OpenDNS

OpenDNS - a biztos alap

Simon János György
Cisco security megoldások - csoportvezető

OpenDNS is
now part of Cisco.

Az 1993-ban alapított
és 2003 óta a frankfurti
tőzsdén jegyzett S&T
Közép-Kelet Európa

20
ORSZÁGÁBAN
VAN JELEN

2200
ALKALMAZOTTJÁVAL

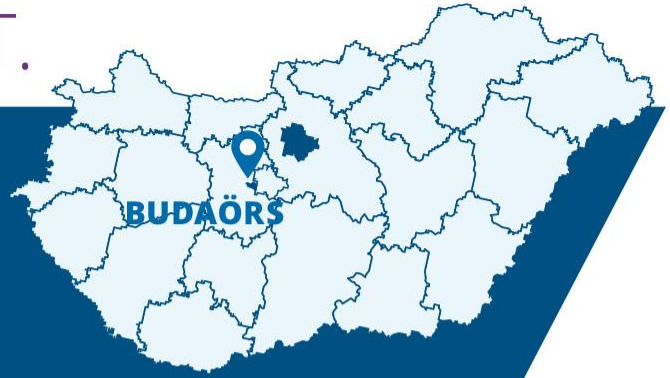
VEZETŐ REGIONÁLIS SZOLGÁLTATÓ
a teljes körű tanácsadás, az outsourcing,
a rendszerintegráció
és IT szolgáltatások területén.

2015-ben értékesítési árbevétele

420 M €

S&T CONSULTING HUNGARY KFT.

Az S&T Csoport magyarországi leányvállalataként
egyszerre építhet 22 éves helyismeretére
és a Csoport erejére és szakembergárdájára.



120+
ALKALMAZOTT

70%
SZAKÉRTŐ

7,6 MRD FT
árbevétel 2015-ben

Tematika

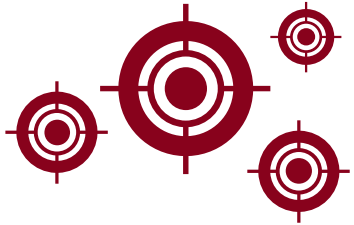
- Mi is az OpenDNS?
- Termékek bemutatása
  - Umbrella
  - Investigate
- Integrációs lehetőségek és előnyök

OpenDNS

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



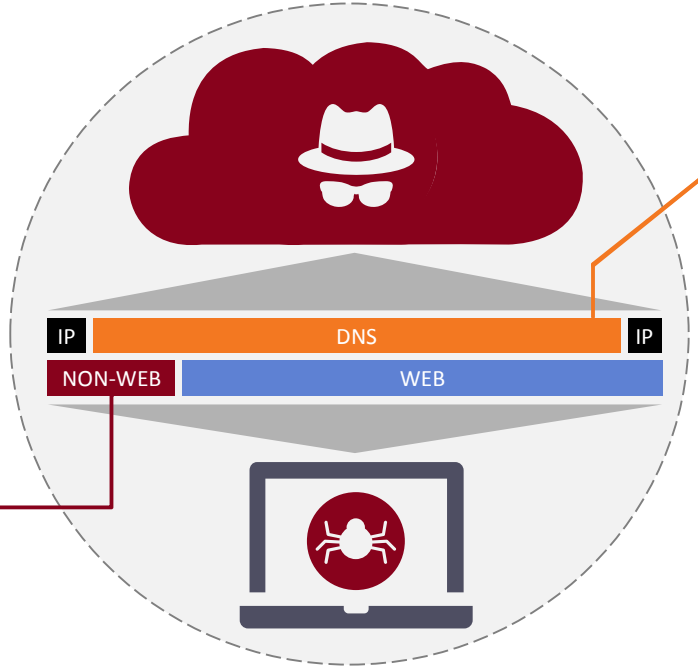
70-90% of Malware is Unique to Each Org

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

You Need a Different Approach to Block Threats Others Miss



91%

of C2 can be blocked at the DNS layer

15%

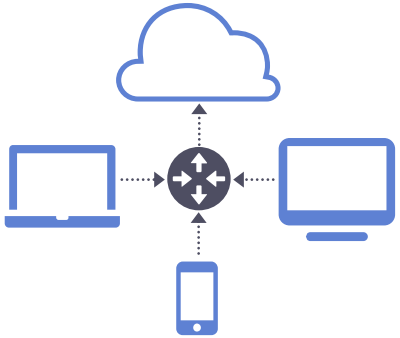
of C2 bypasses web ports 80 & 443

OpenDNS

“By 2018, Gartner estimates that 25% of corporate data traffic will bypass perimeter security and flow directly from mobile devices to the cloud.”

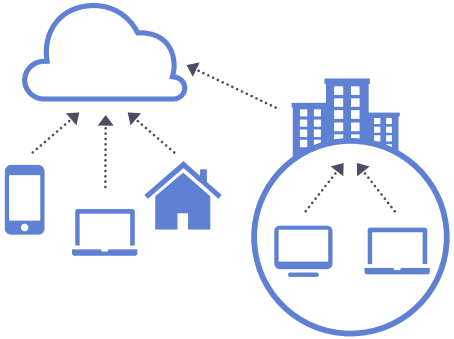
Gartner

DNS is *Used by Every Device* on Your Network



ANY OWNER

network's DHCP tells every connected device where to point DNS



ANY TOPOLOGY

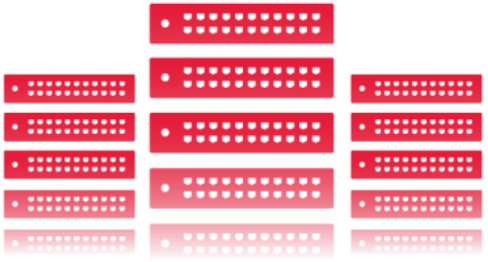
no matter how your LAN or WAN is set up, it simply works

ANY OPERATING SYSTEM

Win, Mac, iOS, Android, Linux, custom app servers, and even IoT

DNS as a Security tool

A blind spot for attackers to gain command and control, exfiltrate data, and redirect traffic



91.3%

of malware uses DNS

68%

of organizations don't monitor it

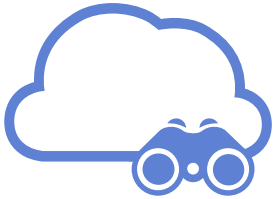
Problems We Solve

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

OpenDNS

Mi is az OpenDNS?

OpenDNS is
now part of Cisco.

cisco

OpenDNS

PRODUCTS & TECHNOLOGIES

UMBRELLA

Enforcement

Network security service
protects any device, anywhere

INVESTIGATE

Intelligence

Threat intelligence on domains
and IPs across the Internet

OpenDNS

OpenDNS

Acquires data from

2%

of the Internet

80B+ requests per day

65M+ daily-active users

160+ countries

24 data centers *(and more coming)*

No One Combines Better Performance & Effectiveness

#1
Fastest & Most Reliable DNS w/ **65M+ Users**

3M+
Daily New Domain Names **Discovered**

60K+
Daily Malicious Destinations **Identified**

7M+
Total Malicious Destinations **Enforced**

OpenDNS

Umbrella

OpenDNS is
now part of Cisco.

cisco

Umbrella: The Fastest & Easiest Way To Block Threats

BENEFITS

Simple to point DNS w/o technical or pro services

No hardware to install
No software to maintain

Provision globally in under 30 minutes

Infinitely scalable enforcement platform

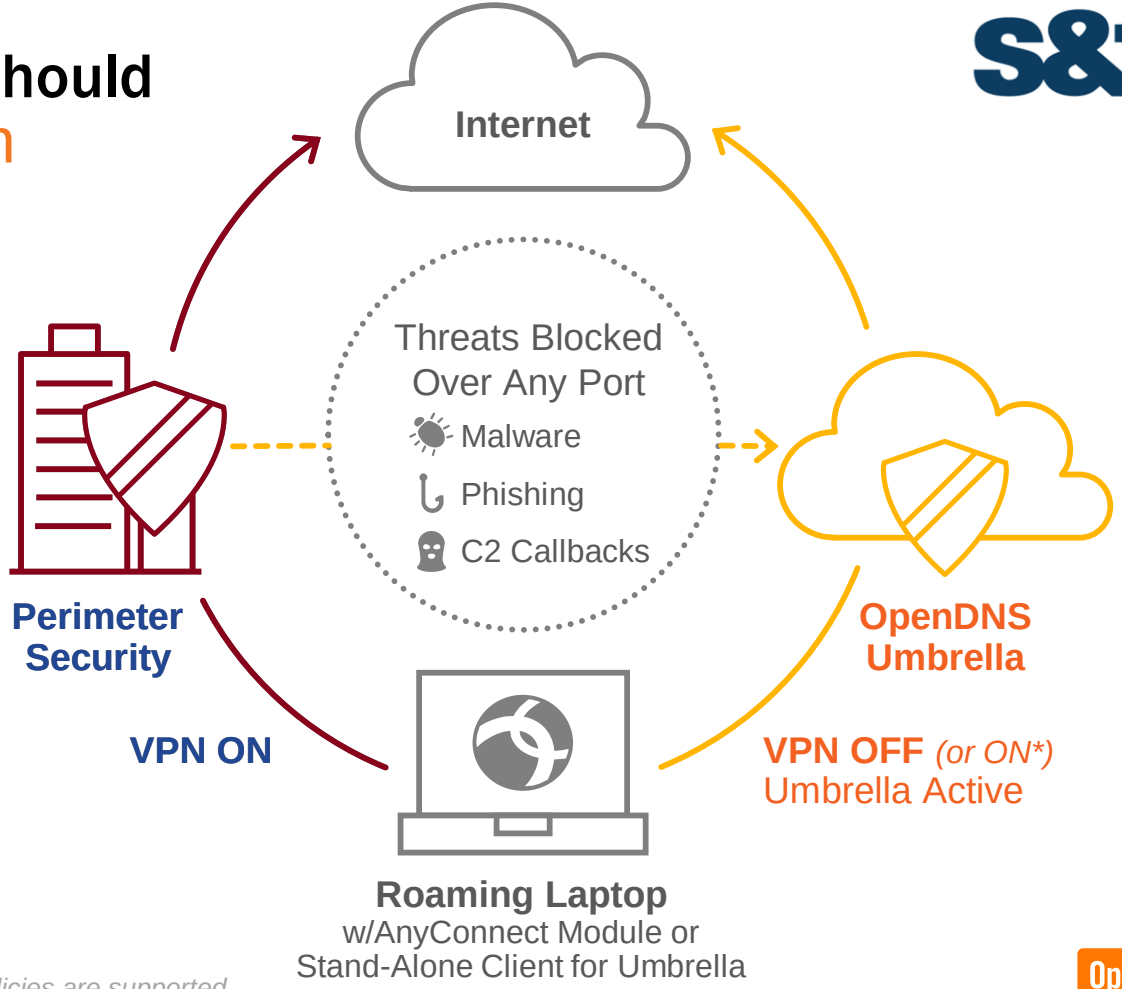
OpenDNS

DNS-Layer Security Should
Protect Any Location

NEED OFF-NETWORK SECURITY

Protect mobile workforce with always-on security

Integrate w/your security stack to extend protection



always-on or location-aware policies are supported

OpenDNS Umbrella
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

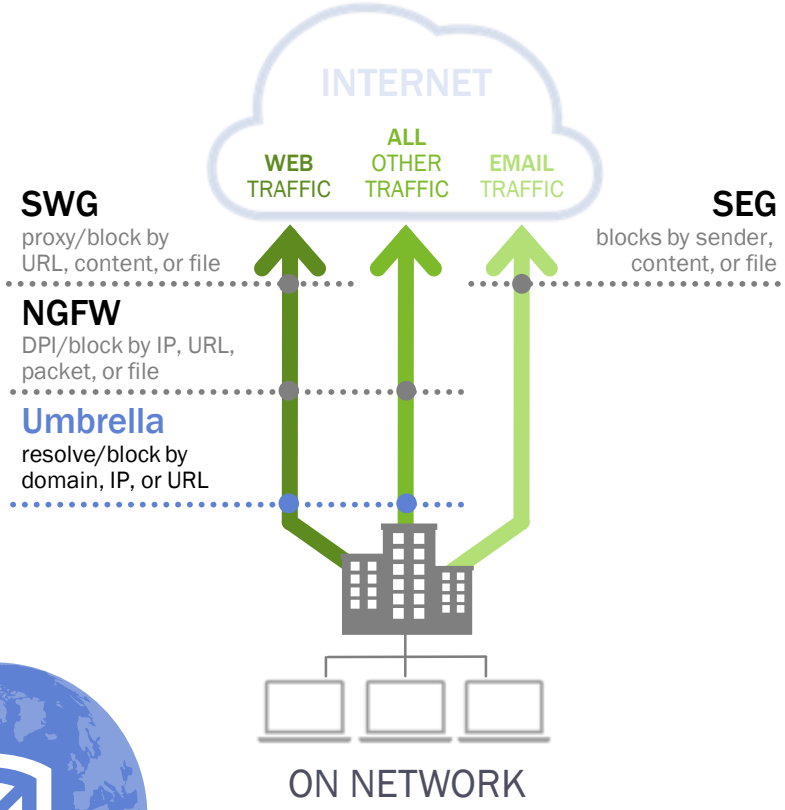
Block by Domains, IPs & URLs for All Ports
Not just ports 80/443 or only IPs

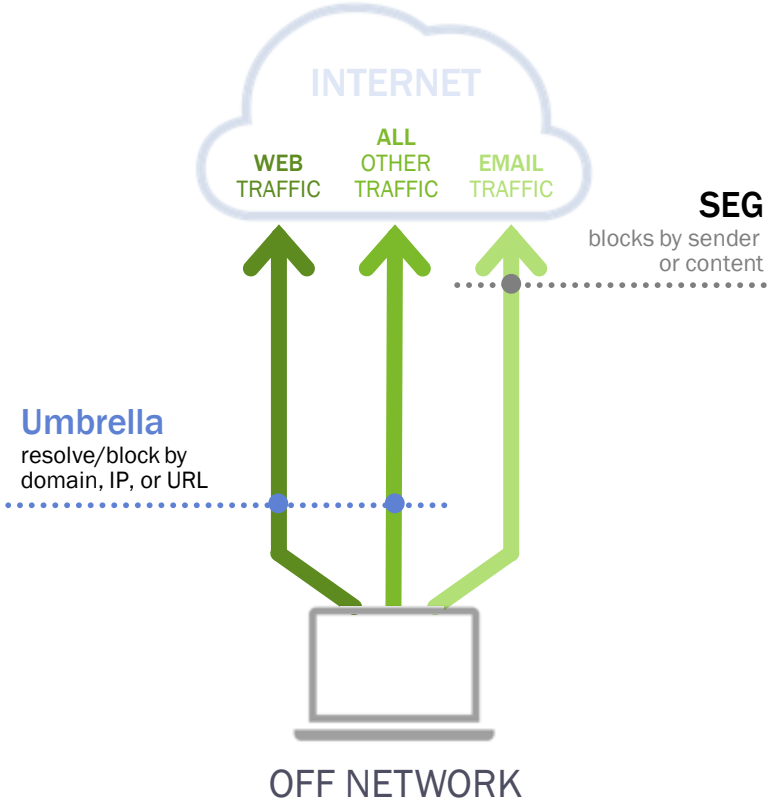
Turn-Key & Custom API-Based Integrations
Does not require professional services to setup

OpenDNS

Where Does Umbrella Fit?

Precedes Traditional Web and Network Security

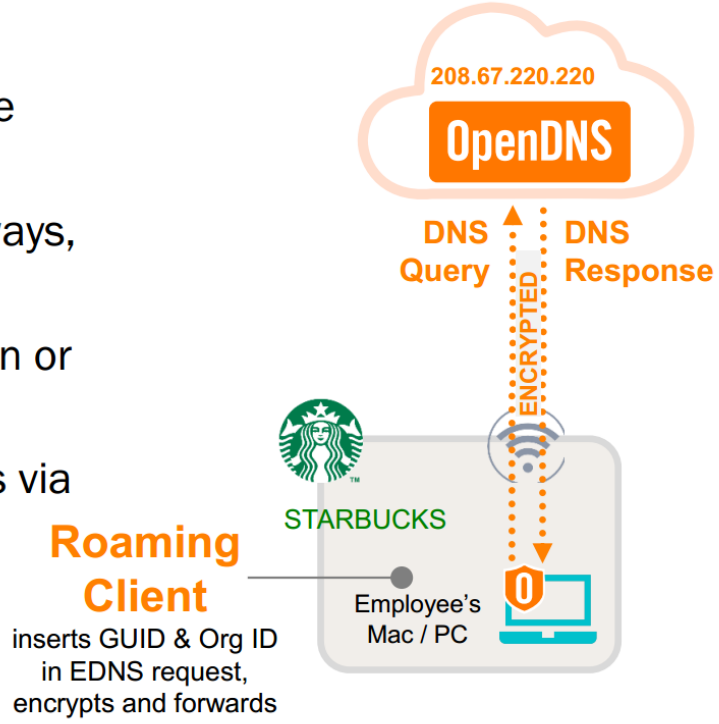




OpenDNS

Umbrella Roaming client

- **Extend protection** to laptops beyond the network perimeter
- Unlike Cloud-based Proxy or VPN gateways, we add **no latency**
- **Pinpoint activity** to specific endpoints on or off the network (location aware)
- **Prevent DNS man-in-the-middle** attacks via untrusted networks



Umbrella Packages

	Professional	Insights	Platform
Cloud-Delivered Network Security	✓	✓	✓
On & Off Network Coverage	✓	✓	✓
Centralized Management	✓	✓	✓
Real-Time & Scheduled Reports	✓	✓	✓
Content Filtering & Custom Block Lists	✓	✓	✓
Internal Networks & AD Integration		✓	✓
Cloud Service & Security Insight Reports		✓	✓
Intelligent Proxy & IP Layer Enforcement		✓	✓
Log Management with Amazon S3		✓	✓
Access to Investigate Console			✓
Turn-Key Partner Integrations			✓
API-Based Custom Integrations			✓

https://learn-umbrella.cisco.com/datasheets/umbrella-package-comparison

OpenDNS

OpenDNS

Investigate

OpenDNS is
now part of Cisco.

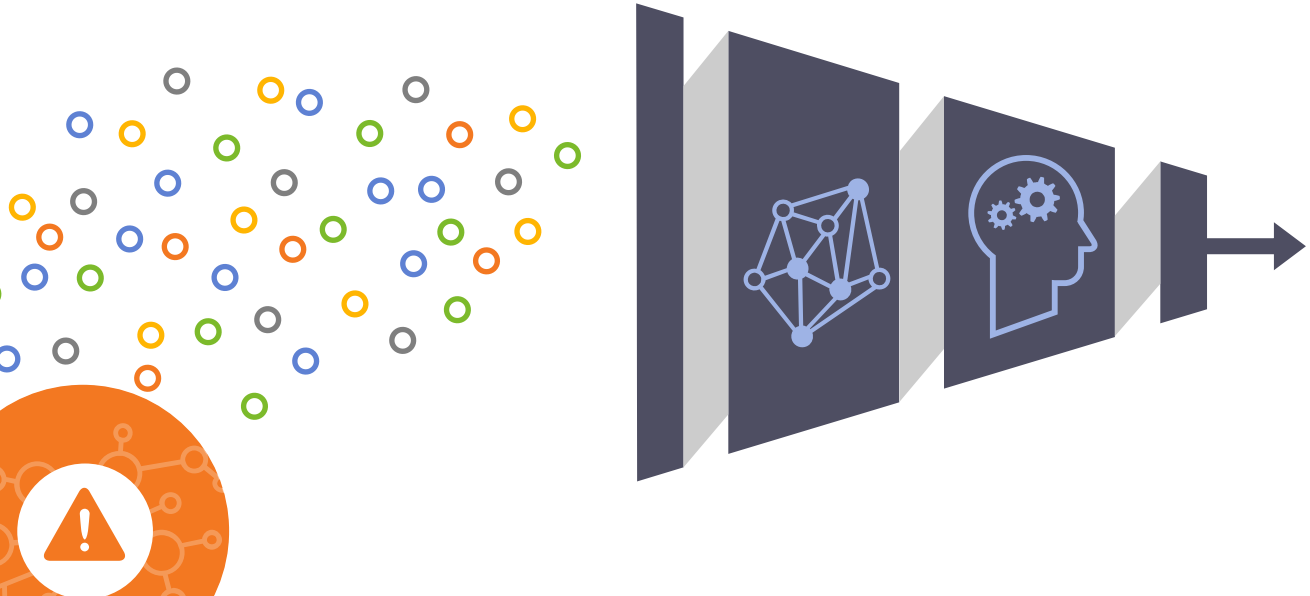
cisco

OpenDNS Investigate
How Our Security Classification Works

Ingest
millions of data points per second

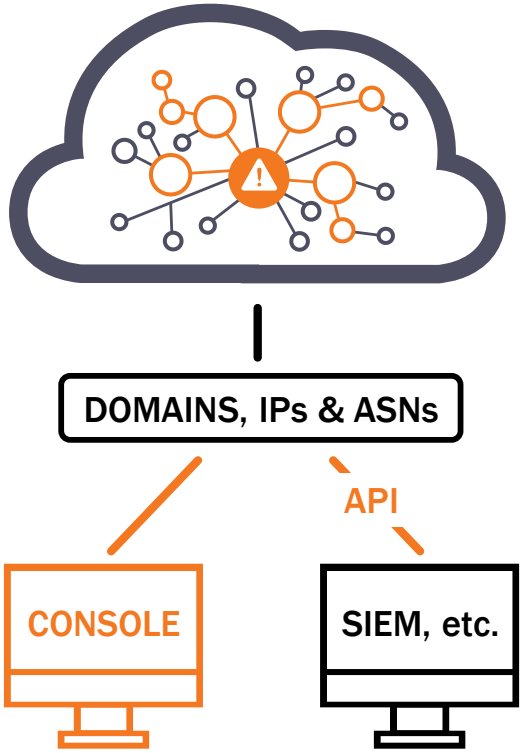
Apply
statistical models and human intelligence

Identify
probable malicious sites



OpenDNS

Investigate: The Most Powerful Way to Uncover Threats



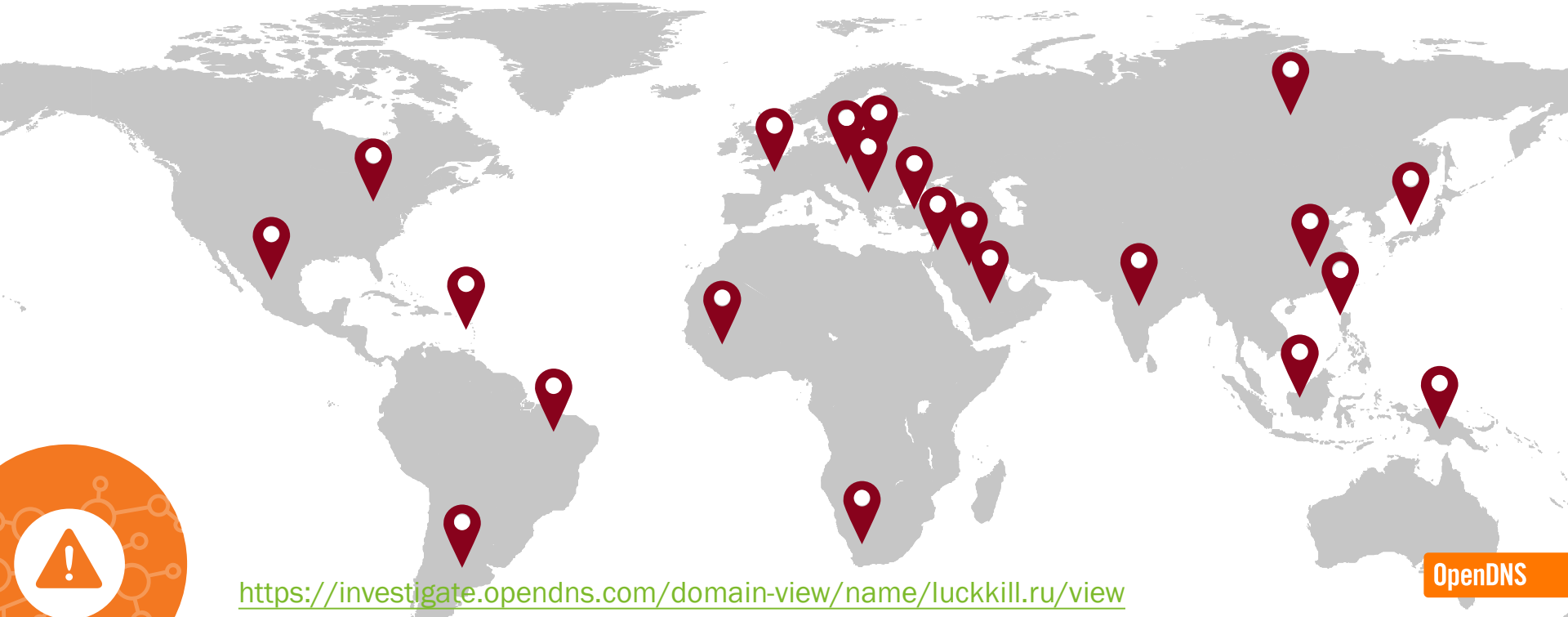
Key Points

- Intelligence about domains and IPs across the Internet
- Live graph of DNS requests and other contextual data
- Correlated against statistical models
- Discover & predict malicious domains & IPs
- Enrich security data with global intelligence

OpenDNS

IP Geography Analysis

Domain: Luckkill.ru



https://investigate.opendns.com/domain-view/name/luckkill.ru/view

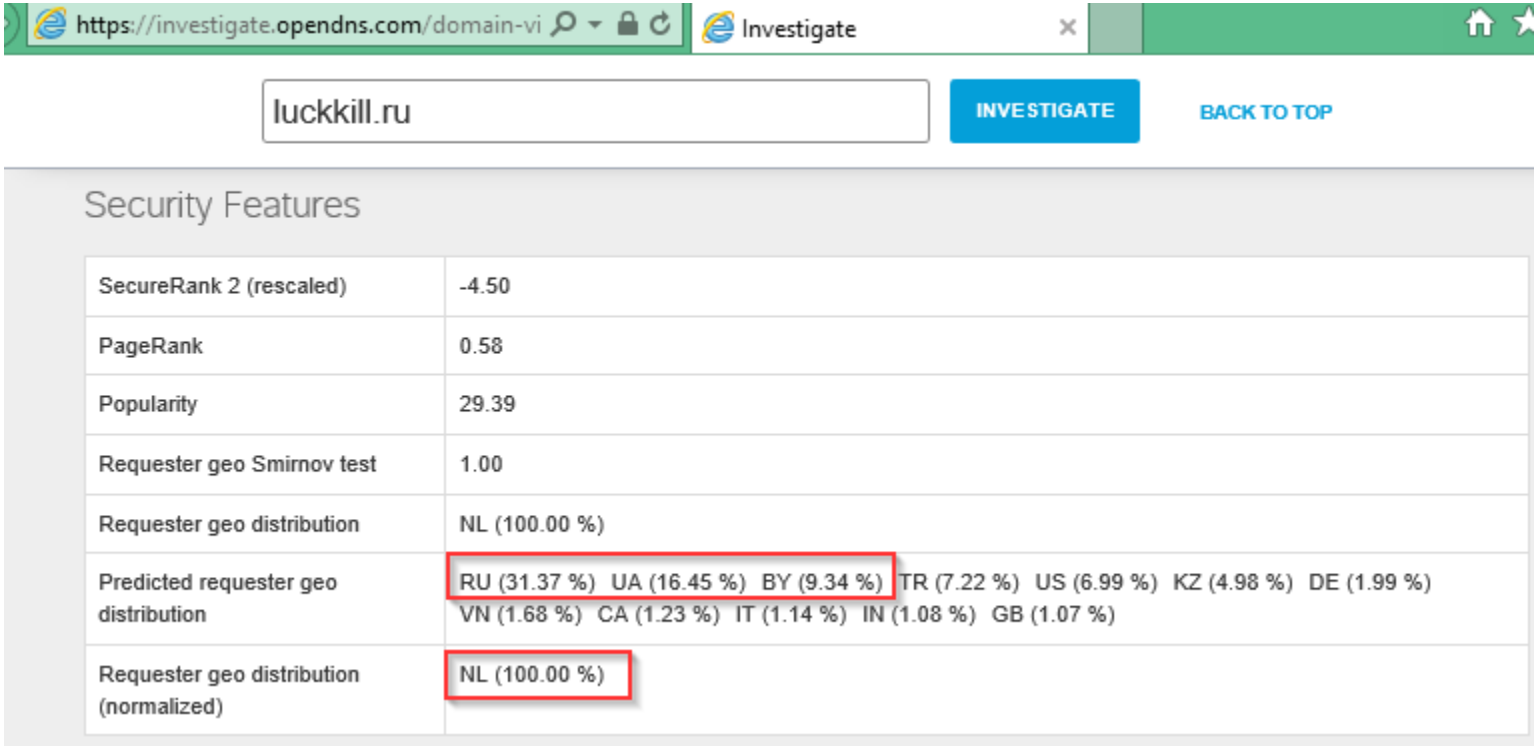
OpenDNS

Who's Requesting This Domain?

Requester Geo Location

OpenDNS

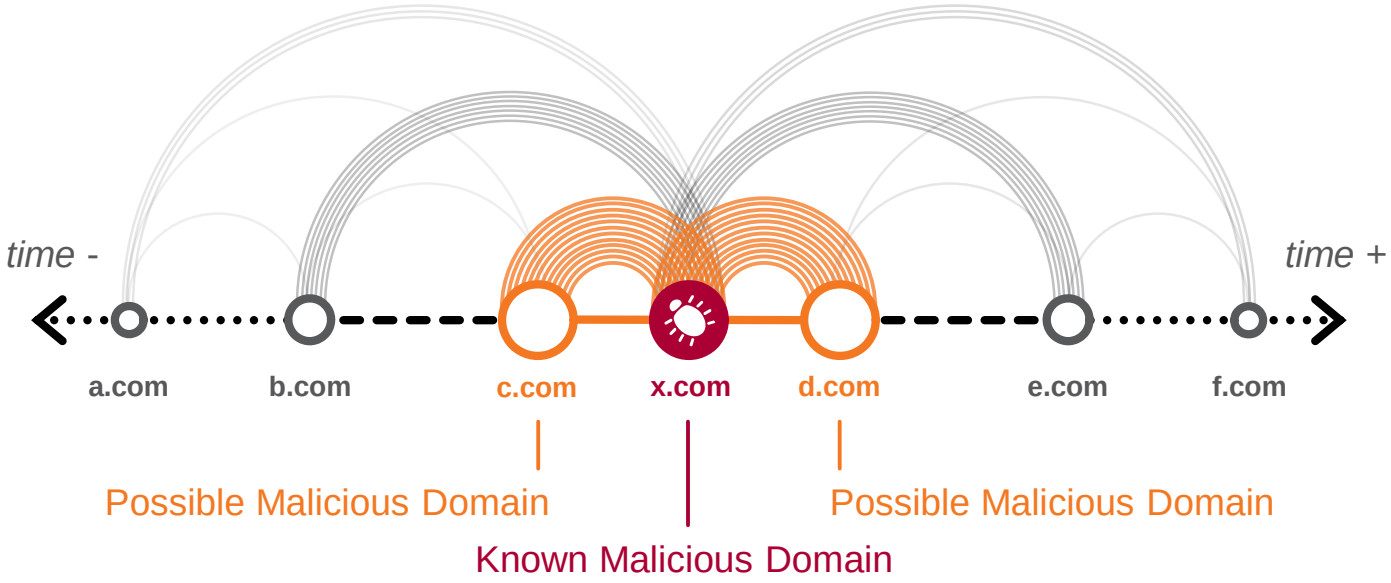
Example: Geo distribution for luckkill.ru



OpenDNS

Co-Occurrence Rank

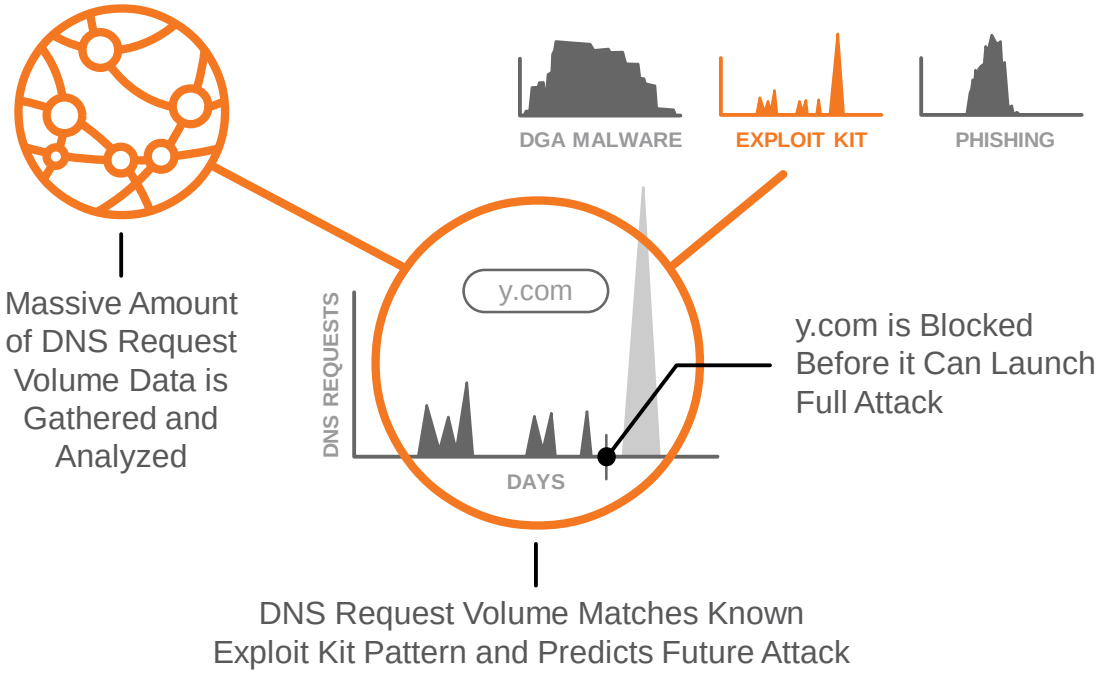
Domains Guilty by Inference



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

Spike-Rank

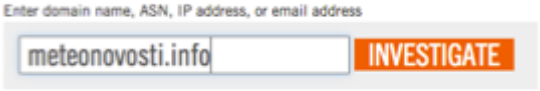
DNS Activity Analyzed for Attack Patterns



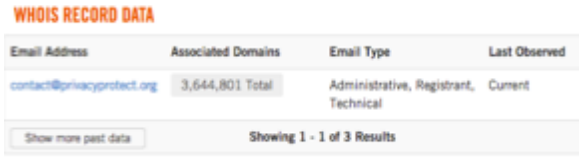
OpenDNS

Speed up investigations with WHOIS

Query suspicious domain found in proxy logs



Find site was registered by a privacy protection service



Looks like someone was trying to cover their tracks...

Historical data shows previous registrants

Email Address	Associated Domains	Last Observed
contact@privacyprotect.org	3,644,801 Total	Current
webmaster@pewinternet.name	5 Total - 4 malicious	September 25, 2013

Was registered with email used with other malicious domains

Uncover other contact information

Contact Name	Phone Number
billionaire	4536946676

Address
...dcoad 21 (view map)
...scow, Moskovskaya oblast 68774
...IAN FEDERATION

See name server history

Name Server	Associated Domains	Last Observed
mydomens.mars.obox-dns.com	154 Total - At least 6 malicious	Current
mydomens.venus.obox-dns.com	139 Total - At least 7 malicious	Current
marketwire1.ddns.net	4 Total	October 19, 2014
ns1.datastats.me	6 Total - 1 malicious	October 19, 2014

Pivot to find other malicious domains

DOMAINS ASSOCIATED WITH WEBMASTER@PEWINTERNET.NAME

Domain Name	Security Categories
bere-bere-bere.biz	Malware
bara-bara-bara.biz	
mmg-studios.org	Malware
bara-bara-bere.biz	Malware
push-sport-simple.info	Malware

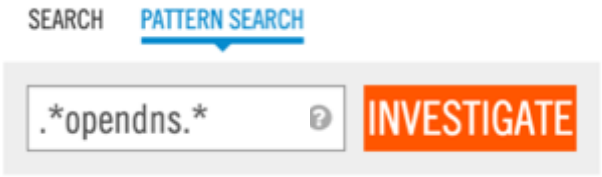
Single, correlated source

OpenDNS

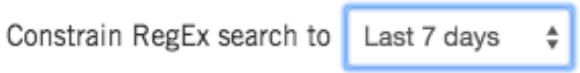
Find domains impersonating brand names

(a.k.a. cybersquatting or typosquatting)

Use pattern search to look for a brand name



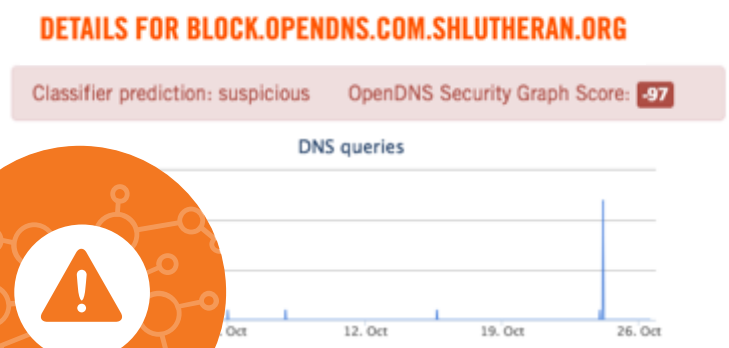
Decide to look for domains queried in past 7 days



Uncover all domains containing the brand name

Domain Name	First Seen
republika.co.id.opendns.com	October 22, 2015, 11:02pm
block.opendns.com.shlutheran.org	October 23, 2015, 11:20am
prefs-sync.e1.usw1.opendns.com	October 22, 2015, 4:53pm

Pivot on domains to further research



- Domain registered by privacy protection service

Email Address
privacyprotect@hebeidomains.com

- Hosted on different ASN from all OpenDNS domains

ASNs	AS 16276

- IP hosts more than 140 malicious domains

First seen	IPs
10/4/15	167.114.156.214 (TTL: 600)

Take action

Proactively block access for internal users & work to take down the domain

OpenDNS

Use Our Global Intelligence To...

- Speed up investigations
- Stay ahead of attacks
- Prioritize investigations & response
- Enrich security systems with real-time data

https://investigate.opendns.com/domain-view/name/goloduha.info/view

OpenDNS

MEASUREABLE VALUE ADD

OpenDNS

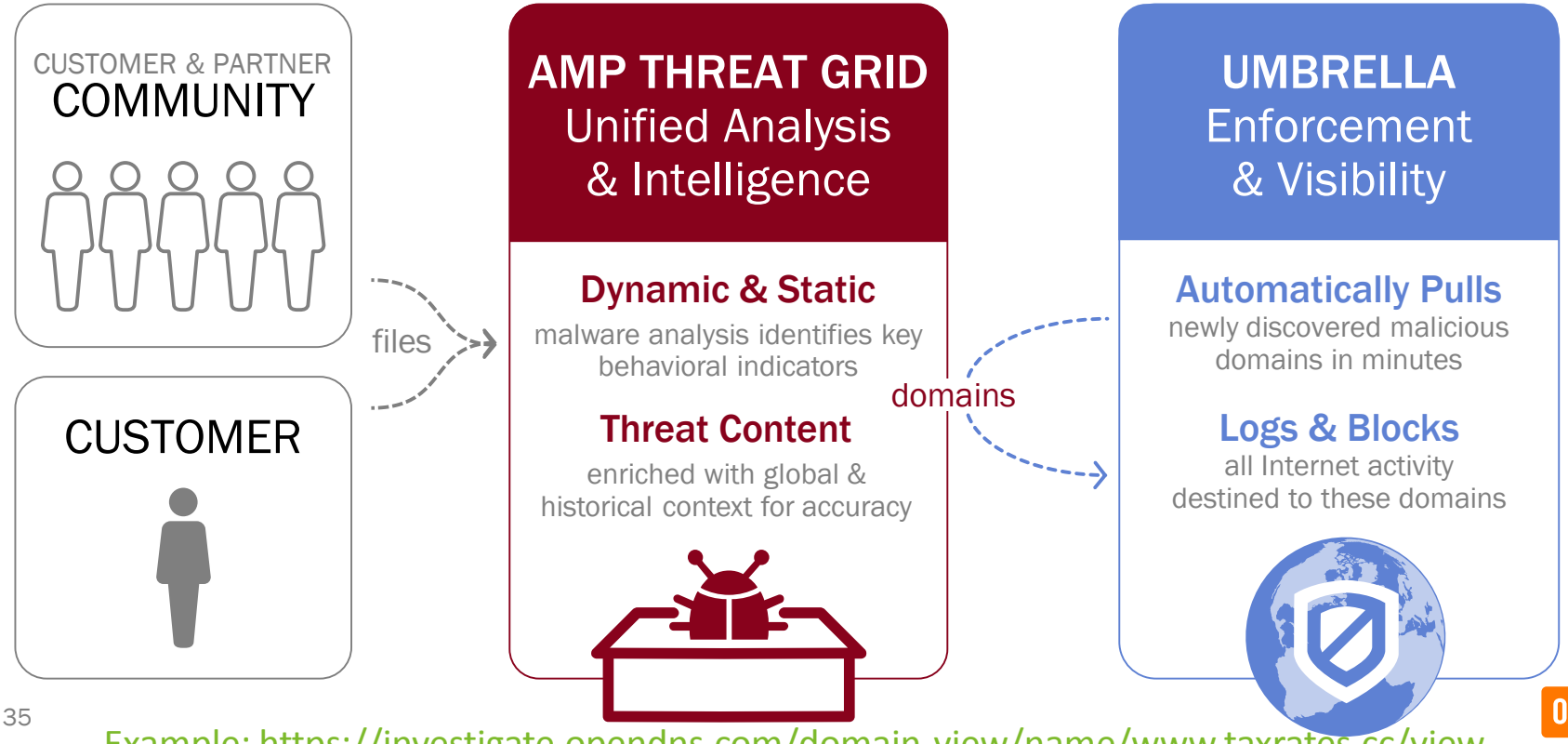
Integráció

OpenDNS is
now part of Cisco.

cisco

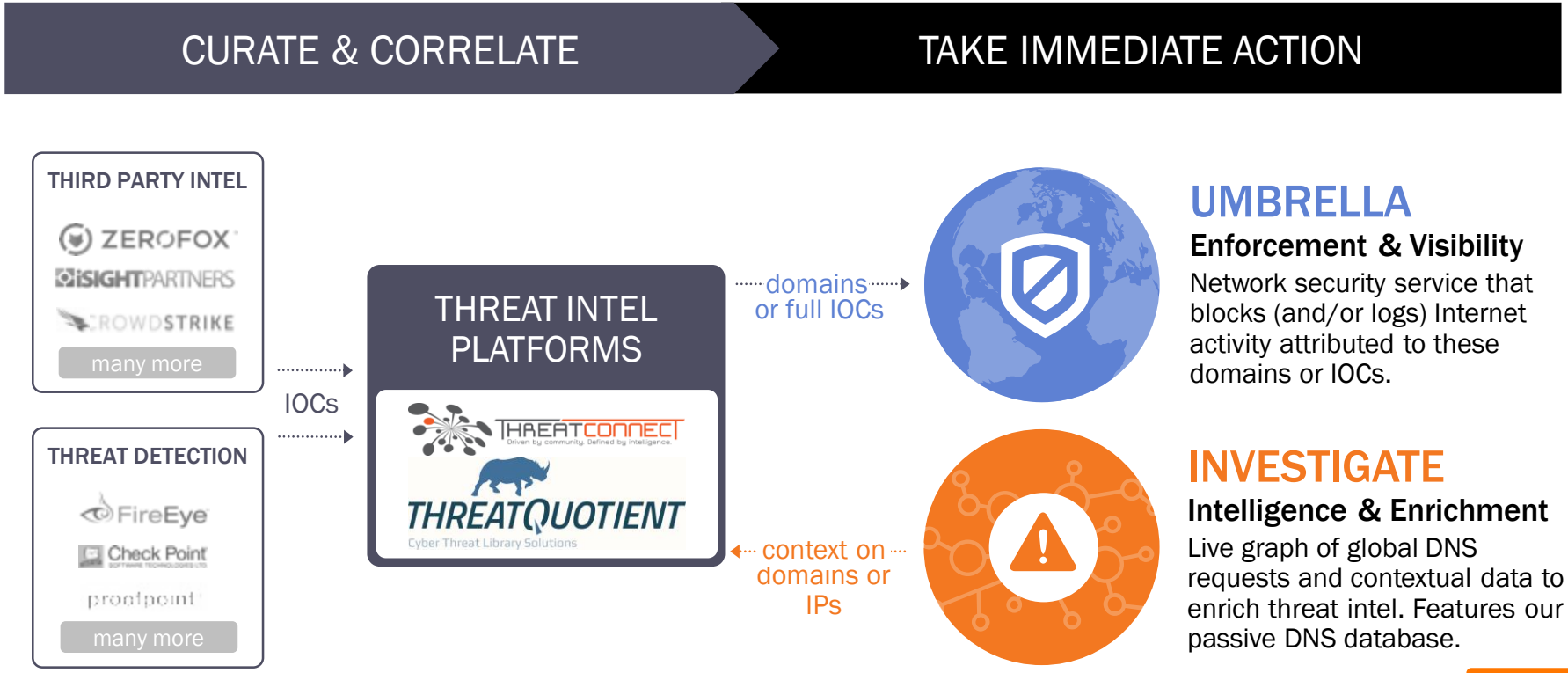
The Power of Integrating Umbrella + AMP Threat Grid

Automate Enforcement & Visibility



Example: https://investigate.opendns.com/domain-view/name/www.taxrates.cc/view

Partner Integrations With Two TIP Partners



OpenDNS

How Cisco Protects Customers from Ransomware

Umbrella blocks the request

NGFW blocks the connection

Web or Email Security w/**AMP** blocks the file

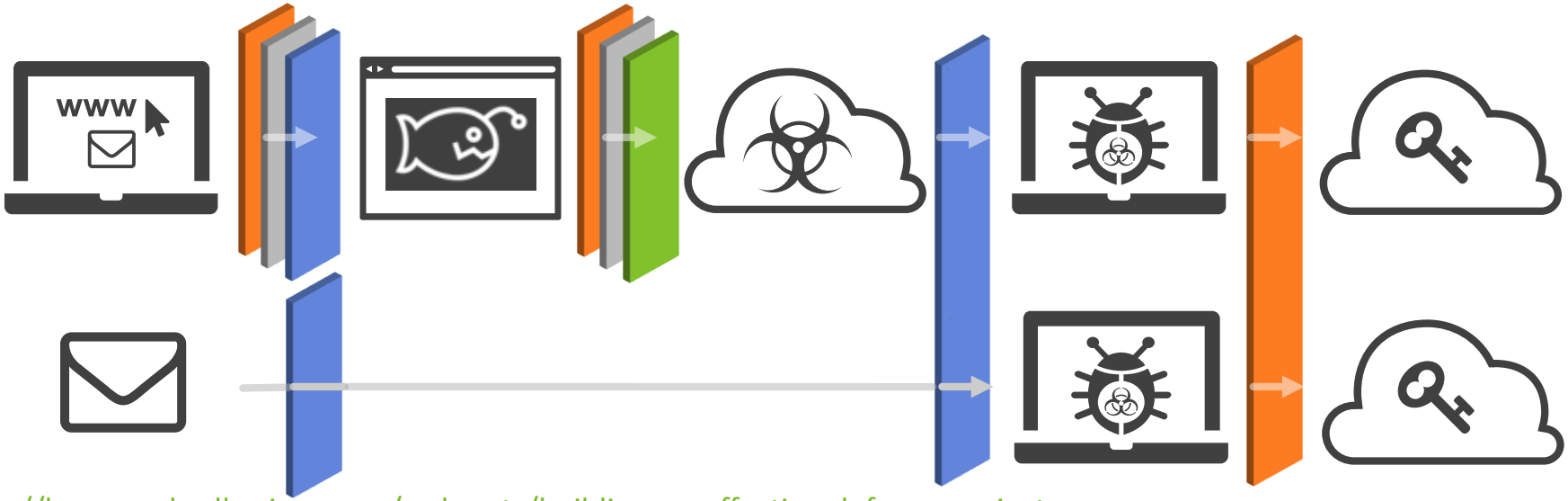
Umbrella blocks the request

NGFW blocks the connection

Lancope detects the activity

AMP for Endpoints blocks the file

Umbrella blocks the request



https://learn-umbrella.cisco.com/webcasts/building-an-effective-defense-against-ransomware

Umbrella | Next-Gen Firewall | AMP | Lancope

OpenDNS

Use cases

- Umbrella
  - Malware protection for mobile devices of VIP users (even without any agent)
  - Control of guest network
  - IoT environment
  - Content filtering for distributed branch offices (mobile users)
  - Block targetted zero-day attacks for roaming clients
- Investigate
  - Ease/speed up investigation for SOC (Security Operation Center) team

Top Use Cases to Add OpenDNS to Your Security Stack

OFF-NETWORK SECURITY

50% of PCs are already mobile[1]

SECURE DIRECT-TO-NET OFFICES

70% of offices already go direct[2]

NEW LAYER OF PREDICTIVE SECURITY

70-90% of malware is unique to each org[3]

SPEED UP INCIDENT RESPONSE

Only 4% of alerts are investigated per week

AUTOMATE ENFORCEMENT & VISIBILITY

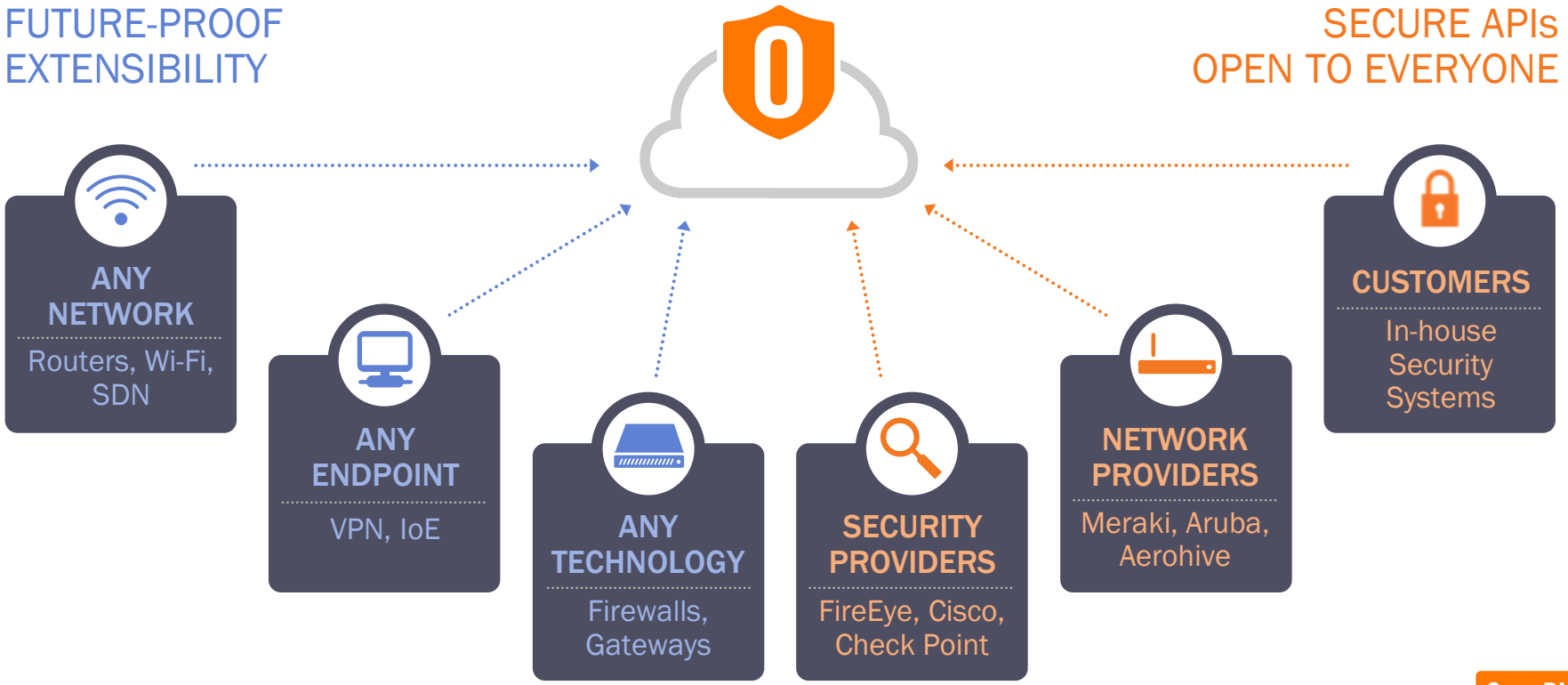
mean time-to-contain threats 26-39 hours[4]

WHY?

Sources: (1) Gartner, (2) Forrester, (3) Verizon, and (4) Ponemon

OpenDNS

OpenDNS Works With Everything You Use



OpenDNS

Useful links about OpenDNS

- Free account for Home users (single IP)
  - https://www.opendns.com/home-internet-security/
- Package comparison
  - https://learn-umbrella.cisco.com/datasheets/umbrella-package-comparison
- Documentation
  - https://docs.umbrella.com/

OpenDNS

Köszönöm a figyelmet!

OpenDNS is
now part of Cisco.

cisco

OpenDNS

Backup slides

OpenDNS is
now part of Cisco.

cisco

Leveraging a Single Global Recursive DNS Service

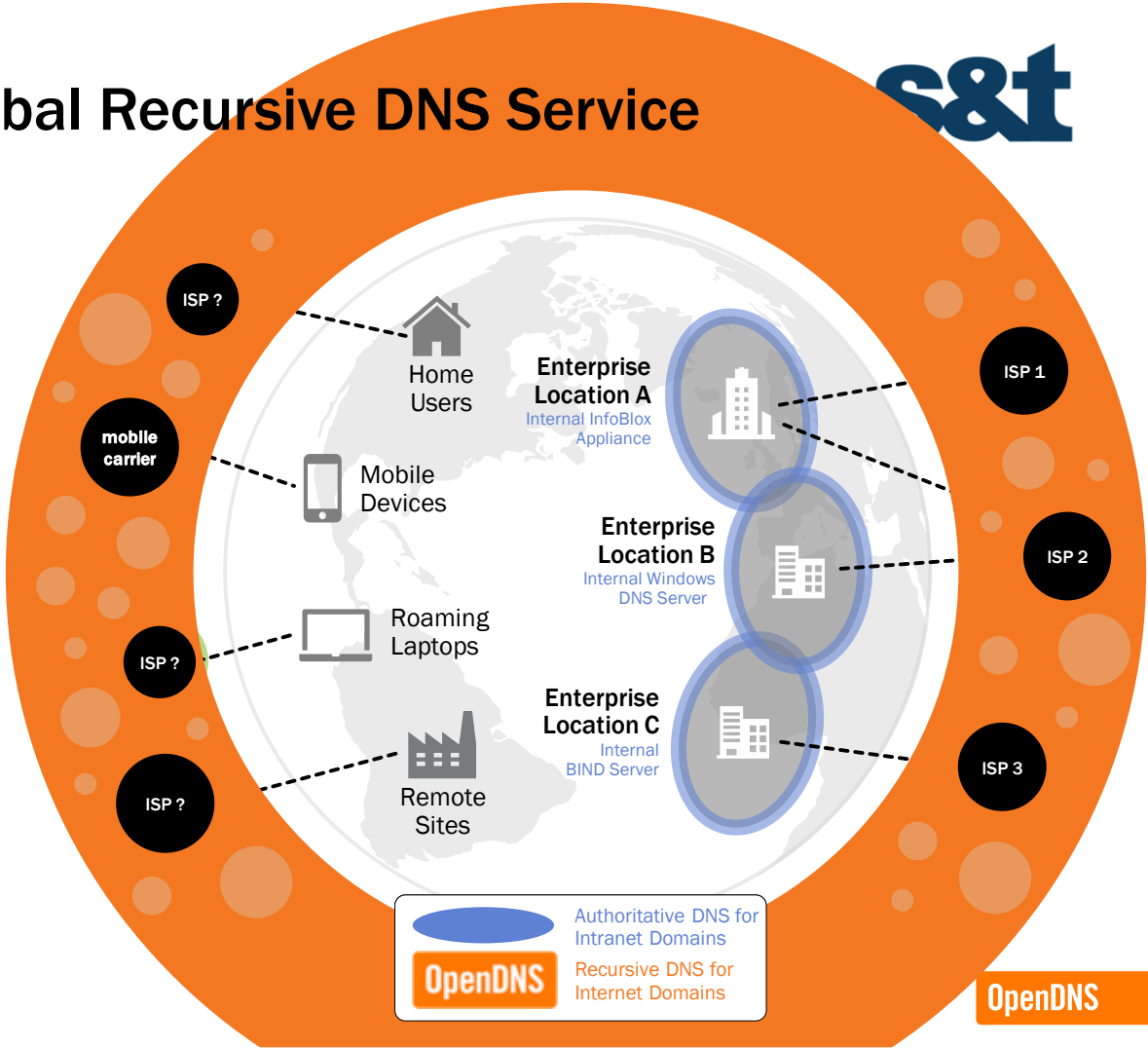
BENEFITS

Global Internet Activity Visibility

Network Security w/o Adding Latency

Consistent Policy Enforcement

Internet-Wide Cloud App Visibility



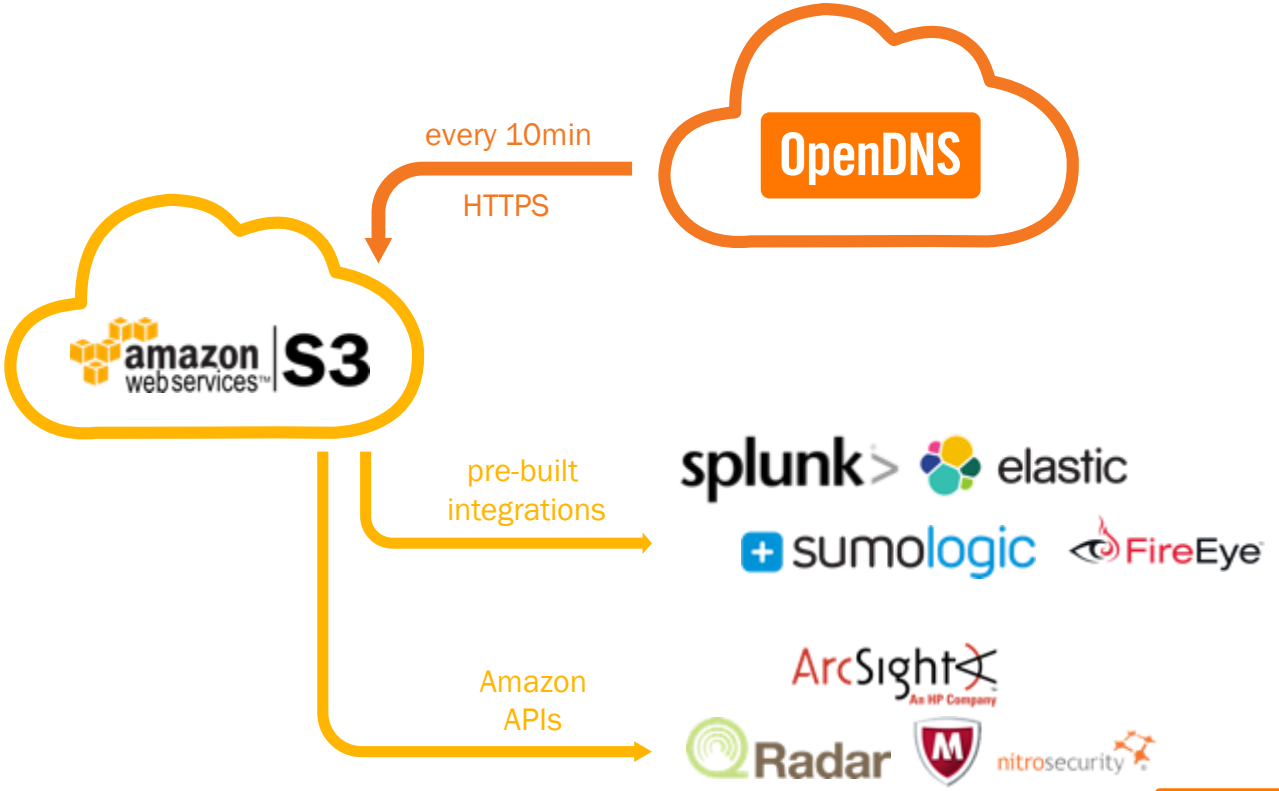
Retain Your Logs Forever with Our Amazon S3 Integration

S3 BENEFITS

Triple Redundant & Encrypted Storage

Pre-Built SIEM/Log Analytic Integrations

Elastic: Pay Only For The Storage Used



OpenDNS

Investigate

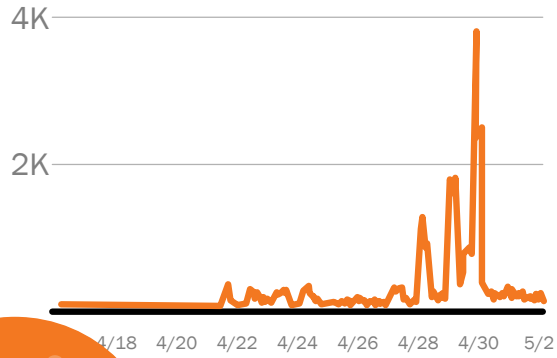
OpenDNS is
now part of Cisco.

cisco

Speed Up Investigations

See spikes in global requests to a domain

DNS Queries/Hour



Determine if malicious with attribution and tagging

This domain is **attributed** to the following attack: CryptoWall Ransomware

DOMAIN TAGGING

Period	Category
Apr 29, 2015 - Current	Malware

Discover attack details: IP and ASN reputation

Domain and IP are Located in a “Bad Neighborhood”

This domain has a suspicious **ASN score**

IP ADDRESSES

First seen	Last seen	IPs
5/14/15	5/14/15	62.162.192.216 (TTL: 0)
5/13/15	5/13/15	178.54.179.60 (TTL: 0)
5/11/15	5/11/15	109.86.140.145 (TTL: 0) 31.19.221.228 (TTL: 0) 95.87.9.11 (TTL: 0)
5/10/15	5/10/15	190.246.56.28 (TTL: 0) 77.121.91.21 (TTL: 0) 91.203.158.237 (TTL: 0)

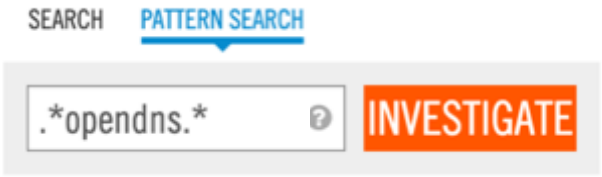
Domain associated with **many IPs** with very **short TTL**

OpenDNS

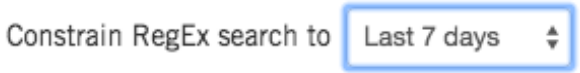
Find domains impersonating brand names

(a.k.a. cybersquatting or typosquatting)

Use pattern search to look for a brand name



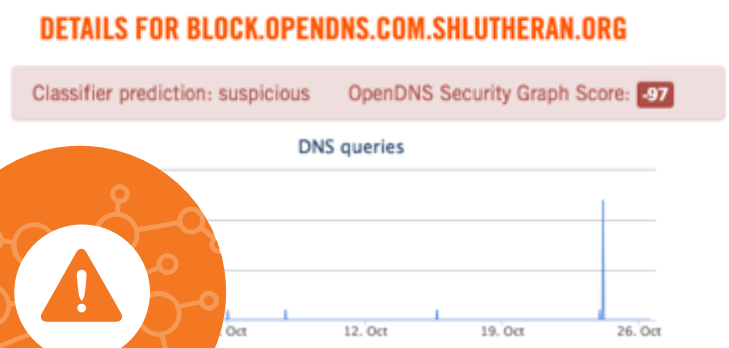
Decide to look for domains queried in past 7 days



Uncover all domains containing the brand name

Domain Name	First Seen
republika.co.id.opendns.com	October 22, 2015, 11:02pm
block.opendns.com.shlutheran.org	October 23, 2015, 11:20am
prefs-sync.e1.usw1.opendns.com	October 22, 2015, 4:53pm

Pivot on domains to further research



- Domain registered by privacy protection service

Email Address
privacyprotect@hebeidomains.com

- Hosted on different ASN from all OpenDNS domains

ASNs	AS 16276

- IP hosts more than 140 malicious domains

First seen	IPs
10/4/15	167.114.156.214 (TTL: 600)

Take action

Proactively block access for internal users & work to take down the domain

OpenDNS

OpenDNS

Integrations

OpenDNS is
now part of Cisco.

cisco

Turn-Key and API-Based Integrations

Works with what you already have

THREAT DETECTION

FireEye · Check Point SOFTWARE TECHNOLOGIES LTD. + OTHERS

THREAT ANALYSIS & INTEL FEEDS

cisco · ZEROFOX + OTHERS

THREAT INTEL PLATFORMS

THREATQUOTIENT · THREATCONNECT + CUSTOM

Indicators of Compromise

UMBRELLA

Enforcement & Visibility

Logs or blocks domains sent from partner or custom systems

OpenDNS

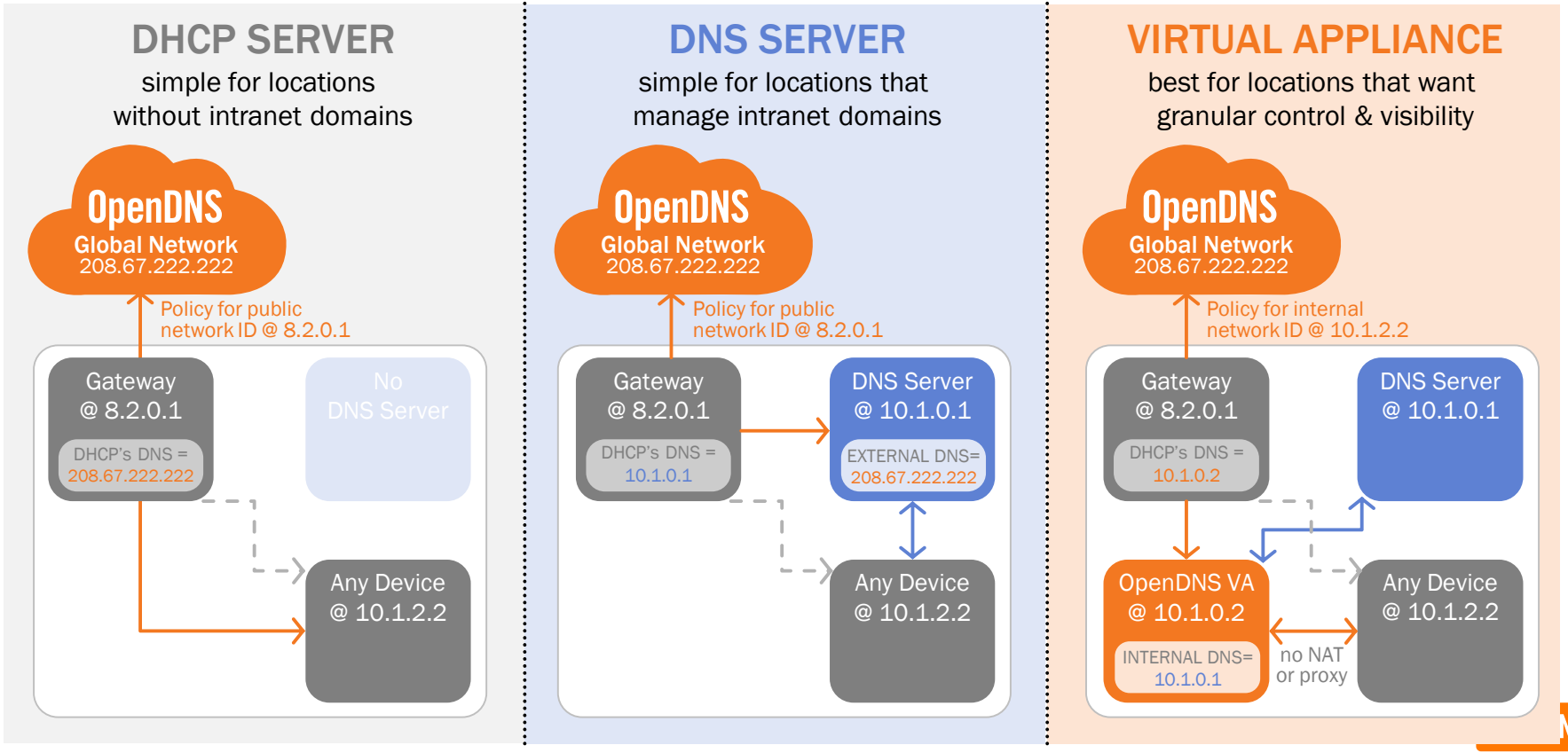
OpenDNS

How Coverage & Enforcement Work

OpenDNS is now part of Cisco.

cisco

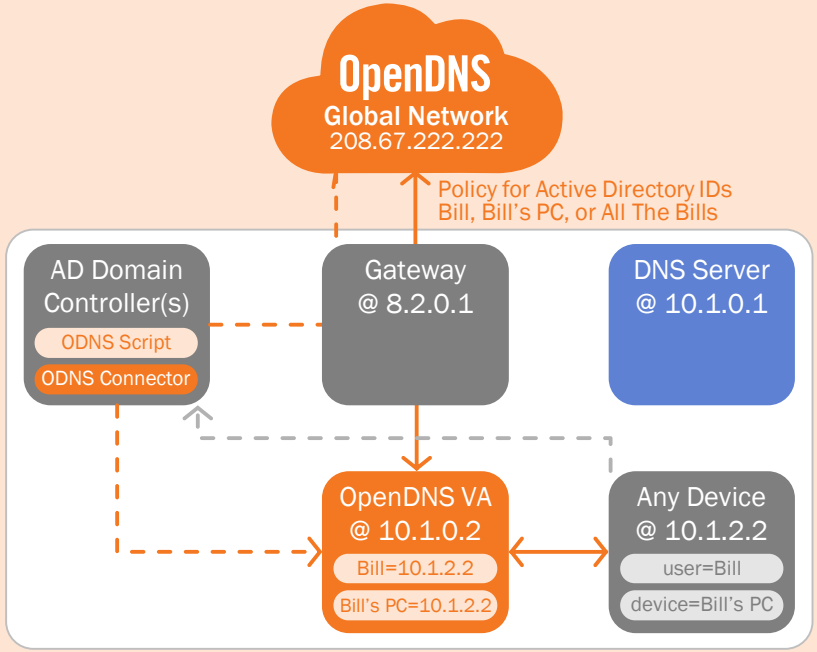
ON-NET: How We Enforce by Public or Internal Networks



ON-NET: How We Enforce by AD User/Device/Group

VIRTUAL APPLIANCE AND CONNECTOR

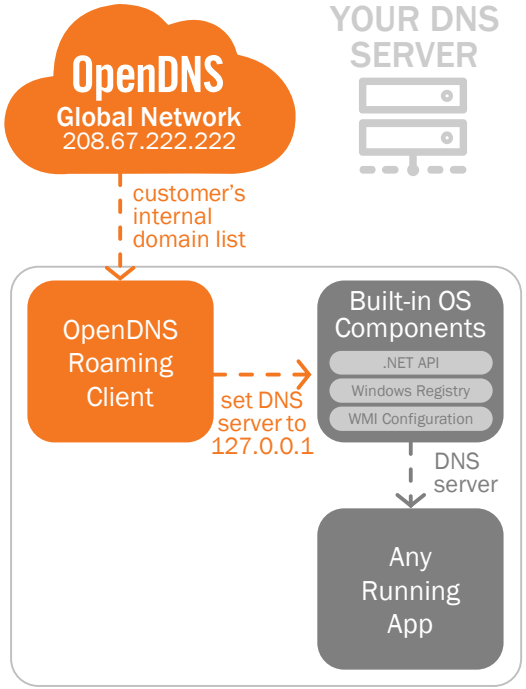
best for locations that want granular control & visibility integrated with AD



OFF-NET: How We Enforce Security at the DNS Layer

STEP 1

watch for new networks
& continuously set DNS



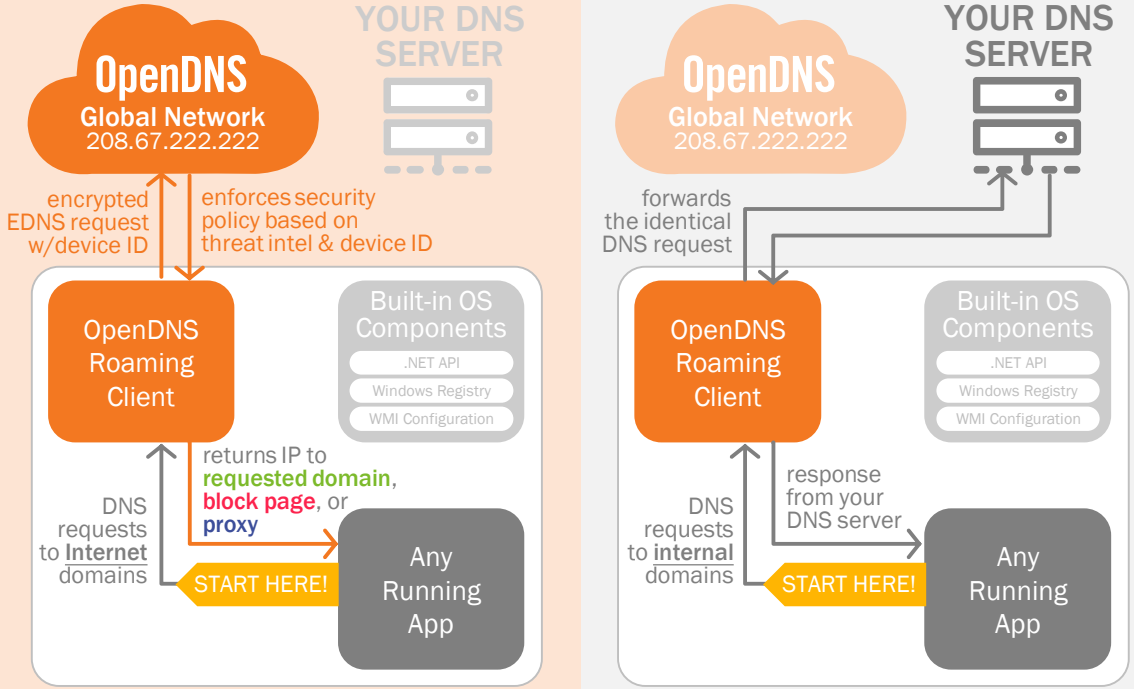
STEP 2a

Internet domains
resolved by OpenDNS

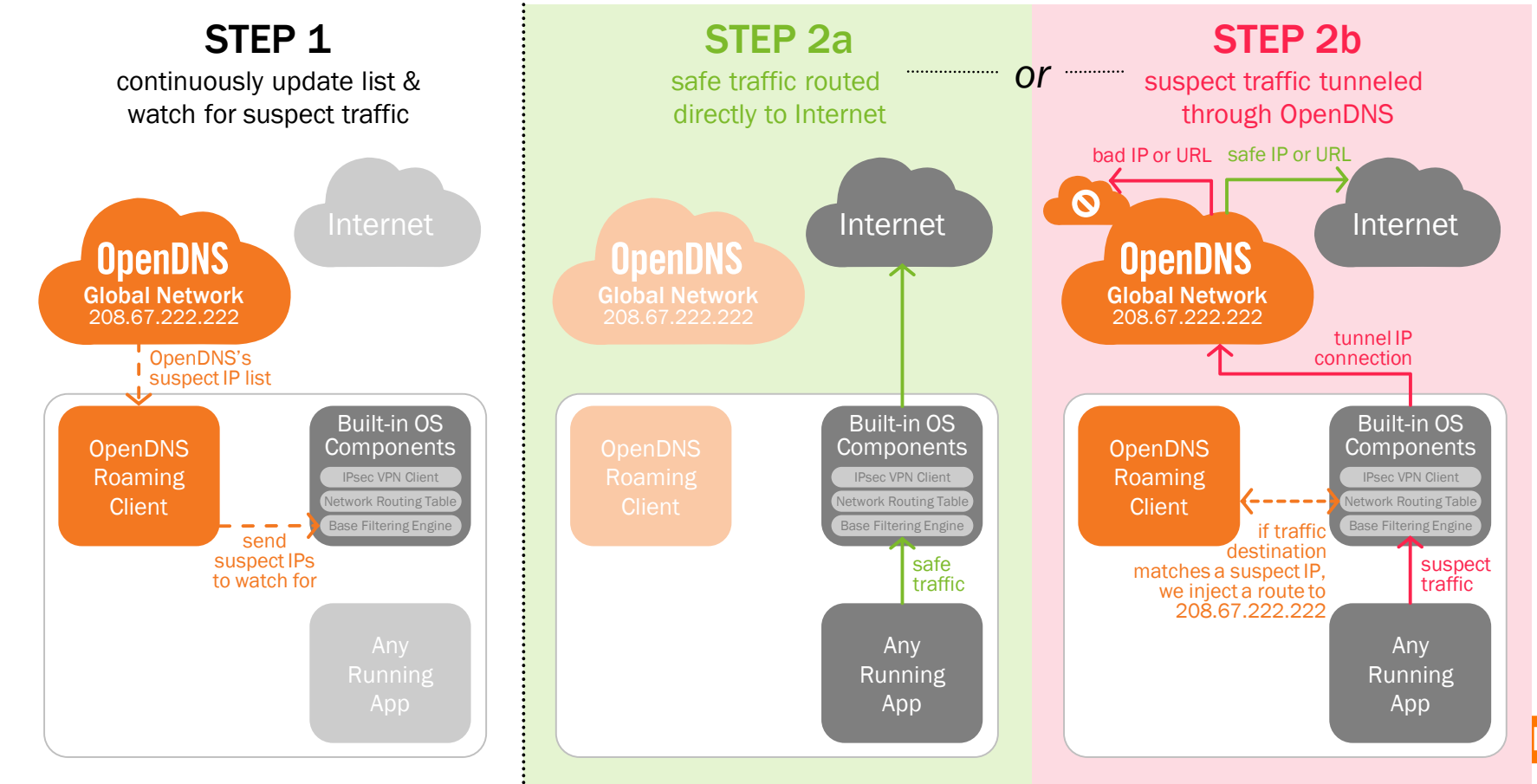
or

STEP 2b

Internal domains
resolved by your DNS server



OFF-NET: How We Enforce Security at the IP Layer

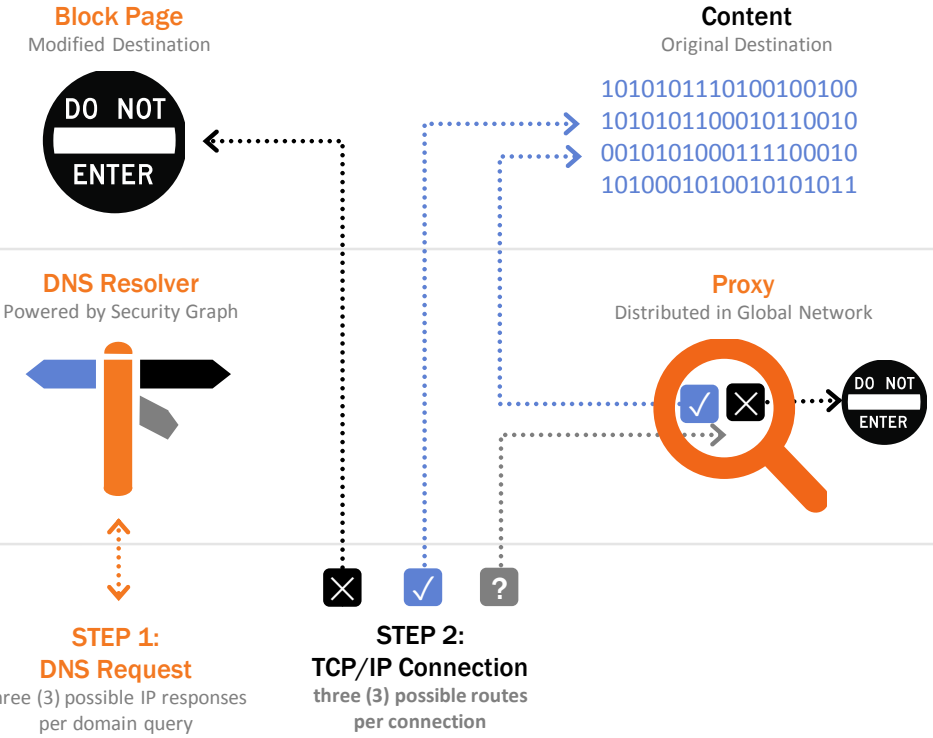


How Stuff Works: Intelligent Proxy

Internet Locations
Connections are only made to safe Internet locations by modifying the original destination

Security Controls
DNS provides Internet-wide enforcement, then proxy provides deep inspection at URL-level

Network Traffic
On- and off-network devices send requests to our resolvers, then connections are implicitly enforced



OpenDNS