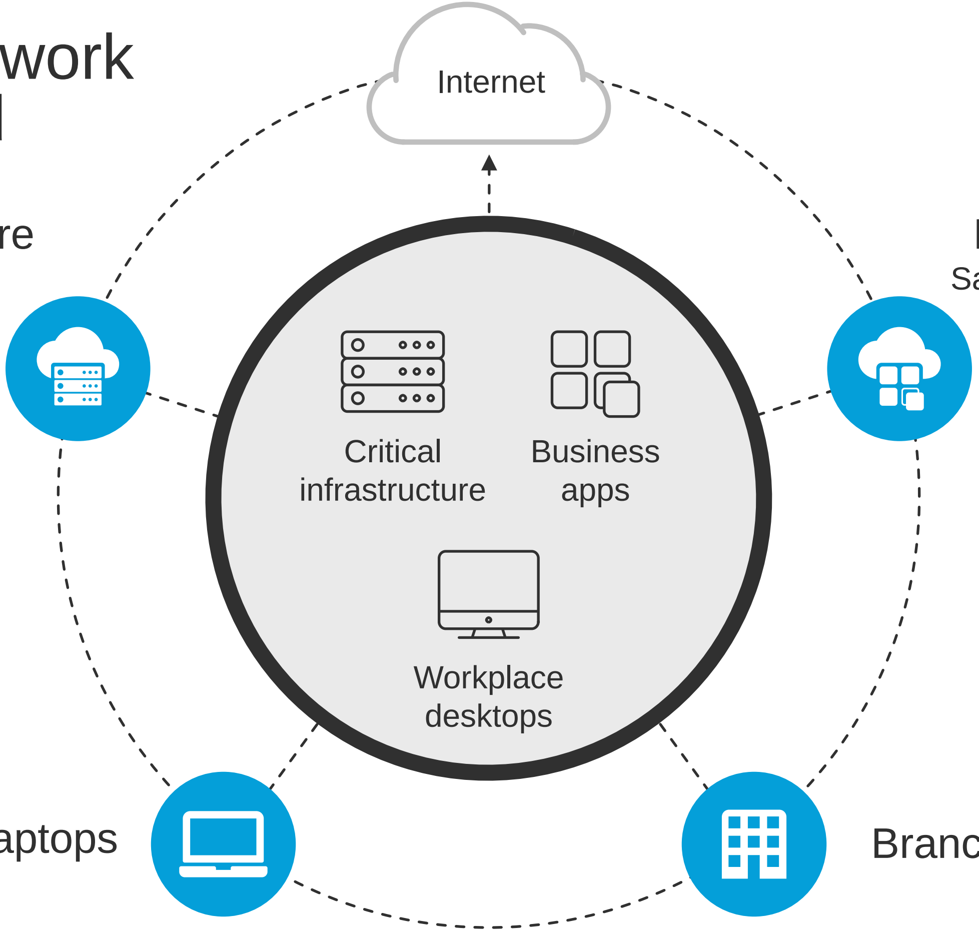
# Next Generation DNS Security

First line of defense for threats on the internet

Willy Huang
Product/Technical Manager, Cisco

# The way we work has changed



Critical infrastructure
Amazon, Rackspace, Windows Azure, etc.

Business apps
Salesforce, Office 365, G Suite, etc.

Roaming laptops

Branch office

# Users and apps have adopted the cloud, security must too

**49%**
of the workforce is mobile

**82%**
admit to not using the VPN

**70%**
increase in SaaS usage

**70%**
of branch offices have DIA

Security controls must shift to the cloud

# Your security challenges

Malware and ransomware

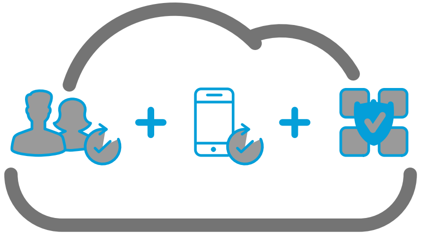
Gaps in visibility and coverage

Cloud apps and shadow IT

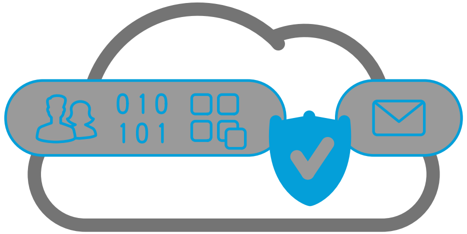
Difficult to manage security

# Cloud Security Solution

Secure Internet Gateway (SIG)



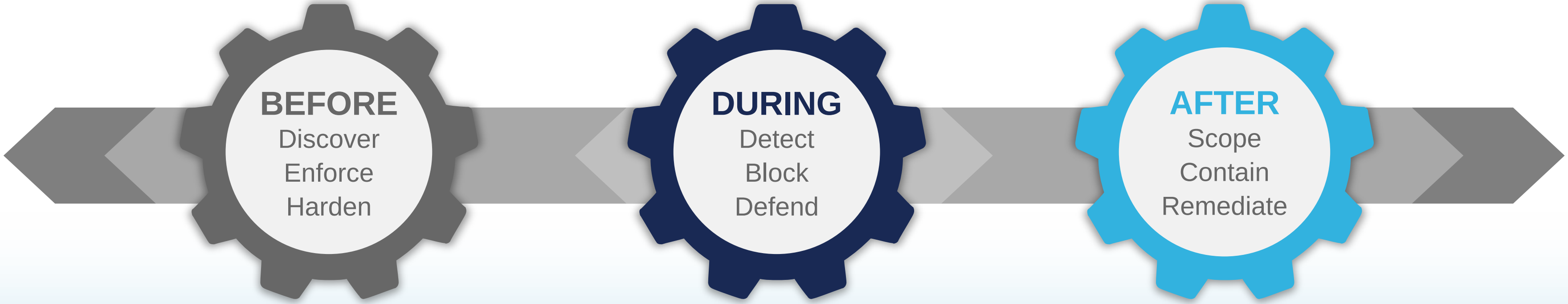
Multi-Factor Authentication (MFA),
Single Sign-on (SSO),
Software-Defined Perimeter (SDP)



Cloud Access Security Broker
(CASB) and Email

Public cloud visibility
and threat detection

# Threat Centric model to cover the Entire Attack Continuum



**BEFORE**
Discover
Enforce
Harden

**DURING**
Detect
Block
Defend

**AFTER**
Scope
Contain
Remediate

**DNS Layer Protection**

Firewall

VPN

NGIPS

Cognitive Threat Analytics (CTA)

NGFW

UTM

Email & Web Security

**Network Behavior Analysis**

Secure Access + Identity Services

**Advanced Malware Protection (AMP) & Threat Grid (Sandbox)**

Visibility, Context, Segmentation & Threat Intelligence

# Have you been Attacked?

Abfahrt
Linie
Zeit
Über
Nach
Gleis
22:10 RB81 Flöha - Pockau-Lengefeld Olbernhau 8
22:30 RB30
22:31 RB30 Hohenstein
22:36 RB80
22:36 RB45 Geithain
22:44 RE6 Einsiedel - Thalheim (Erzgeb) Aue (Sachs)
22:45 RB89 Flöha - Freiberg (Sachs) - Tharandt Dresden Hbf
23:30
Ooops, your files have been encrypted!

# Ransomware is a Massive Market

$325M

2015

$5B

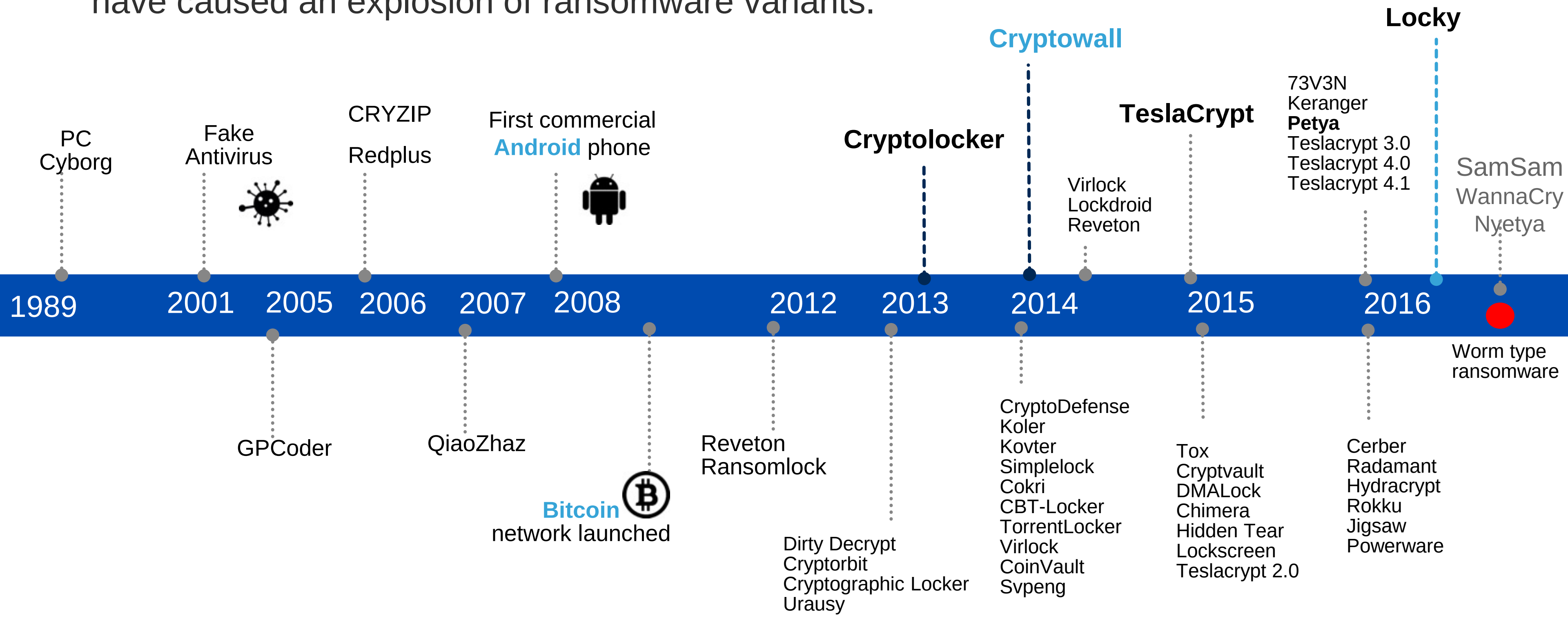
2016

$11.5B

Predicted in 2019

# The Evolution of Ransomware Variants

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and a willingness for victims to pay have caused an explosion of ransomware variants.



1989
PC Cyborg

2001
Fake Antivirus

2005
GPCoder

2006
CRYZIP
Redplus

2007
QiaoZhaz

2008
First commercial **Android** phone

**Bitcoin** network launched

2012
Reveton
Ransomlock

2013
**Cryptolocker**

Dirty Decrypt
Cryptorbit
Cryptographic Locker
Urausy

2014
**Cryptowall**

CryptoDefense
Koler
Kovter
Simplelock
Cokri
CBT-Locker
TorrentLocker
Virlock
CoinVault
Svpeng

Virlock
Lockdroid
Reveton

2015
**TeslaCrypt**

Tox
Cryptvault
DMALock
Chimera
Hidden Tear
Lockscreen
Teslacrypt 2.0

2016
73V3N
Keranger
**Petya**
Teslacrypt 3.0
Teslacrypt 4.0
Teslacrypt 4.1

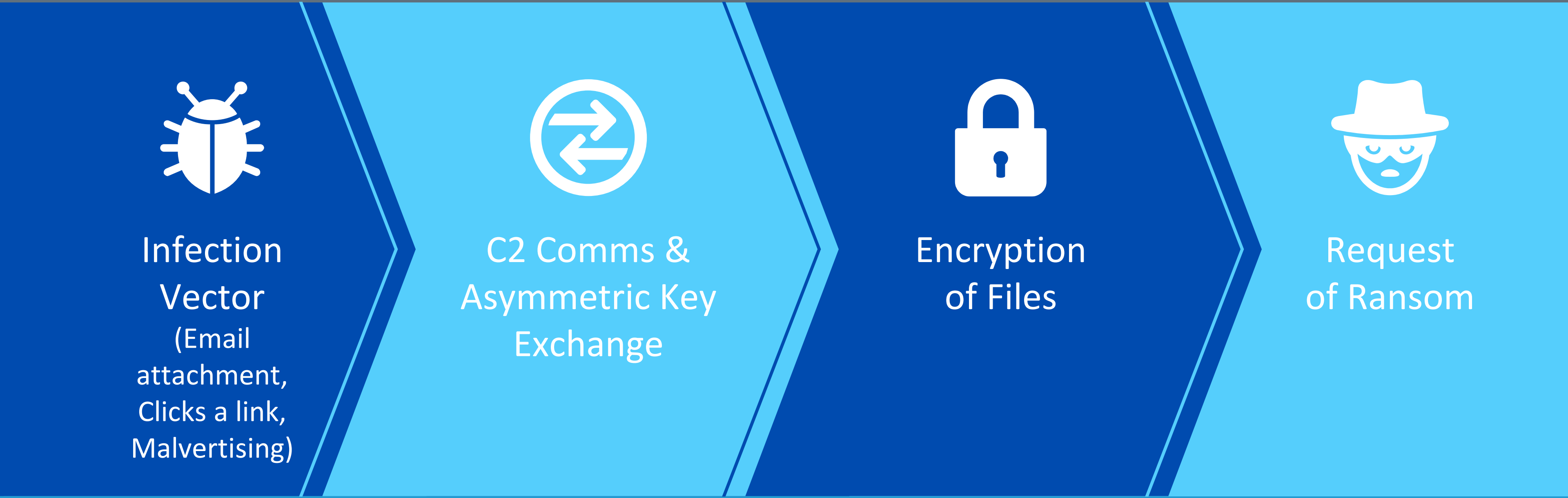
**Locky**

Cerber
Radamant
Hydracrypt
Rokku
Jigsaw
Powerware

SamSam
WannaCry
Nyetya

Worm type ransomware

# Typical Ransomware Infection



Infection Vector (Email attachment, Clicks a link, Malvertising)

C2 Comms & Asymmetric Key Exchange

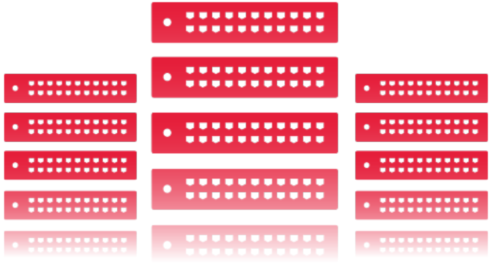
Encryption of Files

Request of Ransom

|  | Encryption C&C |  |  |  | Payment MSG |
|---|---|---|---|---|---|
| **NAME** | **DNS** | **IP** | **NO C&C** | **TOR** | **PAYMENT** |
| Locky | ● | ● |  |  | DNS |
| SamSam |  |  | ● |  | DNS (TOR) |
| TeslaCrypt | ● |  |  |  | DNS |
| CryptoWall | ● |  |  |  | DNS |
| TorrentLocker | ● |  |  |  | DNS |
| PadCrypt | ● |  |  |  | DNS (TOR) |
| CTB-Locker | ● |  |  | ● | DNS |
| FAKBEN | ● |  |  |  | DNS (TOR) |
| PayCrypt | ● |  |  |  | DNS |
| KeyRanger | ● |  |  | ● | DNS |

# DNS: a Security perspective

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



91.3%

of malware uses DNS

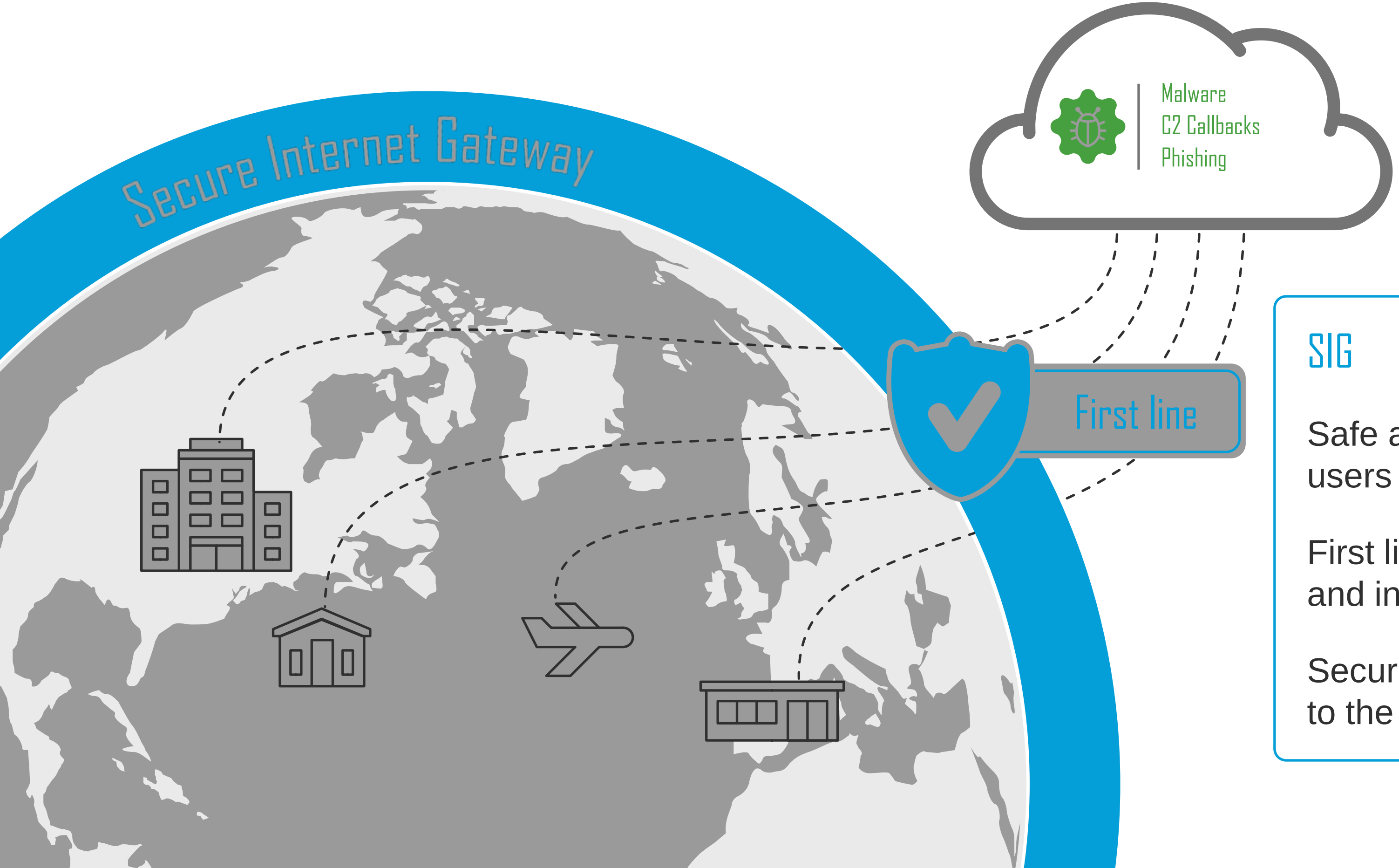
68%

of organizations **don't** monitor it

Source: Cisco Annual Security Report, 2016

# Secure Internet Gateway (SIG)

## Protect anywhere users connect



### SIG

Safe access anywhere users go, even off VPN

First line of defense and inspection

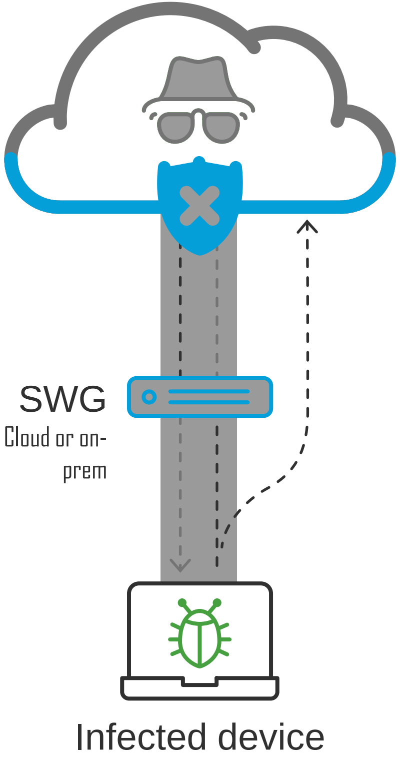
Secure onramp to the internet

ENFORCEMENT

# Protection for command and control (C2) callbacks

**91%**

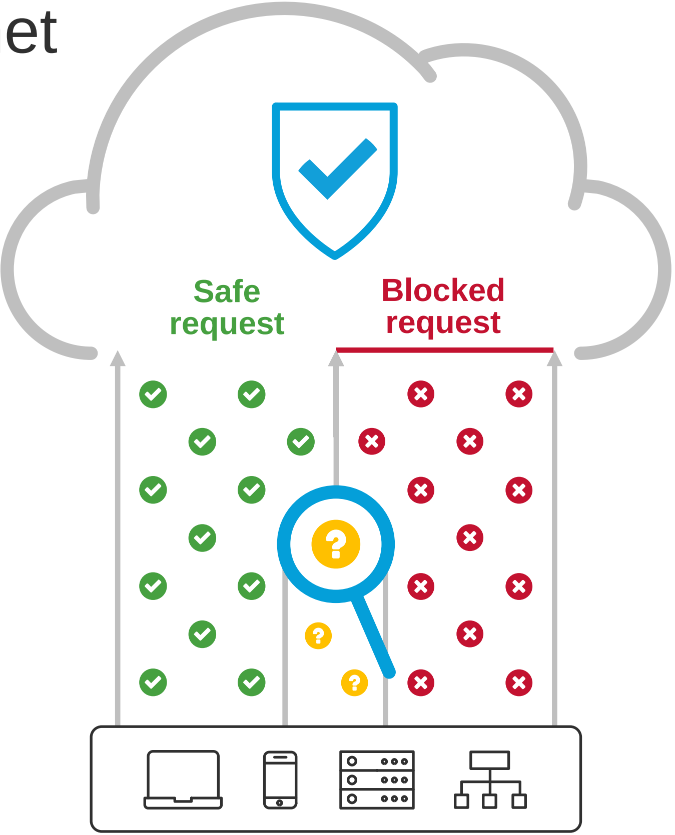
of C2 can be blocked at the DNS layer



**15%**

of C2 bypasses web ports 80 & 443

# Built into foundation of the internet



Umbrella provides:

Connection for safe requests

Prevention for user and malware-initiated connections

Proxy inspection for risky domains

# 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

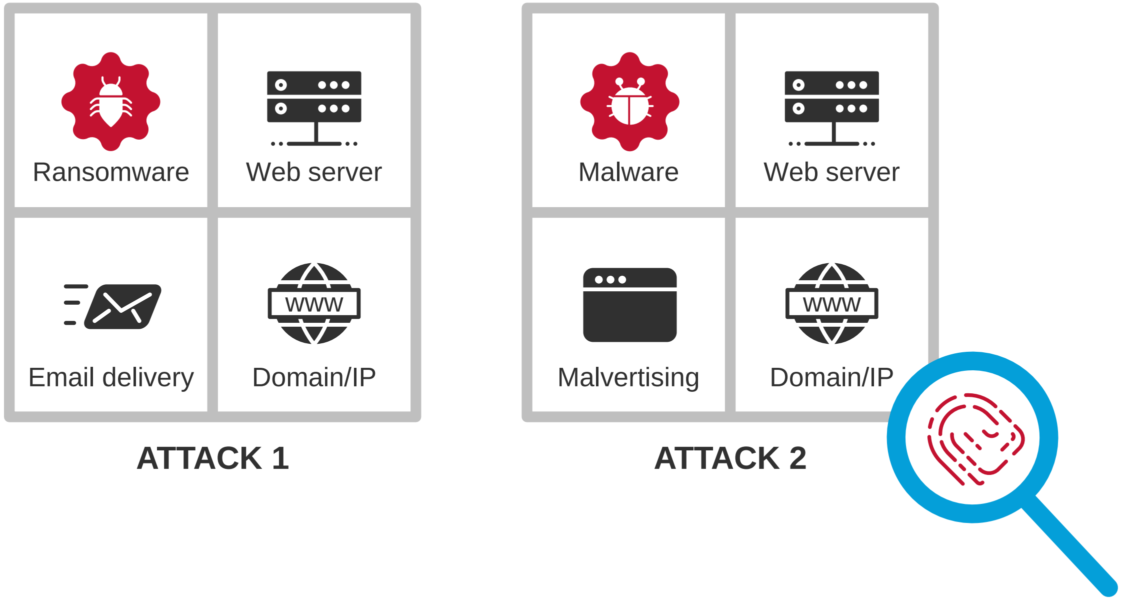
Updated instructions

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

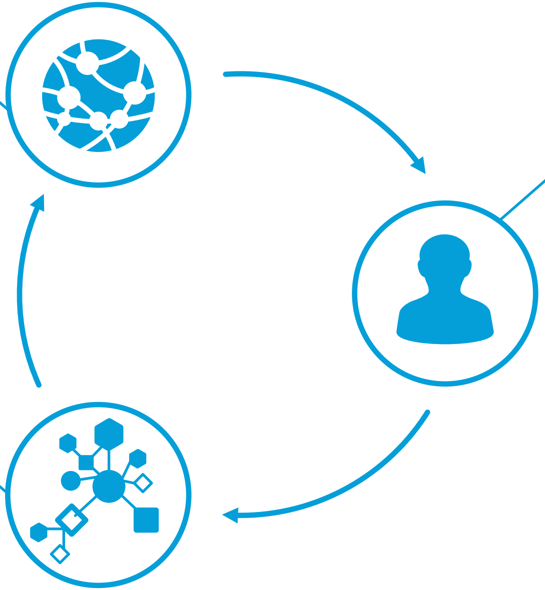
Domain/IP

**ATTACK 2**

# Intelligence to see attacks before launched

## Data

- Cisco Talos feed of malicious domains, IPs, and URLs
- Umbrella DNS data — 100B requests per day

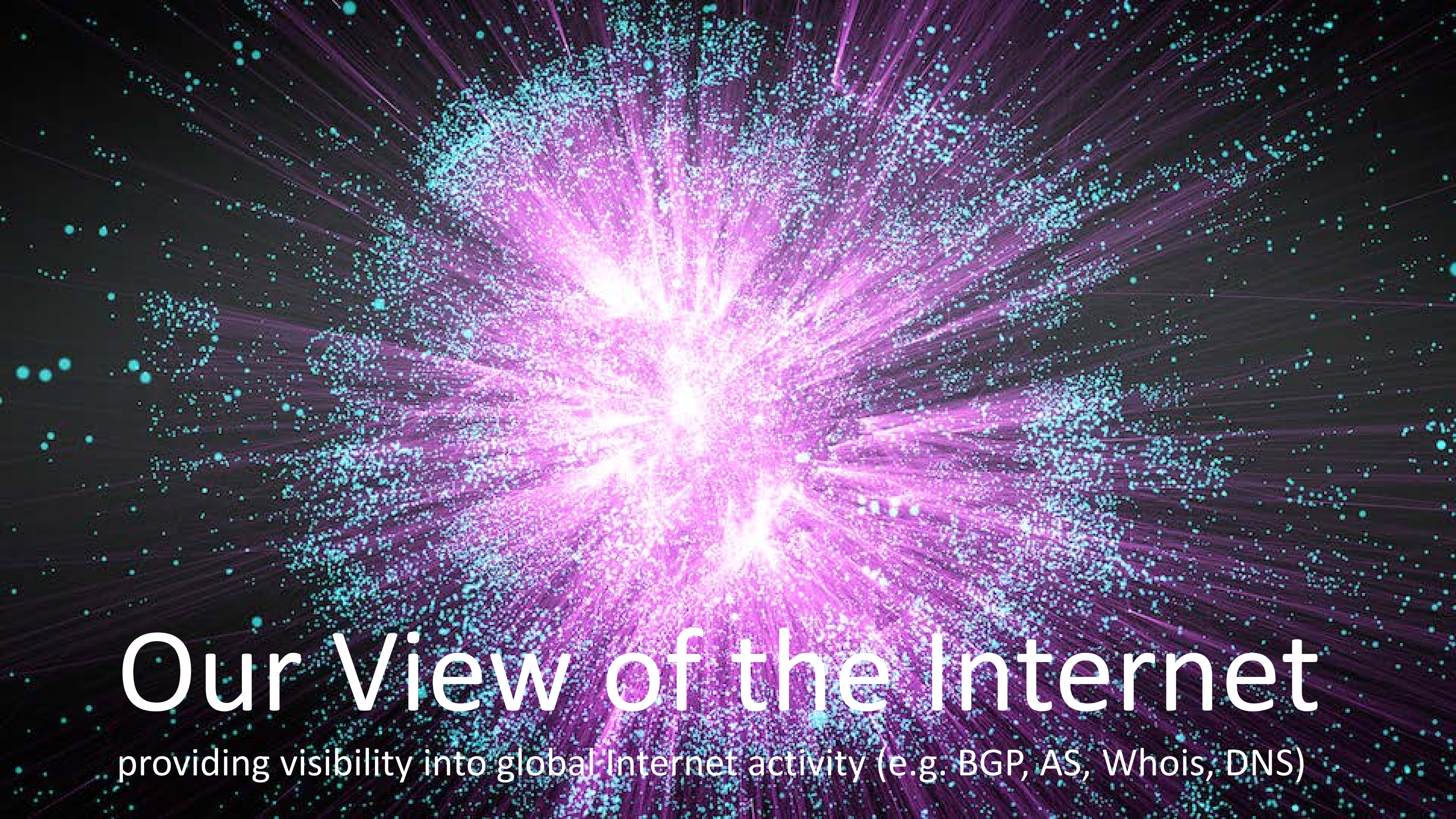


## Security researchers

- Industry renown researchers
- Build models that can automatically classify and score domains and IPs

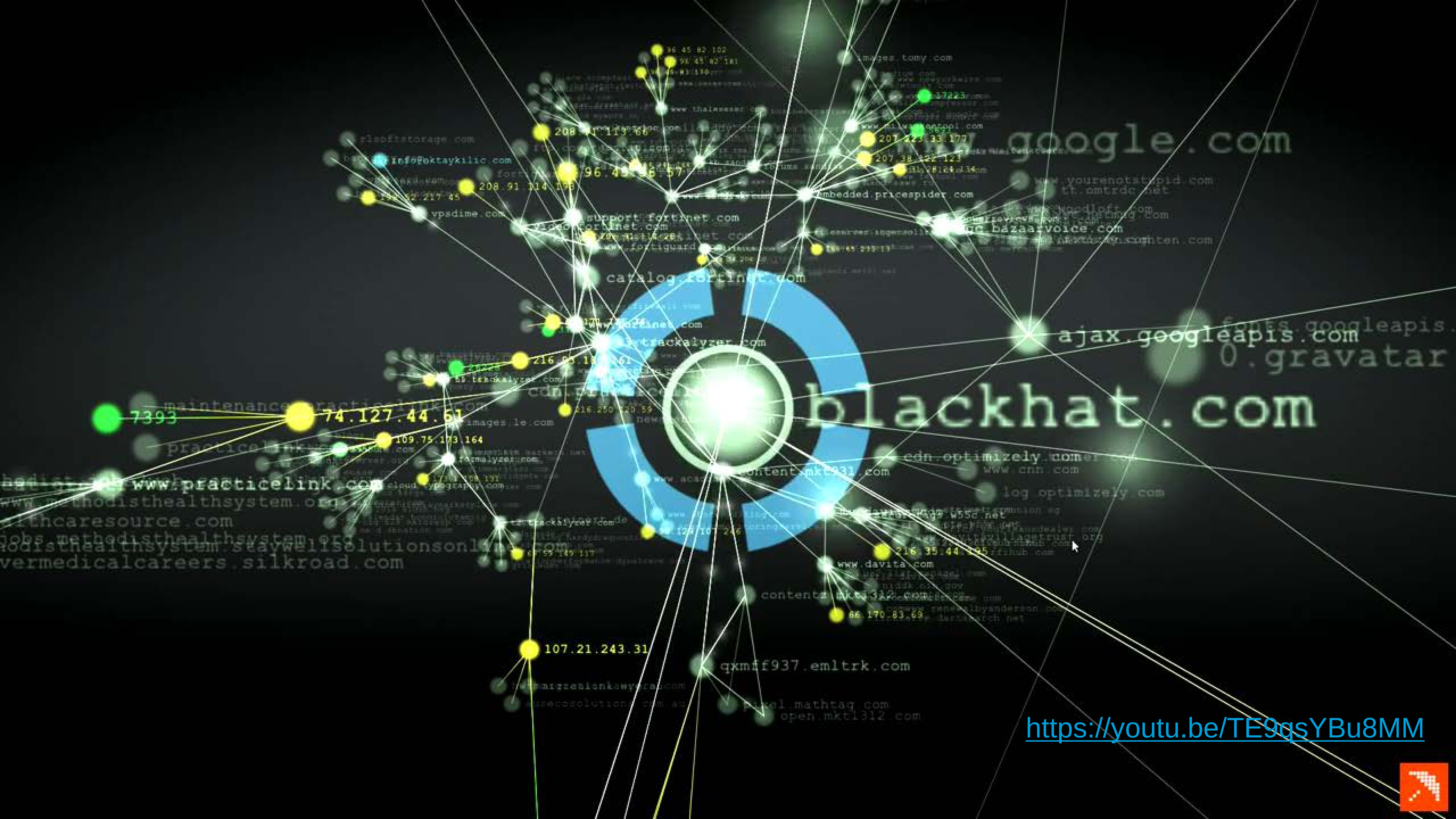
## Models

- Dozens of models continuously analyze millions of live events per second
- Automatically uncover malware, ransomware, and other threats



# Our View of the Internet

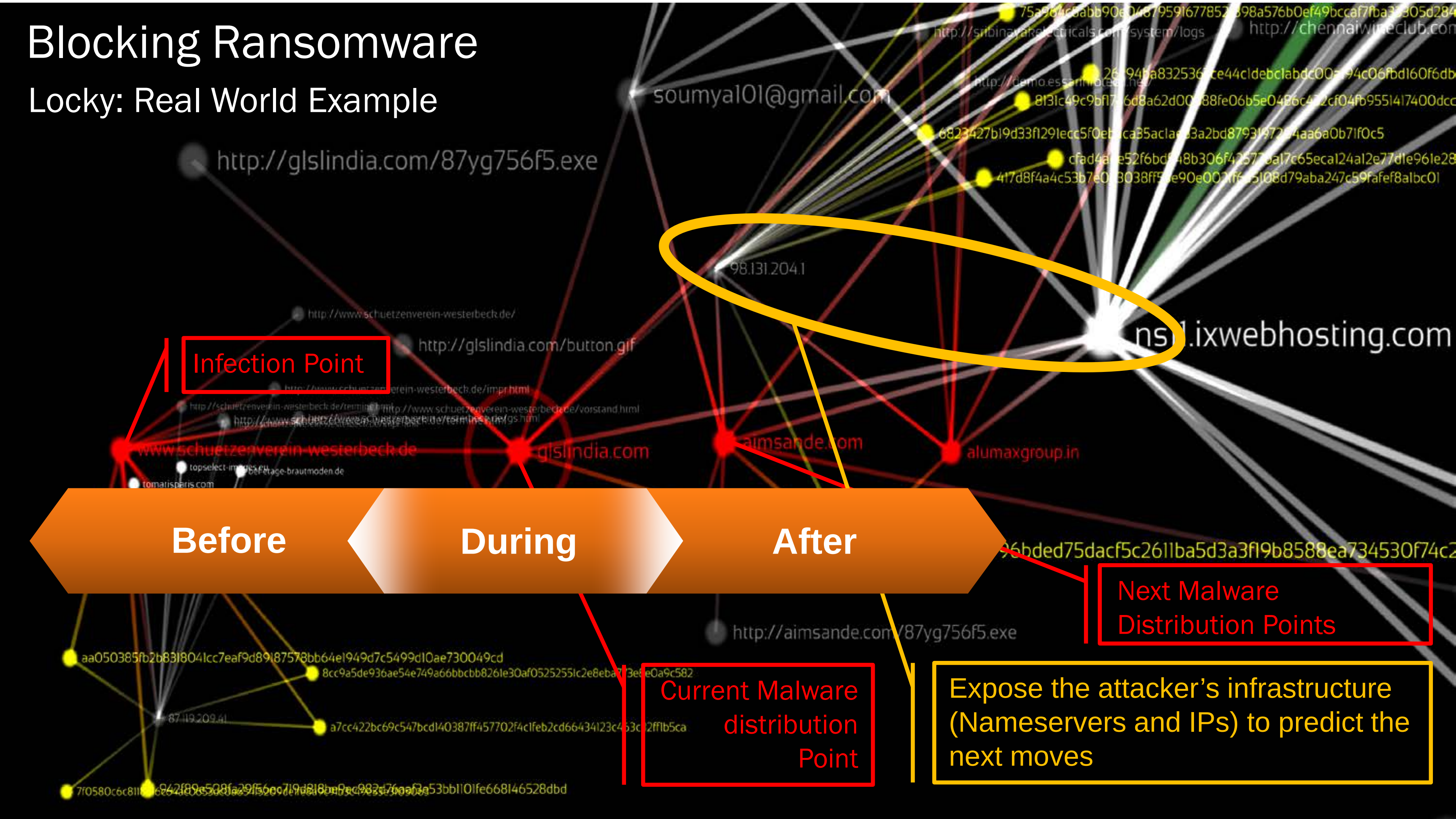
providing visibility into global Internet activity (e.g. BGP, AS, Whois, DNS)



https://youtu.be/TE9qsYBu8MM

# Blocking Ransomware

## Locky: Real World Example



soumya101@gmail.com
http://glslindia.com/87yg756f5.exe
98.131.204.1
ns1.ixwebhosting.com
http://www.schuetzenverein-westerbeck.de/
http://glslindia.com/button.gif
http://www.schuetzenverein-westerbeck.de/vorstand.html
www.schuetzenverein-westerbeck.de
glslindia.com
aimsande.com
alumaxgroup.in
topselect-images.eu
tomarisparis.com
http://aimsande.com/87yg756f5.exe
87.119.209.41
http://chennaiwineclub.com
http://demo.essaninfotech.net
813lc49c9bf17c6d8a62d00388fe06b5e0486c42cf04fb955l417400dcc
6823427b19d33f129lecc5f0ebca35acla63a2bd87939720aa6a0b7lf0c5
417d8f4a4c53b7e0l3038ff5e90e007ff45108d79aba247c59fafef8albc0l
aa050385fb2b83l804lcc7eaf9d89187578bb64el949d7c5499dl0ae730049cd
8cc9a5de936ae54e749a66bbcbb826le30af0525255lc2e8eba73e6e0a9c582
a7cc422bc69c547bcdl40387ff457702f4clfeb2cd66434123c463c2fflb5ca

Infection Point

Before

During

After

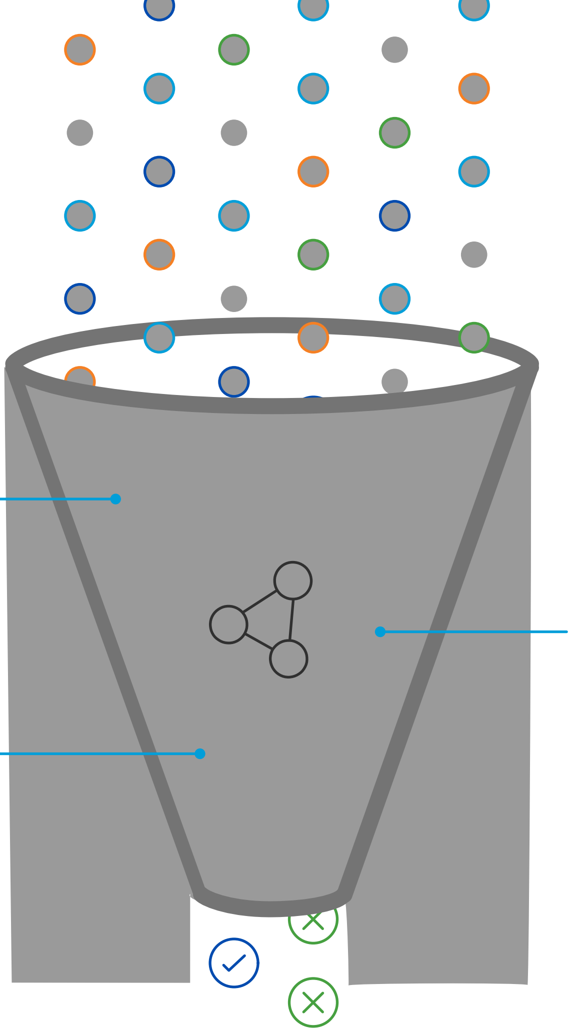
Next Malware Distribution Points

Current Malware distribution Point

Expose the attacker’s infrastructure (Nameservers and IPs) to predict the next moves

# Intelligence

## Statistical models



2M+ live events per second

11B+ historical events

### Guilt by inference

- Co-occurrence model
- Sender rank model
- Secure rank model

### Guilt by association

- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

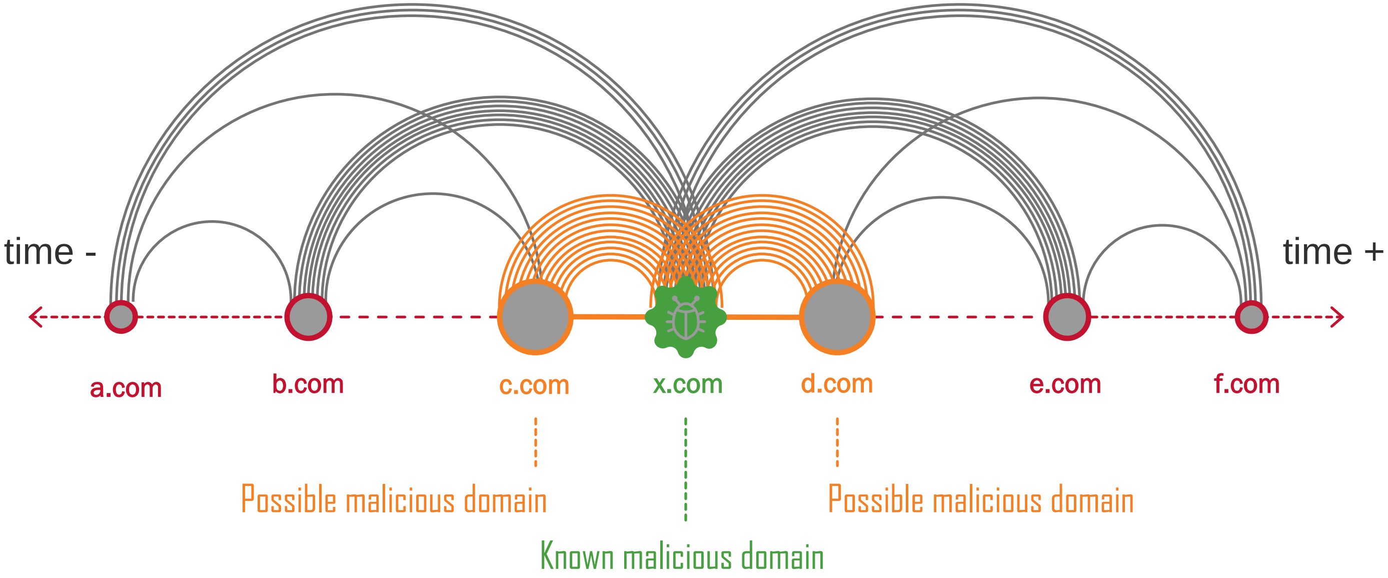
### Patterns of guilt

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

INTELLIGENCE

# Co-occurrence model

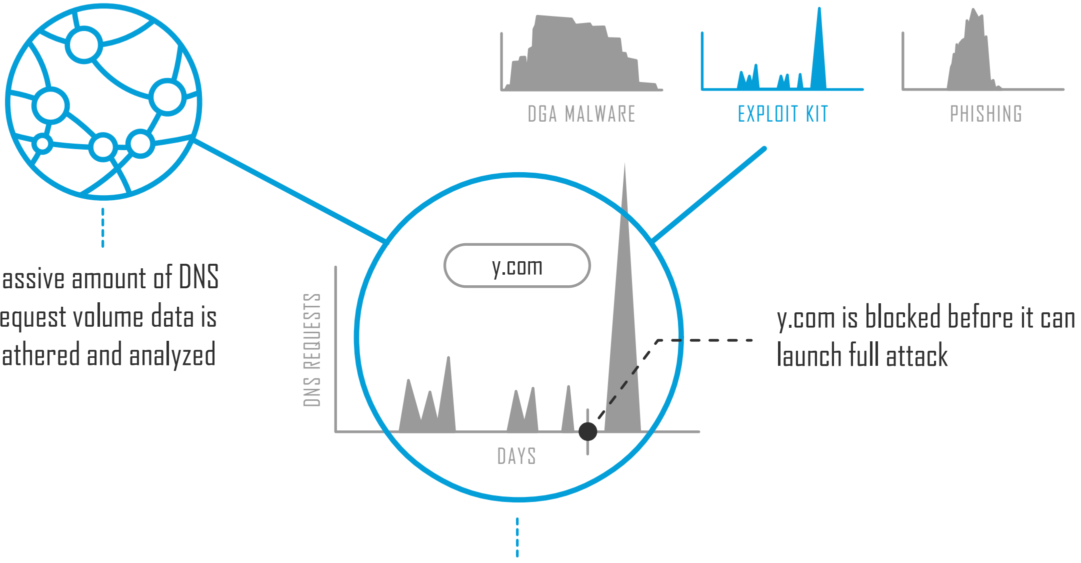
## Domains guilty by inference



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



Massive amount of DNS request volume data is gathered and analyzed

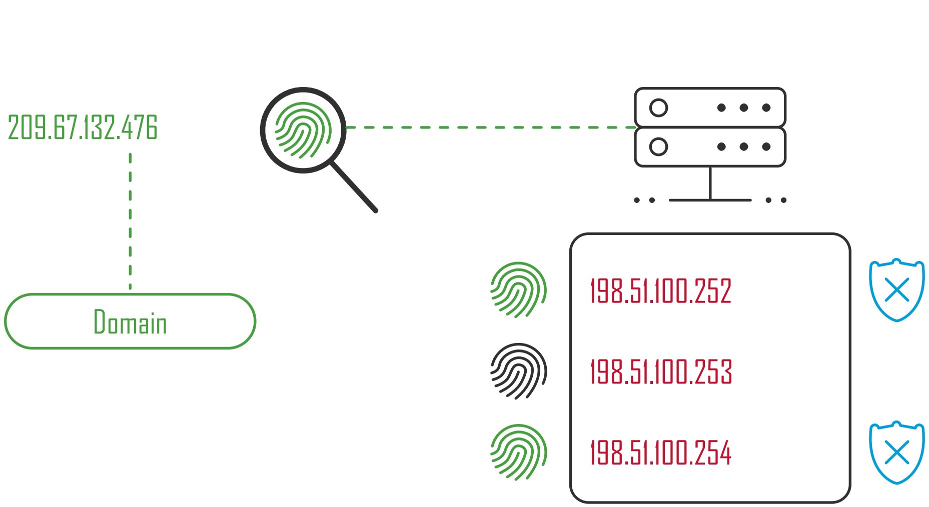
y.com is blocked before it can launch full attack

DNS request volume matches known exploit kit pattern and predicts future attack

INTELLIGENCE

# Predictive IP Space Monitoring

## Guilt by association

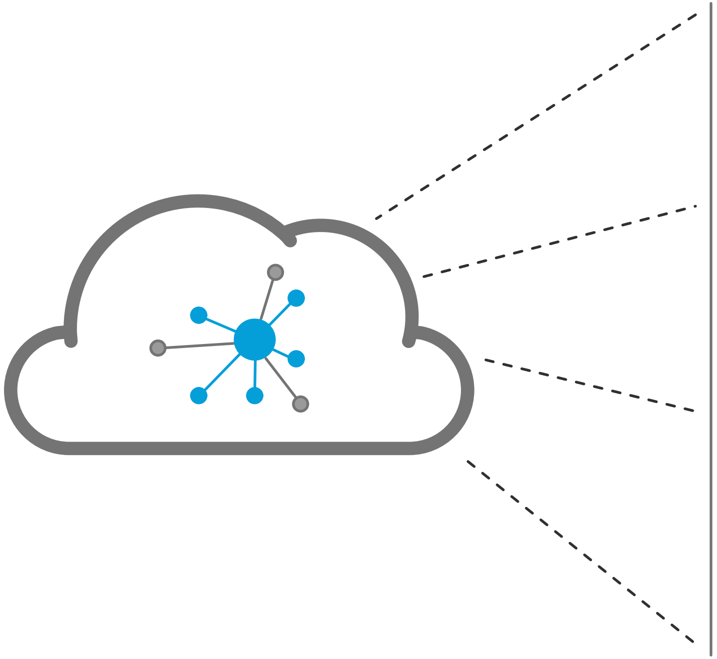


Pinpoint suspicious domains and observe their IP’s fingerprint

Identify other IPs – hosted on the same server – that share the same fingerprint

Block those suspicious IPs and any related domains

# A single, correlated source of intelligence



Passive DNS database

WHOIS record data

Malware file analysis

ASN attribution

IP geolocation

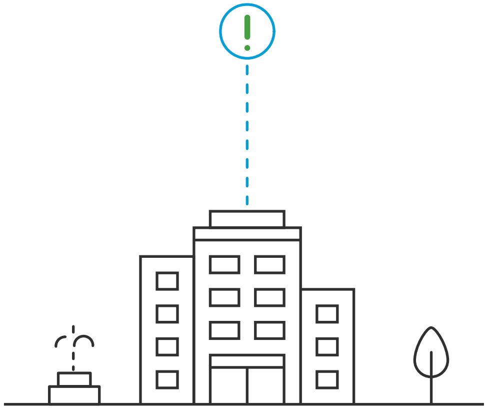
Domain and IP reputation scores

Domain co-occurrences

Anomaly detection (DGAs, FFNs)

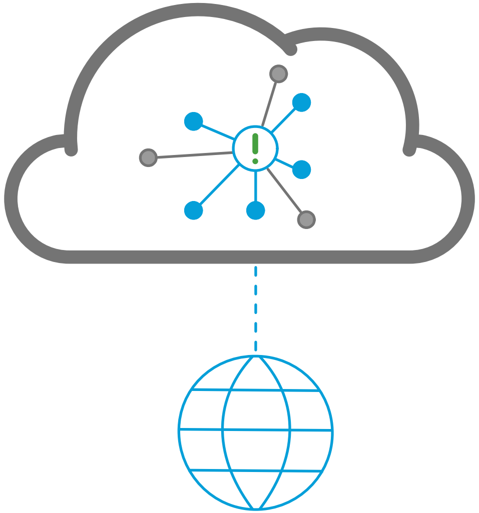
DNS request patterns/geo. distribution

## You know one IOC



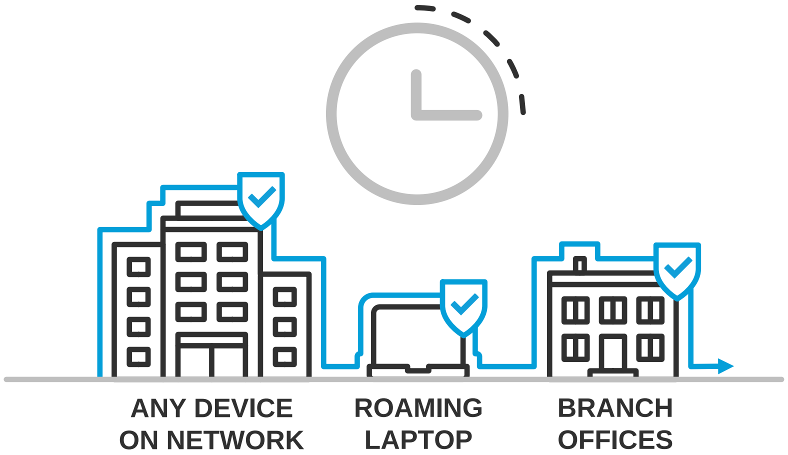
Your local intelligence

## We know all its relationships



Our global context

# Enterprise-wide deployment in minutes



## On-network coverage

With one setting change

Integrated with Cisco ISR 4K series and Cisco WLAN controllers

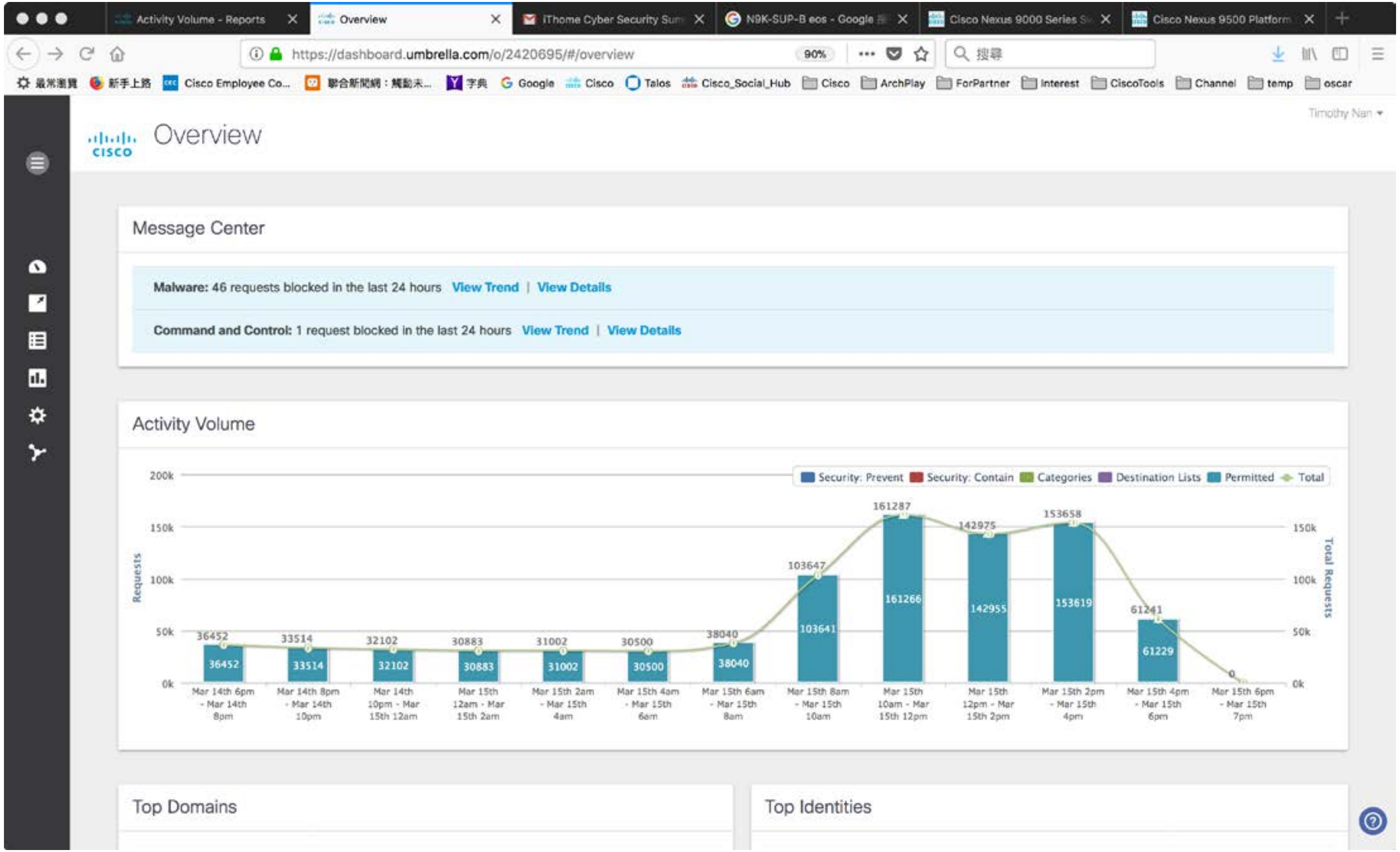
## Off-network coverage

With AnyConnect VPN client integration

Or with any VPN using lightweight Umbrella client

# 2018 台灣資安大會實例

# 2018 台灣資安大會實例


Activity Volume - Reports
Overview
iThome Cyber Security Sum
N9K-SUP-B eos - Google
Cisco Nexus 9000 Series S
Cisco Nexus 9500 Platform
https://dashboard.umbrella.com/o/2420695/#/overview
90%
搜尋
最常瀏覽
新手上路
Cisco Employee Co...
聯合新聞網：觸動未...
字典
Google
Cisco
Talos
Cisco_Social_Hub
Cisco
ArchPlay
ForPartner
Interest
CiscoTools
Channel
temp
oscar
Timothy Nan
cisco

Overview

Message Center

**Malware:** 46 requests blocked in the last 24 hours View Trend | View Details

**Command and Control:** 1 request blocked in the last 24 hours View Trend | View Details

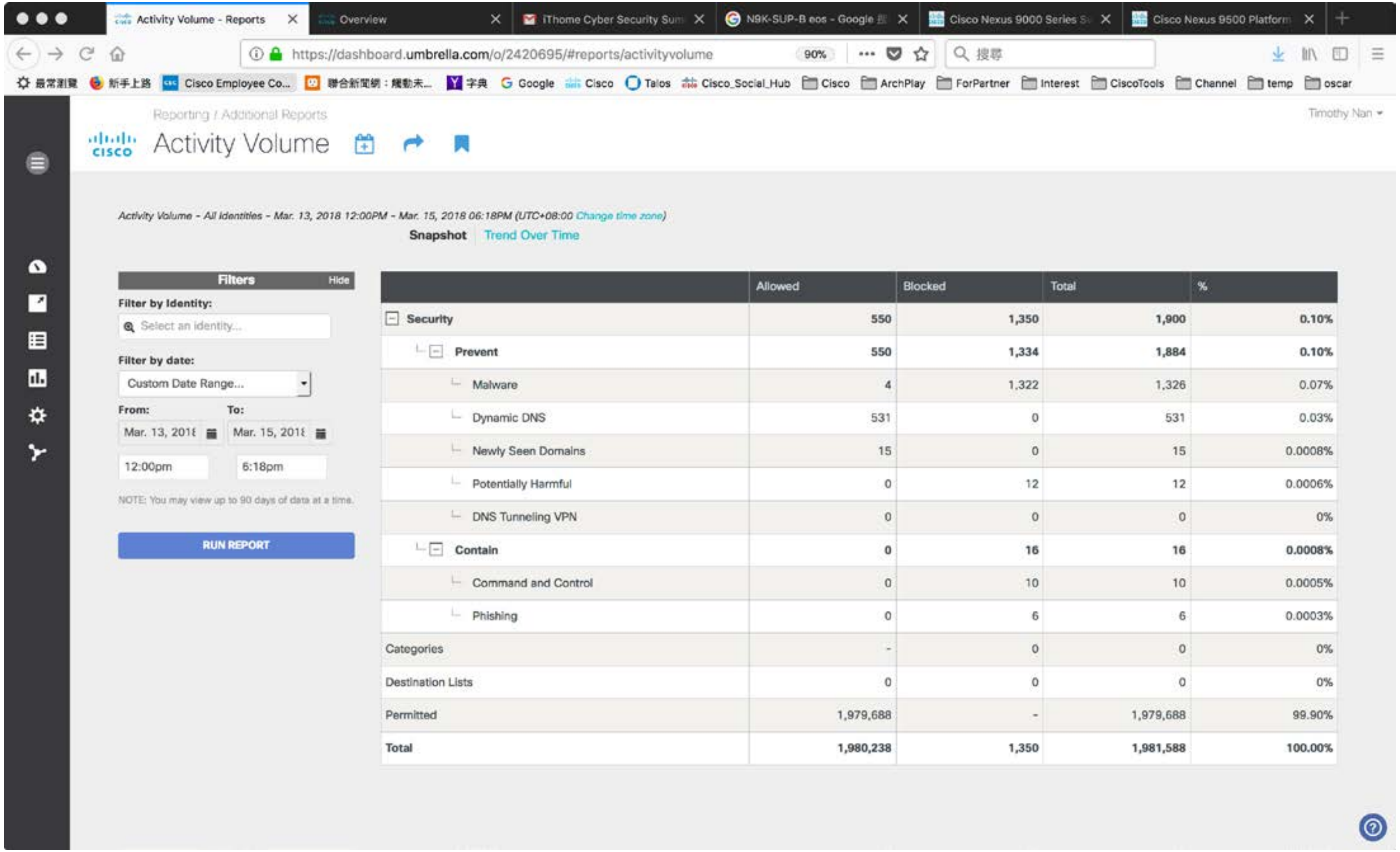
Activity Volume

200k
150k
100k
50k
0k
Requests
Total Requests
Security: Prevent
Security: Contain
Categories
Destination Lists
Permitted
Total
36452
33514
32102
30883
31002
30500
38040
103647
103641
161287
161266
142975
142955
153658
153619
61241
61229
0
Mar 14th 6pm - Mar 14th 8pm
Mar 14th 8pm - Mar 14th 10pm
Mar 14th 10pm - Mar 15th 12am
Mar 15th 12am - Mar 15th 2am
Mar 15th 2am - Mar 15th 4am
Mar 15th 4am - Mar 15th 6am
Mar 15th 6am - Mar 15th 8am
Mar 15th 8am - Mar 15th 10am
Mar 15th 10am - Mar 15th 12pm
Mar 15th 12pm - Mar 15th 2pm
Mar 15th 2pm - Mar 15th 4pm
Mar 15th 4pm - Mar 15th 6pm
Mar 15th 6pm - Mar 15th 7pm

Top Domains

Top Identities

# 2018 台灣資安大會實例



Activity Volume

*Activity Volume - All identities - Mar. 13, 2018 12:00PM - Mar. 15, 2018 06:18PM (UTC+08:00 Change time zone)*

**Snapshot** | Trend Over Time

**Filters** Hide

**Filter by Identity:** Select an identity...

**Filter by date:** Custom Date Range...

**From:** Mar. 13, 2018 12:00pm

**To:** Mar. 15, 2018 6:18pm

NOTE: You may view up to 90 days of data at a time.

RUN REPORT

|  | Allowed | Blocked | Total | % |
|---|---|---|---|---|
| **Security** | **550** | **1,350** | **1,900** | **0.10%** |
| **Prevent** | **550** | **1,334** | **1,884** | **0.10%** |
| Malware | 4 | 1,322 | 1,326 | 0.07% |
| Dynamic DNS | 531 | 0 | 531 | 0.03% |
| Newly Seen Domains | 15 | 0 | 15 | 0.0008% |
| Potentially Harmful | 0 | 12 | 12 | 0.0006% |
| DNS Tunneling VPN | 0 | 0 | 0 | 0% |
| **Contain** | **0** | **16** | **16** | **0.0008%** |
| Command and Control | 0 | 10 | 10 | 0.0005% |
| Phishing | 0 | 6 | 6 | 0.0003% |
| Categories | - | 0 | 0 | 0% |
| Destination Lists | 0 | 0 | 0 | 0% |
| Permitted | 1,979,688 | - | 1,979,688 | 99.90% |
| **Total** | **1,980,238** | **1,350** | **1,981,588** | **100.00%** |

# Thank You!