



Introducing Cisco Umbrella for Cloud Based Threat Protection

Szilard Csordas,

Consulting Security Engineer

Agenda

Introduction

- What is Cisco Umbrella
- Architecture & Data Flow
- Statistical Models



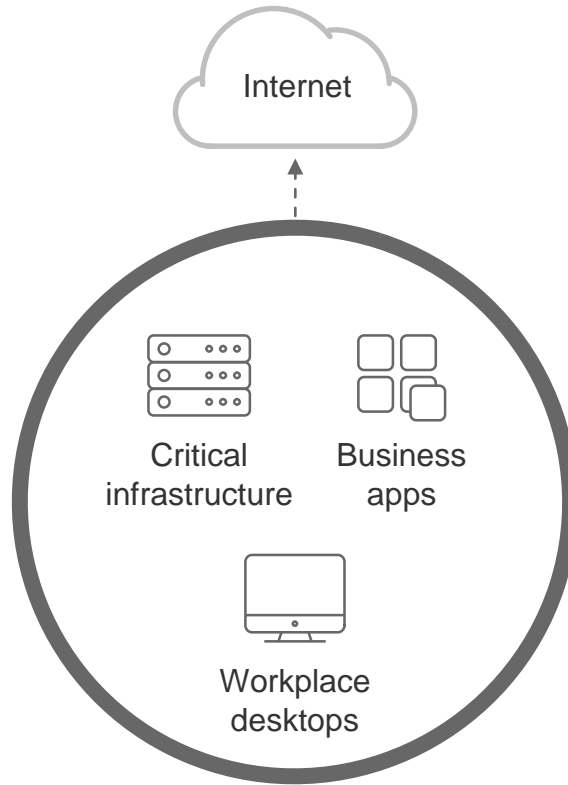
By 2020, Cisco Global Cloud Index estimates:

92% of global data
center traffic will come
from the cloud

By 2021, Gartner estimates:

25% of corporate
data traffic will **bypass**
perimeter security

How IT was Built



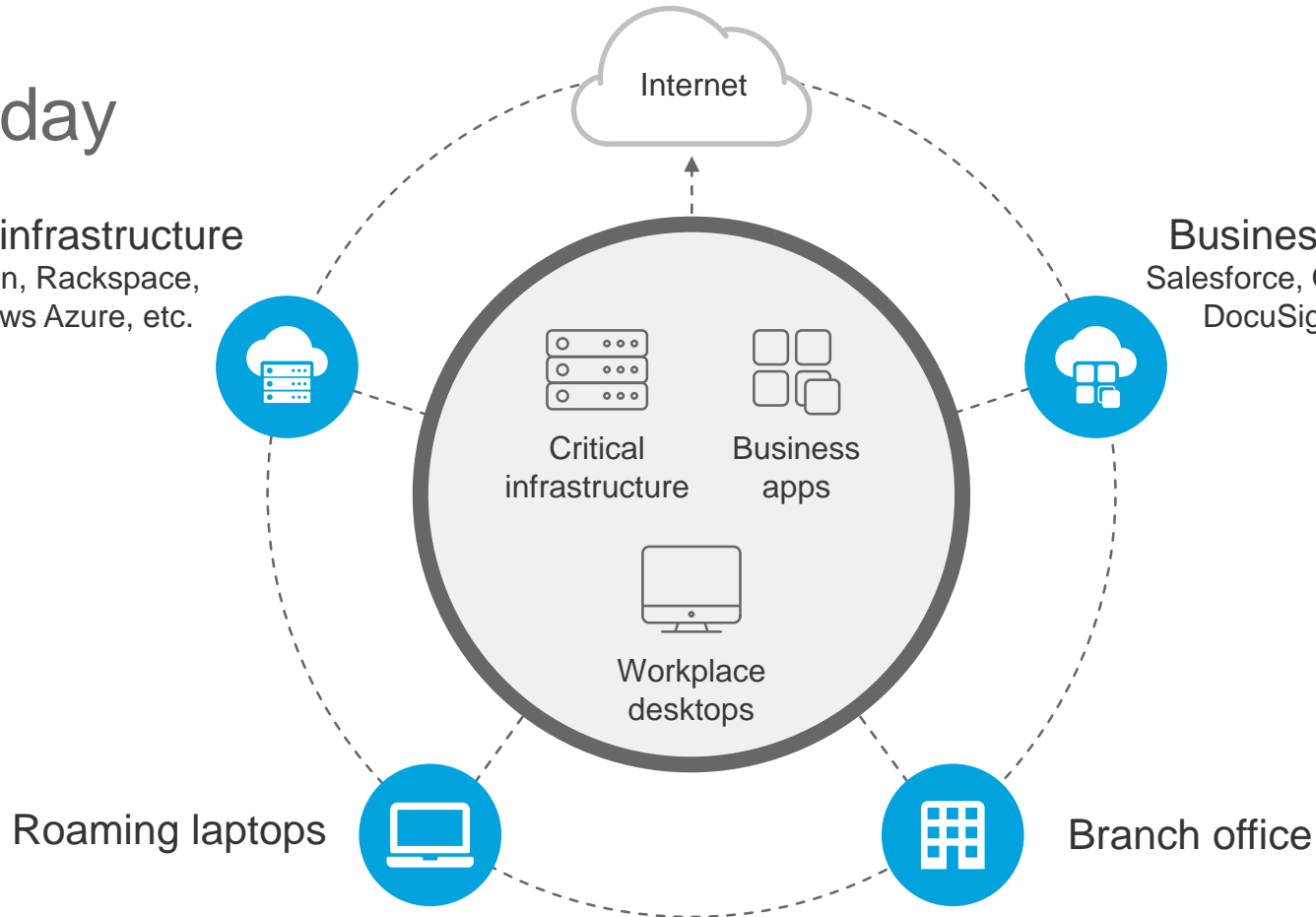
IT Today

Critical infrastructure

Amazon, Rackspace,
Windows Azure, etc.

Business apps

Salesforce, Office 365,
DocuSign, etc.



Agenda

- 👤 Introduction
- 👤 What is Cisco Umbrella
 - Architecture & Data Flow
 - Statistical Models





On and off the corporate network

All ports and protocols

Open platform

Live threat intelligence

Proxy and file inspection

Discovery and control of SaaS

DNS Overview



Domain registrar

Maps and records names to #s in “phone books”



Authoritative DNS

Owens and publishes the “phone books”



Recursive DNS

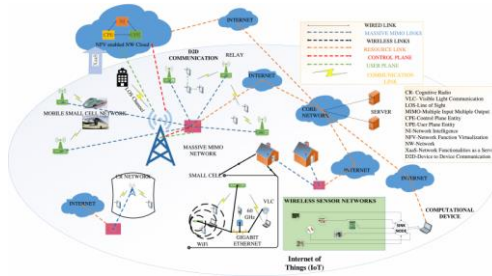
Looks up and remembers the #s for each name



DNS is the Critical Lifeline of the Network



Every possible Device

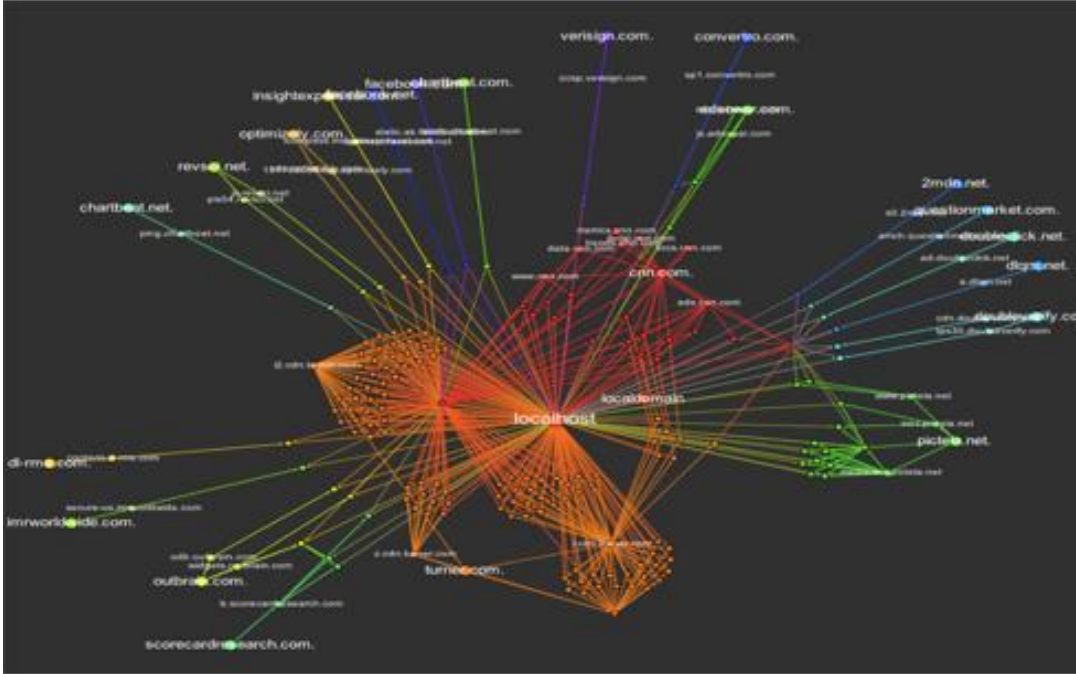


All Network Architectures



All Operating Systems

What happens when you visit a single site?



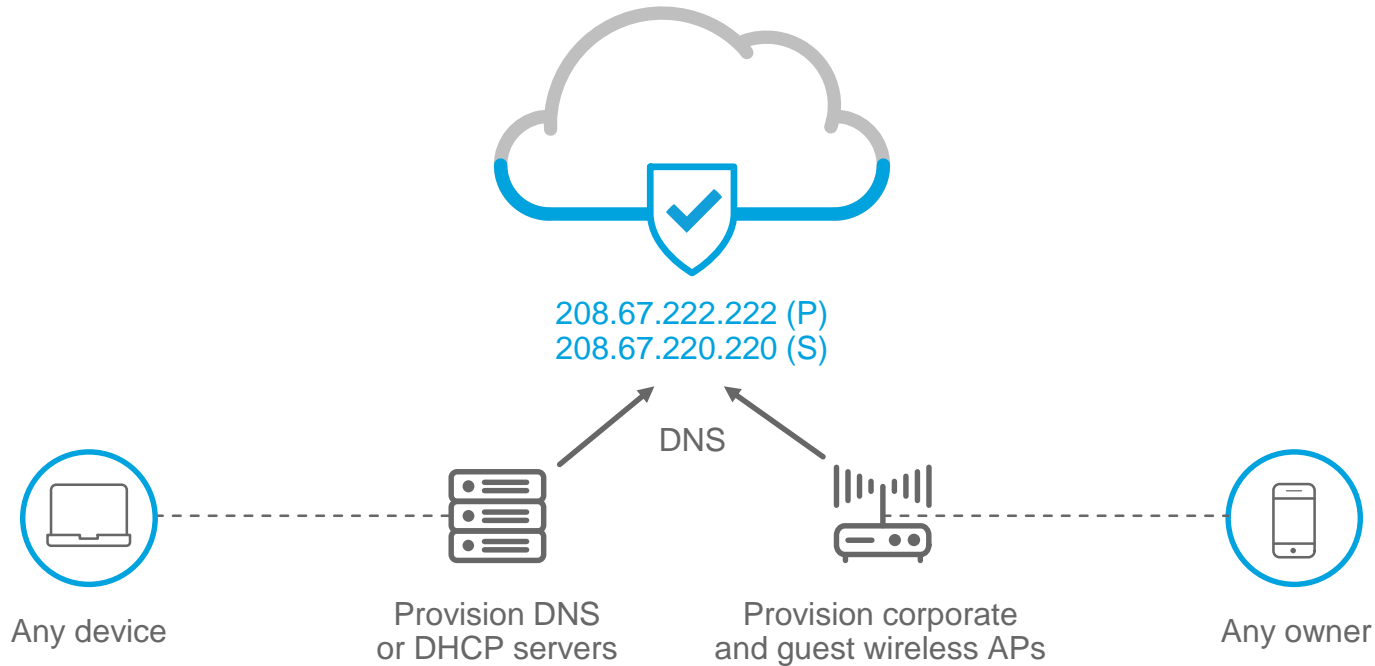
68%

of organizations
don't monitor
DNS

Simplest Security Deployment on the Planet

Point external DNS traffic to Umbrella

NETWORK DEPLOYMENT

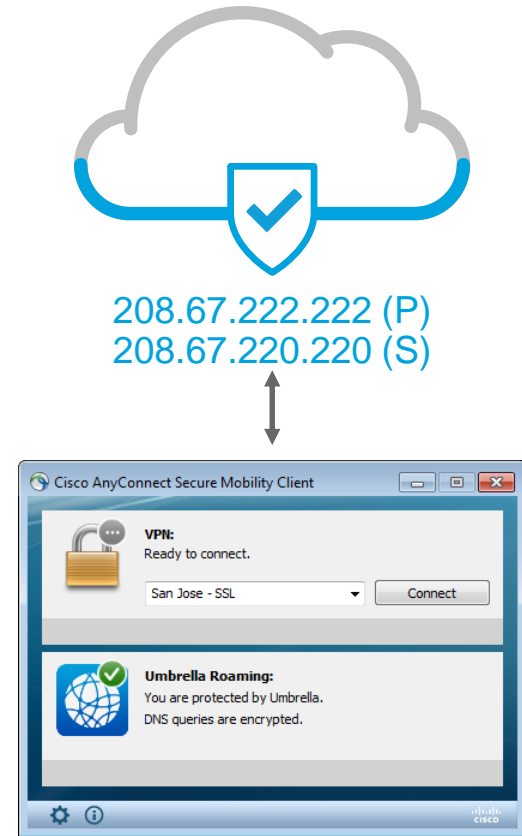


Cisco AnyConnect Module

Roaming protection without another agent

ENDPOINT DEPLOYMENT

- 1 Enable roaming security module
- 2 Set roaming policy in Umbrella
- 3 Gain visibility into internet activity and detailed logs for incident response



Cisco Security Connector

One app, two layers of security to protect enterprise iOS users

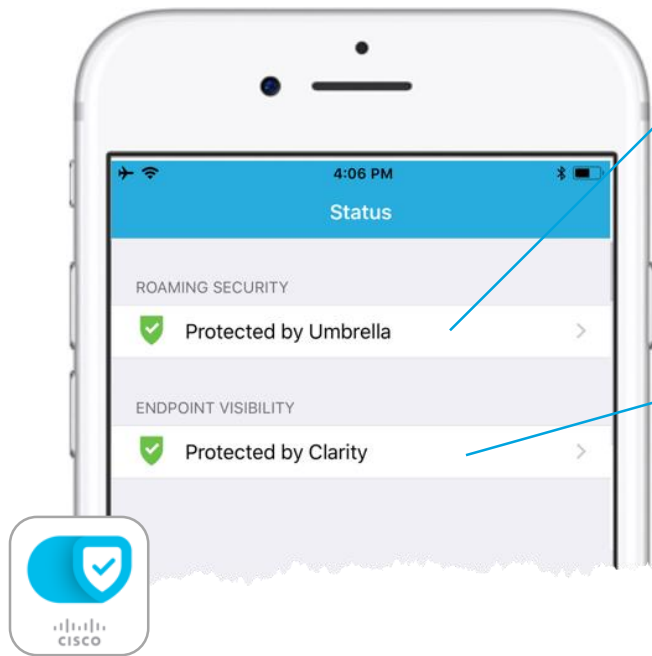
MOBILE DEPLOYMENT

VISIBILITY & CONTROL

- DNS-layer enforcement and encryption via net new iOS 11 functionality
- Customizable URL-based protection with intelligent proxy
- Available to Umbrella¹ customers at no extra charge if subscription already covers iOS users

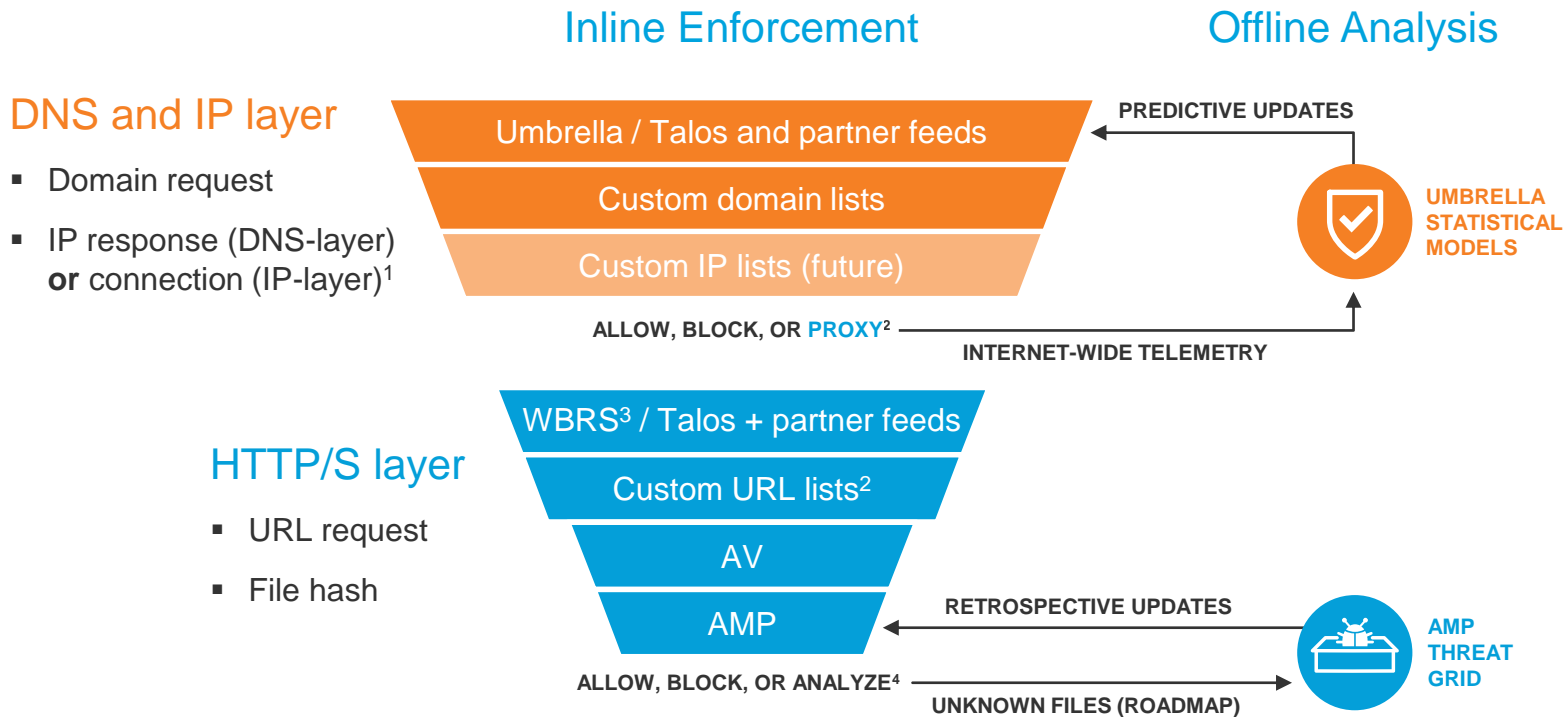
VISIBILITY

- App-layer auditing and correlation via net new iOS 11 functionality
- Logs encrypted URL requests without SSL decryption
- Available to AMP for Endpoints customers at no extra charge if subscription already covers iOS devices

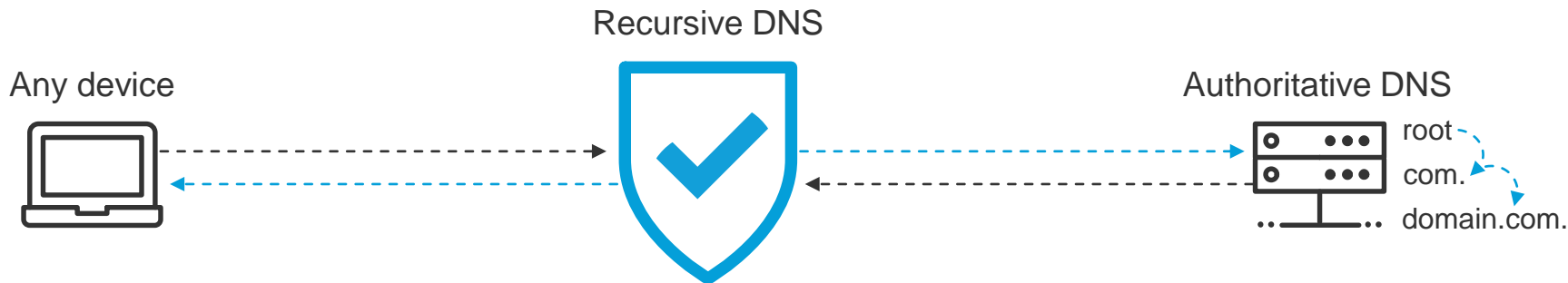


Enforcing Inline, Analyzing Offline

Breadth to cover all ports and depth to inspect risky domains



Gather Intelligence, Enforce Security at the DNS Layer



User request patterns

Used to detect:

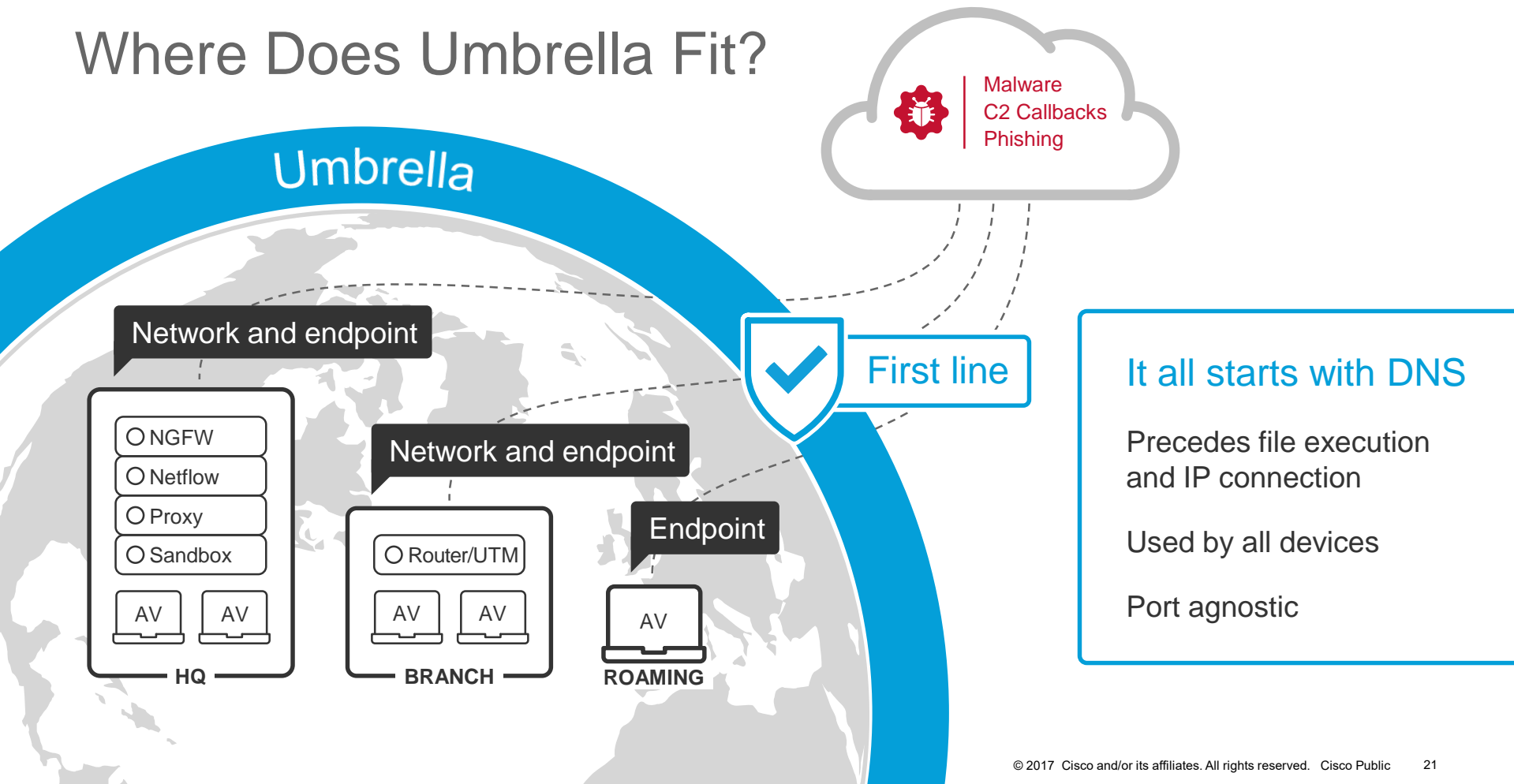
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs

Used to find:

- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

Where Does Umbrella Fit?



Umbrella Resolver Flow

Destinations

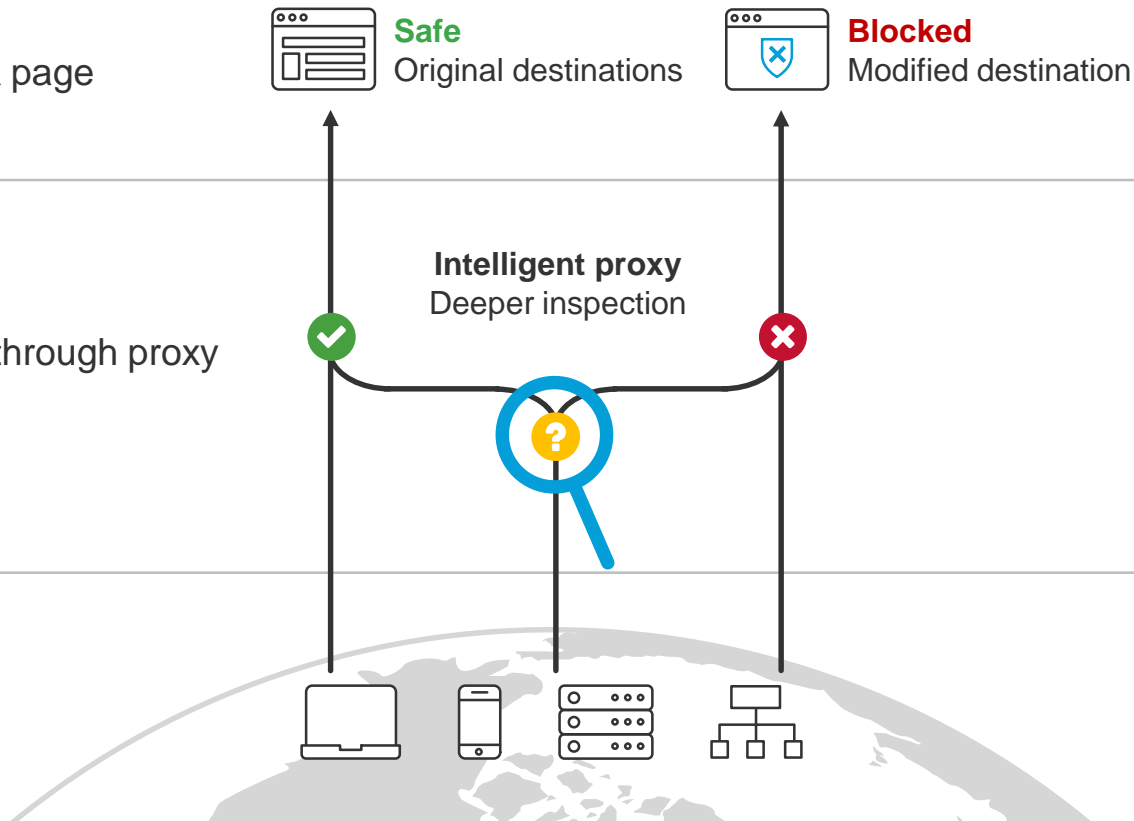
Original destination or block page

Security controls

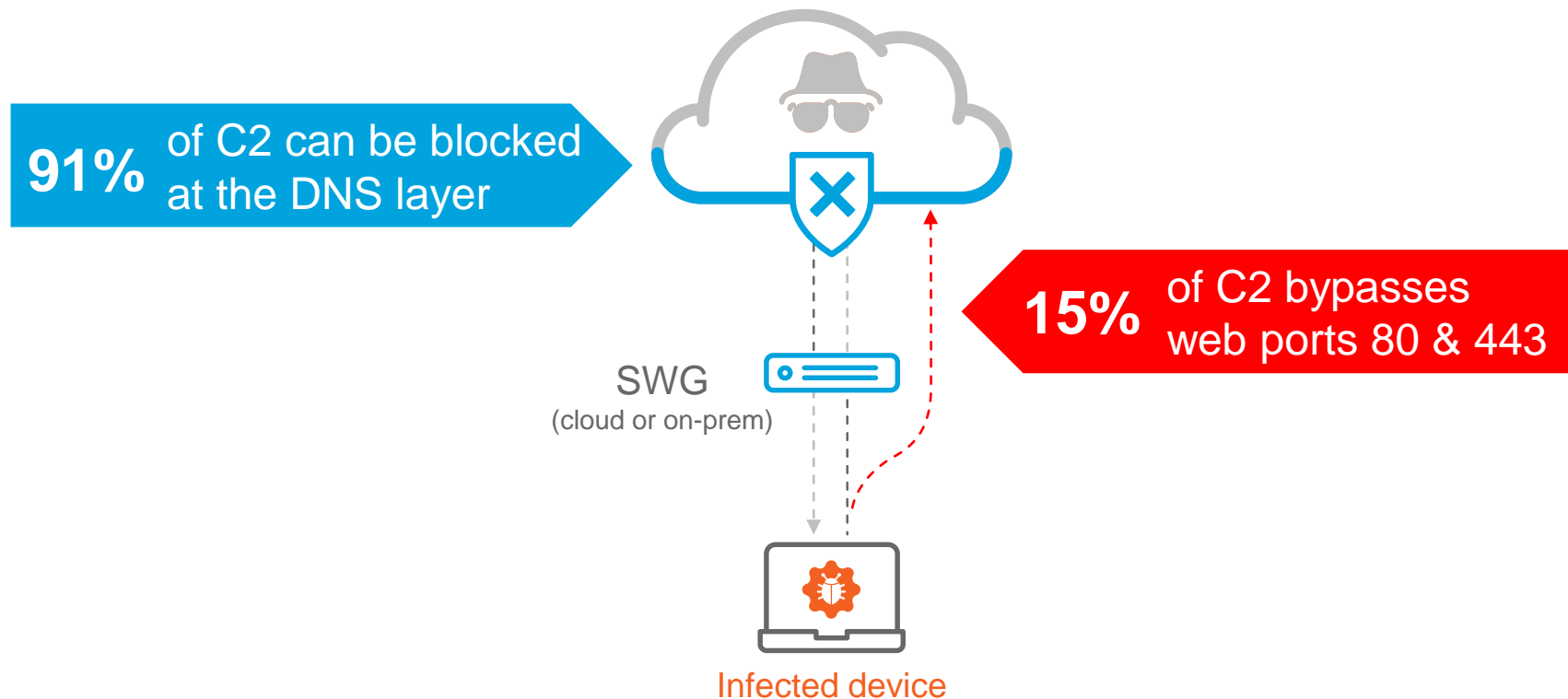
- DNS and IP enforcement
- Risky domain inspection through proxy
- SSL decryption available

Internet traffic





On- and off-network



Protection for Command and Control Callbacks



Agenda

-  Introduction
-  What is Cisco Umbrella
-  Architecture & Data Flow
-  Statistical Models



Umbrella Data Centers Co-located at Major IXPs

Umbrella Datacenters

- Amsterdam
- Berlin
- Bucharest
- Chicago
- Copenhagen
- Dallas
- Frankfurt
- Hong Kong
- Johannesburg
- London
- Los Angeles
- Miami
- New York
- Palo Alto
- Paris
- Prague
- Seattle
- Singapore
- Sydney
- Tokyo
- Toronto
- Vancouver
- Warsaw
- Washington DC



<https://system.opendns.com/>

Current Status

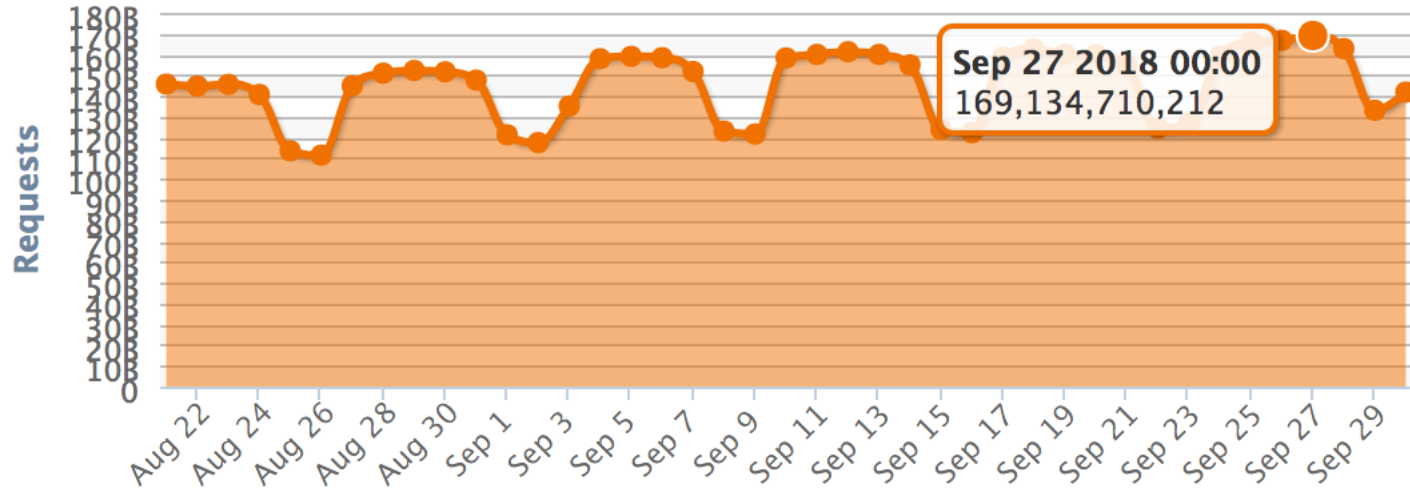
Location Status

AMS	ASH	BER	CDG1	CHI	CPH1	DFW	DUB1	DXB1	FRA	HKG	JNB	LAX	LON	MEL1	MIA	MIL1	MUM1	NRT	NYC	OTP1	PAO	PRG1	SAO1	SEA	SIN	SYD	WRW	YVR	YYZ
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

System is currently online.

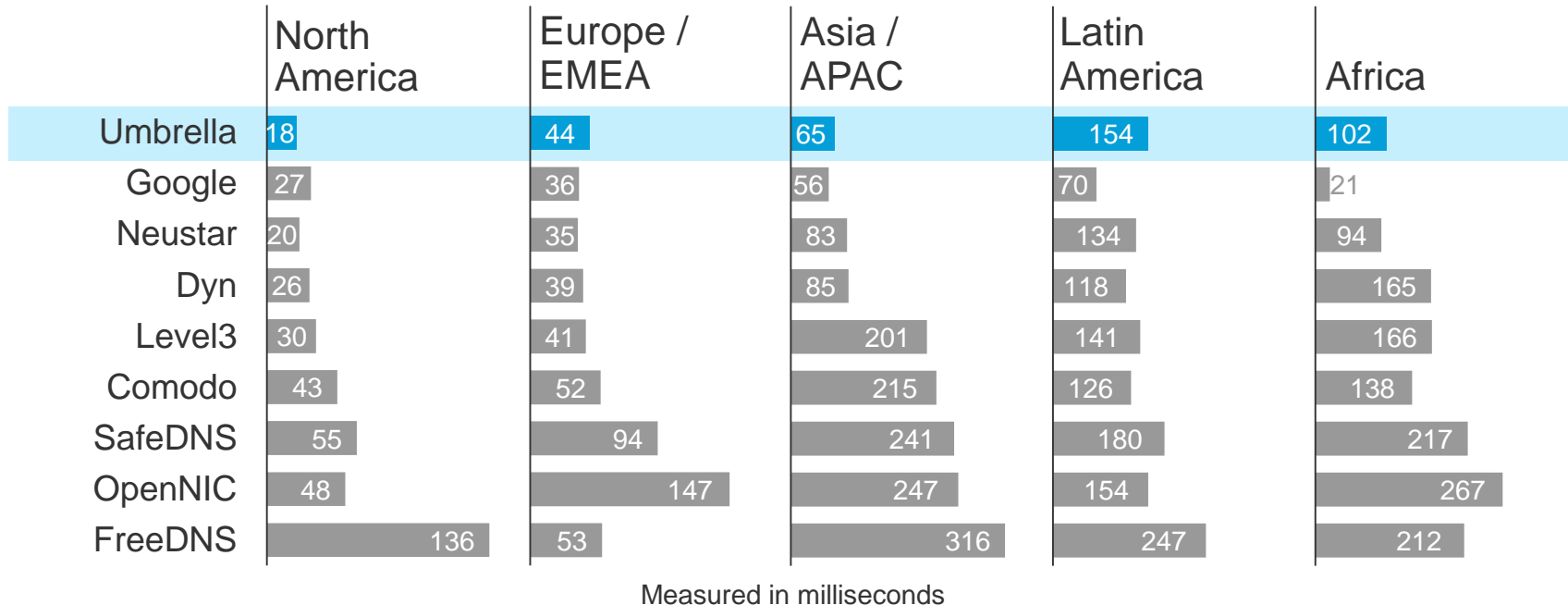
Total Activity

Number of DNS requests per day in billions





How Fast does Umbrella Resolve DNS Requests?

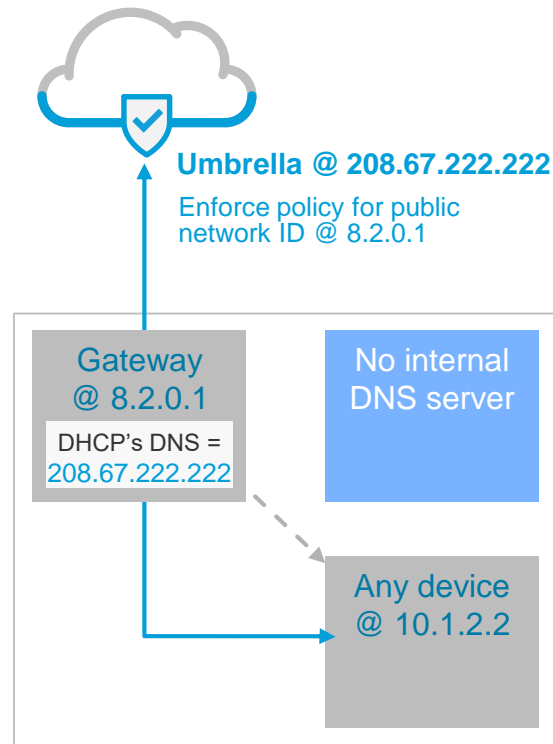


Source: MSFT Office 365 Researcher,
ThousandEyes Blog Post, May 2015

On-network Protection

DHCP Server – For locations without internal domains

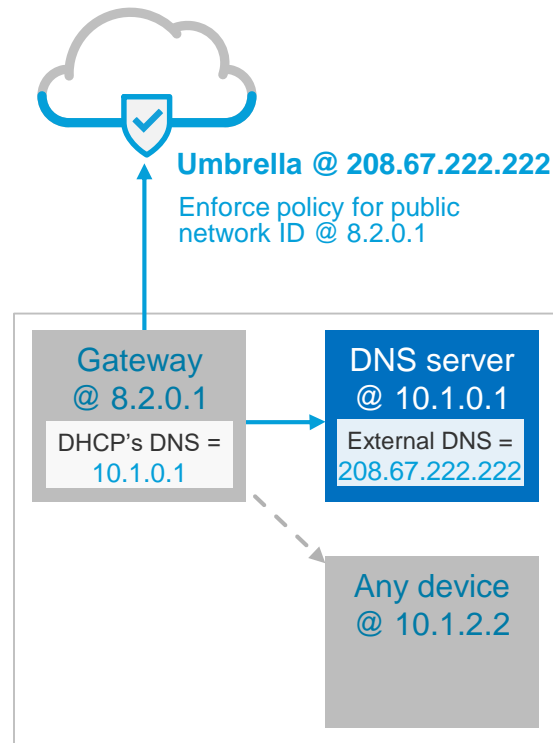
- Uses built-in DHCP server on router, switch, Wi-Fi AP, firewall, SWG, or Windows Server
- DNS IP address is changed to Umbrella
- All devices connected to the network will point DNS requests to Umbrella
- Works best if there are no internal domains i.e. printers or intranet that require local resolution



On-network Protection

DNS Server – For locations that manage internal domains

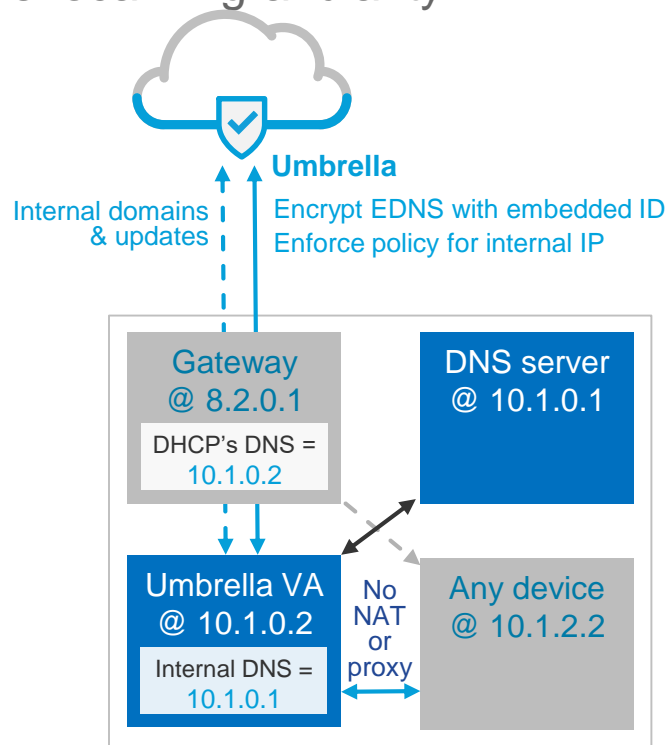
- DNS server (or any device performing resolution) present on the network for internal resolution
- DNS server is configured to forward all external DNS requests for Internet domains to Umbrella
- In this and previous deployment scenario, policy control and visibility is still limited to the network's public facing IP address



On-network Protection

Umbrella Virtual Appliance – For locations that require local IP granularity

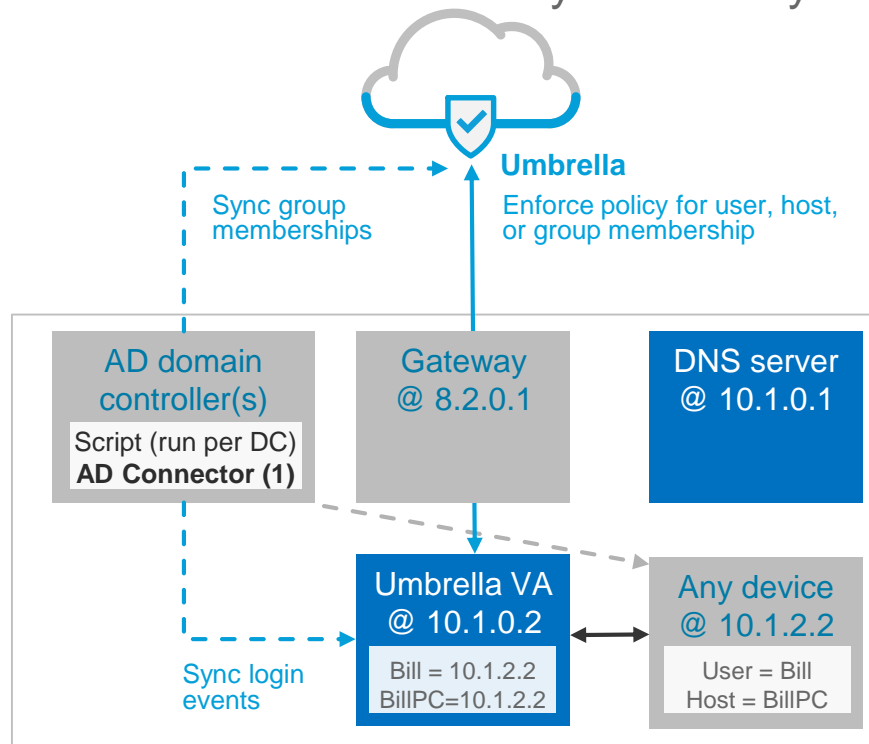
- Supported on VMware and Hyper-V
- Internal/external requests sent to VA
- Internal requests resolved locally
- VA embeds local IPs into RFC-compliant extension mechanisms for DNS



On-network Protection

Virtual Appliance + AD Connector – For granular control and visibility with AD sync

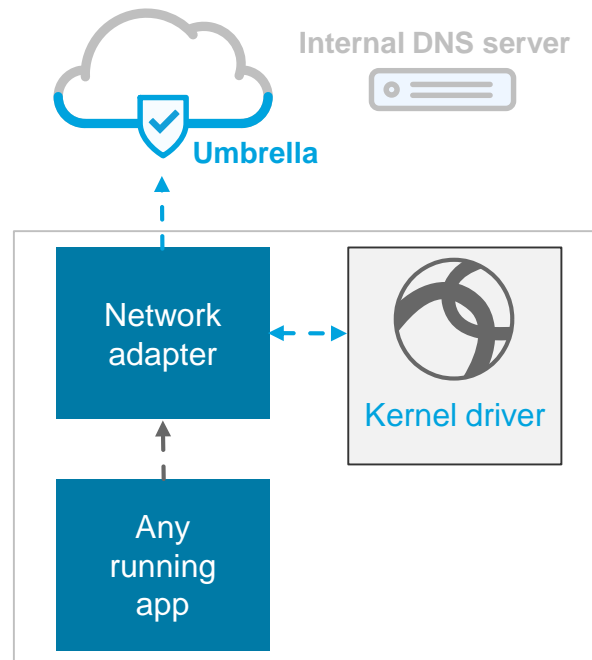
- DCs registered with Umbrella
- Connector service is installed on **one** DC/member:
 1. Syncs group memberships of users and computers with Umbrella
 2. Sends IP to user mapping to VAs
- VA embeds unique identifiers that Umbrella uses for control & visibility



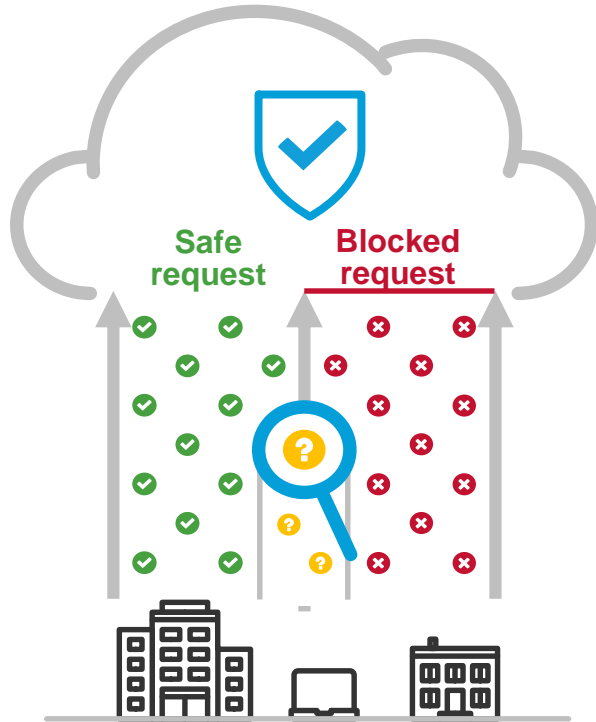
AnyConnect

Off-network protection, with and without VPN

- Captures all DNS traffic locally transparently, and redirects from Kernel level to Umbrella (Uses the AC Kernel driver)
- Supported when on and off VPN
- Supports optional binary updates (for all AC modules) without the need of an ASA head-end



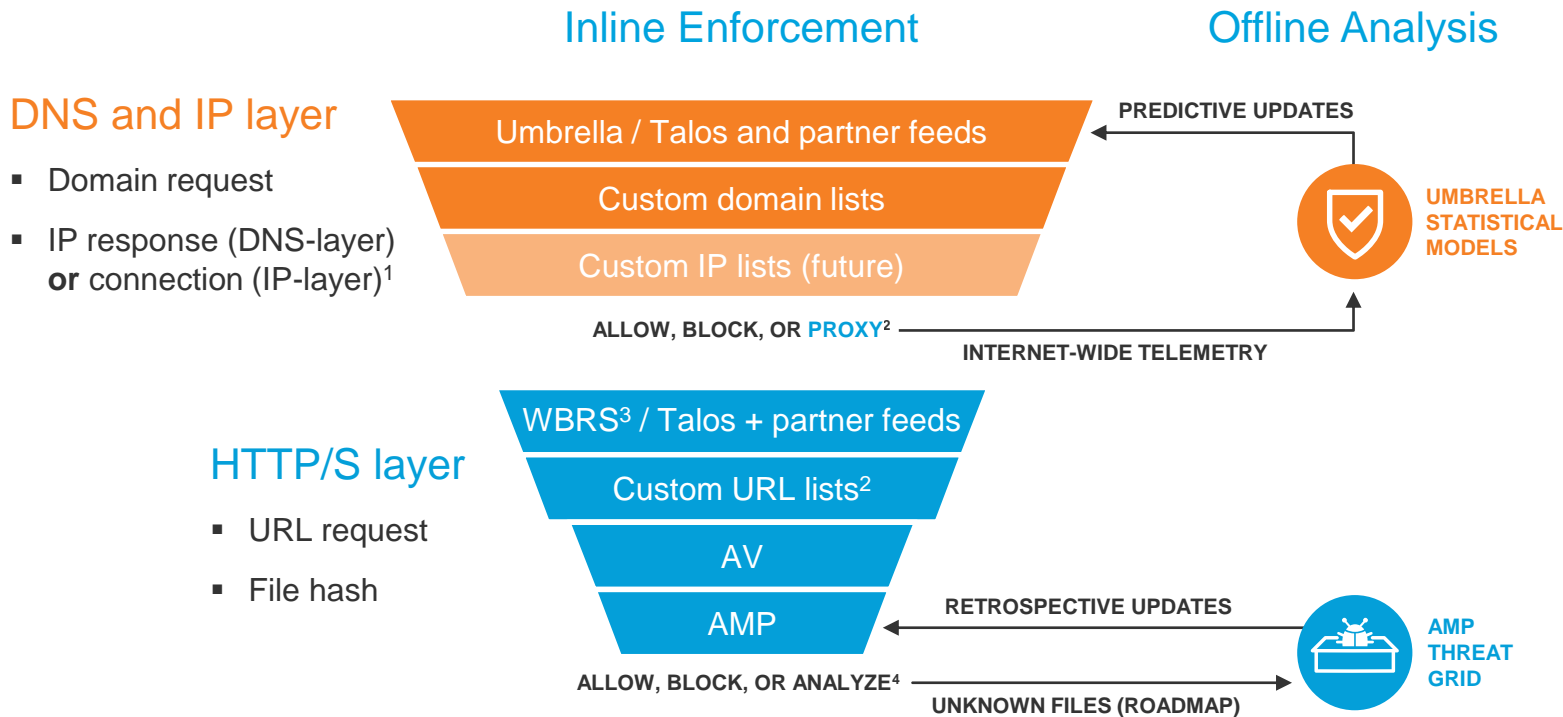
Data Flow - Recap



- DNS request sent to Umbrella
- For safe requests that are not blocked by policy, the resolved IP address is returned
- Requests to malicious or prohibited destinations get redirected to block page (hosted by Umbrella or company)
- Requests to unknown destinations, or those that were defined for further inspection will be redirected to the intelligent proxy for further analysis

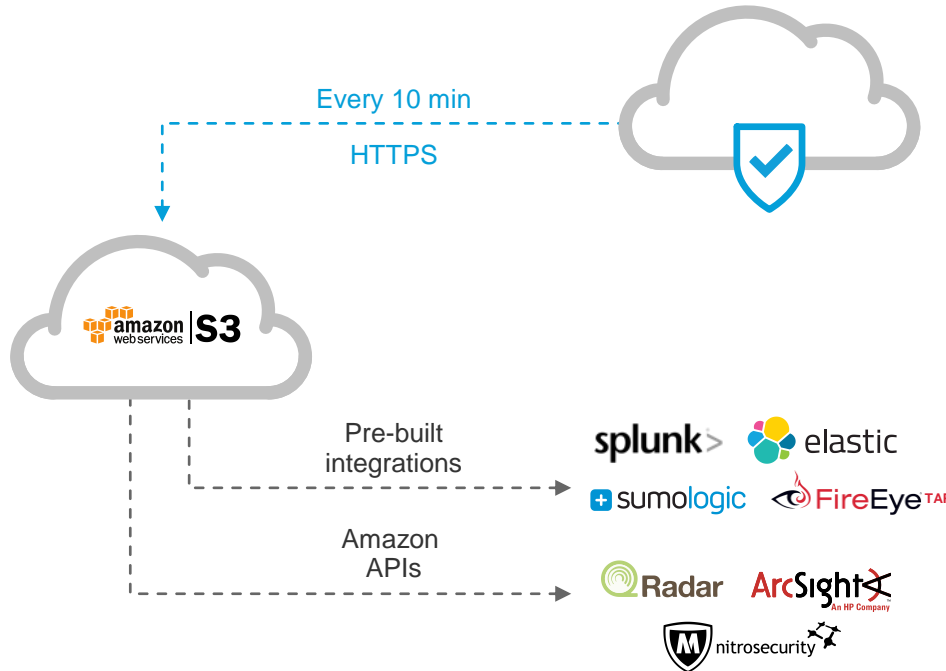
Enforcing Inline, Analyzing Offline

Breadth to cover all ports and depth to inspect risky domains



Cloud-to-Cloud Log Storage Solution

with Amazon S3







S3 Benefits

Triple redundant and encrypted storage

Pre-built SIEM / log analytic integrations

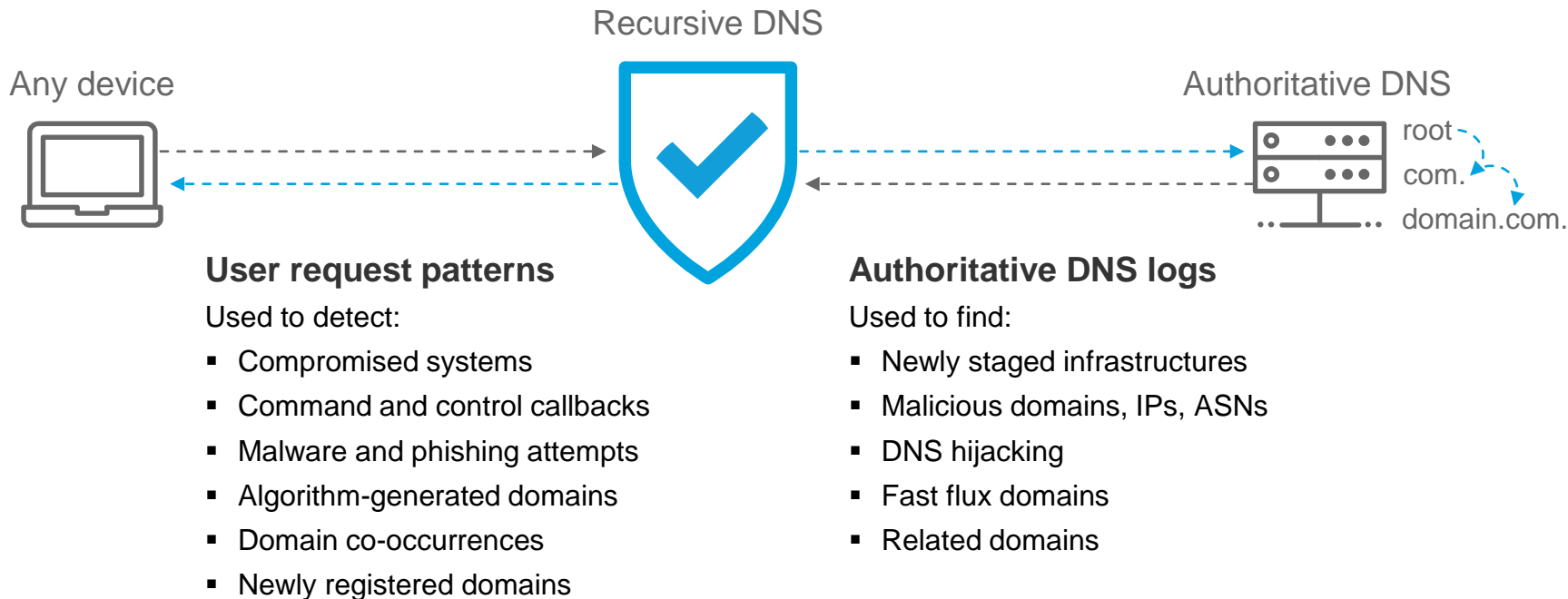
Elastic: pay only for the storage used

Agenda

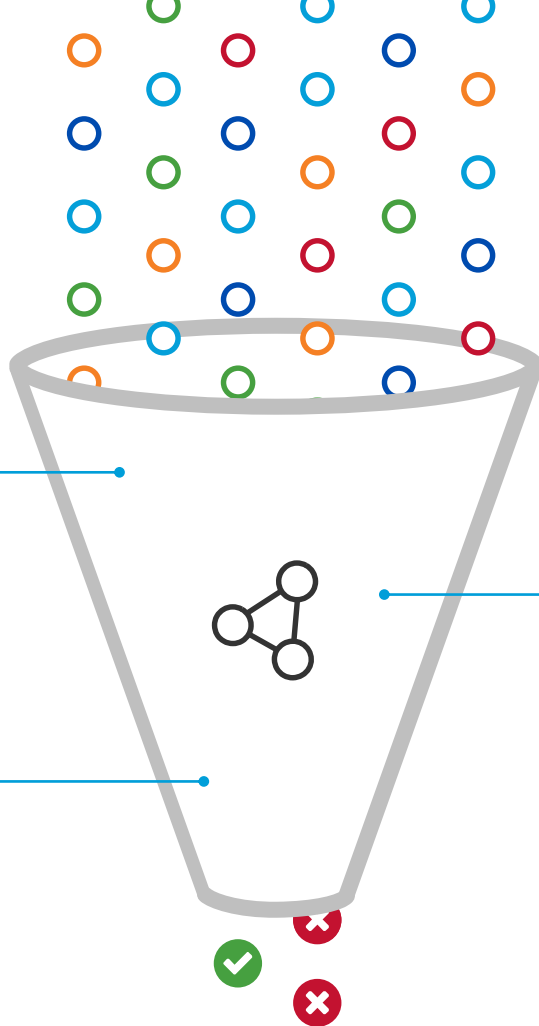
-  Introduction
-  What is Cisco Umbrella
-  Architecture & Data Flow
-  Statistical Models



Gathering Intelligence at the DNS Layer



Statistical Models



2M+ live events per second

11B+ historical events

Guilt by inference

- Co-occurrence model
- IP Geo-Location model
- Secure rank model
- Sender rank model

Guilt by association

- Predictive IP Space Modeling

Patterns of guilt

- Spike rank model
- Natural Language Processing rank model
- Live DGA Prediction

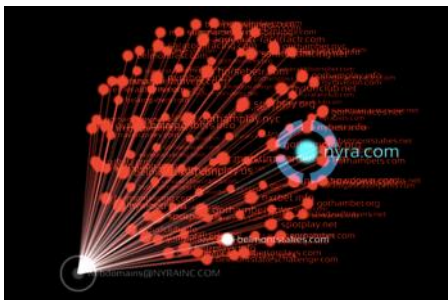
Statistical Models: Inference Graph



Domain-IP Relationships in C2 Infrastructure



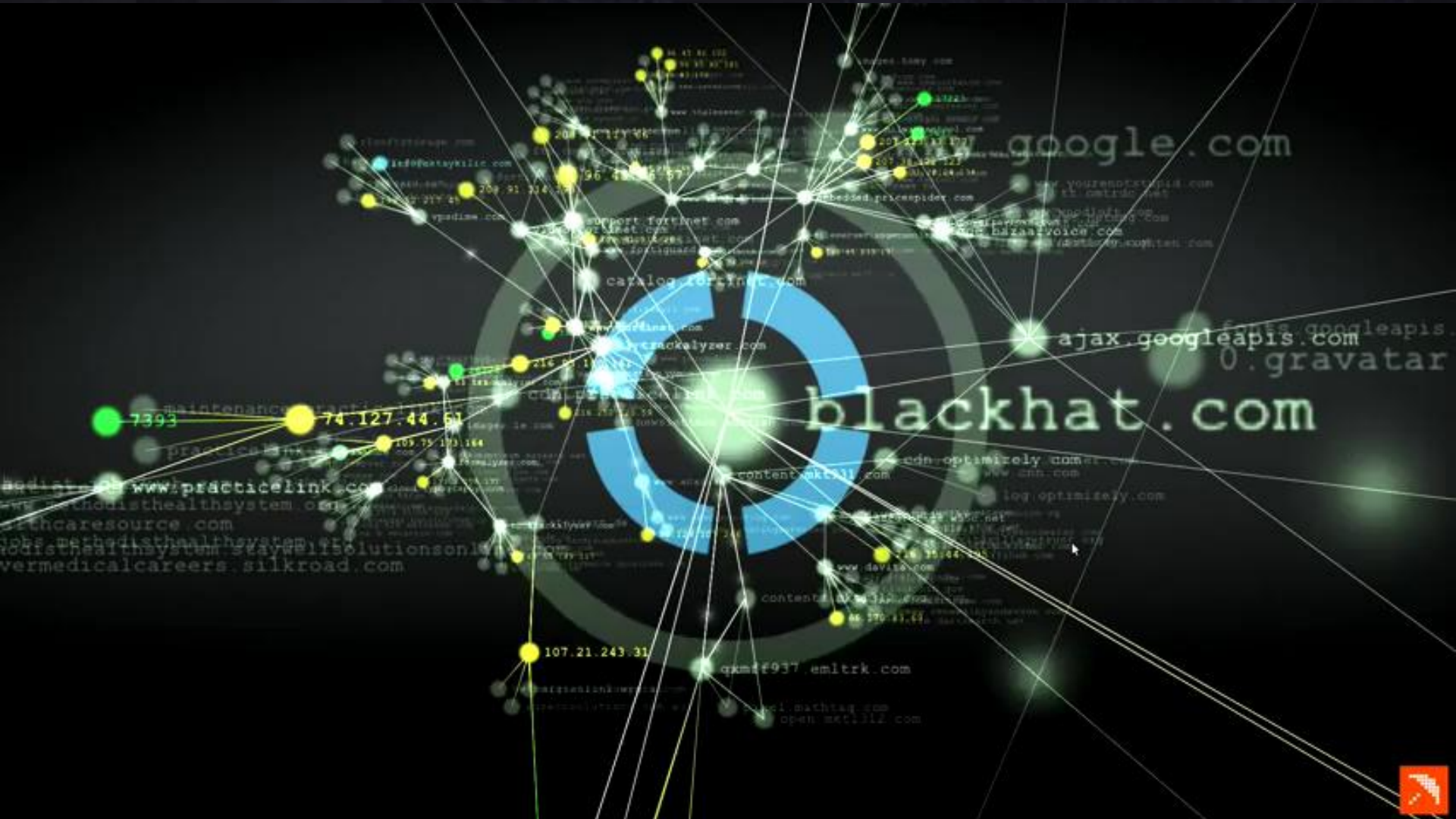
Domains Related to Malware Hashes



Domains Related to Malicious Registrant Email

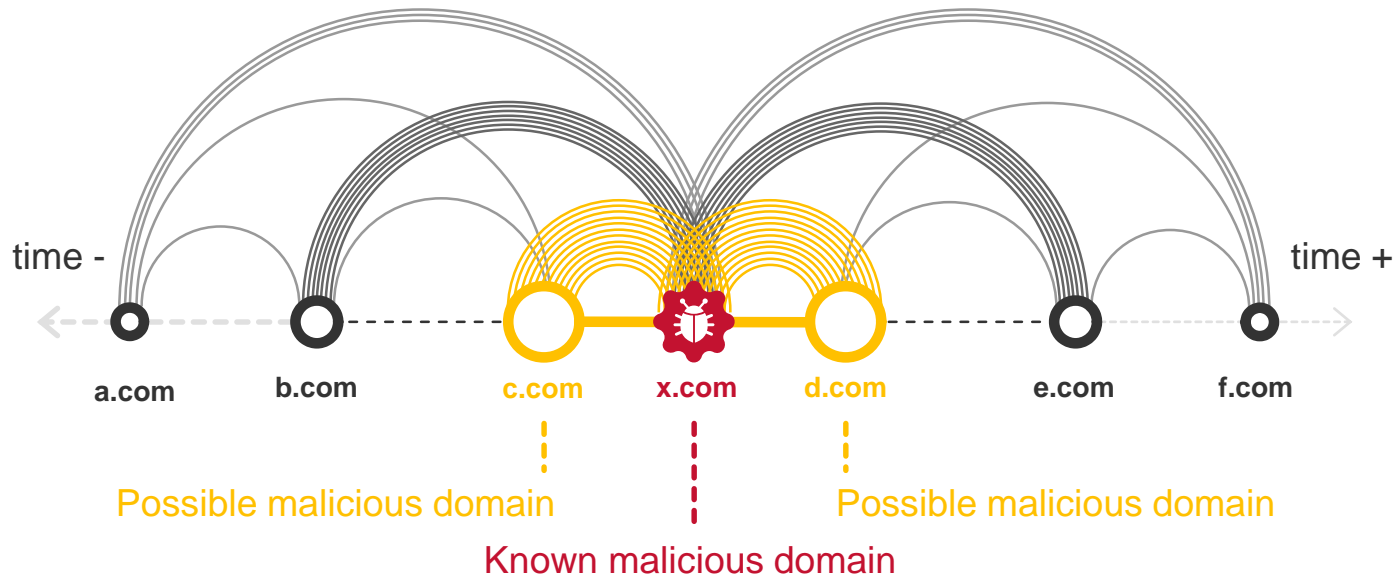


...



Co-occurrence Model

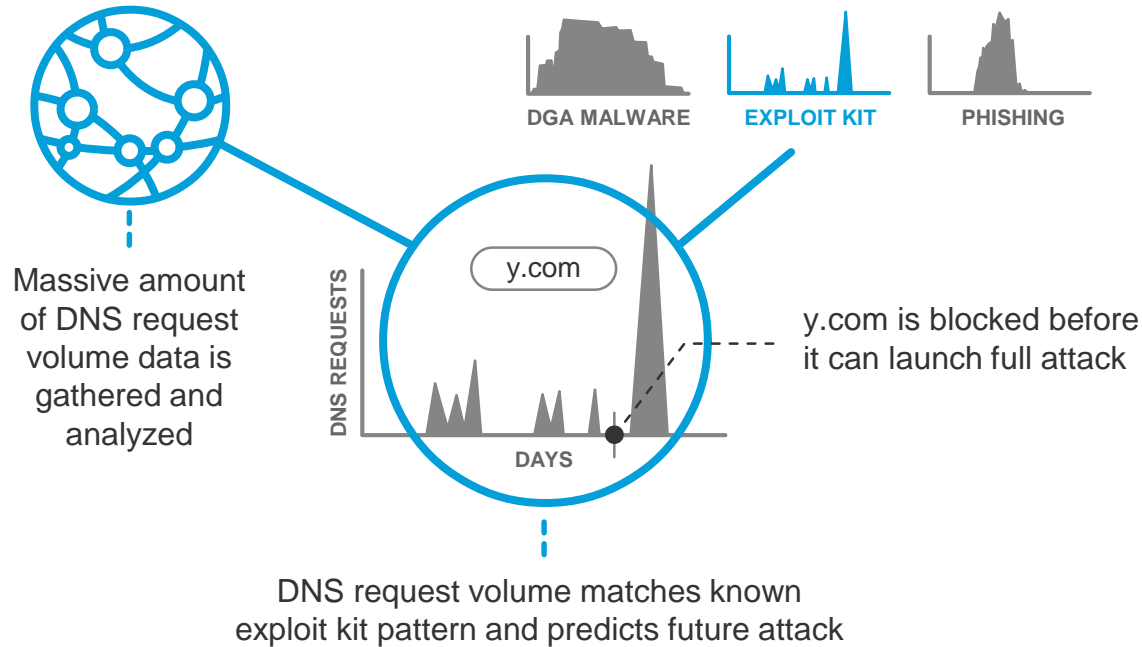
Domains guilty by inference



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

Spike Rank Model

Patterns of guilt



j8le7s5q745e.org

INVESTIGATE

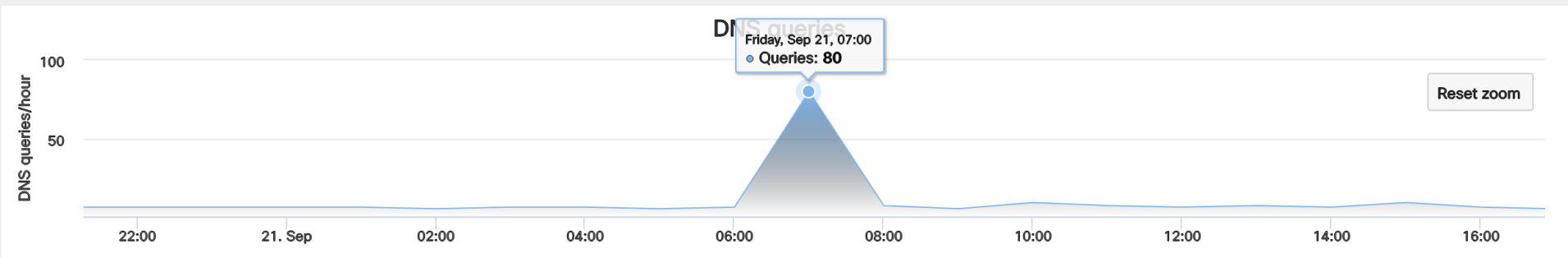


Details for j8le7s5q745e.org

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 71 ?

This domain may have been created using a domain generation algorithm (DGA)



Details for 1dnscontrol.com

[SEARCH IN GOOGLE](#)[SEARCH IN VIRUSTOTAL](#)

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: [5.61.37.209](#)

This domain is currently in the Umbrella block list

This domain has a suspicious SecureRank 2

DNS queries

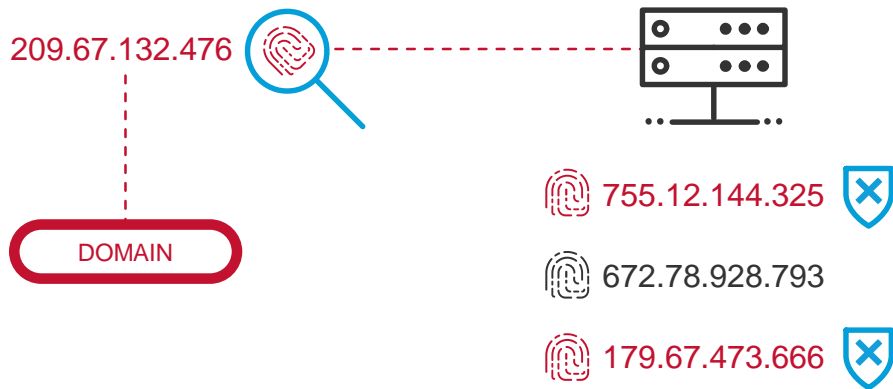


Co-occurrences

[autoecoleboisdesroches.com](#) (100.00)

Predictive IP Space Monitoring

Guilt by association



Pinpoint suspicious domains,
and observe their IP's fingerprint

Identify other IPs (hosted on the
same server) that share the same
fingerprint

Block those IPs and their
malicious domains

SEARCH [PATTERN SEARCH](#)

50.63.202.44

INVESTIGATE



Details for 50.63.202.44

Hosting 613 malicious domains for 1 week

AS

Prefix	ASN	Network Owner Description
50.62.0.0/15	AS 26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US 86400
50.63.200.0/22	AS 26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US 86400

Malicious domains hosted by 50.63.202.44

0102004.com 0392004.com 0412004.com 0632004.com 0922004.com 101shenbo.com 1032004.com 16155.com 17155.com 1912004.com 1982004.com 1camper1tree.com 1da.mobi 1jianbao.com 2003xx.com 2012004.com 2043kutaha.info 2242004.com 2772004.com 2991000.com 2992000.com 3002004.com 3010222.com 3113000.com 3221000.com 3361000.com 34t55.com 3542004.com 3692004.com 3866000.com 3912004.com 3mngtnews.info 4002004.com 4182777.com 4392004.com 4402004.com 4622004.com 4716555.com 4761555.com 4806777.com 4892004.com 4932004.com 4eyesonly.com 4rx.cc 56155.com 5880333.com 6012004.com 6072004.com 6083777.com 60t55.com 6192004.com 6524555.com 6666301.com 6666309.com 6666901.com 6780299.com 6nerthhome.info 71743226.com 79t55.com 813881.net 8386q.com 8386x.com 8866xsj.com 886yb.com 888whyroof.com 890s.cc 89t55.com 98t55.com 99flithub60.club 9satimmobile30.club 9v56.com a-sign.xyz aaa-win.com aasdn.co abcmall.com abumussa.com access-online-chas-sign.xyz acustay.com adaptating.com afmicrosoft.info airbandbplaces.com airbnbnepal.com aladinghk.com alfaliaval.com alfaromeoofalabama.com alliedmedicalsolutions.com allollur1292.info alone000.club alone111.club alone333.club alotta-colada.com amandalopesmakeup.com amma.com.co angelatworktoday.com anticomethods48.info apaulorecordshawaii.com apeironexousiacorp.com applesecurityserver.com aquatixbottle.com areaajo.com arizonaic.com armanibitcoin.org ashirwadgifts.com asjhe1tech.club assabirahschool.com assistancetechnician.us astutlman.com ath-sa.com atlantahomefindersite.com auctionceleb.com auctionexec.net auroramalta.com avalonsport.net ba022.com ba099.com ba1444.com ba1777.com ba266.com ba331.com ba3355.com ba440.com ba445.com ba477.com ba5444.com ba599.com ba660.com ba7799.com ba883.com ba9111.com ba9222.com ba995.com bababharti.com bababhole.xyz babamahakal.xyz badvets.com baisafoto.com bank-new.com bankmarket.us bb-site.mobi bbcompanies.com bblmedia.com bccp6.com bearingone.com beforeme.org berrysbarber.com bestflop232.info bestoffbroil23.club bholbaba.xyz bhole66.club wholebababombom.xyz bholegod.xyz bholesankar.xyz biglifehomes.com bilinrentals.com billsouth.net bitcoinallstate.org bitcoincornell.net bitcoinholidayinn.com bitcoinkraftrecipes.org bitcoinprincetonuniversity.org bitcoinqatarairways.org bitcoinxfinity.org bittrex.cc blockchainilluminati.com blockchainins.info blr1236.com blr1688.com blr1819.com blr7892.com bluecampusfoundation.com blueprintscapecolorado.com bmscuredssl-activusers.com bncp10.com boeingbitcoin.com bom22.xyz bottle2.xyz brazilvideos.net brianlonchar.com brownbrand.in buildingtogether.net bukitbunga.com businesalwaysthings.com businesssoftwareexperts.com camisetasdefutbol2020.net camisetasfutbol.org carolinatrrips.com cascadedcrops.com caterpillaribitcoin.org celebratrecplab.today cerazyworx.xyz charitymeetings.com charlesshawwines.com chase-login16.xyz chasebanklogon.xyz chiefcola.com chiropacticlosangeles.net ciocceleb.com cityladder.in classyandsingle.com classynewyorkingles.com classyoregonsingles.com clothesfashion.info cloudrule.net cnbuyingagent.com collectingcoinz.xyz comarcewabmail.info communicationtrainingforathletes.com compte-nous.com computersolutionsworks.com connectwithhexcs.com consumerrightslawyerblog.com coperate999pro.today coreldrawhome.club creepyunclejo.com cryptocurrencypaperwalletcertificate.net customerfacetime.com cz1305.com dacqs.com dadwe5space.info dataconnectinfotrends.com ddewlab.xyz deallk.com dealsad.com deborahramanathan.com debu777.club defconfidant.com depolan.com desertcomfortassistedliving.com dev44.xyz dianegiddens.com dickswingsgrill.com digjollur1289.info digisassy23.club diphthys.com direktologistics.com docanswer.com docbuyshouses.com doctransfer.co dolbycheckz.xyz drmyshope25.club dsclub.org dtispr.com dumpcars.com dunwoodypress.com dxx55.com e5515.com e5521.com e5535.com e5536.com e5562.com e5576.com e5578.com e6610.com e6617.com e6620.com e6638.com e6641.com e6643.com e6650.com e6670.com e6671.com e6685.com e7b8m21.info elmonteplaza.com emeetingauction.com emp3ror.com employeesynergy.com entrails.net equifaxlegal.com equifaxprivacybreach.com erosdiary.com esighaspetroleumtools.com estresoxidativo.com etimemachines.com ezollur1285.info fab-branding.com facebookpro.info fasterinfra.com

WHOIS Record Data

Registrar Name: ENOM, INC. **IANAID:** 48

Last retrieved April 12, 2017

[GET LATEST](#)

Created: July, 29, 2015

Updated: July, 29, 2015

Expires: July, 29, 2016 **EXPIRED**

[Raw data](#)

Email Address	Associated Domains	Email Type	Last Observed
BOTSMUSTDIE@GMAIL.COM	Greater than 500 Total - At least 403 malicious	Administrative, Registrant, Technical	July, 29, 2016

Showing 1 of 1 Results

Nameserver	Associated Domains	Last Observed
ns1.sugarbucket.us	Greater than 500 Total - At least 270 malicious	July, 29, 2016
ns2.sugarbucket.us	Greater than 500 Total - At least 270 malicious	July, 29, 2016

Showing 2 of 2 Results

NLP-Rank Model (natural language processing)

Identifies malicious domain-squatting and targeted phishing domains

1

Read APT reports



2

Patterns in domains
used in attacks

- Domain spoofing used to obfuscate
- Often saw brand names and terms like “update”
- Examples:
update-java[.]net
adobe-update[.]net

3

Checked data &
confirmed intuition

- Dictionary words & company names merged
- Changed small # of characters to obfuscate
- Domains hosted on ASNs unassociated w/company
- Different webpage fingerprints

4

Built model and
continue to tune

Detects
fraudulent brand
domains:

✗ 1linkedin.net

✓ linkedin.com

IP Geo-location Analysis

Host Infrastructure

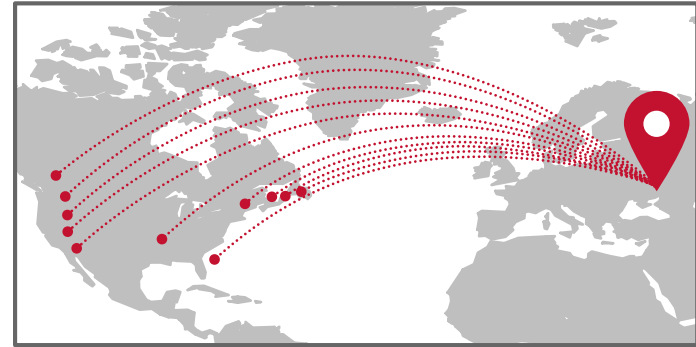
Location of the server
IP addresses mapped to domain



Hosted across 28+ countries

DNS Requesters

Location of the network and off-network device
IP addresses requesting the domain



Only US-based customers
requesting a .RU TLD

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 46 ?

This domain is associated with a Trojan attack called Emotet

DNS queries



Host

IP Count 1
Geo Distance (sum, mean) 0, 0 km
Registrant Country RU

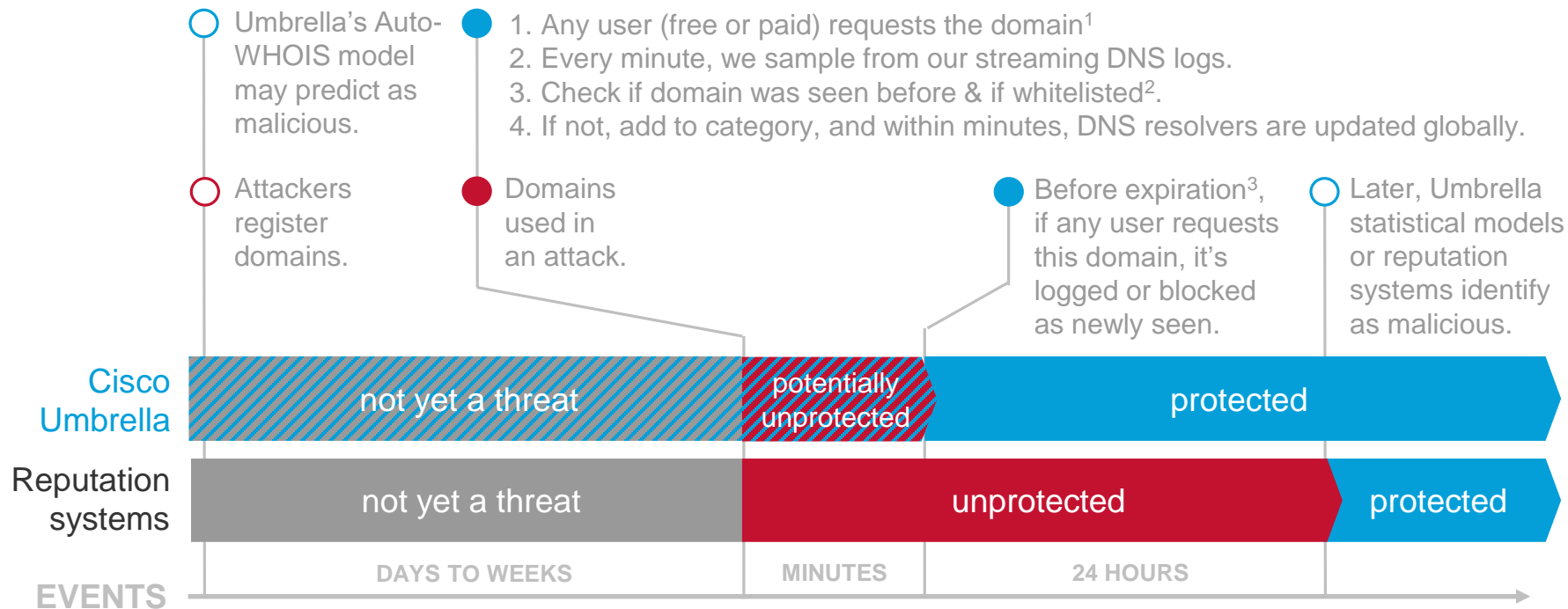
Requester Distribution

COUNTRY	PERCENTAGE
Cyprus	100.00%



'Newly Seen Domains' Category

Reduces risk of the unknown



iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com

INVESTIGATE



Details for iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 28 ?

This domain is associated with a Ransomware attack called WannaCry

This domain has a suspicious SecureRank 2

This domain may have been created using a domain generation algorithm (DGA)

DNS queries



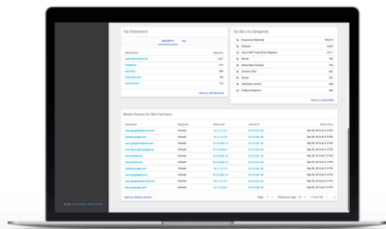
14 Day Free Trial of Cisco Umbrella

Get started in 30 seconds

No credit card or phone call required

WHAT IS INCLUDED?

- ✓ Threat protection like no other – block malware, C2 callbacks, and phishing.
- ✓ Predictive intelligence – automates threat protection by uncovering attacks before they launch.
- ✓ Worldwide coverage in minutes – no hardware to install or software to maintain
- ✓ Weekly security report – get a personalized summary of malicious requests & more, directly to your inbox.
- ✓ 1,000+ users? – You're eligible for the [Umbrella Security Report](#), a detailed post-trial analysis.



All fields are required

Account Type

First Name

Last Name

Company Email

Select your country

Company phone

Company Name

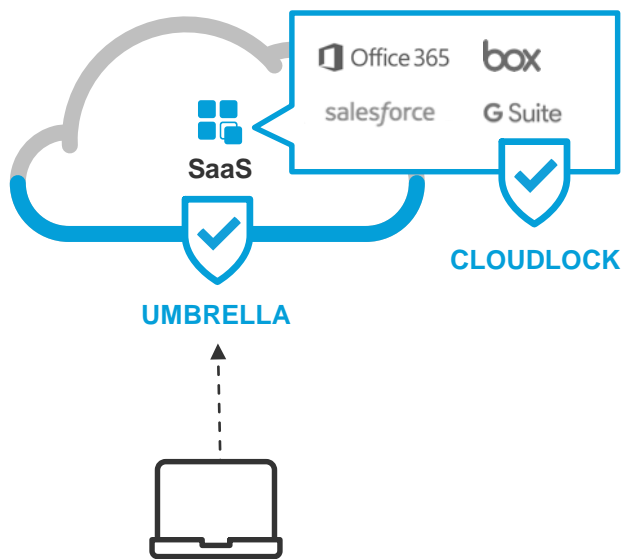
Employee Count

CREATE MY TRIAL

Thank You

How Umbrella integrates with Cisco Cloudlock

Complete discovery and control for SaaS apps



Umbrella identifies all the SaaS apps across an organization

Cloudlock revokes authentication for risky or inappropriate apps

Using Umbrella's enforcement API, Cloudlock can programmatically add domains to Umbrella

3,141 apps discovered

 3,007 unreviewed apps

 26 apps under audit

 45 apps not approved

 63 apps approved

Category: Anonymizer

4 unreviewed apps

Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

[DETAILS](#)



Category: P2P

1 unreviewed apps

P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

[DETAILS](#)



Category: Games

63 unreviewed apps

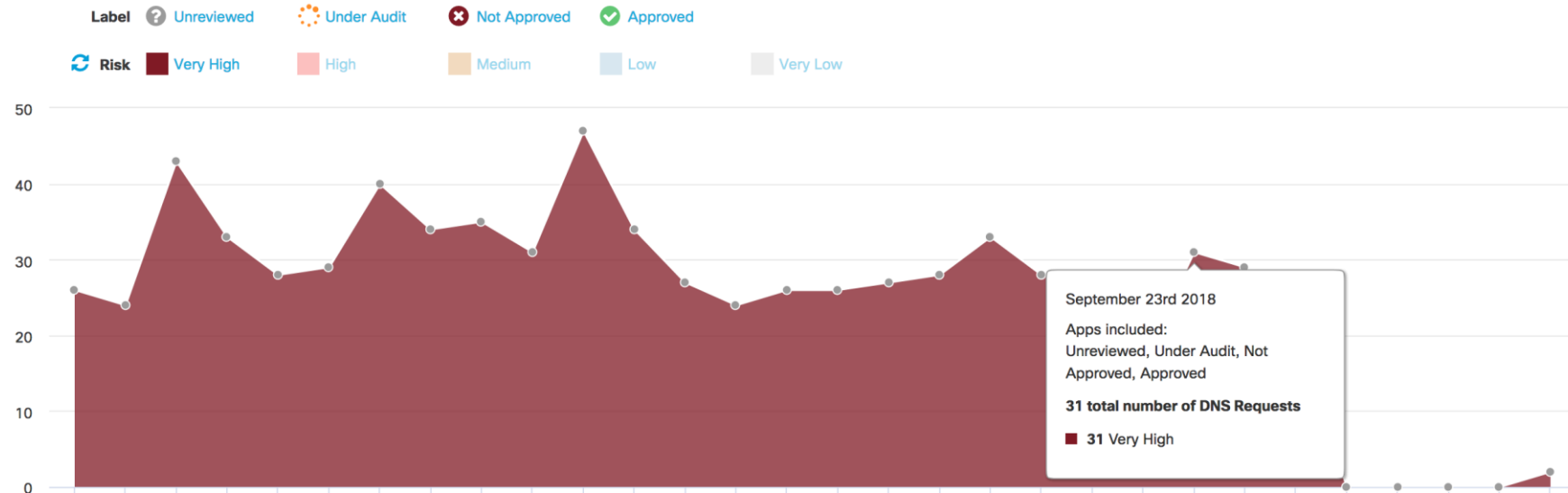
Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

[DETAILS](#)



DNS Requests by App Risk

Total number of DNS requests of apps discovered in the past 30 days



Search for App / Vendor

Category

Risk

App Type

Label

Date

Risk: High

Category: Cloud Storage

Clear all filters



UNREVIEWED (35)





UNDER AUDIT (1)

NOT APPROVED (0)

APPROVED (1)

ALL APPS (37)

All Apps (37 Found)

Application	Vendor	Weighted Risk	Identities	DNS Requests	Blocked	Label
 Flickr Cloud Storage	Flickr	High	50	260	-	<div>Unreviewed</div> <div>Block this app</div>
 Snapfish Cloud Storage	Snapfish	High	48	248	<1%	<div>Unreviewed</div> <div>Block this app</div>
 Fileserve Cloud Storage	Bigfile to	High	48	245	-	<div>Unreviewed</div>
 LinkedIn SlideShare Cloud Storage	Linkedin	High	41	174	-	<div>Unreviewed</div>