to a network protected by OpenDNS' advanced security. It's entirely device-agnostic!

How do I find out how a site is categorized?

Our domain checker tool will tell you! Go to <http://www.opendns.com/community/domaintagging/>. Note: This tool is only for non-security related sites – malware and botnet related blocks will not appear for security reasons.

Why don't I see the content filtering section in my dashboard?

Business users on our Premium DNS product get speedy DNS resolution and basic stats. For advanced Web security features, like content filtering, upgrade to OpenDNS Enterprise.

How do I find out about pricing?

Our sales team will develop a custom quote for you and your organization that is based on the size of your deployment. We offer special packages for non-profits and schools.

How do I ensure that users on my network don't bypass OpenDNS?

In general, the easiest thing to do is limit System Administrator level permissions. Restricting a user's access is generally the first and easiest step anyone can take to securing their computers and network. Limited users do not have permissions to change the necessary TCP/IP settings to override the DNS settings set by DHCP and/or the actual System Administrator. Additionally, it is also best common practice to create a firewall rule blocking or transparently redirecting outbound port 53 (DNS) traffic to ensure all DNS traffic is going to OpenDNS' IP addresses.

While no solution is 100% effective (and why security experts recommend a defense-in-depth strategy), keep in mind that OpenDNS offers port-agnostic proxy and anonymizer blocking, so you can be confident that users won't be able to circumvent your content filtering settings using either method.

We occasionally are asked by customers, "what if the user types in a website's IP address into the browser?" With most modern websites, content is asynchronously downloaded to the browser using multiple requests to decrease page load time. These requests almost always refer back to a domain name. Furthermore, third-party scripts and any "AJAX" style requests must use the DNS in order to function. The browser must therefore resolve these subsequent domain requests, which will be blocked if not allowed with your policy settings. If you perform an evaluation of OpenDNS, you can experience this for yourself.

Does OpenDNS cache or optimize bandwidth of Internet traffic?

OpenDNS does help prevent bandwidth loss by controlling unacceptable Internet access to high bandwidth sites, while never adding a point of failure or latency in the network. However, if despite the commoditization of Internet access costs causing rapid price decreases, you still need to shape traffic, firewalls may be better suited to optimize such traffic both within and external to the network. This is why an effective and affordable defense-in-depth strategy is needed. It's worth noting that Web caching has become less effective due to dynamic user-generated content and diversity of content. Also, proxy-based solutions required to cache traffic do not scale well and often require a high amount of maintenance to create exceptions for problematic websites.

For a free trial or more information, contact our team:

1-877-811-2367 | www.opendns.com/work