

Solution Brief

# Easily extend threat protection on- and off-campus.

## CLOUD-DELIVERED NETWORK SECURITY AND WEB FILTERING THAT PROTECTS ANY DEVICE, ANYWHERE.

Your goal is simple: to provide fast, safe, reliable Internet service to faculty, staff, and students. A safe Internet requires preventing device infections, data theft, and network breaches. But it's difficult to effectively address the security needs of today's higher education network environments.

Antivirus and other signature-based defenses can't detect or stop the majority of malware, which leaves systems vulnerable and your team faces time-consuming cleanup. And with faculty and staff working on research projects off campus, the traditional appliance-based infrastructures can't scale or extend to protect.

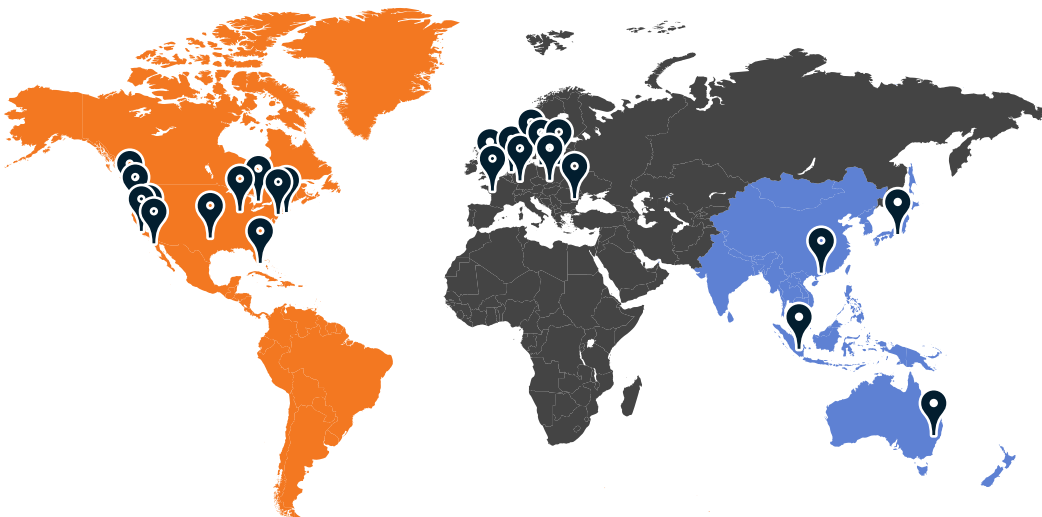
OpenDNS Umbrella is an additional layer of security that not only blocks malware, botnets, and phishing over any port, protocol, or app, but also detects and contains advanced attacks before they can cause damage. Over 200 higher education organizations rely on OpenDNS to deliver fast, secure access across campuses and reduce malware infections—all with a cloud infrastructure and minimal maintenance for IT staff to handle.

*"With Umbrella, we can easily look at a high-level flyover of all of our networks and identify trends before they become problems. That means we're preventing malware instead of cleaning it up."*

— Jonathan Harrell,  
Director of Network Engineering  
Regent University

### Cloud-Delivered Security That Scales

- 80+ billion daily Internet requests.
- 65+ million users.
- 80+ million malware, botnet and phishing requests blocked daily.



24 load-balanced data center locations across 160+ countries

### TRUSTED BY LEADING COLLEGES AND UNIVERSITIES



## STOP THREATS THAT FIREWALLS, WEB FILTERS, AND ANTIVIRUS MISS

- Prevent malware, phishing, and illegal P2P file shares by blocking threats' Internet origins.
- Contain infected devices' ability to phone home to botnet controllers over DNS, P2P, IRC, or any other non-web application, protocol, or port.
- OpenDNS sees over 1 million Internet events every second, so we can discover and predict when and where on the Internet new attacks are being staged.

## PROTECT OFF NETWORK

- Extend protection for faculty and staff when they are off-campus by leveraging the OpenDNS global network of 24 geographically distributed datacenters.
- Expand coverage of FireEye, Check Point, and other partners with OpenDNS's cloud enforcement.

## SIMPLE TO DEPLOY AND EASY TO MANAGE

- No new boxes. Leverage your existing network infrastructure and add Umbrella's cloud-delivered, DNS-based service.
- Secure all devices connecting to your network—without the need to install any software.
- On average, a campus-wide deployment takes only 30 minutes.

## DEPLOY IN MINUTES WITHOUT COMPLEX SIZING GUIDES

- You won't receive complex tech docs and sizing guides from us. They're not necessary for deploying Umbrella to your networks.
- Whether you're managing one campus location or dozens, scalability won't be an issue. Umbrella scales on-demand.
- Umbrella doesn't require topology changes, regardless of how complex your network is.



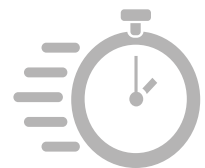
STOP THREATS THAT  
FIREWALLS, WEB FILTERS,  
AND ANTIVIRUS MISS



PROTECT OFF  
NETWORK



SIMPLE TO DEPLOY  
AND EASY TO MANAGE



DEPLOY IN MINUTES  
WITHOUT COMPLEX  
SIZING GUIDES

### PARTNER INTEGRATIONS:



AMP Threat Grid



### FREE TRIAL

- Visit our website to sign up for a free, 2 week trial: [www.opendns.com](http://www.opendns.com).
- Get started in 30 seconds without any user, bandwidth, or device count restrictions.
- Our team will be in touch to help, if needed.

OpenDNS

OpenDNS is  
now part of Cisco.



Contact NFF at 202-783-9011 and learn more about your first line of defense.