

Securing Inbound and Outbound Communications at the DNS Layer

The domain name system (DNS) is one of the most critical elements in the network, and nearly all network applications rely on DNS to establish connectivity between hosts. Due to its criticality, DNS is often deliberately left open and unfiltered on corporate firewalls, effectively being a fire hose for information entering and exiting your network. As a consequence of this historical trend by security vendors to ignore DNS it is quickly becoming a favorite of hackers, botnet owners, malware authors, and other malicious actors on the Internet.

Unlike exiting Web security applications and appliances, **OpenDNS Enterprise is the only enterprise-grade security solution to provide complete inspection, filtering, protection and reporting on the DNS traffic entering and exiting your network, enabling complete inbound and outbound network protection for IT administrators.**

OpenDNS Enterprise proactively stops threats designed to infect your network's computers – reducing employee productivity, compromising sensitive (proprietary) information, and increasing costs. Malware (inbound) and botnet (outbound) infections can seize network resources to commit denial of service attacks, steal confidential data from within your network, and waste precious bandwidth and computer resources.

Consider a compromised machine on your network, infected via a USB stick or email attachment. Nearly all malware today will “phone home” **often over non-Web traffic** to a malicious **botnet** host using DNS to communicate with its master. Malware uses DNS because hardcoding an IP address is too easy to thwart by security vendors. By using DNS, malware authors hope that they can constantly hop from domain name to domain name, or frequently update the IP address a domain points to in order to evade take-down efforts by the security community. By using OpenDNS, it doesn't matter if the domain is active or not: it can be blocked from resolving on your network immediately. This effectively cuts malware off at the knees. Not to mention, OpenDNS can now alert the IT administrator to the compromise so further remediation efforts can take place.

Benefits-at-a-Glance

OPEN DNS ENTERPRISE	FEATURE	BENEFIT
Threat Prevention	Malware Protection	Keeps your network secure from inbound threats that steal confidential data
	Botnet Protection	Prevents outbound attacks from being launched on your network's resources and prevents compromised machines from connecting to and leaking information to command and control servers
Web-Based Management	Simple Setup	Easy deployment across multiple locations without any hardware
	Remote Management	Change settings from anywhere with the intuitive Web interface. Gain insight into recently blocked malware and botnet attacks across all protected devices on your network
Network Insights and Reporting	Access Reports Anytime	Use the Web interface to run reports without storing any data locally
	Store Up to Two Years of Data	Reduce your reporting time by scheduling and running regular reports

Introducing the only DNS-based Internet Security Solution:

- Inbound and outbound threat prevention
- Customizable Web content filtering
- Web-based management and reporting

No Installation. No Training. No Maintenance.

As a premium managed service, you don't need to invest in hardware or software. With no hardware or software to deploy, there is no installation required. There's never any maintenance or updates to worry about. No need to hire and train staff to become experts on Internet security threats. OpenDNS is your network security expert!

Don't wait until your organization experiences a devastating malware or botnet attack!

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

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

OpenDNS Enterprise secures the DNS layer to block these attacks before they have a chance to infect your network. Like a firewall for DNS, OpenDNS is application agnostic and can control any traffic that relies on DNS — not just Web traffic — without increasing latency. In fact, OpenDNS often speeds up domain resolution for users.

One of the most appealing aspects of OpenDNS is that because it is a service, **there is no expensive appliance to buy or software that needs to be installed on every computer or device in your network.** This means OpenDNS can protect all the devices on your network, regardless of operating system or platform.

And, best of all, OpenDNS Enterprise is easy to implement: a quick change on your router, gateway or DHCP server is all that's required to secure your network. **No intrusive proxy-based traffic redirection is required on devices or anywhere in the network.** The protection is comprehensive — any **managed employee or unmanaged guest** device accessing your network, when your network is secured by OpenDNS Enterprise, is protected.

It's worth recognizing that OpenDNS can complement existing security solutions. Unlike hardware appliances that often require a rip-and-replace mentality, OpenDNS believes in a defense-in-depth strategy and encourages a heterogeneous network security strategy.

Internet Protection by Sinkholing Connections

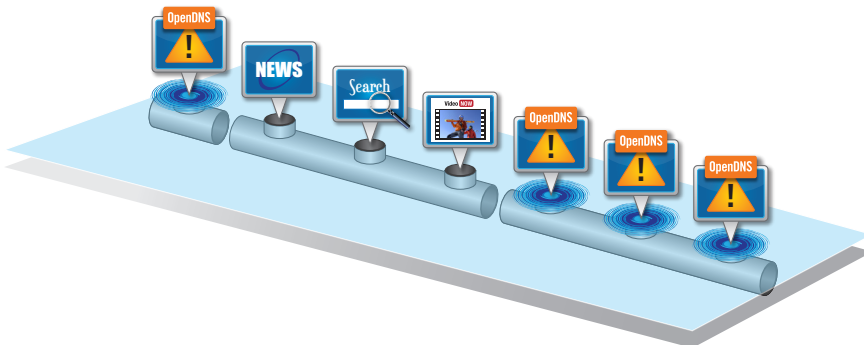


Figure 2:

As the only security solution that proactively filters malicious DNS traffic and only allows legitimate DNS traffic into and out of your network, every major threat on the Internet using DNS is blocked from reaching the network. It is entirely a new layer of protection for your organization. Working on the DNS layer, OpenDNS Enterprise operates as a lightweight, no-latency protection point that blocks malicious traffic.

As the only security solution that proactively filters malicious DNS traffic and only allows legitimate DNS traffic into and out of your network, every major threat on the Internet is blocked from reaching the network. It is entirely a new layer of protection for your organization. Working on the DNS layer, OpenDNS Enterprise operates as a lightweight, no-latency protection point that blocks malicious traffic.

OpenDNS Enterprise is the only enterprise-grade security solution to provide complete inspection, filtering, protection and reporting on the DNS traffic entering and exiting your network, enabling complete inbound and outbound network protection for IT administrators.

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

1-877-811-2367

www.opendns.com/work