Agenda

- Spojrzyć na internet z satelity
- Umbrella i Investigate
- Demonstracja
- Program Partnerski
Our View of the Internet

providing visibility into global Internet activity (e.g. BGP, AS, Whois, DNS)
What if you could see this?

YOUR VISIBILITY TODAY
What If You Could See This?

pervyclass.su

horoshiyden.ru

Statecollegenow.com

pervylich.ru

AS 5662

157.166.226.25

www.cnn.com

AS 3561

173.236.173.144

igloofire.com

216.35.221.76:43

bobnpr.com
Our Perspective

Diverse Set of Data

80B
Requests
Per Day

160+
Countries

65M
Daily Active
Users

10K
Enterprise
Customers
Why OpenDNS?
DNS Services Built for World’s Largest Security Platform

GLOBAL NETWORK
• 80B+ DNS requests/day
• 65M+ biz & home users
• 100% uptime
• Any port, protocol, app

UNIQUE ANALYTICS
• security research team
• automated classification
• BGP peer relationships
• 3D visualization engine

= 80M+
malicious requests blocked/day
Common Security Challenges

50% of PCs are Mobile
70% of Offices go Direct
Most mobile & remote workers don’t keep VPN always on, most branch offices don’t backhaul traffic, and most new endpoint tools only detect

70-90% of Malware is Unique to Each Org
Signature-based tools, reactive threat intelligence, and isolated security enforcement cannot stay ahead of attacks

Shortage of Security Talent
Many tools require more resources than you have available to make work
Problems We Solve

**Breach and Malware Protection**
Prevent data exfiltration and compromised systems by blocking C2 callbacks and malicious sites

**Internet-wide Visibility**
Speed up incident response with a live, up-to-date view of the Internet

**Web Filtering and Cloud/IoT Visibility**
Enforce acceptable use, see cloud services & IoT devices in use, and keep guest Wi-Fi safe
UMBRELLA
Enforcement
Network security service protects any device, anywhere

INVESTIGATE
Intelligence
Discover and predict attacks before they happen
A New Layer of Breach Protection

- **Threat Prevention**: Not just threat detection
- **Protects On & Off Network**: Not limited to devices forwarding traffic through on-prem appliances
- **Always Up to Date**: No need for device to VPN back to an on-prem server for updates
- **Block by Domains, IPs & URLs for All Ports**: Not just ports 80/443 or only IPs
- **Turn-Key & Custom API-Based Integrations**: Does not require professional services to setup

**UMBRELLA Enforcement**
Where Does Umbrella Fit?

INTERNET

ON NETWORK

OFF NETWORK

WEB TRAFFIC
ALL OTHER TRAFFIC
EMAIL TRAFFIC

NGFW
DPI/block by IP, URL, packet, or file

SWG
proxy/block by URL, content, or file

Umbrella
resolve/block by domain, IP, or URL

SEG
blocks by sender, content, or file

SEG
blocks by sender or content

Umbrella
resolve/block by domain, IP, or URL
Where Does Umbrella Fit Alongside Cisco’s Security Portfolio?

Internet

**WHERE DOES UMBRELLA FIT?**

- **WEB TRAFFIC**
  - WSA/CWS: proxy/block by URL, content, or file
  - ASA/FirePOWER: DPI/block by IP, URL, packet, or file
  - Umbrella: resolve/block by domain, IP, or URL

- **ALL OTHER TRAFFIC**
  - ESA/CES: blocks by sender, content, or file

- **EMAIL TRAFFIC**
  - CWS?: proxy/block by URL, content, or file
  - Umbrella: resolve/block by domain, IP, or URL

**ON NETWORK**

- AMP FOR ENDPOINT: check/block hash

**OFF NETWORK**

- AMP FOR ENDPOINT: check/block hash
The Power of Integrating Umbrella + AMP Threat Grid

Automate Enforcement & Visibility

AMP THREAT GRID
Unified Analysis & Intelligence

Dynamic & Static
malware analysis identifies key behavioral indicators

Threat Content
enriched with global & historical context for accuracy

CUSTOMER & PARTNER COMMUNITY

CUSTOMER

files

domains

UMBRELLA
Enforcement & Visibility

Automatically Pulls newly discovered malicious domains in minutes

Logs & Blocks all Internet activity destined to these domains
OpenDNS INVESTIGATE

Single, correlated source of data about domains and IPs across the Internet

Live graph of DNS requests and other contextual data

Correlated against statistical models

Discover & predict malicious domains

Enrich security data with global intelligence
A Single, Correlated Source of Information

- Passive DNS database
- WHOIS record data
- Domain reputation scores
- ASN attribution
- IP geolocation
- IP reputation scores
- Domain co-occurrences
- Anomaly detection (DGAs, FFNs)
- DNS request patterns/geo. distribution
What We Observe On The Internet
We See Where Attacks Are Staged

using modern data analysis to surface threat activity in unique ways
How Our Security Classification Works

Ingest
millions of data points per second

Apply
statistical models and human intelligence

Identify
probable malicious sites

- a.ru
- b.cn
- 7.7.1.3
- e.net
- p.com/jpg
- 5.9.0.1
### Reputation Analysis

- Infected hosts often connect to known bad sites
- Domains requested primarily by infected host are most likely malicious
- Malicious hosts often found in the same areas
- Flags “sketchy” neighborhoods based on the number of malicious sites hosted there
Example: NLPRank Model

Utilizing natural language processing (NLP), this model identifies potentially malicious domain-squatting and targeted phishing domains.

1. Read APT reports

2. Saw patterns in domains used in attacks
   - Domain spoofing used to obfuscate
   - Often saw brand names and terms like “update”
   - Examples: microsoft-xpupdate[.]com, update-java[.]net, adobe-update[.]net

3. Checked our data and confirmed intuition
   - Certain dictionary words and tech company names merged
   - Changed small number of characters to obfuscate
   - Domains hosted on ASNs unassociated with legitimate company

4. Built model and continue to tune
   - Detects fraudulent brand domains:
     - ✗ 1linkedin.net
     - ✓ linkedin.com
Anomaly Detection: Identify DGAs

Domain Generation Algorithms: technique for generating malware domains on-the-fly

N-gram” analysis
Do letter pairings match normal language patterns?

- yfrscsddkkdl.com
- qgmcgoqeasgommee.org
- iyyxtyxdeypk.com
- diiqngijkpop.ru

Does the probability distribution of letters appear random?
Domain to IP Relationships (Passive DNS)

- **domain1.com**
- **domain2.com**
- **domain3.com**

IP Address: **12.4.0.4/32**

Dates:
- **10 JAN 2015**
- **11 JAN 2015**
- **12 JAN 2015**
Domain → IP → ASN Relationships

AS 3462
1.168.6.17

AS 701
100.2.65.157

domain1.com

AS 12271
104.162.93.136
Domain Co-Occurrences

- domain3.com
- domain4.com
- domain5.com

55.71.2.8/32
IP Geography Analysis

Domain: Luckkill.ru
Who’s Requesting This Domain?

Requester Geo Location
Why Cisco Acquired OpenDNS
Cisco’s Strategy

Security Everywhere
OpenDNS Works With Everything You Use

FUTURE-PROOF EXTENSIBILITY

SECURE APIs OPEN TO EVERYONE

CUSTOMERS
In-house Security Systems

NETWORK PROVIDERS
Meraki, Aruba, Aerohive

SECURITY PROVIDERS
FireEye, Cisco, Check Point

ANY TECHNOLOGY
Firewalls, Gateways

ANY ENDPOINT
VPN, IoE

ANY NETWORK
Routers, Wi-Fi, SDN

CONFIDENTIAL
OpenDNS Adds to Cisco’s Security Portfolio
before, during and after an attack

OpenDNS Umbrella

**BEFORE**
- Discover
- Enforce
- Harden

**DURING**
- Detect
- Block
- Defend

**AFTER**
- Scope
- Contain
- Remediate

**ATTACK CONTINUUM**

- **OpenDNS Investigate**
  - stay ahead of future attacks by blocking malicious domains, IPs, and ASNs
  - block callbacks and exfiltration on any port, protocol, or app at the DNS & IP layers

- **OpenDNS Investigate**
  - query live threat intelligence of all the domains & IPs on the internet
Demonstration
OpenDNS

for Partners
Why Partner with OpenDNS?

**World Class SaaS Business**
- Deliver powerful, yet simple to manage security
- Doubled our business YoY
- Earned trust across customers of all sizes

**Net New Revenue Source**
- Sell our products alongside existing portfolio
- Protection at the DNS layer for any device, anywhere
- New source of predictive threat intelligence

**Increase Your Profitability**
- Add recurring revenue streams for your business
- Easiest security product you’ve ever deployed
- Close deals faster
- 90+% renewal rate

**Quickest Win For Your Customers**
- Easy to trial & deploy OpenDNS products
- Deploy in 30 minutes or less
- See immediate reduction in infected systems
- No hardware to deploy or software to maintain
## Summary of Benefits

<table>
<thead>
<tr>
<th></th>
<th>Select Partners (Entry Level)</th>
<th>Elite Partners (Premier Level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deal Registration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Incumbency Protection on Renewals</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Demo Account Access</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access to OpenDNS Technical Support</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NFR/Internal Use Licenses</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Buy Through Distribution</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Option to Buy Direct From OpenDNS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Distribution of Sales Leads</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Channel Marketing Development Funds</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dedicated Partner Development Manager</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
OpenDNS Partner Portal

- https://communities.cisco.com/docs/DOC-64565
- www.opendns.com/channel
- All content for partners posted here
  - Deal Registration Process
  - Sales & Technical Training
  - Benefits & Requirements
  - Sales Contact Maps
  - Deck, data sheets, cheat sheets, etc.

Welcome to the OpenDNS Partner Portal!

The OpenDNS Channel Program gives Cisco partners the opportunity to become an OpenDNS partner. By joining our program, your organization will be able to:

- Transaction orders of OpenDNS Umbrella and Investigate products
- Participate in Deal Registration
- Receive Demo and NFR accounts
- Access special programs, promotions, and incentives

Becoming an OpenDNS Channel Partner

- Steps to become an OpenDNS Partner
- Requirements for partners
- Benefits for partners
- OpenDNS Partner Development Team