

OpenDNS Security Protects Engineering Firm's Devices Anywhere



THE PROBLEM:

Mobility and multiple office locations made protection too complex

As a civil engineering firm, Pennoni Associates serves its clients through multiple remote offices and field assignments. For Jim Slora, Senior Systems Administrator, and his seven-person IT team, that means providing a consistent level of malware and virus protection to users in-house and on the road, while giving HR one reporting platform to ensure Web-access policy compliance.

Before turning to OpenDNS, Pennoni relied on a Websense gateway appliance installed at its headquarters. "All our remote traffic had to be backhauled through this one appliance," Mr. Slora says. "That meant one point of failure for every office. We were overburdening our MPLS circuits to the server and experiencing too much latency, plus downtimes for our regional offices." Installing more appliances was not an option: "It was too expensive," says Mr. Slora, "plus it wasn't a good solution for our mobile workforce."

THE SOLUTION:

OpenDNS provides reliable threat protection for roaming devices

Pennoni needed a lightweight solution that would work anywhere without putting too much strain on their network and OpenDNS's cloud-based approach was an excellent fit. "We picked up OpenDNS for malware detection because it could work immediately," Mr. Slora says. "For a low price, we got control over our traffic plus malware filtering." Switching to OpenDNS was simple as well: "basic deployment is dead easy," says Mr. Slora. "You change your DNS and you're done."

In addition to quick and effortless deployment, OpenDNS's roaming client functionality enables Pennoni "to apply the same protection in the field as we could in the office." As a result of OpenDNS's implementation, "We went from three to four infections per day to one every few days."

Organization Snapshot

Number of Users Protected: 950

Mobile Users Protected: 350

Why Pennoni Chose OpenDNS: OpenDNS provides a consistent level of malware protection and reporting capability to both in-office and mobile users.

What They're Saying

"The reduction in infections since deploying OpenDNS has saved us close to one full-time help desk tech."

- James Slora, Pennoni Associates, Inc.

Mr. Slora estimates that each infected device costs Pennoni one to two hours of cleaning, or one to two days when computers have to be replaced. Mr. Slora says, “The reduction in infections saved us close to one full-time help desk tech.”

Occasionally, Pennoni’s IT team needs to add or subtract sites from the company’s blacklists and whitelists, otherwise, “Most of the company doesn’t even know OpenDNS is there. They don’t see it, they don’t think about it. It just works.”

We picked up OpenDNS for malware detection because it could work immediately...for a low price, we got control over our traffic plus malware filtering.

- **James Slora**, Senior Systems Administrator for Pennoni Associates, Inc.

RESULTS:

1. Reduced the number of infections from 3 to 4 per day to one every few days.
2. Saved Pennoni the equivalent of one full-time help desk tech employee.
3. Covered in-office and roaming employees with consistent protection across multiple devices.