

OpenDNS Presentation Slide Notes

Slide 1: Introduction

Your opportunity to welcome your audience and introduce the topic of your presentation — OpenDNS!

Slide 2: What is OpenDNS

Here is where you can provide some basic history and information about OpenDNS. If relevant to your audience, you can also mention that the company has been profitable since 2007, and is funded by Sequoia Capital and Greylock Partners.

Slide 3: What is DNS

If your audience isn't a technical one, this is a good time to explain what DNS is. Note that when an ISP's DNS server goes down, accessing websites becomes extremely difficult. That's just one of the reasons millions of people have chosen OpenDNS.

Slide 4: Company Query Milestones

Here's some context for what being the world's largest and fastest growing DNS provider means: We're doing 27 billion queries per day.

Slide 5: Key Features

This is the meat of the presentation — why would you want to use OpenDNS? You can quickly run through some of the key features OpenDNS offers and let your audience know you'll go more in-depth on these features in your presentation.

Slide 6: DNS Infrastructure

OpenDNS operated 11 datacenters around the globe. Two more are in the works, one in Asia and one in Europe. If your audience is more technical, now is a good time to tell them that OpenDNS uses Anycast routing technology. No matter where you are in the world, your DNS requests are answered by the closest datacenter, making your Internet faster and more reliable.

Slide 7: Web Content Filtering

There are 57 categories of content available for filtering, including adult, social networking, video streaming and P2P filesharing.

Data is gathered from Domain Tagging, a community effort to categorize websites. OpenDNS offers pre-configured levels of filtering (low, medium, high) or will allow you to set up custom filtering.

If you are presenting to an audience of educators, mention that OpenDNS can allow you to achieve CIPA compliance. The two requirements for CIPA compliance are 1) filtering adult content, and 2) being able to make reports on what's been accessed on the network. Both are possible.

Slide 8: Security

OpenDNS can block phishing, botnet and malware from getting onto your network. Additionally, OpenDNS offers the ability to block AdWare (which can sometimes come with spyware) via Web content filtering.

One source of phishing data OpenDNS uses is from PhishTank, a community-driven data-clearinghouse for phishing information. This data is used to help OpenDNS block 1 million phishing attempts per month that are made against its customers. All three OpenDNS services come with protection; OpenDNS Enterprise has additional Malware protection built in.

Slide 9: Cloud-Based Service

OpenDNS is cloud-based, which means there isn't an appliance needed for filtering or any software to install or configure (compared to a WebSense or Barracuda). This means once you've set up your filtering options, new additions are automatically added. There aren't any manual updates required, and filtering is constantly being updated to reflect what's out there.

For networks with multiple locations — school districts, large retail chains, etc – this makes managing the network a much more straightforward process, since going to each physical site is no longer required.

Slide 10: Free Different OpenDNS Services

There are three OpenDNS services offered. OpenDNS Basic is free. The New York Times' David Pogue recently called it "One of the last great freebies of the Web."

OpenDNS Deluxe and Enterprise are more geared toward business customers and offer some additional features, including additional whitelist/blacklist options and enhanced malware protection.

Slide 11: Q & A