



Seguridad Integrada

# Cisco Ransomware Defense

The Ransomware Threat Is Real

Abril 2018



# Ransomware



Malicious  
Software



Encrypts  
Critical Data



Demands  
Payment

# Business Impacts



**Permanent  
Data Loss**



**Operational  
Downtime**



**Reputation  
Damage**

# Did You Know?

---

**Over 99%**

of malware is sent by either  
web server or email



# Did You Know?

---

**Over 90%**

of known-bad malware use DNS to

- gain command and control
- exfiltrate data
- redirect traffic



# Ransomware and DNS

| NAME*         | Encryption Key |    |       |     | Payment MSG |
|---------------|----------------|----|-------|-----|-------------|
|               | DNS            | IP | NO C2 | 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         |

# Best Defenses

Wouldn't it be great if you could...



## Stop Ransomware

from using DNS or arriving by the web



## Stop Ransomware

from arriving by email



## Stop Ransomware

from running on endpoints

You Can

# Cisco Ransomware Defense

Quick Prevention



Cisco  
Umbrella



Cisco Cloud Email Security  
with Advanced  
Malware Protection



Cisco Advanced Malware  
Protection  
for Endpoints



# Break the Ransomware Chain



## Cisco Ransomware Defense



Stopped by Cisco Umbrella

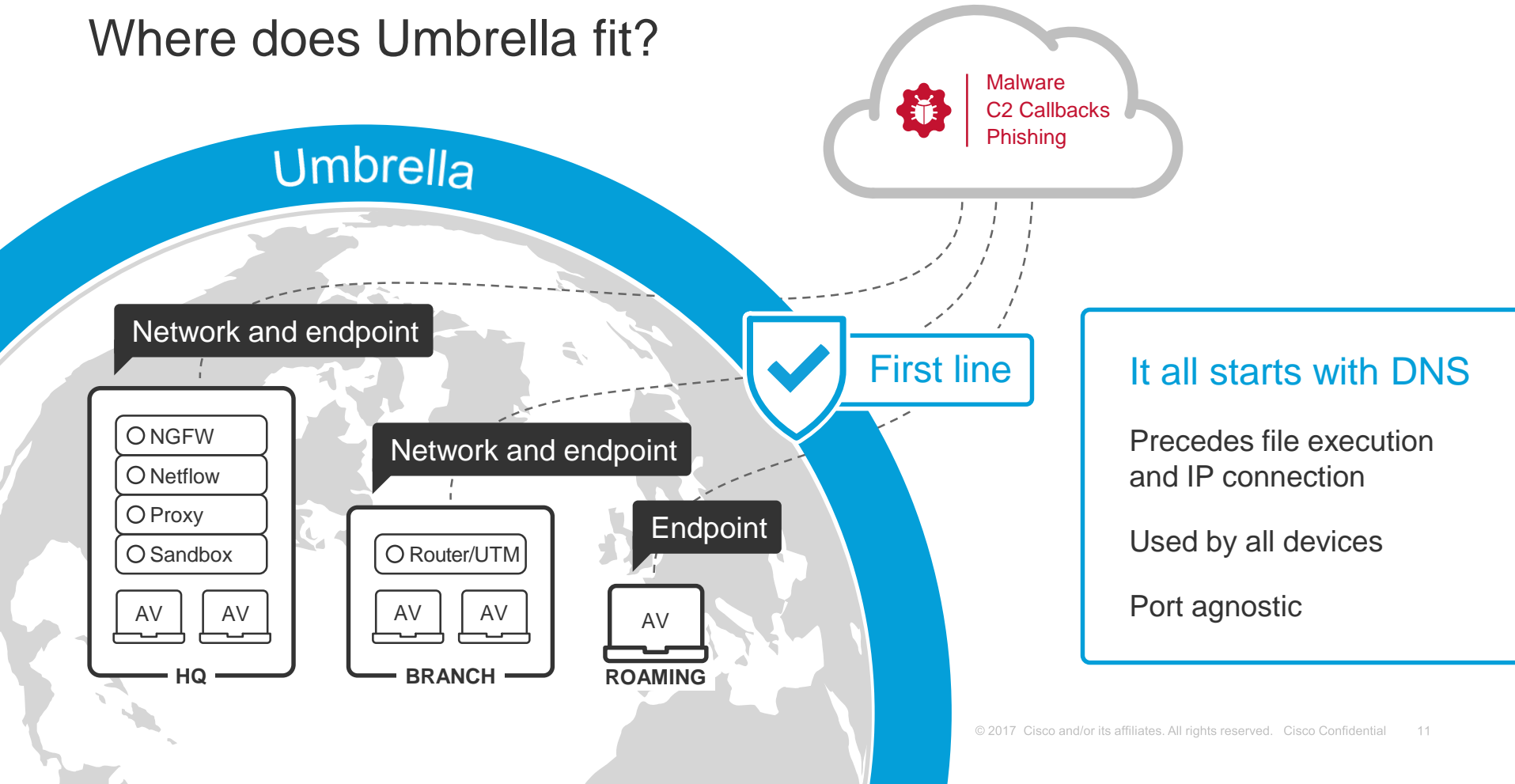


Stopped by Cisco Cloud Email Security with AMP



Stopped by Cisco AMP for Endpoints

# Where does Umbrella fit?



## ENFORCEMENT

# Built into foundation of internet

### Destinations

Original destination or block page



**Safe**  
Original destinations



**Blocked**  
Modified destination

### Security controls

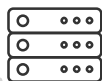
- DNS and IP enforcement
- Risky URL inspection through proxy
- SSL decryption available

**Intelligent proxy**  
Deeper inspection



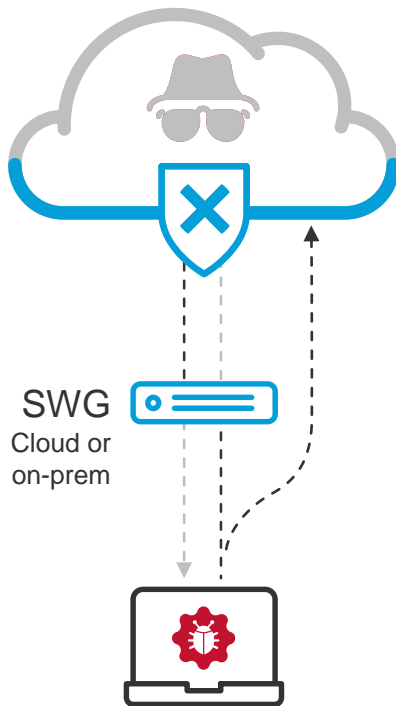
### Internet traffic

On- and off-network



# 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

# Threat Intelligence Sharing for Unified Defense

## Email Security

- Blocks spam, phishing, and malicious executables
- Shares intelligence with web and endpoint defenses

## Web Security

- Blocks access to malicious sites
- Inspects file downloads
- Stops ransomware command and control communications
- Shares intelligence with email and endpoint defenses



## Endpoint Security

- Inspects all executables and quarantines the malicious ones
- Shares intelligence with email and web security defenses

# Beyond Quick Prevention



## Visibility

See and control what's on  
your network



## Segmentation

Limit the lateral  
spread of ransomware



## Response Planning

Prepare now

# Cisco Ransomware Defense

Advanced Prevention

- Next Generation Firewall
- Next Generation IPS
- Web Security with AMP
- Stealthwatch
- Identity Services Engine
- TrustSec
- AMP Threat Grid



# Cisco Ransomware Defense

## Solution Summary

Prevent



Stop



Detect



Contain



Respond



Quick Prevention

Advanced Prevention





# Network Visibility & Segmentation

Deeper Dive

April 21, 2018

# Networks must handle unprecedented traffic



You have to handle  
large volumes of  
data

Annual global IP traffic will reach 2.3  
ZB per year by 2020\*



The number of users  
is growing

4.1B Global Internet users are  
expected by 2020\*



Users require flexible  
support

Connected workforce, cloud, IoT,  
M2M, and other types of users must  
be accommodated\*\*

# Gain endpoint visibility, and detect policy violations and compromised devices

## Network Visibility with Stealthwatch and ISE

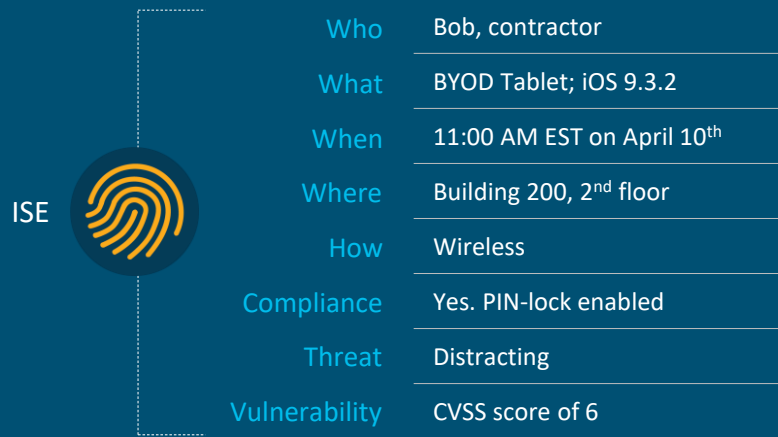
### Detect and correlate network telemetry

Establish a baseline for network behavior so you can uncover network use, misuse, and abuse



### See and share rich user details

Gain better visibility through richer contextual information, including increased visibility into threats and vulnerabilities



# Cisco Network Visibility & Segmentation



Visibility

“See Everything”

Stealthwatch & ISE



Segmentation

“Reduce the Attack Surface”

SD-Access



Threat protection

“Stop the Breach”

Rapid Threat Containment

