

# Cisco Umbrella Roaming

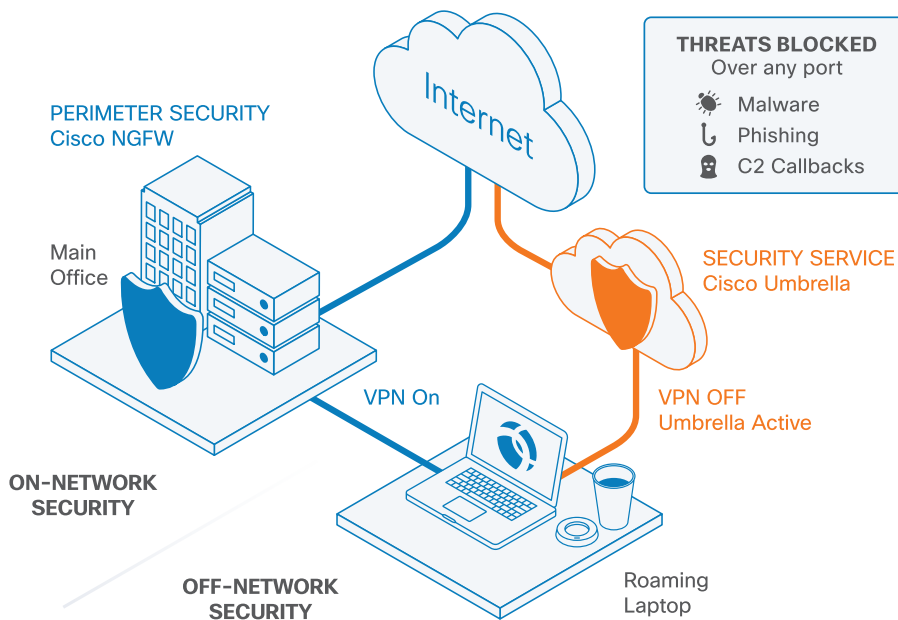
The easiest and fastest way to protect users 100% of the time

## Cloud-delivered security service for Cisco's next-generation firewall

Umbrella Roaming protects employees when they are off the VPN by blocking malicious domain requests and IP responses as DNS queries are resolved. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. Malware will not infect laptops and command & control (C2) callbacks or phishing will not exfiltrate data over any port. Plus, you gain real-time visibility of infected laptops with C2 activity.

## Protect your mobile workforce with no extra agents or user actions

All Internet activity that bypasses your perimeter security is now enforced through our security service, so your off-network blind spot is eliminated. Umbrella Roaming is fully integrated into AnyConnect for Windows or Mac OS X. And unlike using the VPN, there's absolutely nothing new for end-users to do or any performance sacrifice.<sup>2</sup>



## The way your employees work has changed

### 82% of your workers admit to not always using the VPN<sup>2</sup>

Employees are using more cloud apps for work and leveraging their work laptops for personal use—the reality is that not every connection goes through the VPN. Your network extends beyond the perimeter, and your security must too.

### 49% of your workforce is mobile and under defended<sup>3</sup>

Zero-day malware spikes at night and on weekends when we're roaming and attackers know we're vulnerable. In fact, 22% of malicious email links are clicked when roaming.<sup>4</sup> While security may never stop 100% of the threats, it must work 100% of the time.

## The Problem

NGFWs are blind to 25% of traffic<sup>1</sup>

Not all traffic—over all ports, all the time—is backhauled to perimeter security using the Cisco AnyConnect VPN due to:

- Apps & data in the cloud
- Personal web browsing
- Split tunnels configured

And endpoint security (i.e. AV) is not enough to protect your mobile workforce.

## The Solution

### Cisco NGFW + Cisco Umbrella

Security on and off the VPN, over any port, for Windows and Mac OS X roaming laptops.

## No One Combines Effectiveness & Performance Better

- #1** fastest & most reliable DNS w/65M+ daily active users<sup>5</sup>
- 80B+** daily internet requests or connections
- 3M+** daily new domain names discovered
- 60K+** daily malicious destinations identified
- 7M+** total malicious destinations enforced
- 80M+** daily malicious requests blocked

1. cs.co/gartner-prediction  
 2. cs.co/IDG-survey  
 3. cs.co/sans-survey  
 4. cs.co/proofpoint-report  
 5. cs.co/dns-latency, system.opendns.com

# How we predict threats before they happen

## Real-time, diverse data reveals internet activity patterns

Correlating DNS, WHOIS, BGP, IP geolocation, SSL certificates, and even file connectivity provides a complete view of domains and IPs where threats are staged.

## Automated statistical models identify malicious destinations

Similar to Amazon learning from shopping patterns to suggest the next purchase, or Pandora learning from music listening patterns to play the next song, we learn from internet activity patterns to identify attacker infrastructure being staged for the next threat.

## Learn Why We're So Fast & Reliable

- For network teams, go to [cs.co/point-dns/](https://cs.co/point-dns/) to learn how we've maintained 100% uptime since 2006.
- For sysadmin teams, go to [cs.co/lightweight/](https://cs.co/lightweight/) to learn why virtually no PC resources are used.

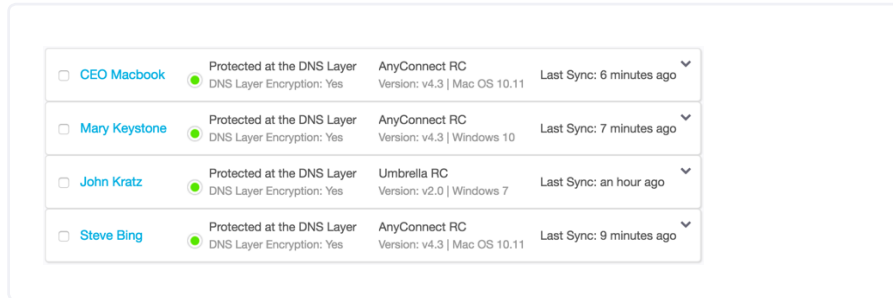
## Simple for both security & sysadmin teams

### 1 Enable Roaming in Minutes

- Simply enable the Roaming Security module available in Cisco AnyConnect v4.3 for Windows or Mac OS X.

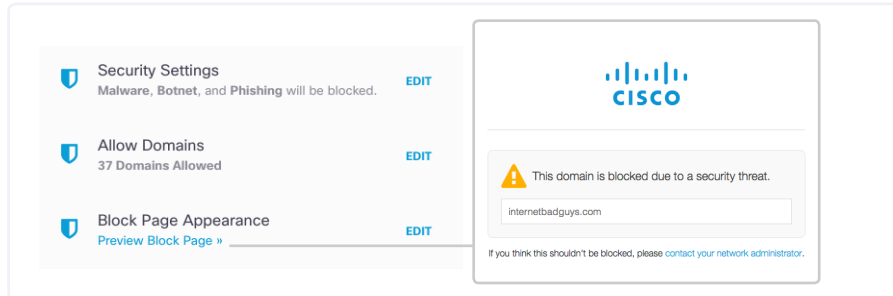
OR

- Deploy a stand-alone Umbrella Roaming Client for Windows or Mac OS X alongside any other remote access VPN client.



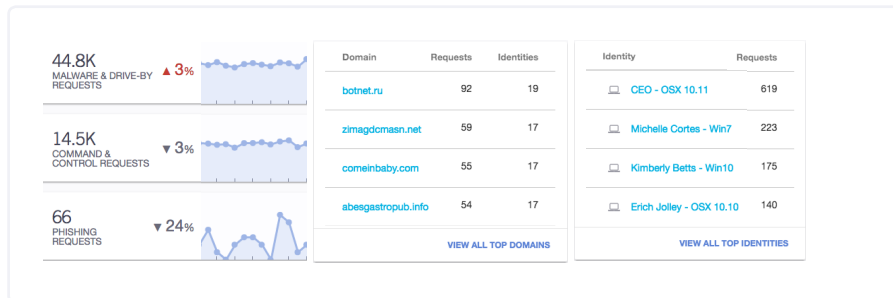
### 2 Global Security by Default

- As soon as Roaming Security is enabled, mobile workers are protected against malicious destinations.
- If a threat is requested via a web browser, end-users receive a customizable block page.
- To immediately access a blocked site, just allow the domain.



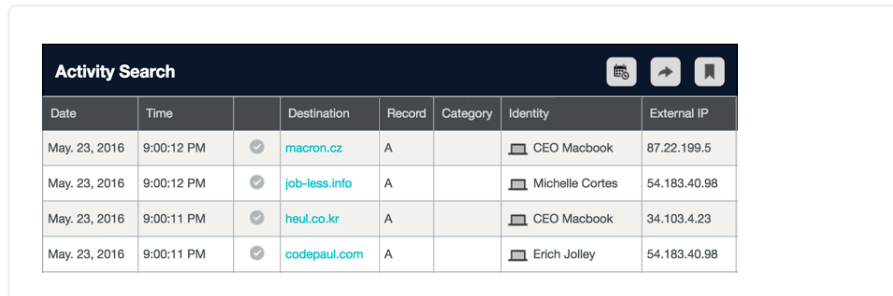
### 3 Instant Visibility into Threats

- View your daily, weekly, or monthly security events occurring off-network either in your inbox or our dashboard.
- Check if threats are trending up or down as well as the domains and laptops with the most security events.
- Respond to an incident by drilling into the full activity per domain or laptop.



### 4 Detailed Logs for Incident Response

- View and optionally filter the last 30 days of detailed, real-time Internet activity by time, domain, category, laptop, or IP location.
- “Top N” summary reports are retained for up to 2 years and can be scheduled to your and others’ inboxes.



Date	Time	Destination	Record	Category	Identity	External IP
May 23, 2016	9:00:12 PM	macron.cz	A		CEO MacBook	87.22.199.5
May 23, 2016	9:00:12 PM	job-less.info	A		Michelle Cortes	54.183.40.98
May 23, 2016	9:00:11 PM	heul.co.kr	A		CEO MacBook	34.103.4.23
May 23, 2016	9:00:11 PM	codepaul.com	A		Erich Jolley	54.183.40.98