

# Two-Person IT Team Effortlessly Manages Security Across Three Sites with OpenDNS

## THE PROBLEM:

**Inconsistent anti-virus solutions and malware remediation absorbed too much time**

At this Marketing and Communications firm, the IT Manager is responsible for the company's entire infrastructure, from servers and routers to laptops and mobile devices. "With just one malware infection," he said, "you can spend three or four hours cleaning or rebuilding a machine." Although the firm deploys anti-virus protection, it is not consistently applied in all locations or on all computers – like the Macs used by their creative team employees. Security for the network perimeter is complicated by a liberal BYOD policy: employees can use their own tablets for work, and can use their own phones with personal apps.

Given these factors, and considering that there were several Windows XP machines still on the firm's network, the IT team needed a more powerful security solution. "We felt that purchasing OpenDNS would provide a strong layer of protection, and help us remediate infections quickly."

## THE SOLUTION:

**OpenDNS protects this marketing company's network from threats and reduces time spent on remediation across multiple sites**

The firm chose OpenDNS to secure all of its endpoints. "OpenDNS allows us to see down to a particular server or computer or site," the IT manager commented. "We see malicious activity on the dashboard, and we can see what's responsible. With the reports, we can also ensure that employees are using our computers for appropriate activities."

Deployment "was very straightforward. OpenDNS provides virtual appliances we can deploy with very little configuration – it's a pre-packaged virtual machine. We just gave it an IP address and point all our clients there. I had it all done in just a couple of hours." The roaming client is not only deployed on all the firm's laptops, but has become the foundation of security for all computers in one of its facilities.

The OpenDNS logo consists of the word "OpenDNS" in a white, sans-serif font, centered within a solid orange rounded rectangle.

---

### Organization Snapshot

**Industry:** Marketing and Communications

**Location:** Locations around the US, headquartered in the Northeast

**Number of users protected:** 280

**Using OpenDNS for:** Enforcing "set it and forget it" security that's quick to deploy and simple to manage.

---

Maintenance? For this IT manager, “mostly it’s just set it and forget it. I just look at the dashboard once or twice a day to see if there’s anything out of the ordinary we need to address. Now that malware infections have gone down, I can spend my time doing more important things.”

*“OpenDNS allows us to see down to a particular server, computer, or site...we see malicious activity on the dashboard, and we can see what’s responsible.”*

## RESULTS:

1. Malware and botnet activity blocked.
2. Easy management of remote devices.
3. Less time spent cleaning infected machines.