Cisco Umbrella

# Cisco Umbrella

## Nová vrstva obrany pred kybernetickými hrozbami

Stanislav Smolár
Security Product Sales Specialist

**Wednesday, 29. March 2017**

# DNS

# DNS

## Overview

### Domain registrar

Maps and records names to #s in "phone books"

GoDaddy

### Authoritative DNS

Owns and publishes the "phone books"

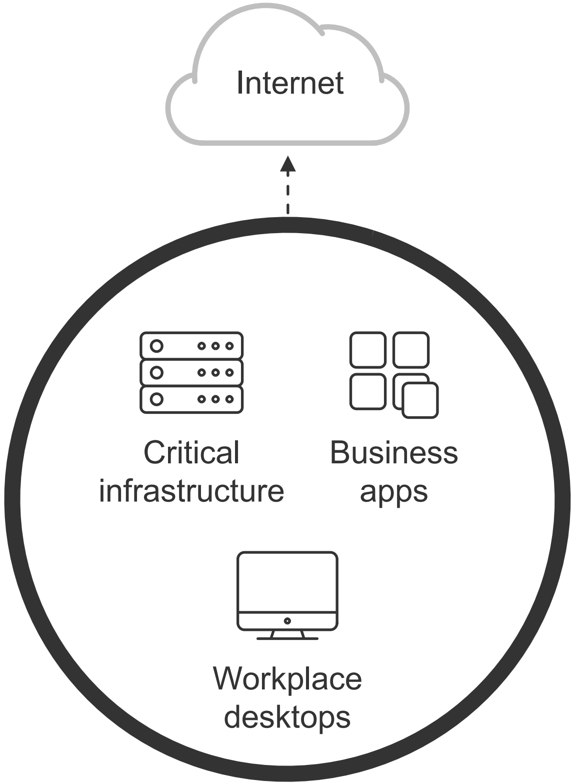
amazon web services Route 53

### Recursive DNS

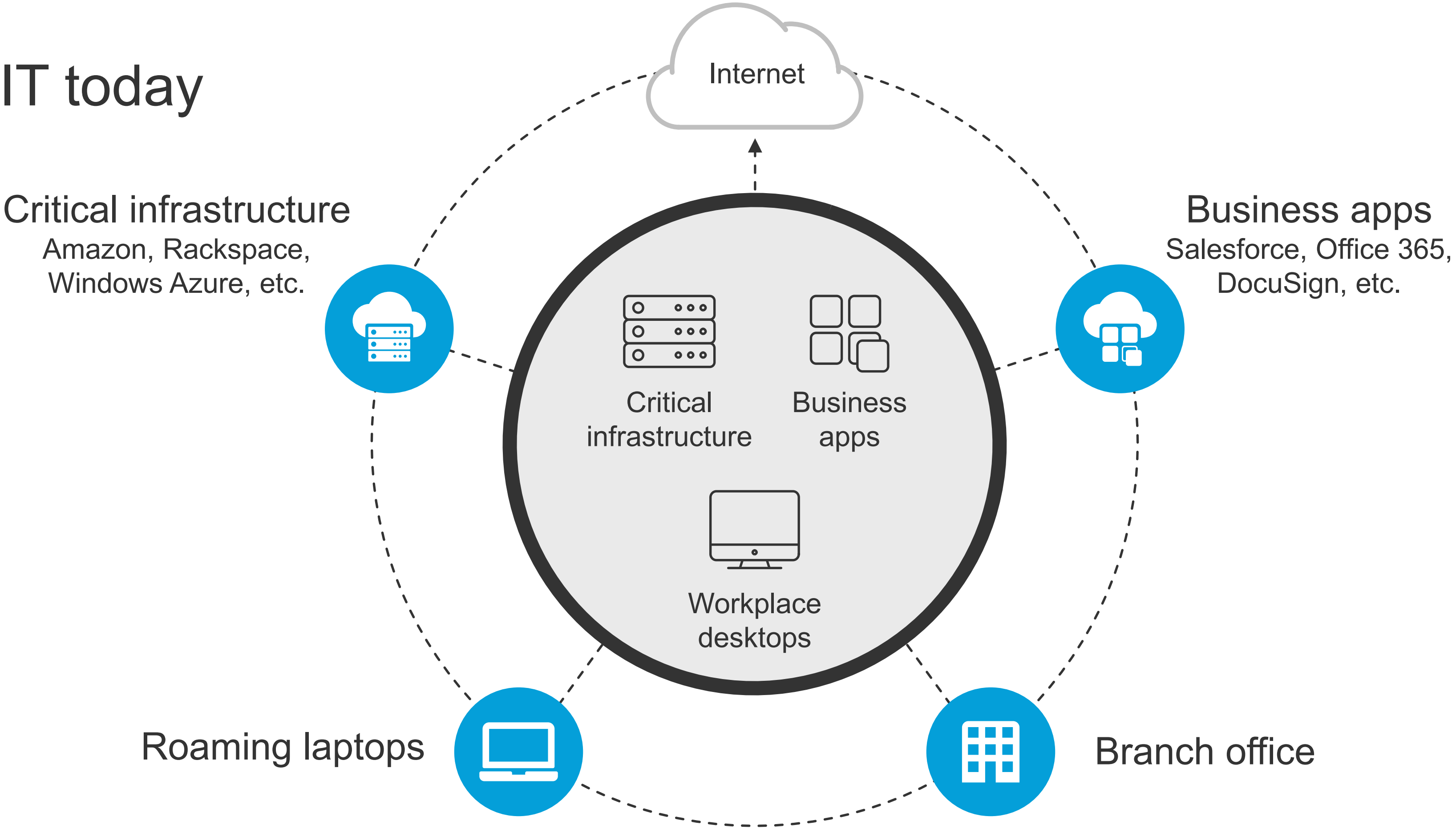
Looks up and remembers the #s for each name

cisco Cisco Umbrella

# How IT was built



# IT today



Internet

Critical infrastructure

Amazon, Rackspace, Windows Azure, etc.

Business apps

Salesforce, Office 365, DocuSign, etc.

Roaming laptops

Branch office

By 2018, Gartner estimates:

# 25% of corporate data traffic will bypass perimeter security.

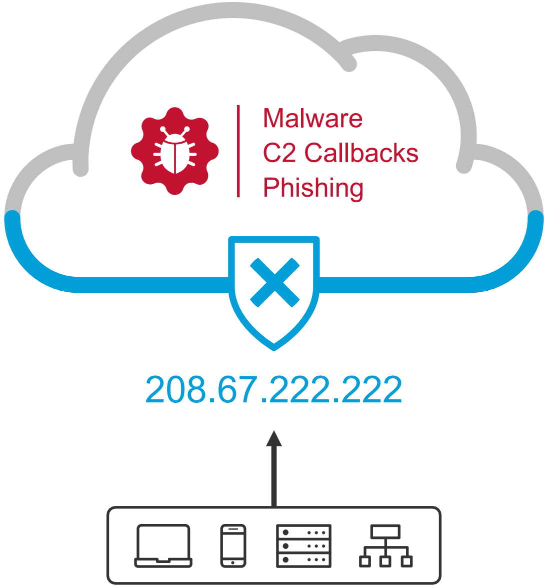
# Your security challenges we can solve

- Malware and ransomware
- Gaps in visibility and coverage
- Cloud apps and shadow IT
- Difficult to manage security

# Introducing Cisco Umbrella

# Cisco Umbrella

## Cloud security platform



Built into the foundation of the internet

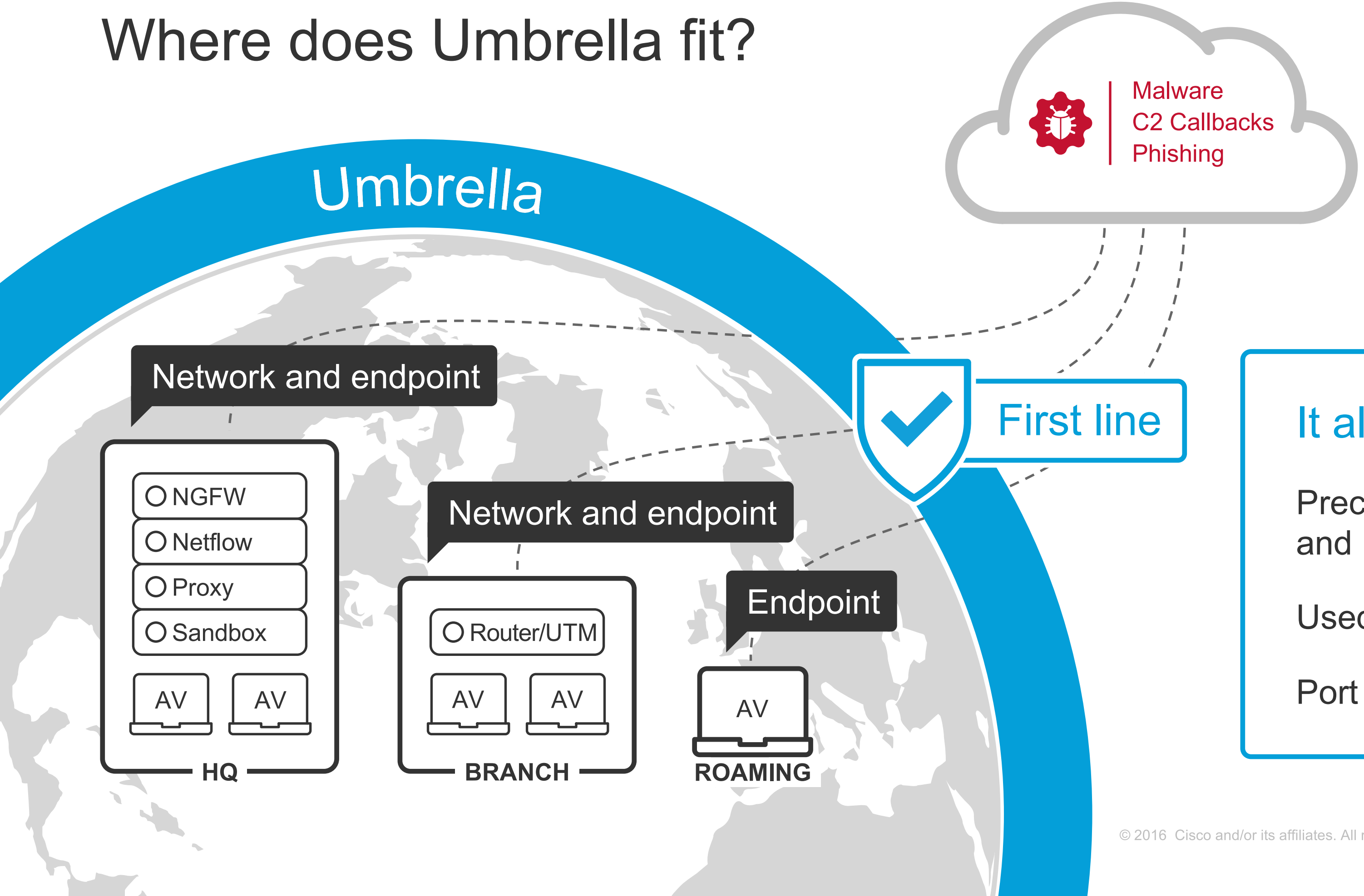
Intelligence to see attacks before launched

Visibility and protection everywhere

Enterprise-wide deployment in minutes

Integrations to amplify existing investments

# Where does Umbrella fit?



## It all starts with DNS

Precedes file execution and IP connection

Used by all devices

Port agnostic

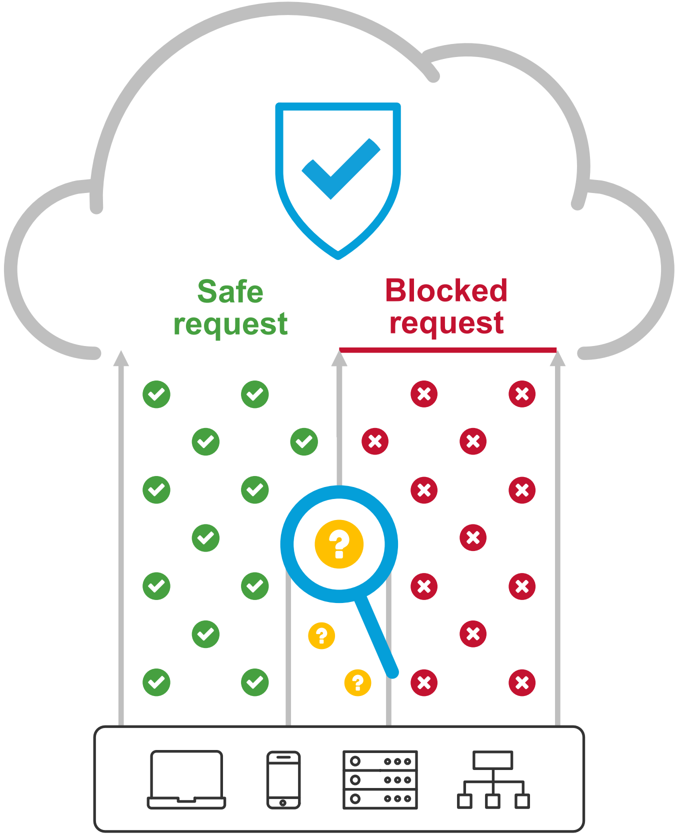
# Built into foundation of internet

Umbrella provides:

Connection for safe requests

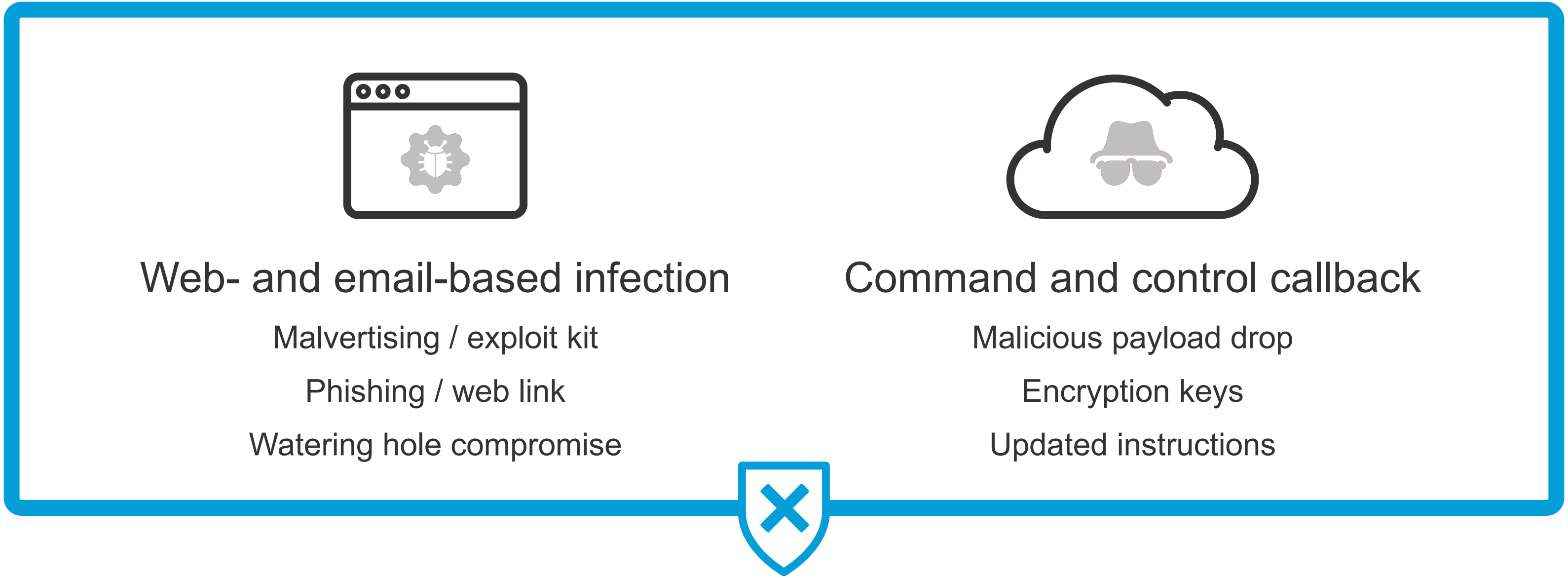
Prevention for user- and malware-initiated connections

Proxy inspection for risky URLs



Cisco Umbrella

# Prevents connections before and during the attack



## Web- and email-based infection

Malvertising / exploit kit

Phishing / web link

Watering hole compromise

## Command and control callback

Malicious payload drop

Encryption keys

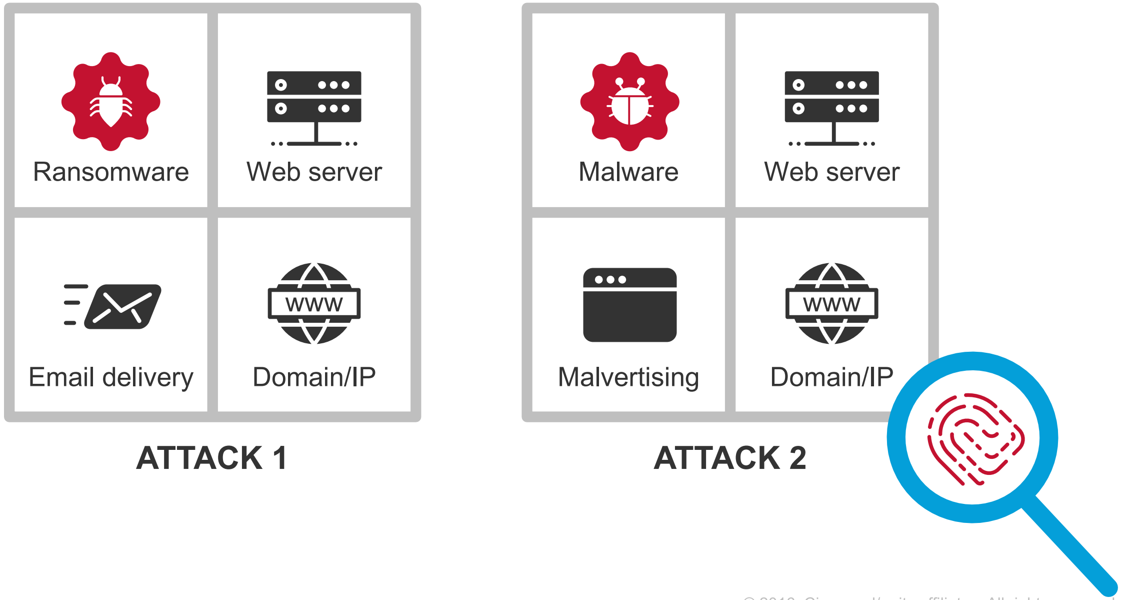
Updated instructions

Stop data exfiltration and ransomware encryption

# Malware doesn't just happen

## Intelligence to see attacks before launched

Build. Test. Launch. Repeat.



Ransomware

Web server

Email delivery

Domain/IP

ATTACK 1

Malware

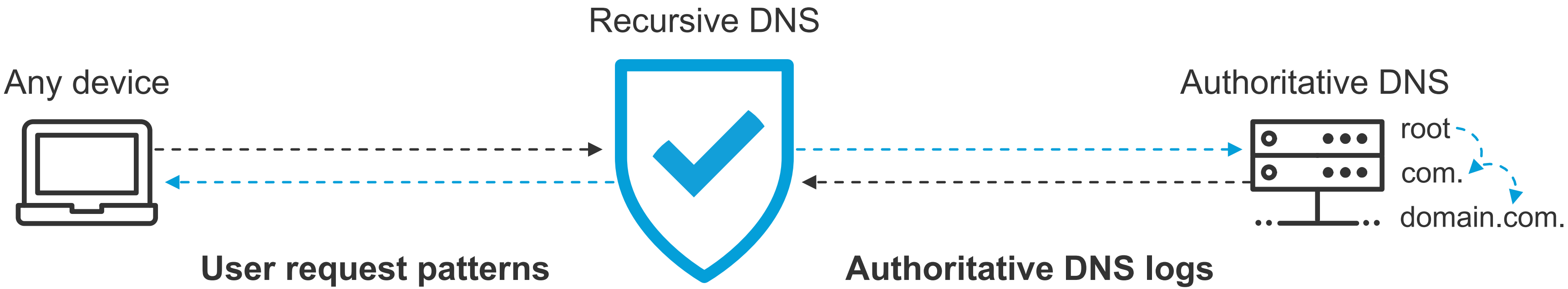
Web server

Malvertising

Domain/IP

ATTACK 2

# Gather intelligence and 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:

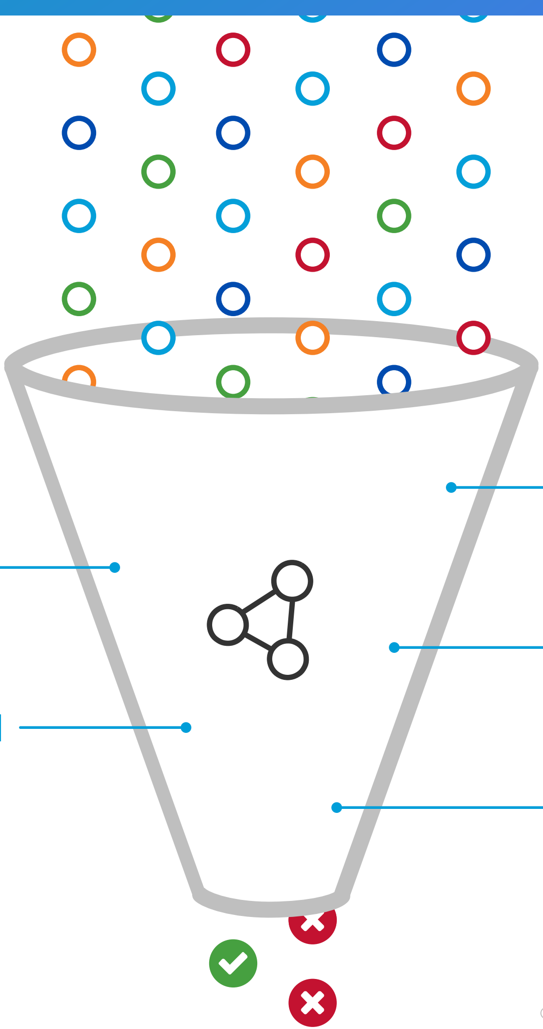
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

# Our view of the internet

| 80B | 65M | 12K | 160+ |
|---|---|---|---|
| requests per day | daily active users | enterprise customers | countries worldwide |

# Intelligence

## Statistical models



2M+ live events per second

11B+ historical events

Spike rank model

Detect domains with sudden spikes in traffic

Co-occurrence model

Identifies other domains looked up in rapid succession of a given domain

Predictive IP space monitoring

Analyzes how servers are hosted to detect future malicious domains

Natural language processing model

Detect domain names that spoof terms and brands

Dozens more models

# Our efficacy

Discover

3M+

daily new domain names

Identify

60K+

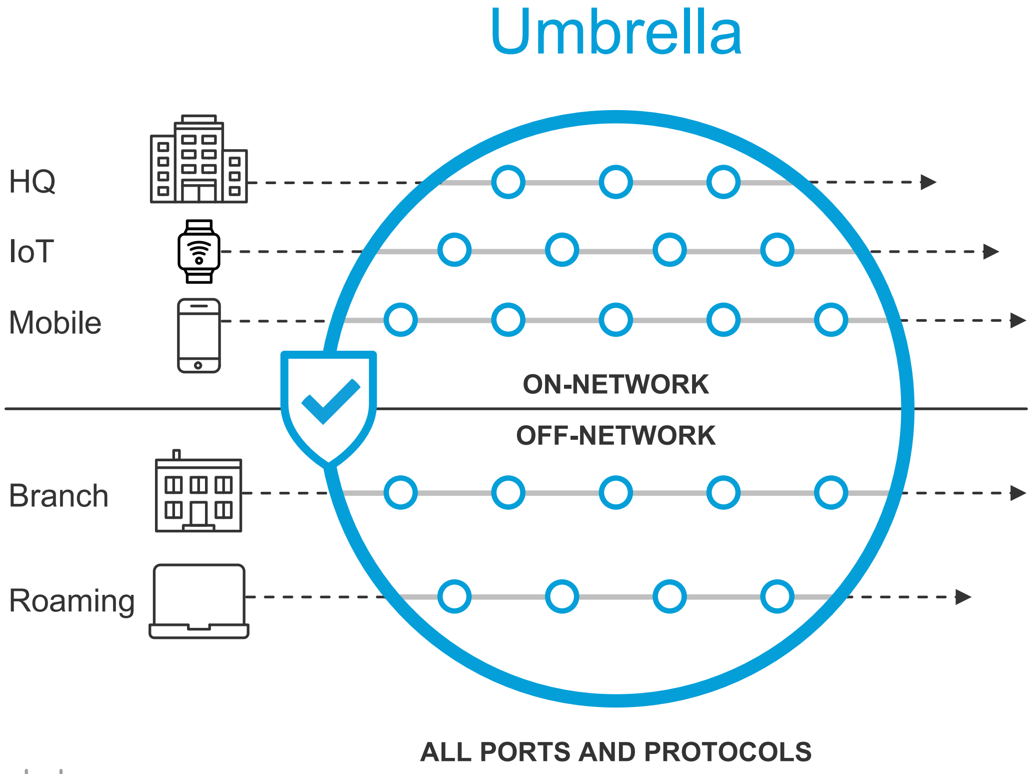
daily malicious destinations

Enforce

7M+

malicious destinations while resolving DNS

# Visibility and protection for all activity, anywhere



All office locations

Any device on your network

Roaming laptops

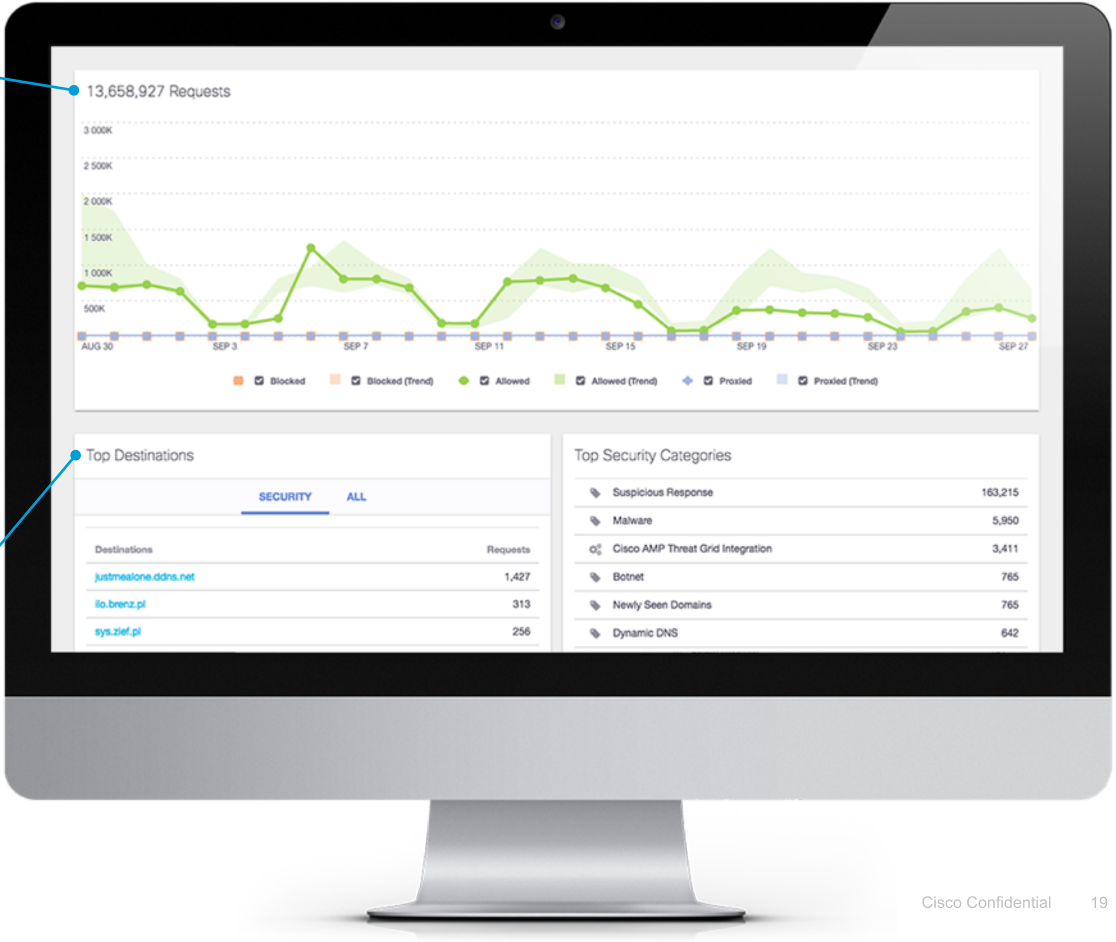
Every port and protocol

Allowed, blocked, and proxied traffic per device or network

IDENTITY REPORTS

# Quickly spot and remediate victims

Top activity and categories per device or network



Top Destinations

| Destinations | Requests |
|---|---|
| justmealone.ddns.net | 1,427 |
| ilo.brenz.pl | 313 |
| sys.zief.pl | 256 |

Top Security Categories

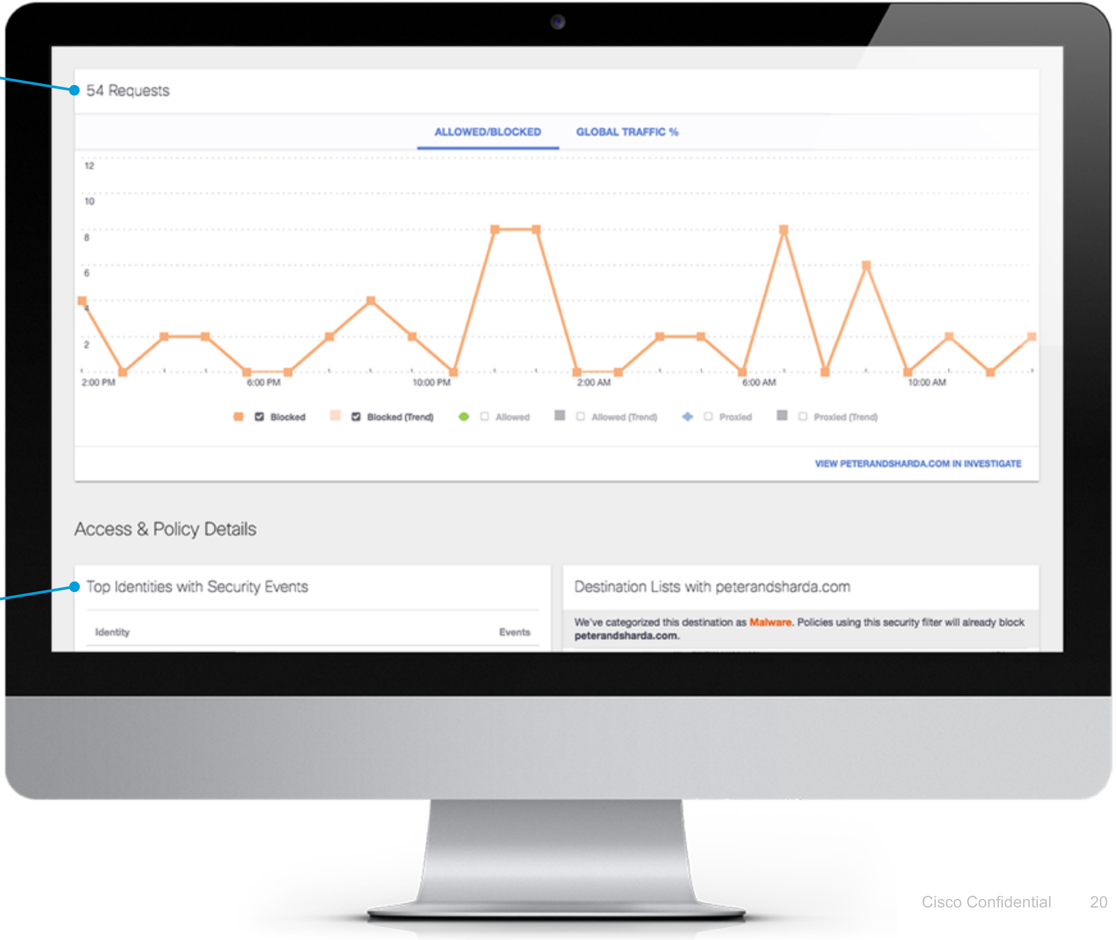
| | |
|---|---|
| Suspicious Response | 163,215 |
| Malware | 5,950 |
| Cisco AMP Threat Grid Integration | 3,411 |
| Botnet | 765 |
| Newly Seen Domains | 765 |
| Dynamic DNS | 642 |

Local vs. global trends for malicious domains

DESTINATION REPORTS

# Quickly assess extent of exposure

Top identities associated with malicious activity



54 Requests

Access & Policy Details

Top Identities with Security Events

| Identity | Events |
|---|---|

Destination Lists with peterandsharda.com

We've categorized this destination as Malware. Policies using this security filter will already block peterandsharda.com.

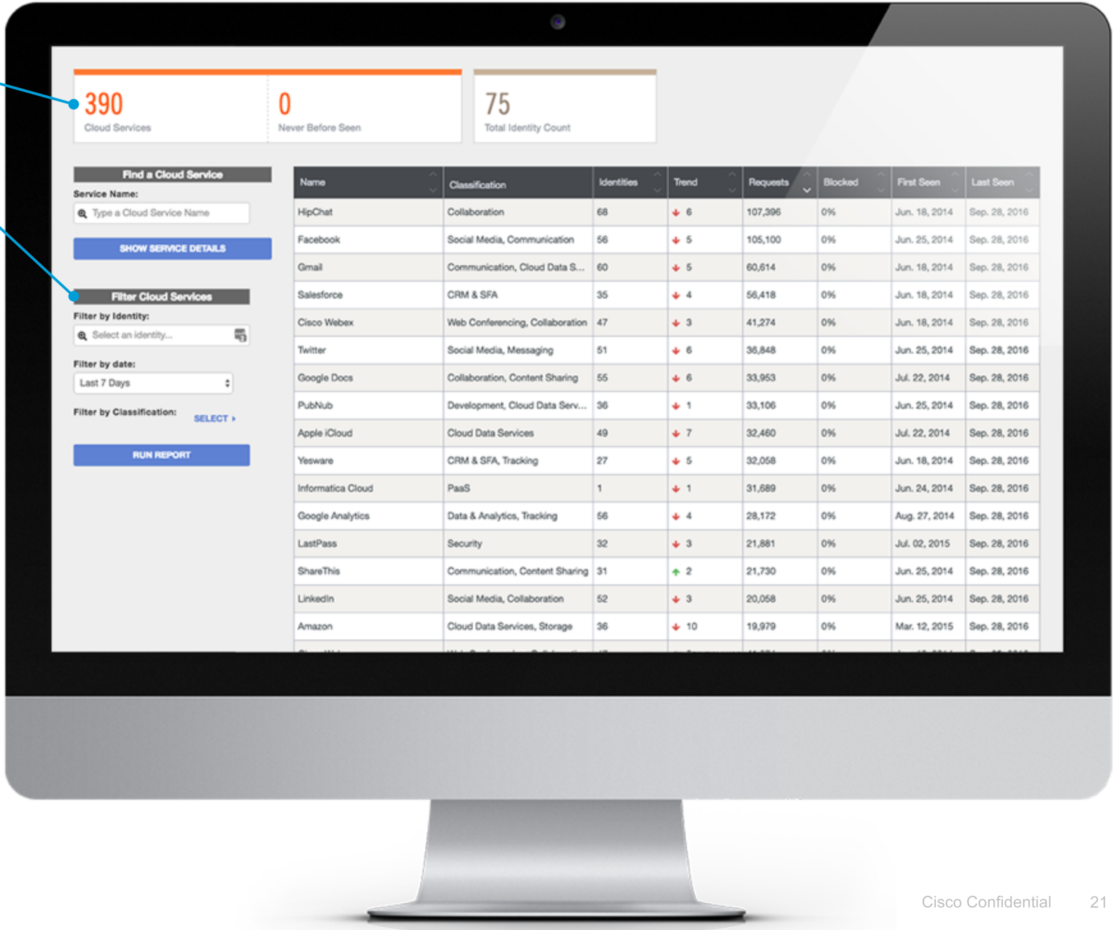
Cisco Umbrella

Total and newly seen cloud services

Cloud apps by classification and traffic volume

### CLOUD SERVICES REPORT

# Effectively combat shadow IT



390
Cloud Services

0
Never Before Seen

75
Total Identity Count

**Find a Cloud Service**

Service Name: Type a Cloud Service Name

SHOW SERVICE DETAILS

**Filter Cloud Services**

Filter by Identity: Select an identity...

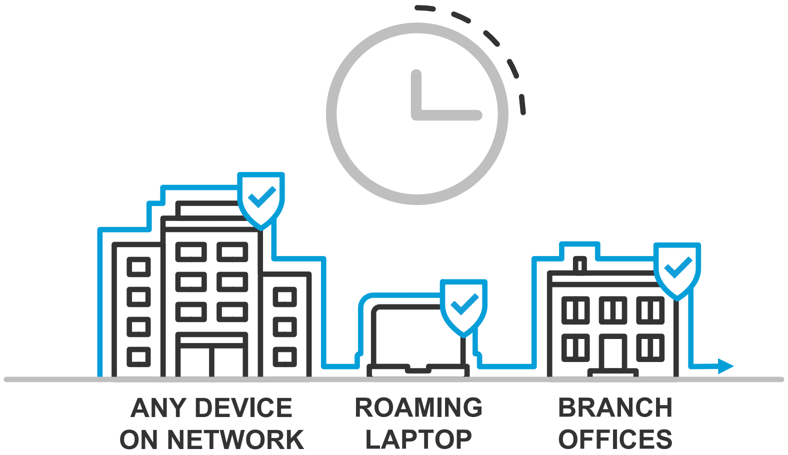
Filter by date: Last 7 Days

Filter by Classification: SELECT ›

RUN REPORT

| Name | Classification | Identities | Trend | Requests | Blocked | First Seen | Last Seen |
|---|---|---|---|---|---|---|---|
| HipChat | Collaboration | 68 | ↓ 6 | 107,396 | 0% | Jun. 18, 2014 | Sep. 28, 2016 |
| Facebook | Social Media, Communication | 56 | ↓ 5 | 105,100 | 0% | Jun. 25, 2014 | Sep. 28, 2016 |
| Gmail | Communication, Cloud Data S... | 60 | ↓ 5 | 60,614 | 0% | Jun. 18, 2014 | Sep. 28, 2016 |
| Salesforce | CRM & SFA | 35 | ↓ 4 | 56,418 | 0% | Jun. 18, 2014 | Sep. 28, 2016 |
| Cisco Webex | Web Conferencing, Collaboration | 47 | ↓ 3 | 41,274 | 0% | Jun. 18, 2014 | Sep. 28, 2016 |
| Twitter | Social Media, Messaging | 51 | ↓ 6 | 36,848 | 0% | Jun. 25, 2014 | Sep. 28, 2016 |
| Google Docs | Collaboration, Content Sharing | 55 | ↓ 6 | 33,953 | 0% | Jul. 22, 2014 | Sep. 28, 2016 |
| PubNub | Development, Cloud Data Serv... | 36 | ↓ 1 | 33,106 | 0% | Jun. 25, 2014 | Sep. 28, 2016 |
| Apple iCloud | Cloud Data Services | 49 | ↓ 7 | 32,460 | 0% | Jul. 22, 2014 | Sep. 28, 2016 |
| Yesware | CRM & SFA, Tracking | 27 | ↓ 5 | 32,058 | 0% | Jun. 18, 2014 | Sep. 28, 2016 |
| Informatica Cloud | PaaS | 1 | ↓ 1 | 31,689 | 0% | Jun. 24, 2014 | Sep. 28, 2016 |
| Google Analytics | Data & Analytics, Tracking | 56 | ↓ 4 | 28,172 | 0% | Aug. 27, 2014 | Sep. 28, 2016 |
| LastPass | Security | 32 | ↓ 3 | 21,881 | 0% | Jul. 02, 2015 | Sep. 28, 2016 |
| ShareThis | Communication, Content Sharing | 31 | ↑ 2 | 21,730 | 0% | Jun. 25, 2014 | Sep. 28, 2016 |
| LinkedIn | Social Media, Collaboration | 52 | ↓ 3 | 20,058 | 0% | Jun. 25, 2014 | Sep. 28, 2016 |
| Amazon | Cloud Data Services, Storage | 36 | ↓ 10 | 19,979 | 0% | Mar. 12, 2015 | Sep. 28, 2016 |

# Enterprise-wide deployment in minutes



## On-network coverage

With one setting change

Integrated with Cisco ISR 4K series

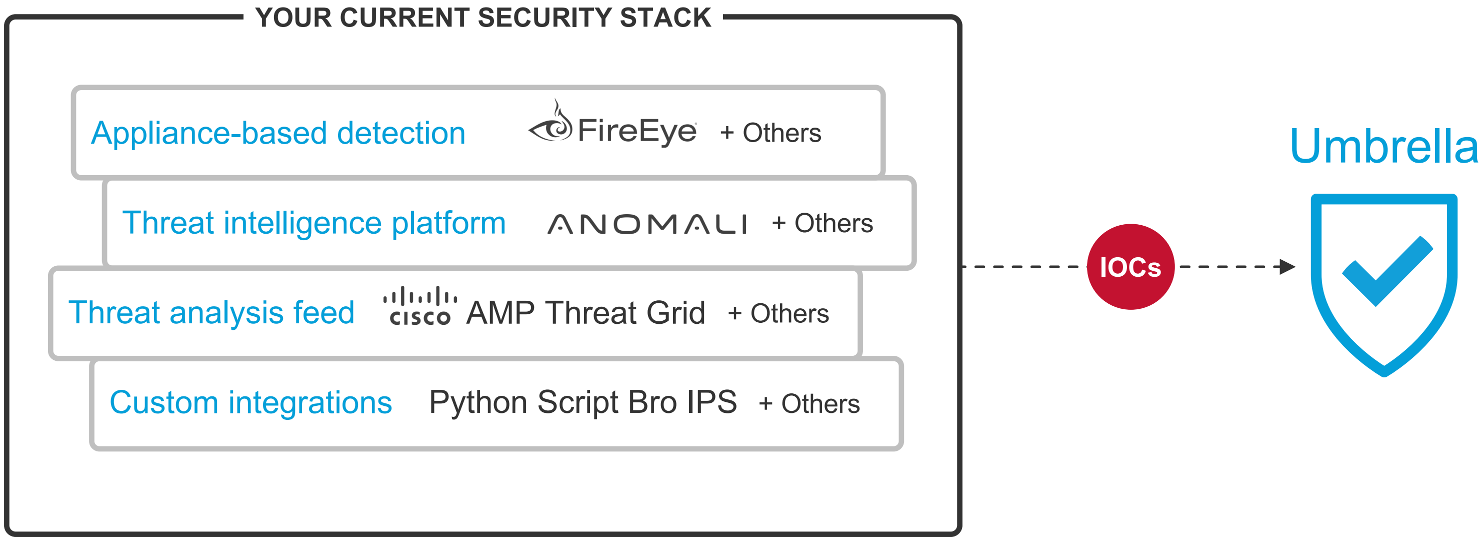
## Off-network coverage

With AnyConnect VPN client integration

Or with any VPN using lightweight Umbrella client

# Integrations to amplify existing security

## Block malicious domains from partner or custom systems



YOUR CURRENT SECURITY STACK

Appliance-based detection FireEye + Others

Threat intelligence platform ANOMALI + Others

Threat analysis feed cisco AMP Threat Grid + Others

Custom integrations Python Script Bro IPS + Others

IOCs

Umbrella

# Umbrella/OpenDNS reference

# Rio Olympic Games 2016

## Use case for Cloud Security

# Rio 2016 – Cisco as strategy partner

- Cisco Umbrella installed 2 days before opening ceremony
- Installation takes 2 hours only!
- Total 7 networks configured in Rio and Sao Paulo
- Handled 22 M requests daily
- Umbrella stoped 23 k threats daily

# Demo

# Easiest security product you'll ever deploy

1. Signup
2. Point your DNS
3. Done