Defense for Evolving Cyber Attacks

Garrick Ng

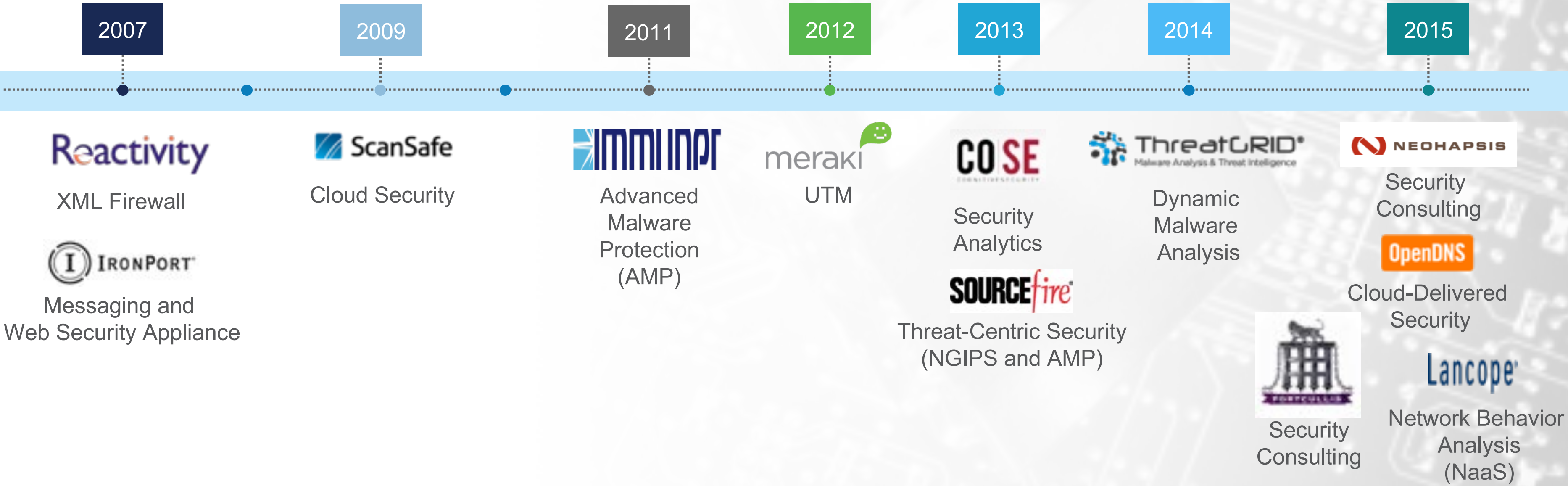
Head of Systems Engineering

Cisco Hong Kong

Nov 2016

Why Cisco for Security?

Over the last three years we've invested more than US$3.8 billion in security. We are transforming to create the industry's broadest security solution portfolio via continued security technology innovation…
Committed to becoming the **#1 security trusted advisor and partner to customers and partners**



2007

Reactivity
XML Firewall

IronPort
Messaging and
Web Security Appliance

2009

ScanSafe
Cloud Security

2011

Immunet
Advanced Malware Protection (AMP)

2012

meraki
UTM

2013

Cognitive Security
Security Analytics

Sourcefire
Threat-Centric Security (NGIPS and AMP)

2014

ThreatGRID
Malware Analysis & Threat Intelligence
Dynamic Malware Analysis

2015

Neohapsis
Security Consulting

OpenDNS
Cloud-Delivered Security

Portcullis
Security Consulting

Lancope
Network Behavior Analysis (NaaS)

The Cybercrime Economy

Social Security
$1

Medical
Record
>$50

Credit
Card Data
$0.25-$60

Bank Account Info
>$1000
depending on account
type and balance

DDOS
as a Service
~$7/hour

Global Cybercrime Market: $450B-$1T

Mobile Malware
$150

Spam
$50/500K emails

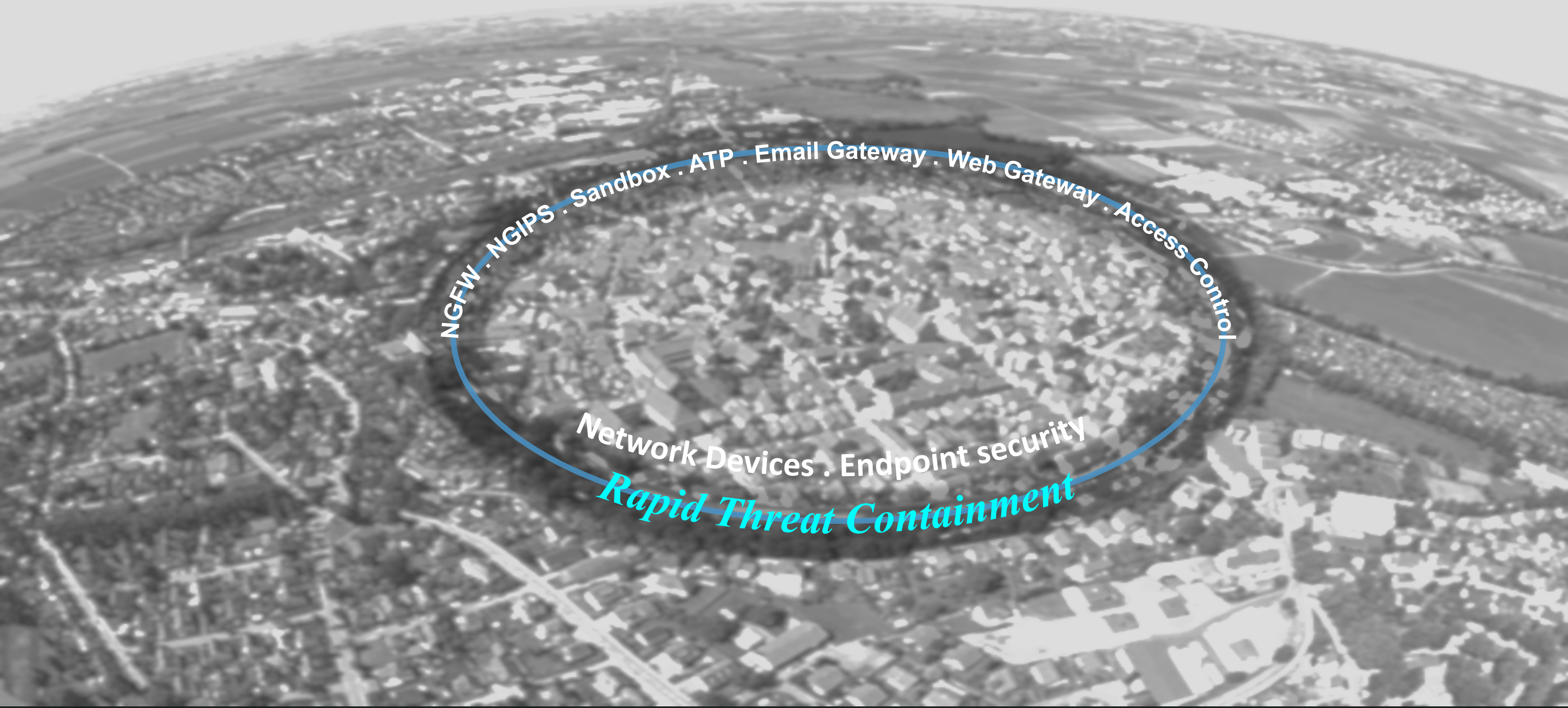
Exploits
$1000-$300K

Malware
Development
$2500
(commercial malware)

Facebook Account
$1 for an account with
15 friends

Security Everywhere: Multi-Layer Integrated Defense

Security Everywhere: Multi-Layer Integrated Defense

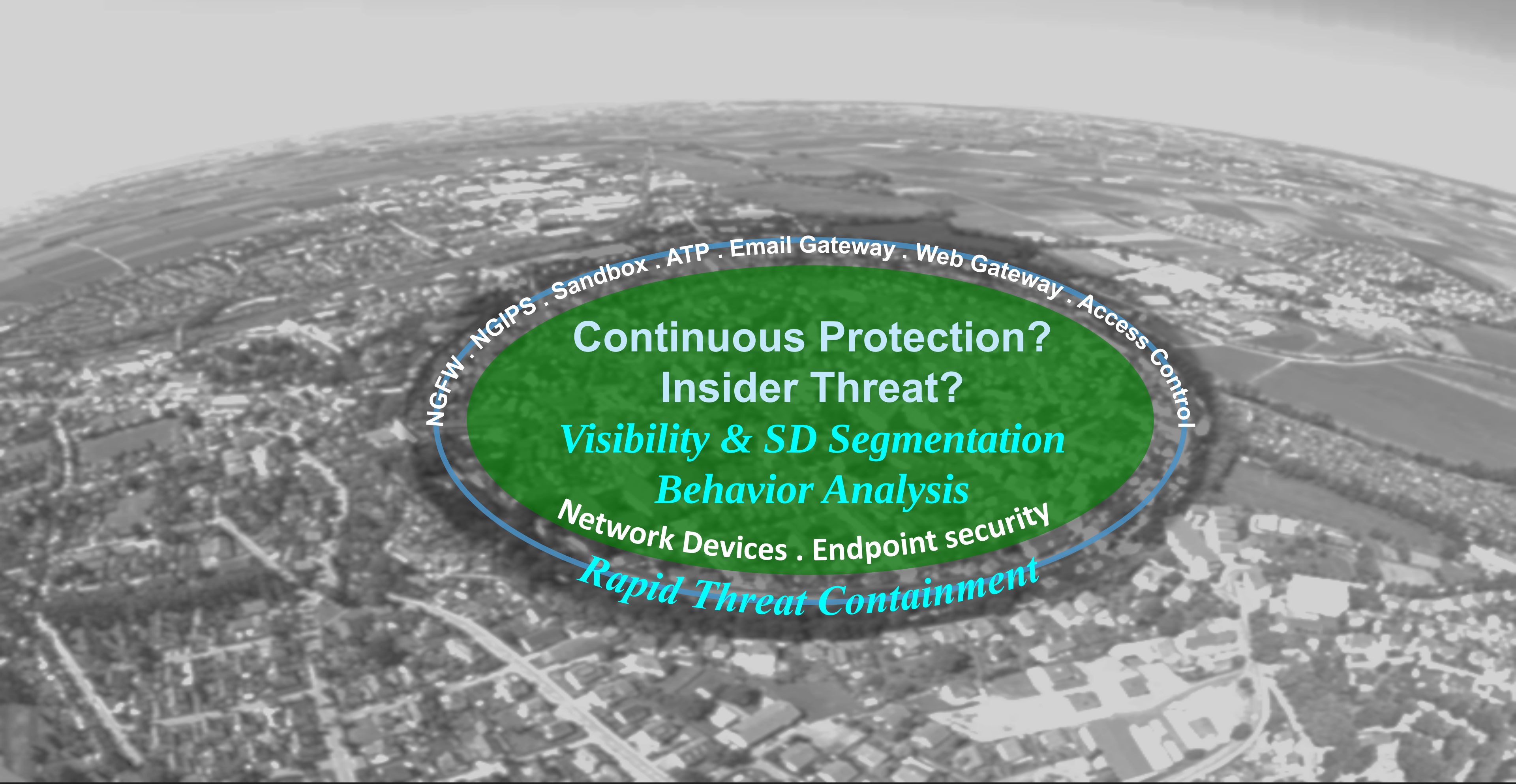


NGFW . NGIPS . Sandbox . ATP . Email Gateway . Web Gateway . Access Control

Network Devices . Endpoint security

Rapid Threat Containment

Security Everywhere: Multi-Layer Integrated Defense



NGFW . NGIPS . Sandbox . ATP . Email Gateway . Web Gateway . Access Control

Continuous Protection?

Insider Threat?

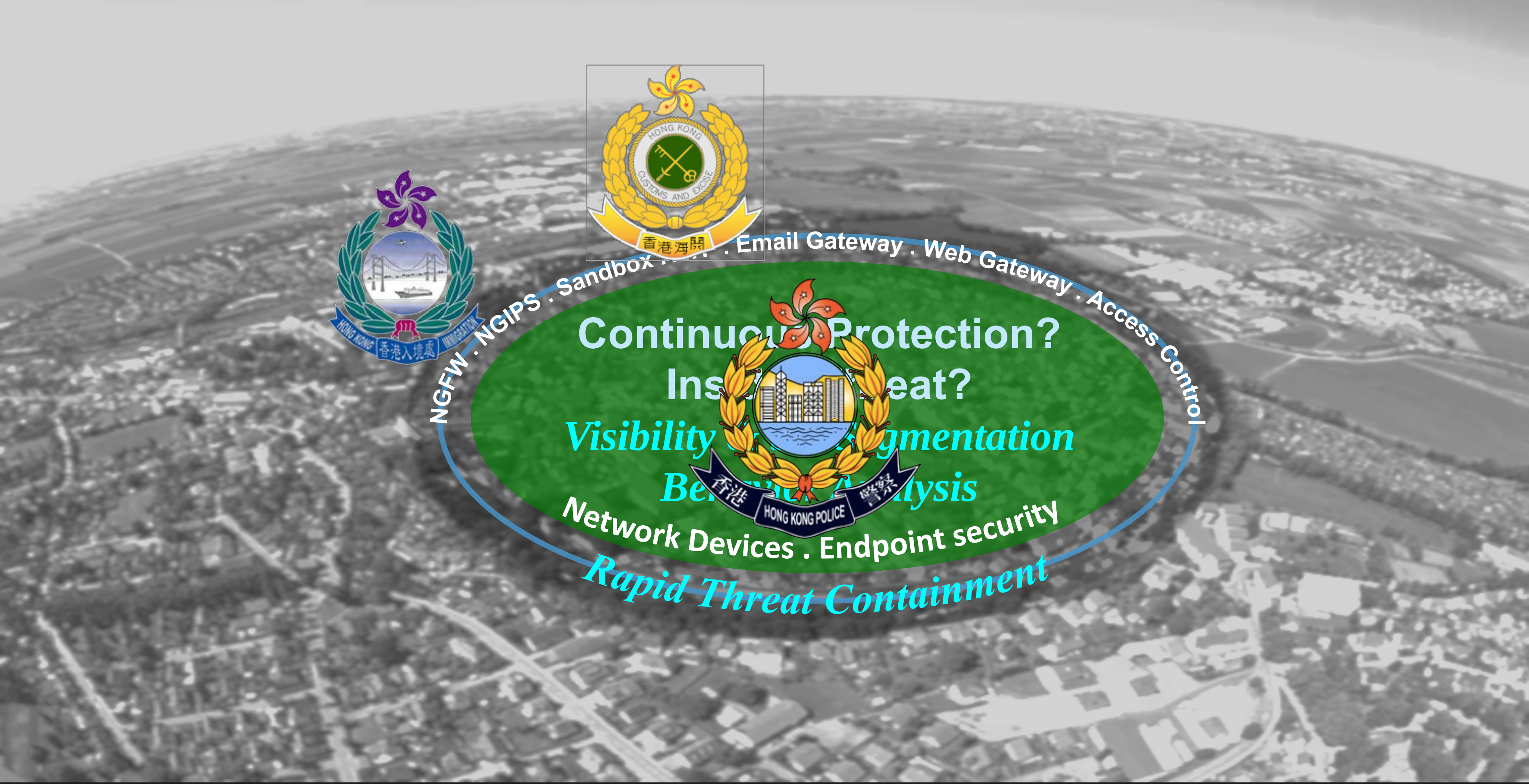
Visibility & SD Segmentation

Behavior Analysis

Network Devices . Endpoint security

Rapid Threat Containment

Security Everywhere: Multi-Layer Integrated Defense



NGFW . NGIPS . Sandbox . [illegible] . Email Gateway . Web Gateway . Access Control

Continuous Protection?

Insider Threat?

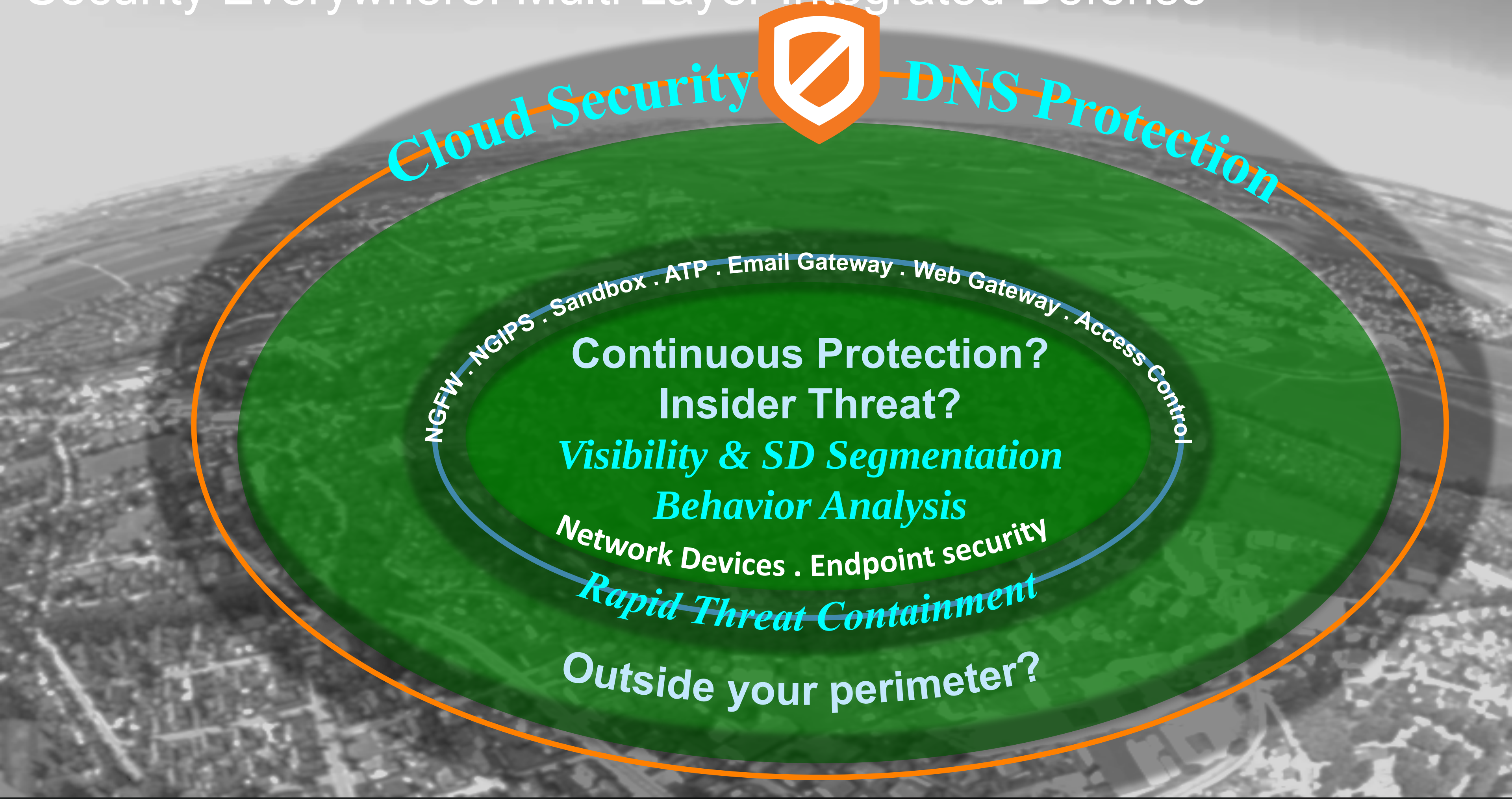
Visibility [illegible] Segmentation

Behavior Analysis

Network Devices . Endpoint security

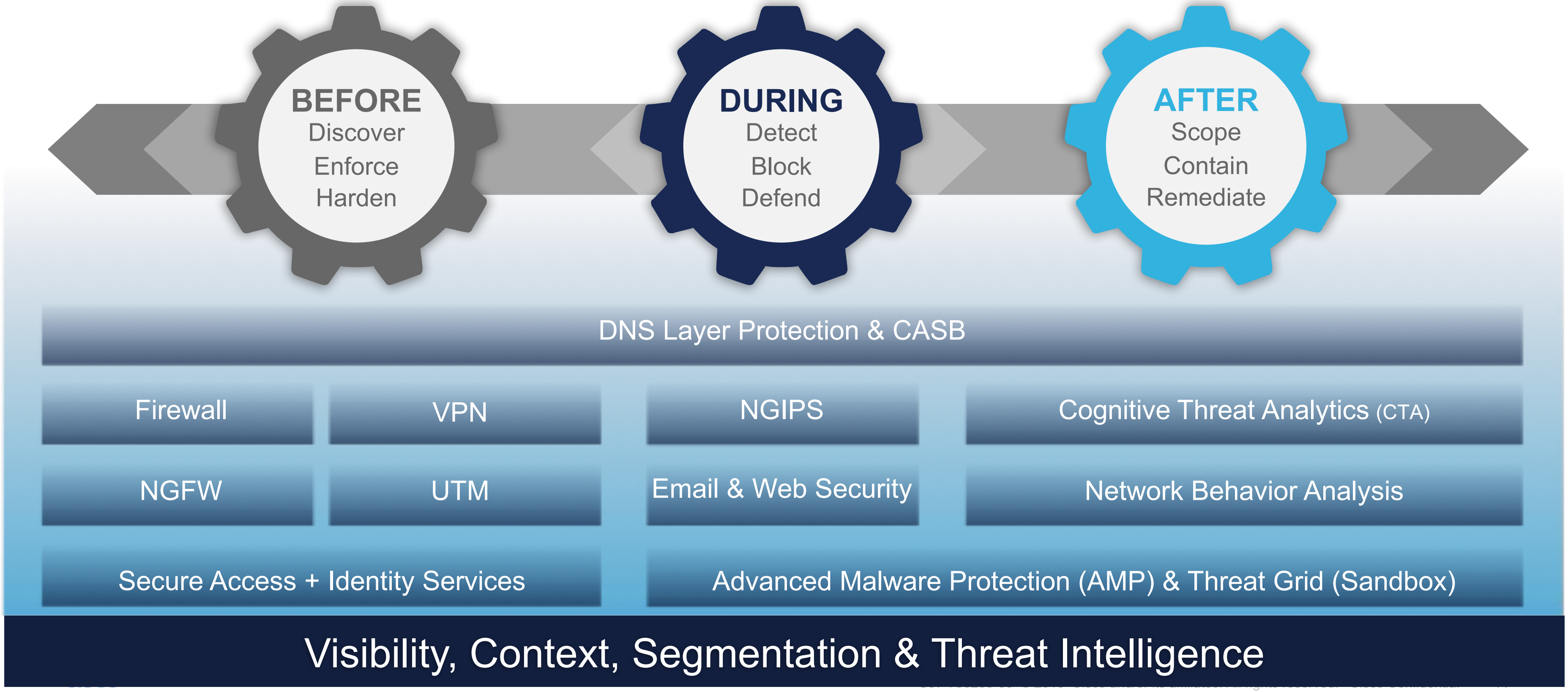
Rapid Threat Containment

Security Everywhere: Multi-Layer Integrated Defense



Cloud Security
DNS Protection
NGFW . NGIPS . Sandbox . ATP . Email Gateway . Web Gateway . Access Control
Continuous Protection?
Insider Threat?
Visibility & SD Segmentation
Behavior Analysis
Network Devices . Endpoint security
Rapid Threat Containment
Outside your perimeter?

Threat Centric model to cover the Entire Attack Continuum



BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

DNS Layer Protection & CASB

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

Time to Detection TTD

When you missed detection,
- Time between the first observation of an unknown file and detection of a threat

Industry

>100

DAYS

VS

Cisco

13

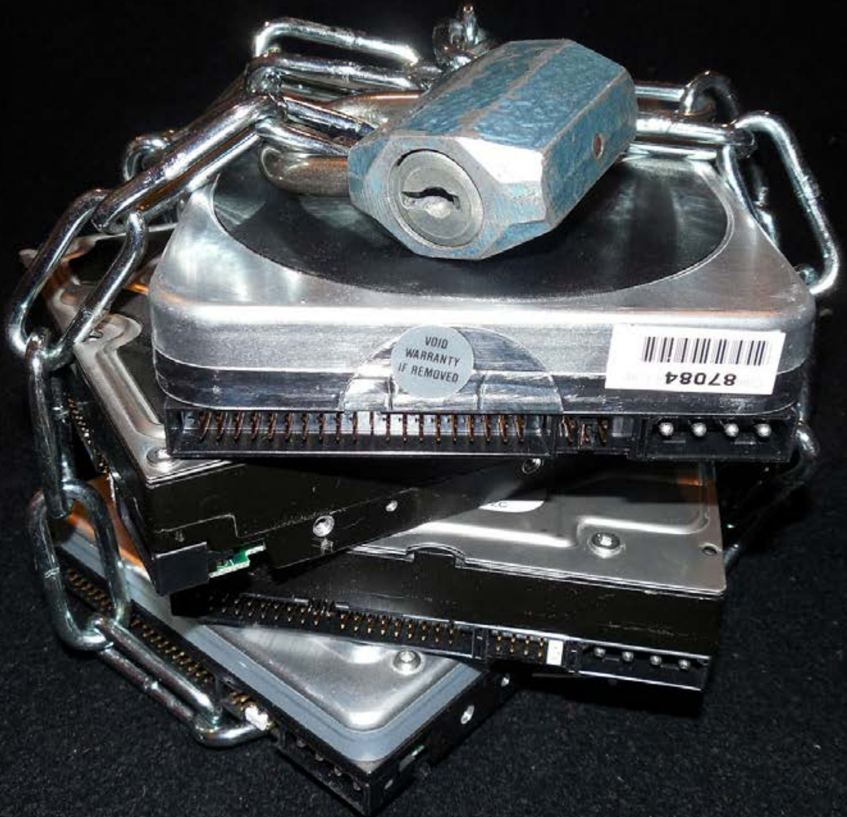
HOURS

Cisco Minimizes the Time to Detect Breaches

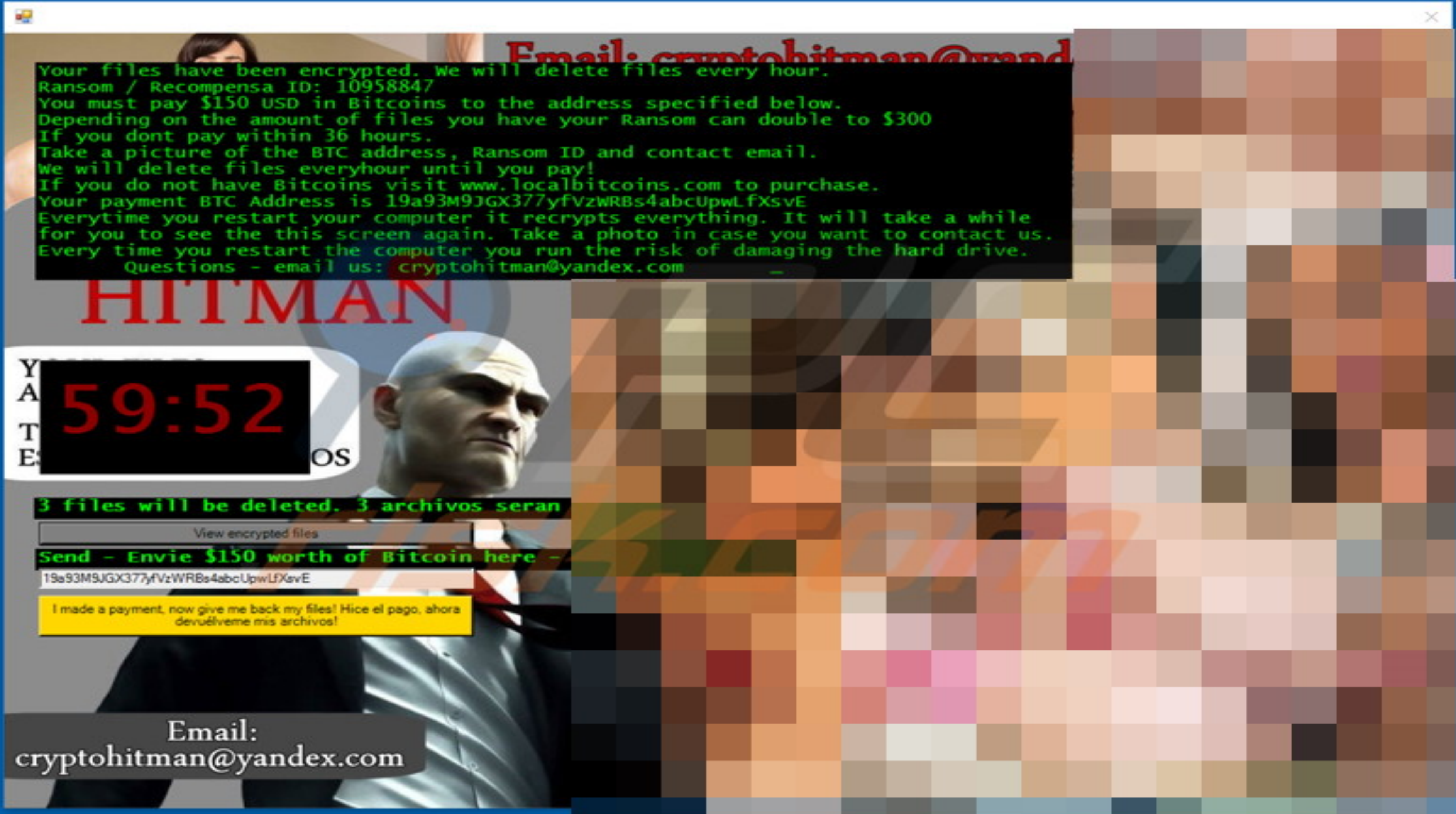
Case Study 1: Ransomware

- DNS Layer Domain level protection
- Predictive Security

Ransomware



- CryptoLocker
- TeslaCrypt 3.0
- Cryptowall 4.0
- CTB-Locker
- KeRanger
- Locky, Zepto
- SamSam
- Cerber
- Petya, Santana
- Jigsaw
- CryptXXX 3.0
- Bart
- CryptoHitman …



```
Your files have been encrypted. We will delete files every hour.
Ransom / Recompensa ID: 10958847
You must pay $150 USD in Bitcoins to the address specified below.
Depending on the amount of files you have your Ransom can double to $300
If you dont pay within 36 hours.
Take a picture of the BTC address, Ransom ID and contact email.
We will delete files everyhour until you pay!
If you do not have Bitcoins visit www.localbitcoins.com to purchase.
Your payment BTC Address is 19a93M9JGX377yfVzWRBs4abcUpwLfXsvE
Everytime you restart your computer it recrypts everything. It will take a while
for you to see the this screen again. Take a photo in case you want to contact us.
Every time you restart the computer you run the risk of damaging the hard drive.
      Questions - email us: cryptohitman@yandex.com
```

3 files will be deleted. 3 archivos seran

Send - Envie $150 worth of Bitcoin here -

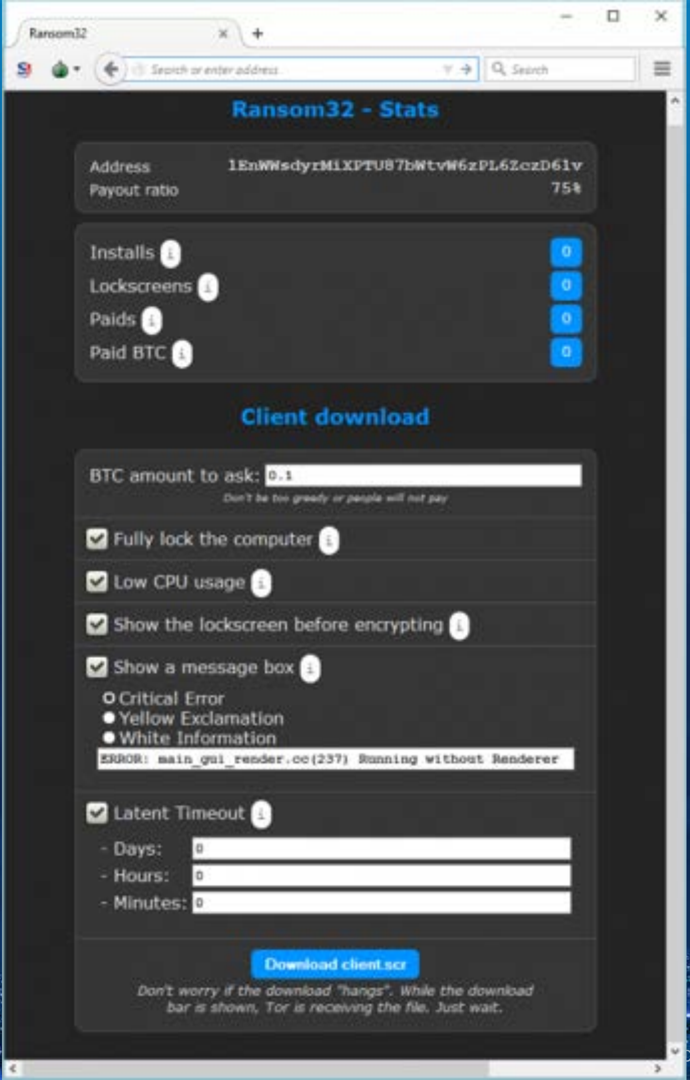
19a93M9JGX377yfVzWRBs4abcUpwLfXsvE

I made a payment, now give me back my files! Hice el pago, ahora devuélveme mis archivos!

Email:
cryptohitman@yandex.com

UNIVERSITY OF CALGARY
2500 University Drive NW

Kansas Heart HOSPITAL



Ransom32 - Stats

Address	1EnWWsdyrMiXPTU87bWtvW6zPL6ZczD61v
Payout ratio	75%

Installs	0
Lockscreens	0
Paids	0
Paid BTC	0

Client download

BTC amount to ask: 0.1

Don't be too greedy or people will not pay

☑ Fully lock the computer

☑ Low CPU usage

☑ Show the lockscreen before encrypting

☑ Show a message box

○ Critical Error
● Yellow Exclamation
● White Information

```
ERROR: main_gui_render.cc(237) Running without Renderer
```

☑ Latent Timeout

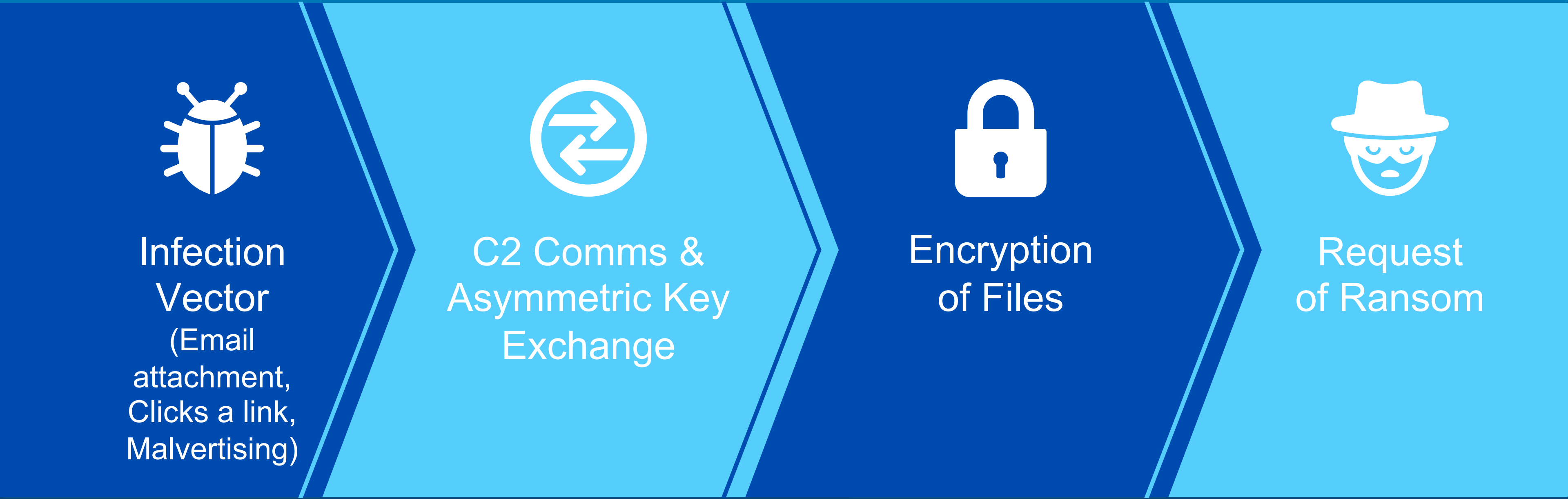
- Days: 0
- Hours: 0
- Minutes: 0

Download client.scr

Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.

isco and/or its affiliates. All rights reserved.

Typical Ransomware Infection



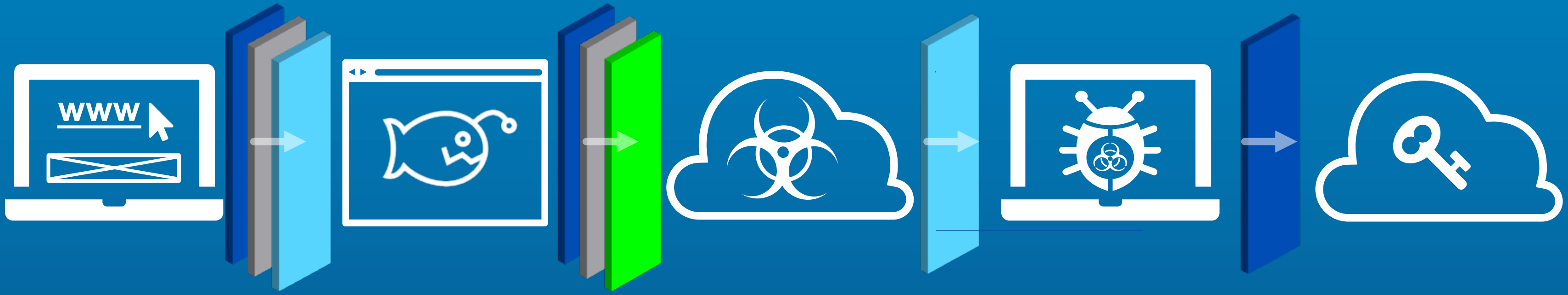
Infection Vector
(Email attachment, Clicks a link, Malvertising)

C2 Comms & Asymmetric Key Exchange

Encryption of Files

Request of Ransom

How Cisco Protects Customers



OpenDNS blocks the request

NGFW blocks the connection

Web Security w/AMP blocks the file

OpenDNS blocks the request

NGFW blocks the connection

Stealthwatch detects the activity

AMP for Endpoint blocks the file

OpenDNS blocks the request to Encryption Key Infrastructure

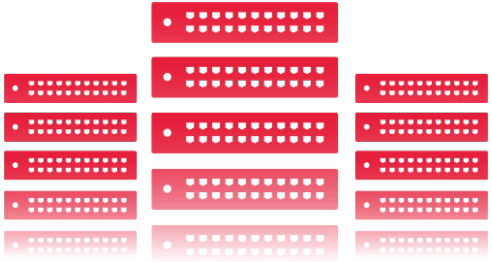
AMP for Endpoint quarantine the ransomware

● OpenDNS ● Next-Gen Firewall ● AMP ● Stealthwatch

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DNS: a Security perspective

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



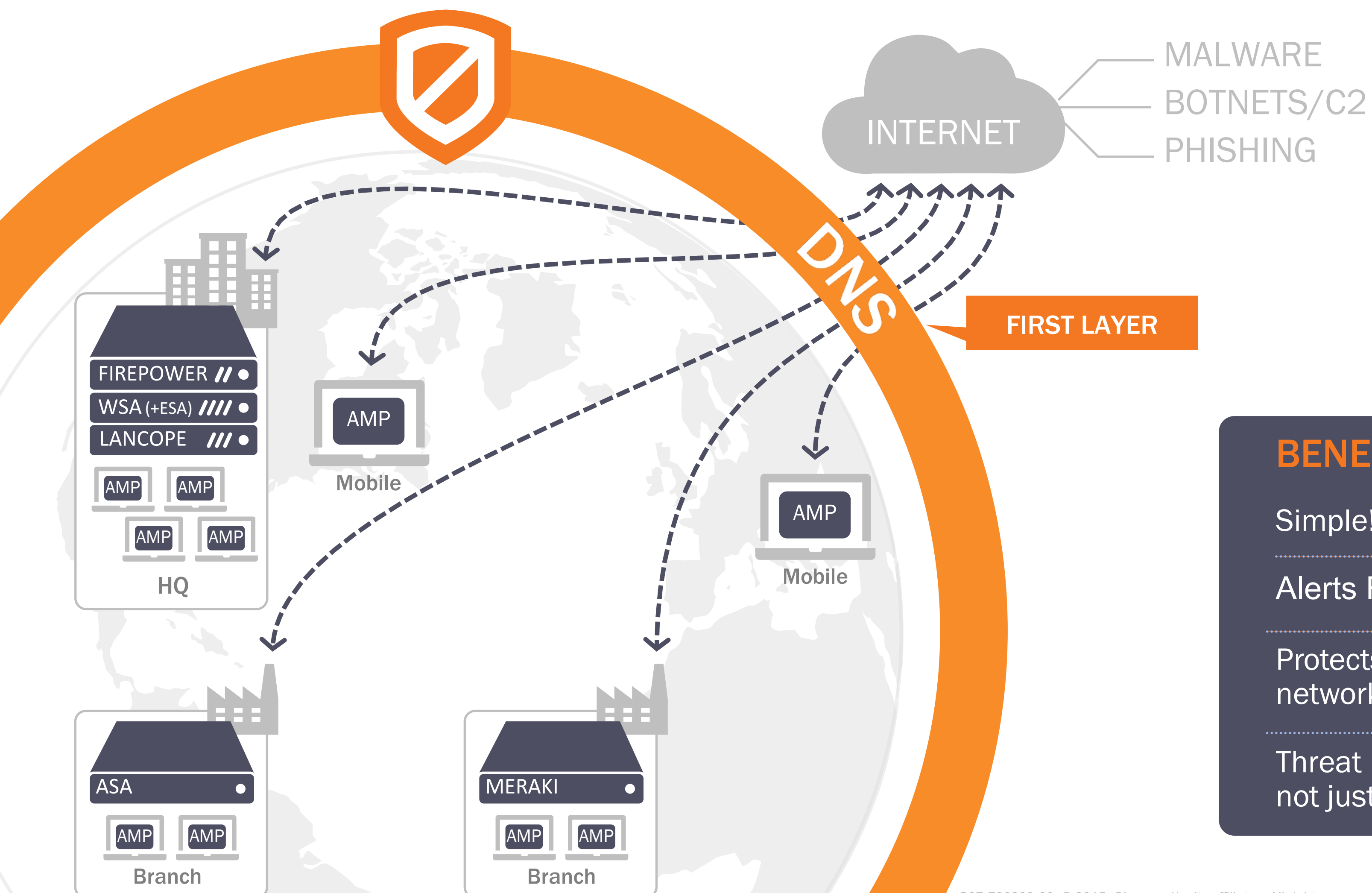
91.3%

of malware uses DNS

68%

of organizations
don't monitor it

Source: Cisco Annual Security Report, 2016



BENEFITS

- Simple!
- Alerts Reduced 2-10x
- Protects ON & OFF network
- Threat prevention, not just detection

OpenDNS Umbrella @ Rio Olympics

Umbrella deployed for entire Olympics 2 days before opening ceremony, in 2hrs

Total of 7 networks configured in Rio and Sao Paulo

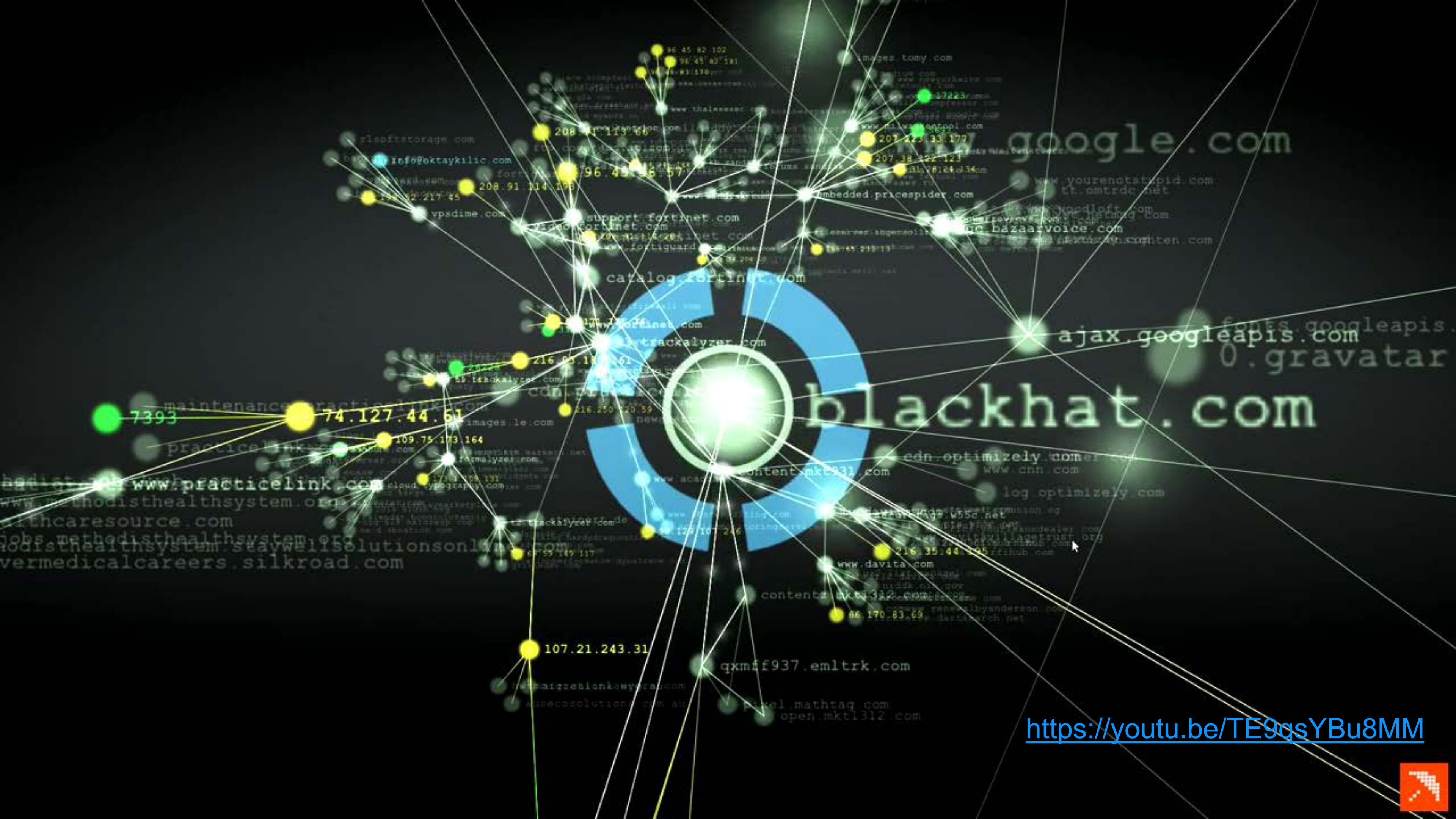
22M requests per day

Umbrella stopped 23,000 threats stopped each day

Reactive

Predictive

90B request/day, 65M active user, 160+ Countries

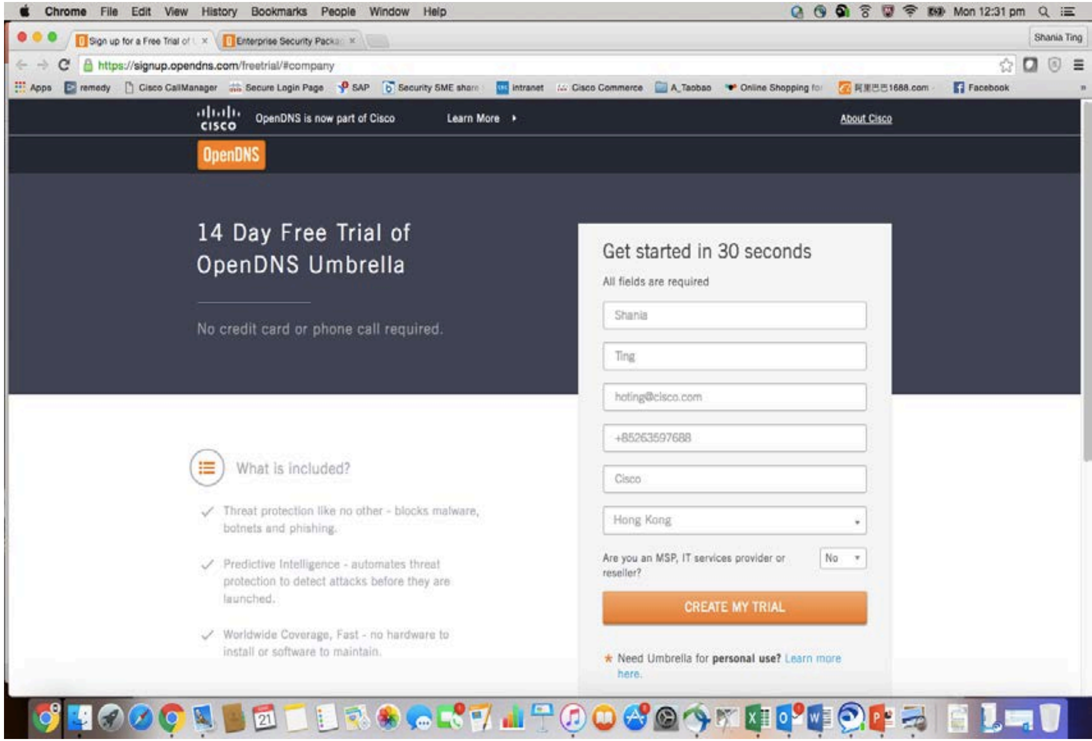


https://youtu.be/TE9qsYBu8MM

https://youtu.be/acwD_OA3QZ4

Start a Free Trial - OpenDNS Umbrella

- Worldwide Coverage, Fast, Simple to deploy with 100% uptime — no hardware to install or software to maintain
- Free to use up to 14 days
- Threat protection like no other - blocks malware, botnets and phishing
- Predictive Intelligence - automates threat protection to detect attacks before they are launched



14 Day Free Trial of OpenDNS Umbrella

No credit card or phone call required.

What is included?

✓ Threat protection like no other - blocks malware, botnets and phishing.

✓ Predictive Intelligence - automates threat protection to detect attacks before they are launched.

✓ Worldwide Coverage, Fast - no hardware to install or software to maintain.

Get started in 30 seconds

All fields are required

Shania

Ting

hoting@cisco.com

+85263597688

Cisco

Hong Kong

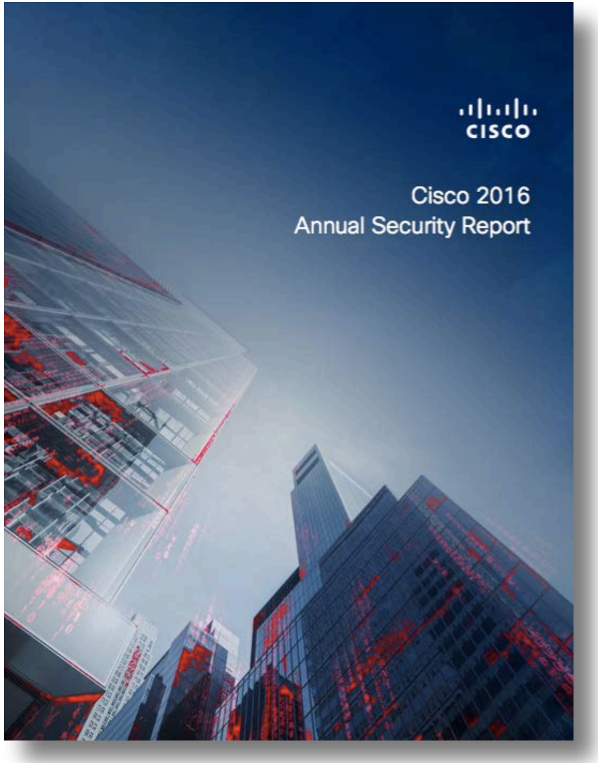
Are you an MSP, IT services provider or reseller? No

CREATE MY TRIAL

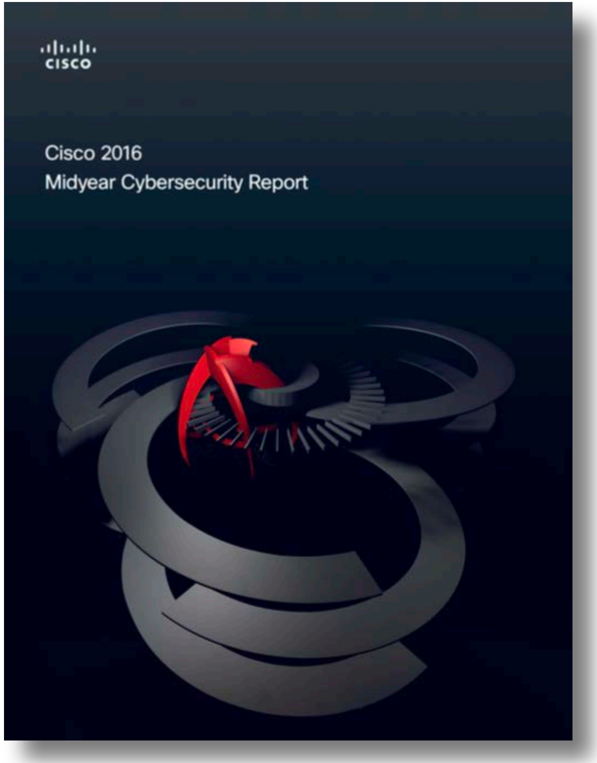
★ Need Umbrella for **personal use?** Learn more here.

- ***Personal use: Free***

Cisco 2016 Annual Security Report
Cisco 2016 Midyear Cybersecurity Report



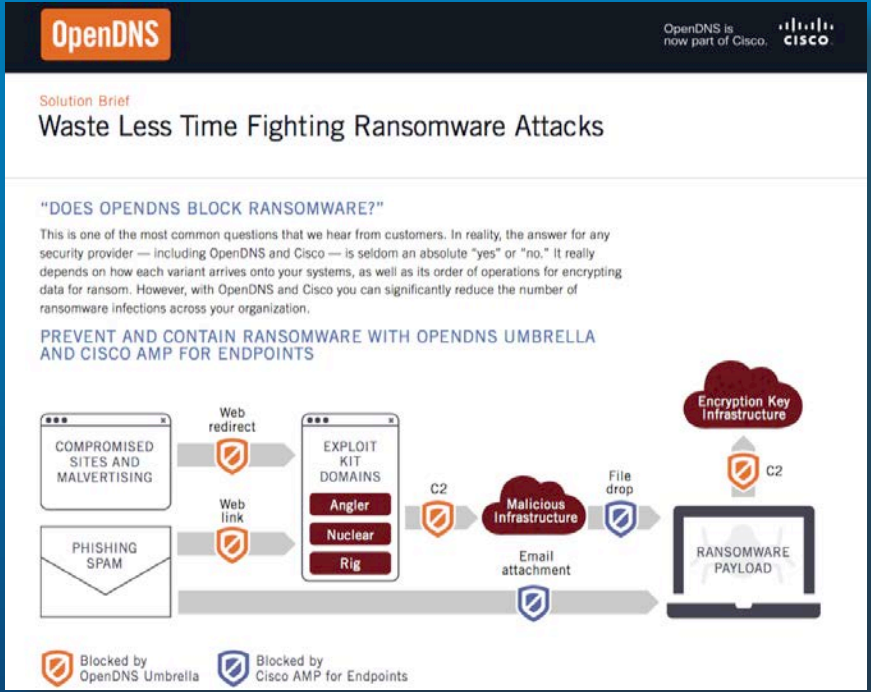
Cisco 2016
Annual Security Report



Cisco 2016
Midyear Cybersecurity Report

http://www.cisco.com/c/en/us/products/security/annual_security_report.html
http://blogs.cisco.com/author/talos

Ransomware



OpenDNS

OpenDNS is now part of Cisco. CISCO

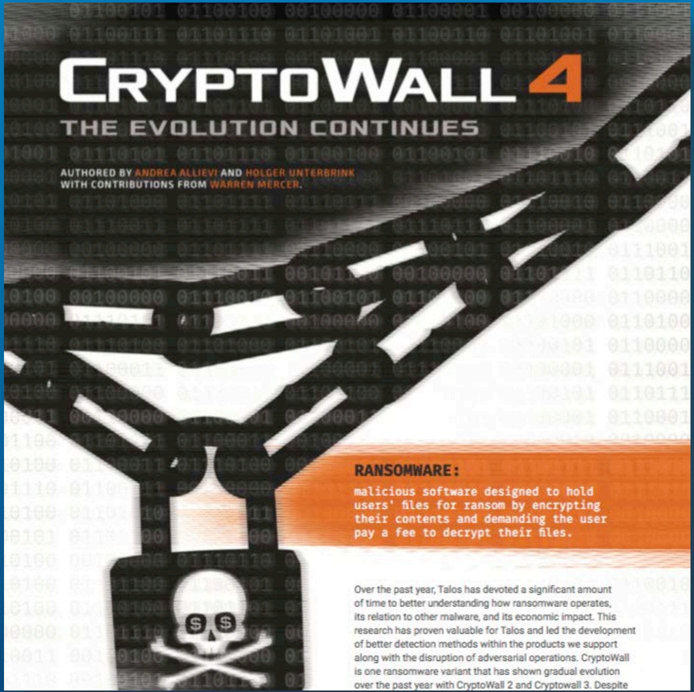
Solution Brief

Waste Less Time Fighting Ransomware Attacks

"DOES OPENDNS BLOCK RANSOMWARE?"

This is one of the most common questions that we hear from customers. In reality, the answer for any security provider — including OpenDNS and Cisco — is seldom an absolute "yes" or "no." It really depends on how each variant arrives onto your systems, as well as its order of operations for encrypting data for ransom. However, with OpenDNS and Cisco you can significantly reduce the number of ransomware infections across your organization.

PREVENT AND CONTAIN RANSOMWARE WITH OPENDNS UMBRELLA AND CISCO AMP FOR ENDPOINTS



CRYPTOWALL 4

THE EVOLUTION CONTINUES

AUTHORED BY ANDREA ALLIEVI AND HOLGER UNTERBRINK
WITH CONTRIBUTIONS FROM WARREN MERCER.

RANSOMWARE:
malicious software designed to hold users' files for ransom by encrypting their contents and demanding the user pay a fee to decrypt their files.

Over the past year, Talos has devoted a significant amount of time to better understanding how ransomware operates, its relation to other malware, and its economic impact. This research has proven valuable for Talos and led the development of better detection methods within the products we support along with the disruption of adversarial operations. CryptoWall is one ransomware variant that has shown gradual evolution over the past year with CryptoWall 2 and Cryptowall 3. Despite

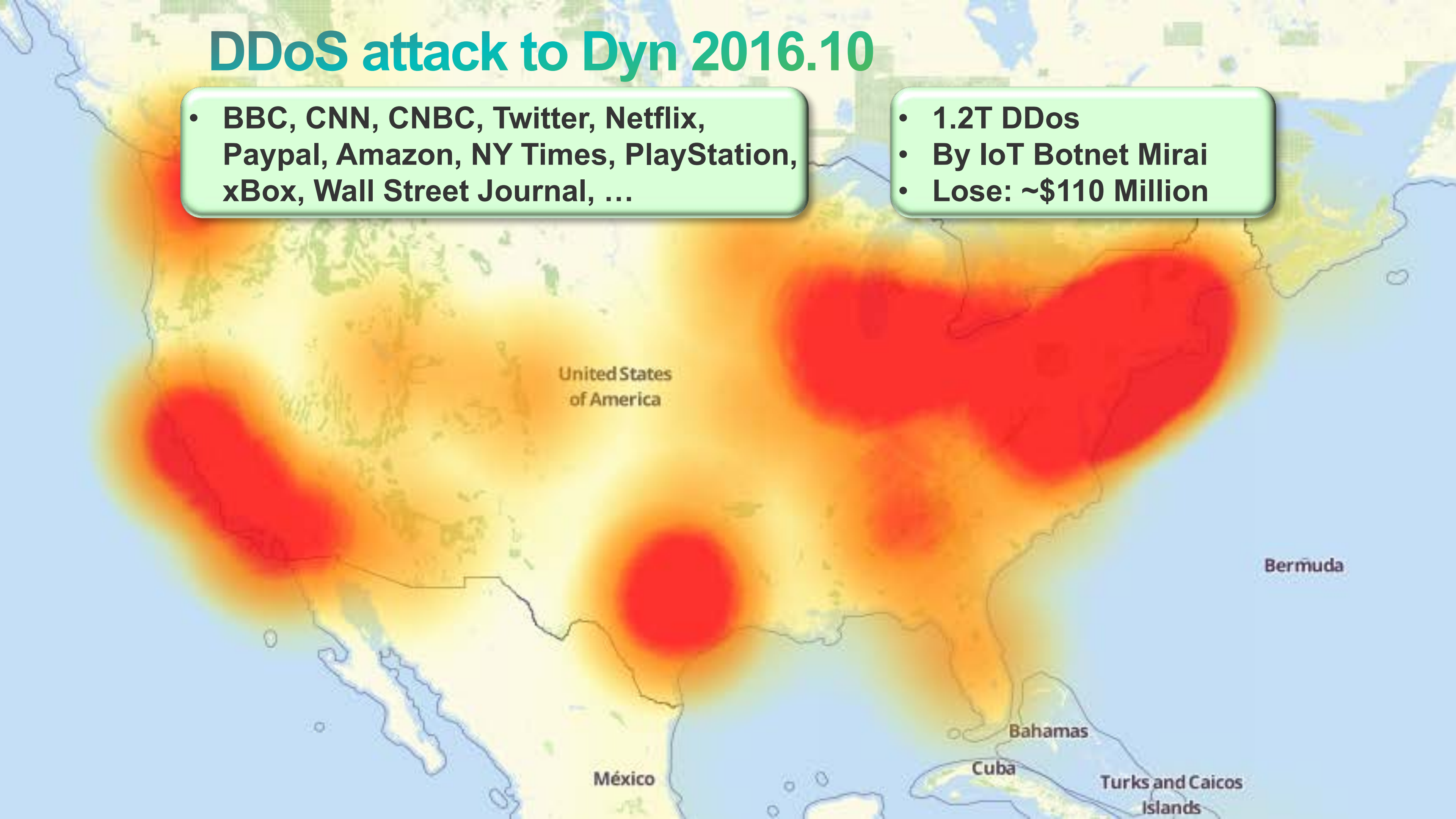
http://info.opendns.com/rs/033-OMP-861/images/SB-OpenDNS-Combating-Ransomware.pdf
http://www.talosintel.com/files/publications_and_presentations/papers/CryptoWall4_WhitePaper.042016.pdf

Case Study 2: Dyn DDoS Attack

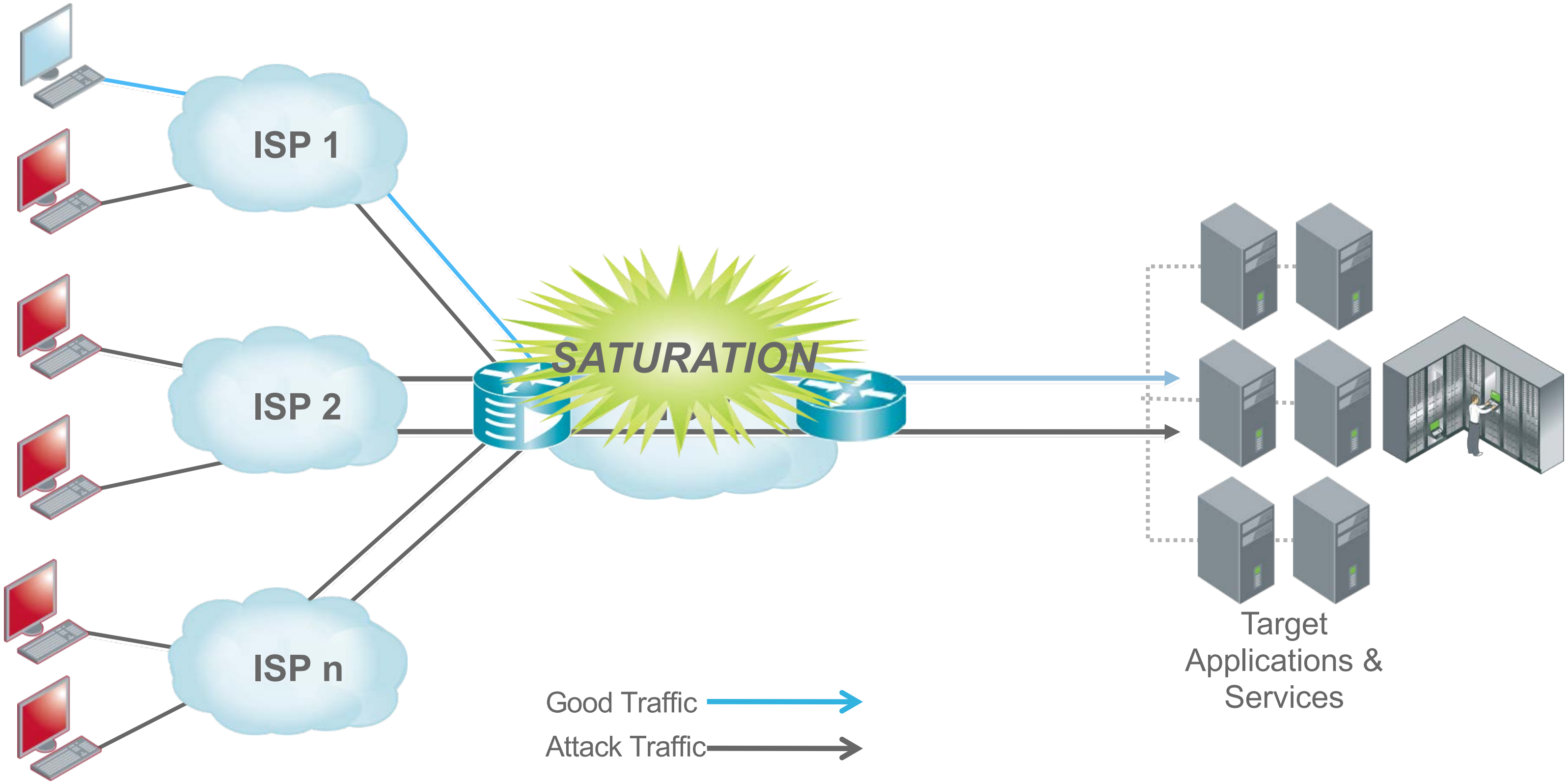
DDoS attack to Dyn 2016.10

- BBC, CNN, CNBC, Twitter, Netflix, Paypal, Amazon, NY Times, PlayStation, xBox, Wall Street Journal, …

- 1.2T DDos
- By IoT Botnet Mirai
- Lose: ~$110 Million



DDoS Attacks Overview

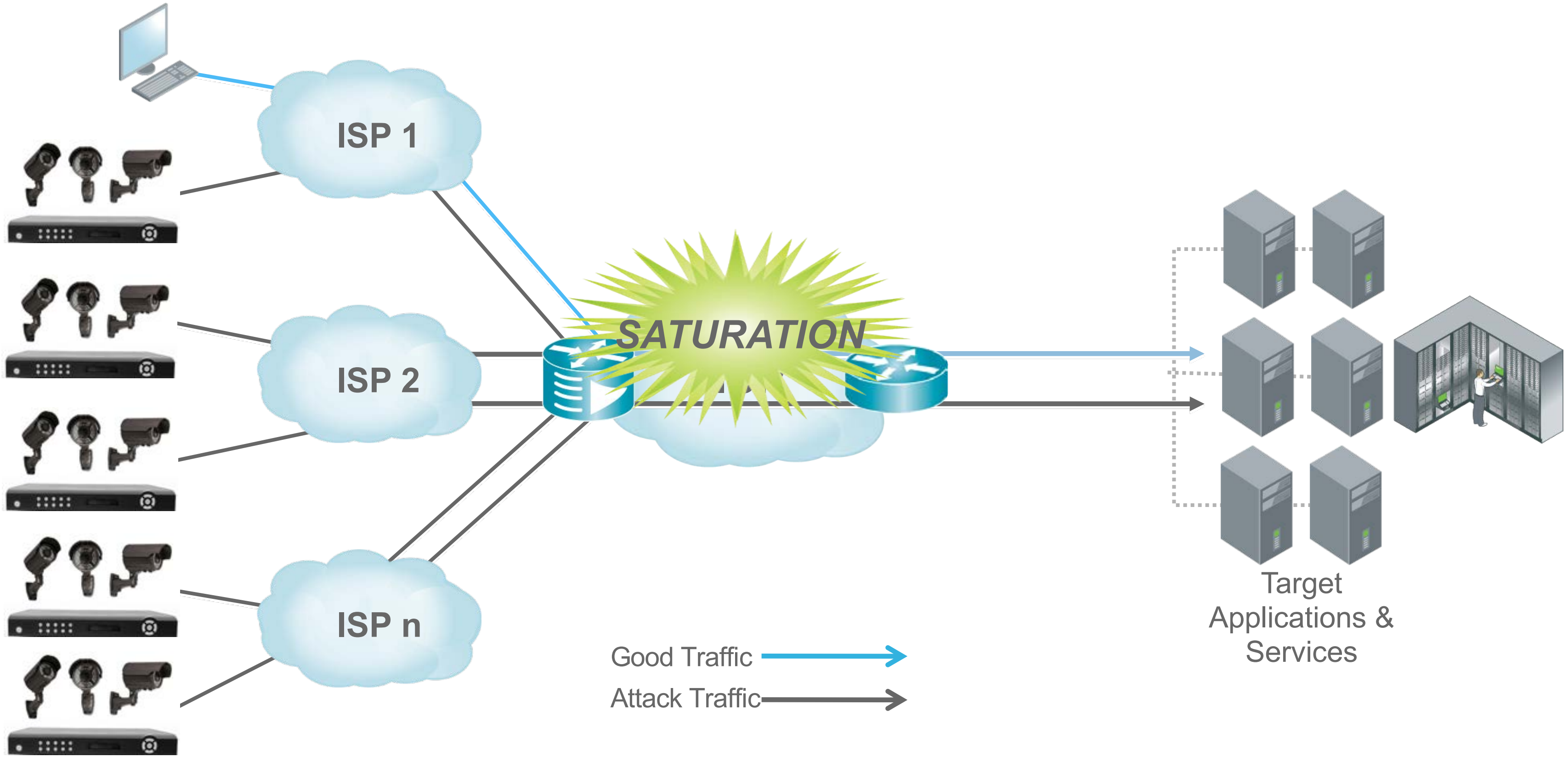


Good Traffic
Attack Traffic

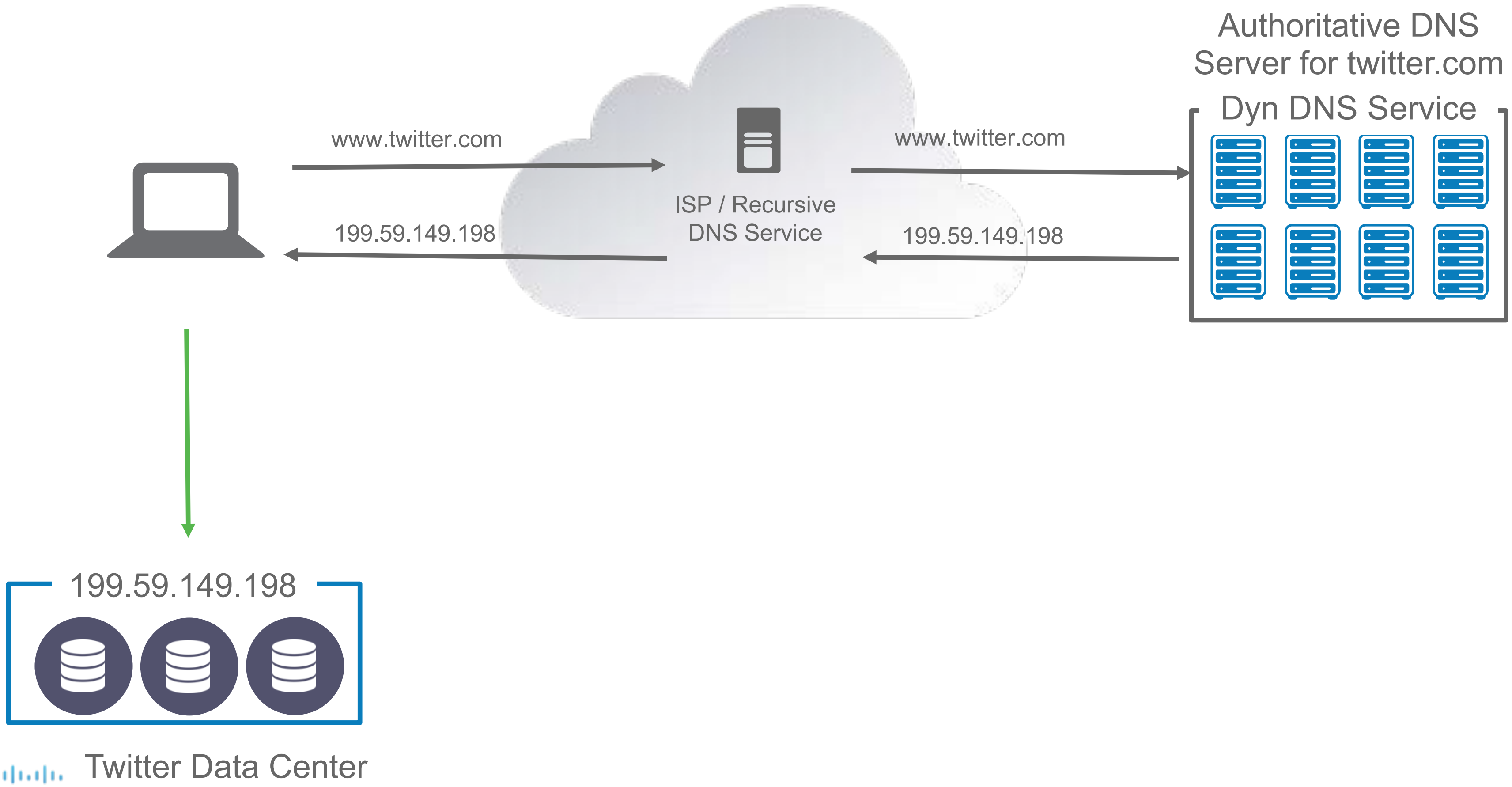
ミライミレニアム
irai ... nium

未來日記
えすのサカエ
1
Kadokawa Comics Ace Series

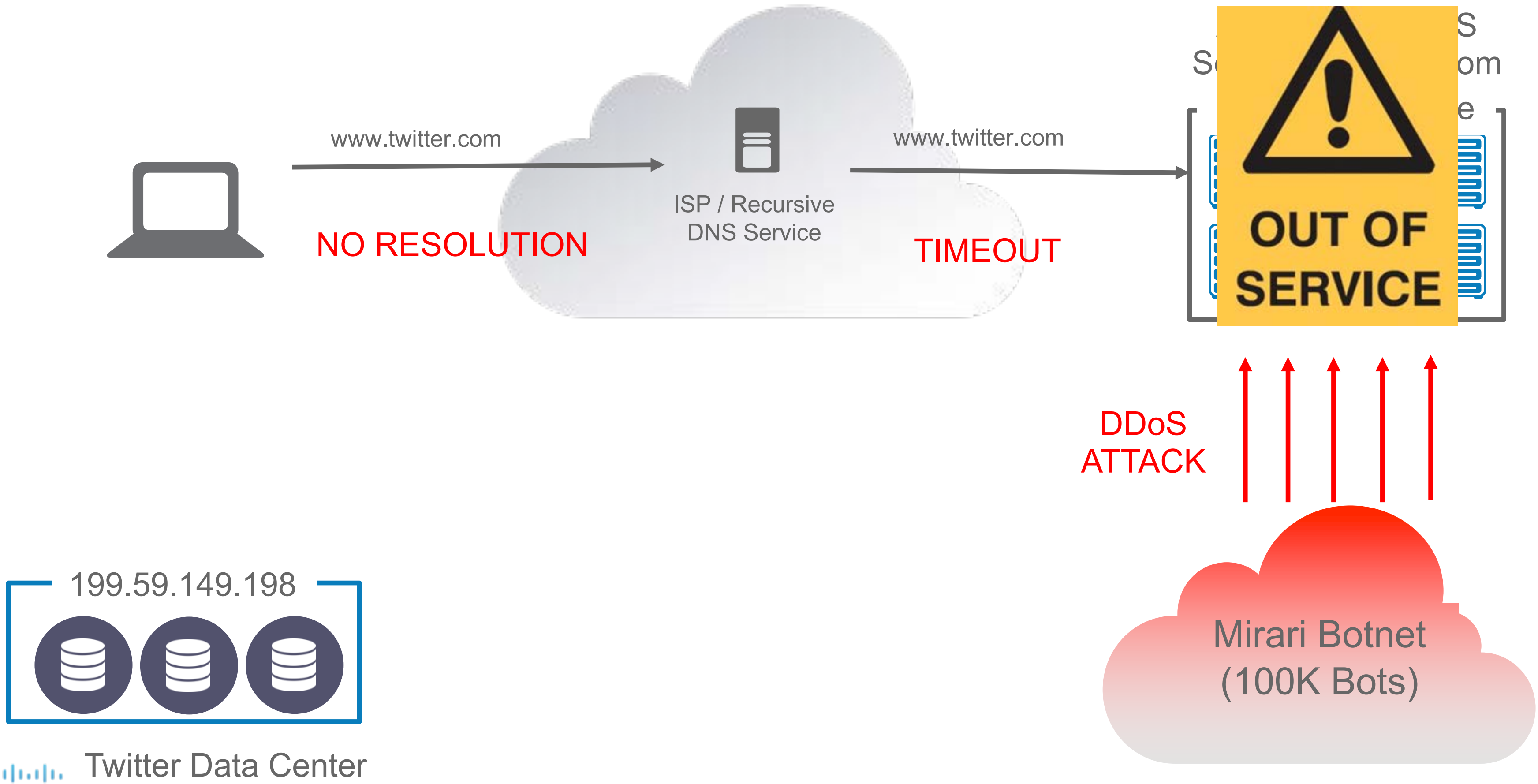
Dyn DDoS attack by Mirai Botnet

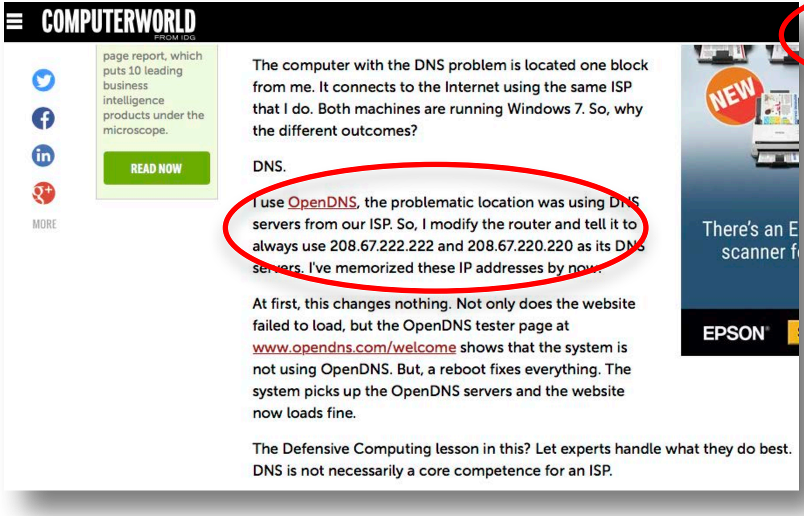


What Exactly Happened?



What Exactly Happened?




COMPUTERWORLD
FROM IDG
page report, which puts 10 leading business intelligence products under the microscope.
READ NOW
MORE
NEW
There's an E
scanner f
EPSON

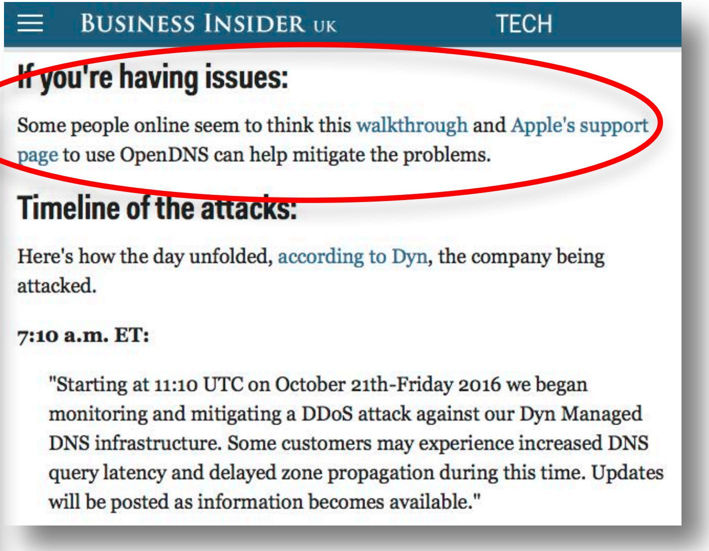
The computer with the DNS problem is located one block from me. It connects to the Internet using the same ISP that I do. Both machines are running Windows 7. So, why the different outcomes?

DNS.

I use OpenDNS, the problematic location was using DNS servers from our ISP. So, I modify the router and tell it to always use 208.67.222.222 and 208.67.220.220 as its DNS servers. I've memorized these IP addresses by now.

At first, this changes nothing. Not only does the website failed to load, but the OpenDNS tester page at www.opendns.com/welcome shows that the system is not using OpenDNS. But, a reboot fixes everything. The system picks up the OpenDNS servers and the website now loads fine.

The Defensive Computing lesson in this? Let experts handle what they do best. DNS is not necessarily a core competence for an ISP.



If you're having issues:

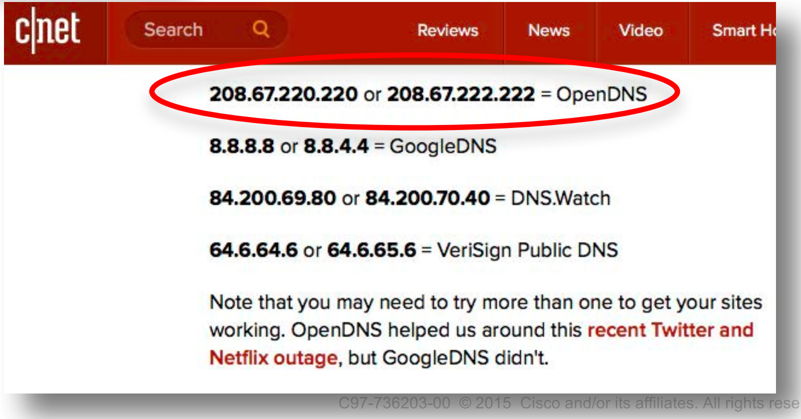
Some people online seem to think this walkthrough and Apple's support page to use OpenDNS can help mitigate the problems.

Timeline of the attacks:

Here's how the day unfolded, according to Dyn, the company being attacked.

7:10 a.m. ET:

> "Starting at 11:10 UTC on October 21th-Friday 2016 we began monitoring and mitigating a DDoS attack against our Dyn Managed DNS infrastructure. Some customers may experience increased DNS query latency and delayed zone propagation during this time. Updates will be posted as information becomes available."



208.67.220.220 or **208.67.222.222** = OpenDNS

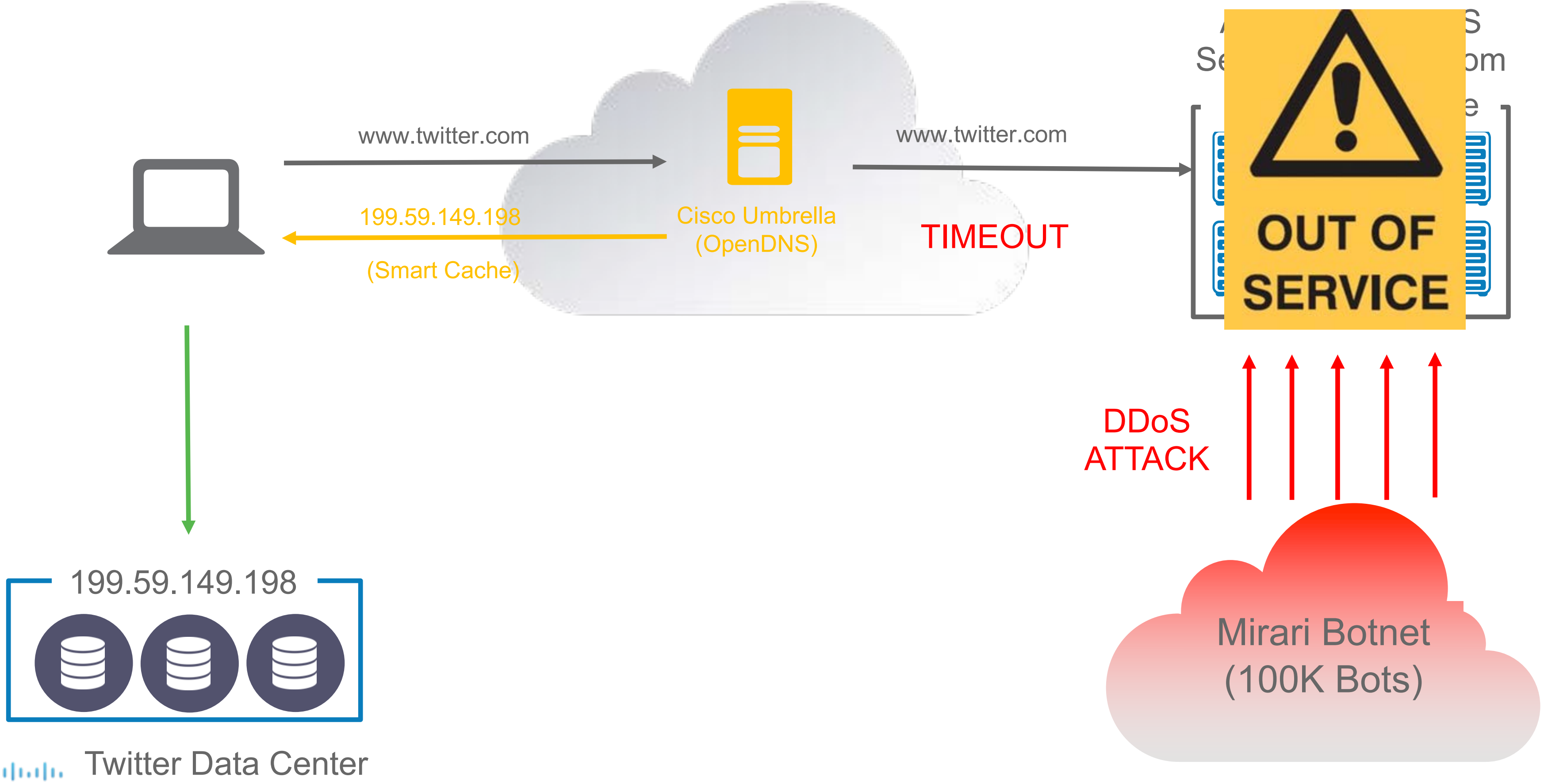
8.8.8.8 or **8.8.4.4** = GoogleDNS

84.200.69.80 or **84.200.70.40** = DNS.Watch

64.6.64.6 or **64.6.65.6** = VeriSign Public DNS

Note that you may need to try more than one to get your sites working. OpenDNS helped us around this recent Twitter and Netflix outage, but GoogleDNS didn't.

Why Cisco Umbrella Customers Were Unaffected

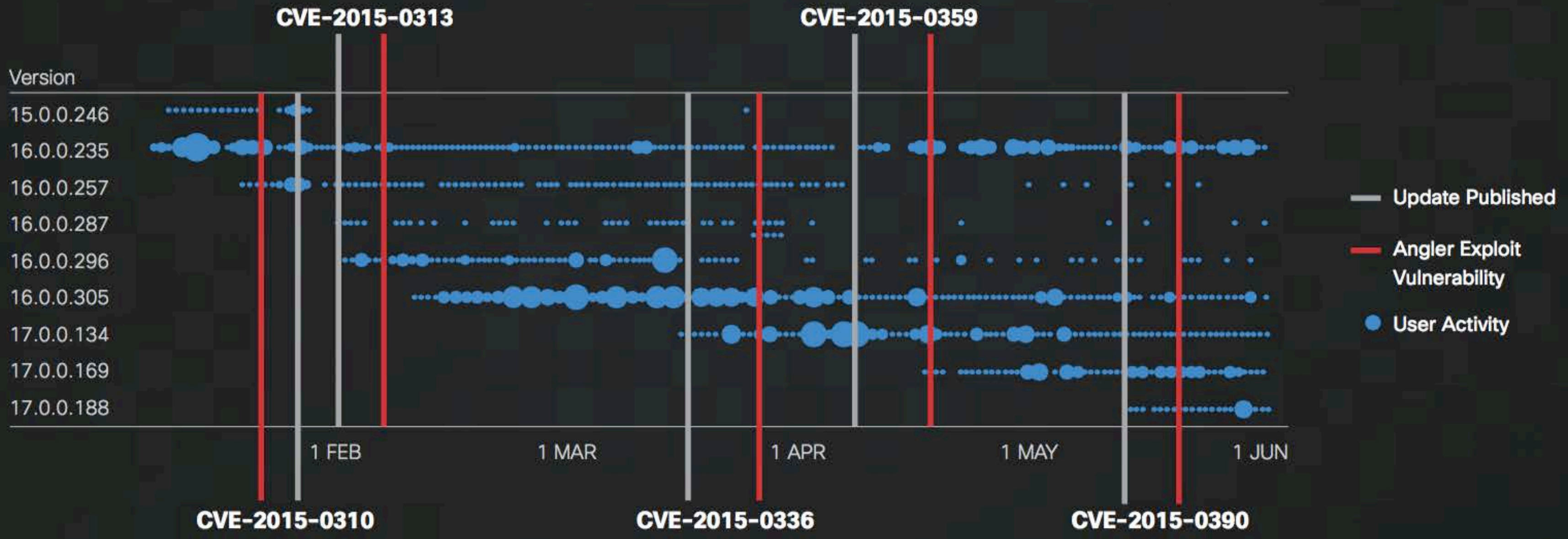


Best Practice

- Multi-layer defense to cover Attack Continuum (Before-During-After)
  - DNS, Email/Web gateway, NGFW/NGIPS/AMP, Endpoint AV/AMP protection
- Back up frequently (and keep away) !!!
- Patch your operating systems and other software (eg. Flash) ASAP!
- Keep your Anti-Virus/Anti-malware updated
- Educate users on emails with links and attachments
- Be careful of email attachment
- Disable macros in office documents and Script in browser
- Don’t stay logged in as administrator
- End of Support hardware and software?

Patching: A Window of Opportunity

Users not moving quickly to the latest Flash versions or updating the patches creates an opportunity for Angler and other exploits to target the vulnerability.



Shania Ting - Security Sales Manager: hoting@cisco.com
Tommy Mak - Security Consultant : tomak@cisco.com
Garrick Ng - Head of SE: garng@cisco.com

TALOS INTEL BREAKDOWN

THREAT INTEL

1.5 MILLION
Daily Malware Samples

600 BILLION
Daily Email Messages

16 BILLION
Daily Web Requests

Honeypots

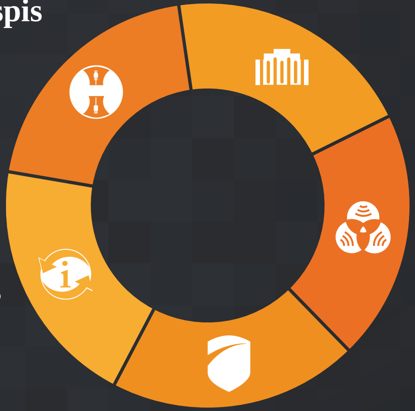
Open Source Communities

Vulnerability Discovery (Internal)

Telemetry

Internet-Wide Scanning

INTEL SHARING



Aspis

Crete

AEGIS

3rd Party Programs (MAPP)

ISACs

250+
Full Time Threat Intel Researchers

MILLIONS
Of Telemetry Agents

4
Global Data Centers

Over 100
Threat Intelligence Partners

1100
Threat Traps