

# **RSA**Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: SPO3-T09

## **The Shift to a 24/7 Security Landscape: Why Cloud Security Is the Answer**



Connect **to**  
Protect

**David Ulevitch**

VP for Cisco's Security  
Business Group  
tweet @davidu  
email d@cisco.com



#RSAC

# Discussion Topics



- What's our state of security?
- Where do we enforce security?
- Can we get ahead of attacks?



OpenDNS is  
now part of Cisco.



A low-angle, upward-looking perspective of several modern skyscrapers with glass facades, creating a sense of height and scale. The buildings are arranged in a way that they seem to converge towards the top center of the frame. The sky is a clear, light blue.

# Are we secure?



OpenDNS is  
now part of Cisco



RSAConference2016



#RSAC



Detection



**Is our  
security  
posture  
effective?**



Remediation

**OpenDNS**

OpenDNS is  
now part of Cisco.



**RSA**Conference2016



# Can we predict attacks?

**OpenDNS**

OpenDNS is  
now part of Cisco.



**RSA**Conference2016

A person wearing a dark beanie and a dark jacket is seen from behind, looking out at a large, misty mountain range. A tall evergreen tree is on the left side of the frame. The scene is hazy and atmospheric.

# Not there yet.

**OpenDNS**

OpenDNS is  
now part of Cisco.



RSAConference2016



Last 20 years of security:  
**Got a problem?**  
**BUY A BOX**





SIEM



IDS



PERSISTENT THREATS



DLP



WEB SECURITY



EMAIL SECURITY



VPN



FIREWALL



# The OLD security stack...

**OpenDNS**

OpenDNS is  
now part of Cisco.





# Complexity is compromising us.

OpenDNS

OpenDNS is  
now part of Cisco



RSAConference2016

# We need simplicity



#RSAC

Google

Google Search

OpenDNS

OpenDNS is  
now part of Cisco.



RSA<sup>®</sup>Conference2016

# But simple isn't easy



#RSAC

Google



Google Search

OpenDNS

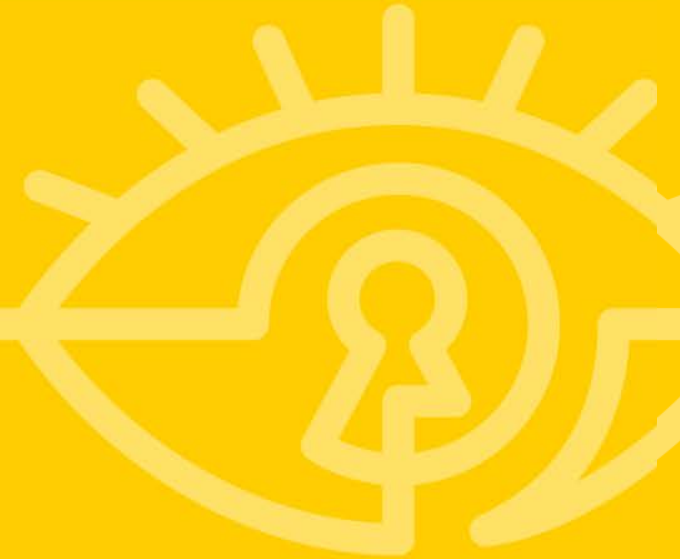
OpenDNS is  
now part of Cisco.



RSAConference2016



## **Where Do We Enforce Security?**

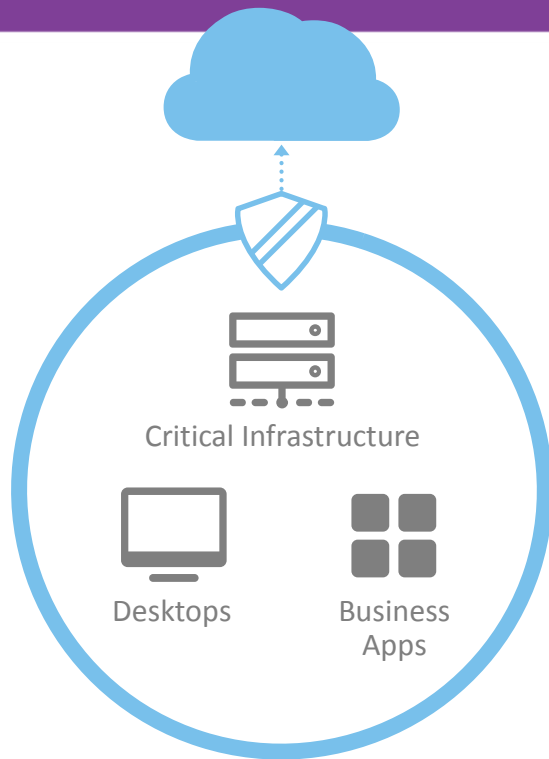




# The Shift from Old to New



#RSAC



**OpenDNS**

OpenDNS is  
now part of Cisco.

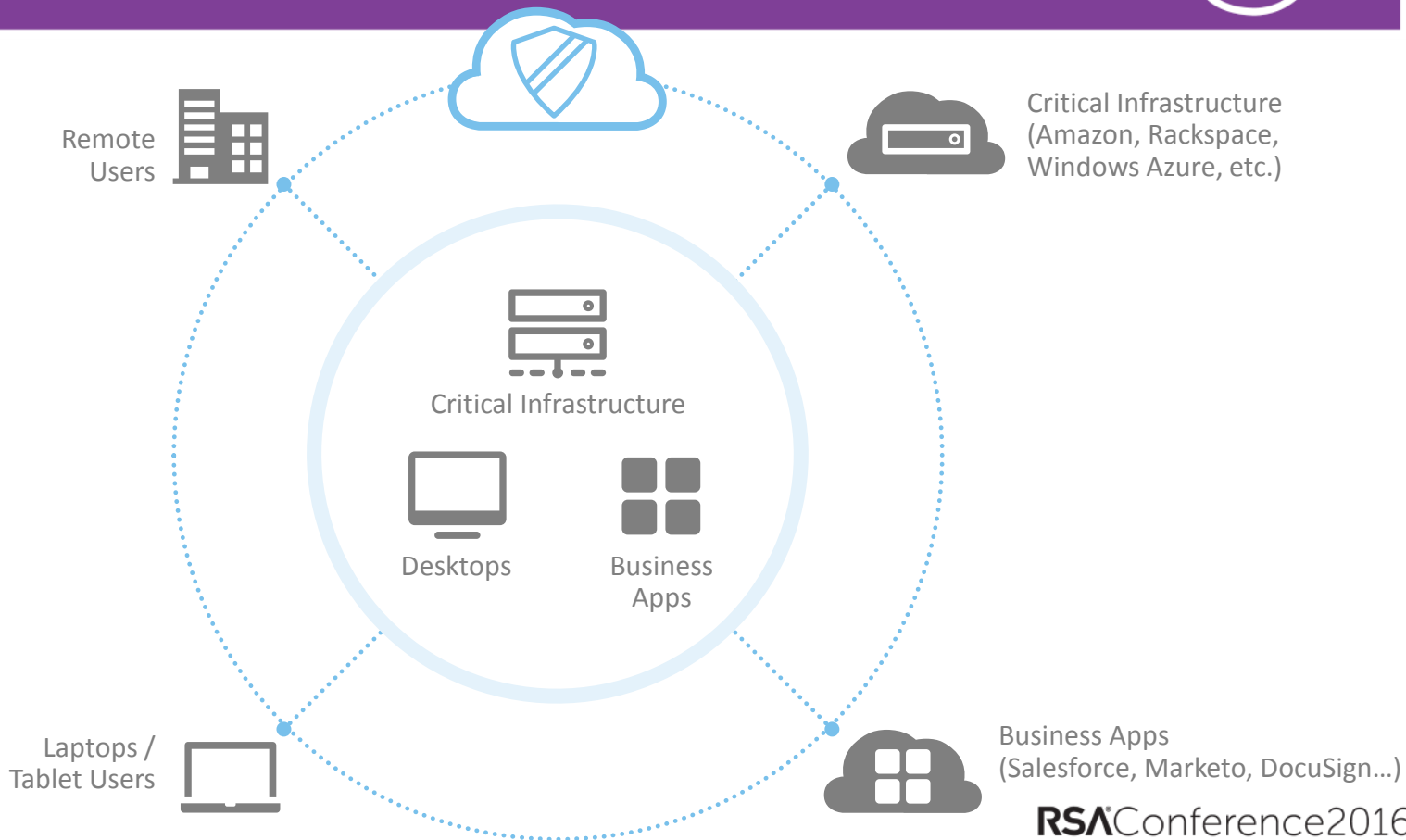


**RSA**Conference2016

# The Shift from Old to New



#RSAC



**OpenDNS**

OpenDNS is  
now part of Cisco.

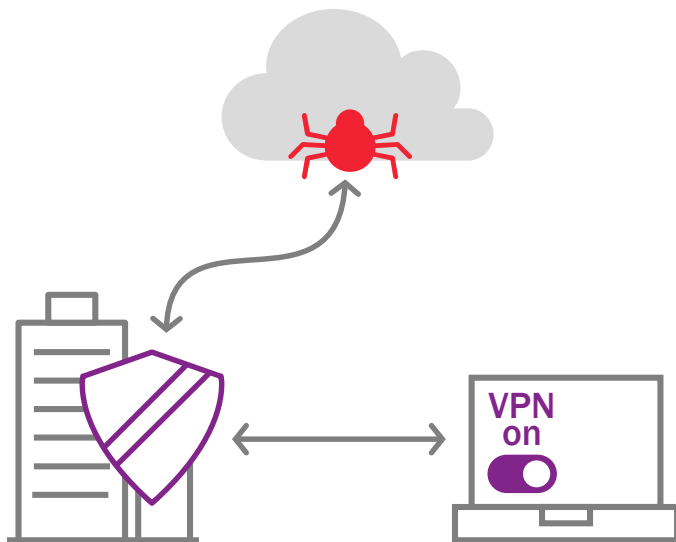


**RSA**Conference2016

# You Cannot Rely on the VPN



#RSAC



Last 20 years of  
off-network security:

## REMOTE ACCESS

OpenDNS

OpenDNS is  
now part of Cisco.

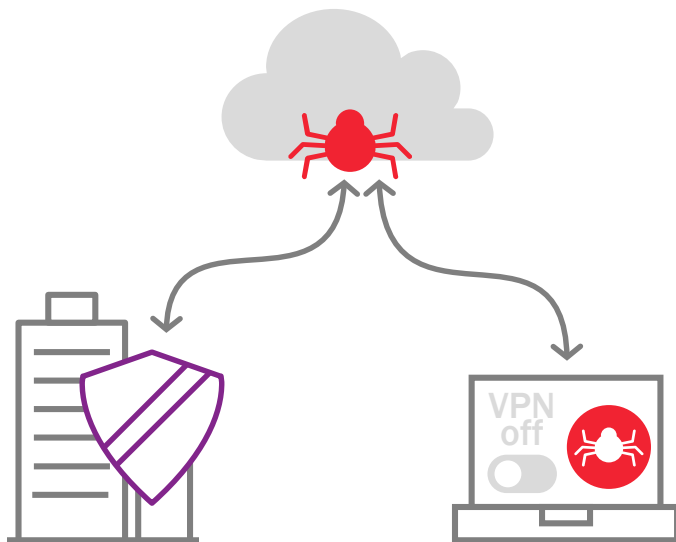


RSA Conference 2016

# You Need a New 24x7 Security Landscape



#RSAC



But the **VPN** is  
not on 24x7...

OpenDNS

OpenDNS is  
now part of Cisco.



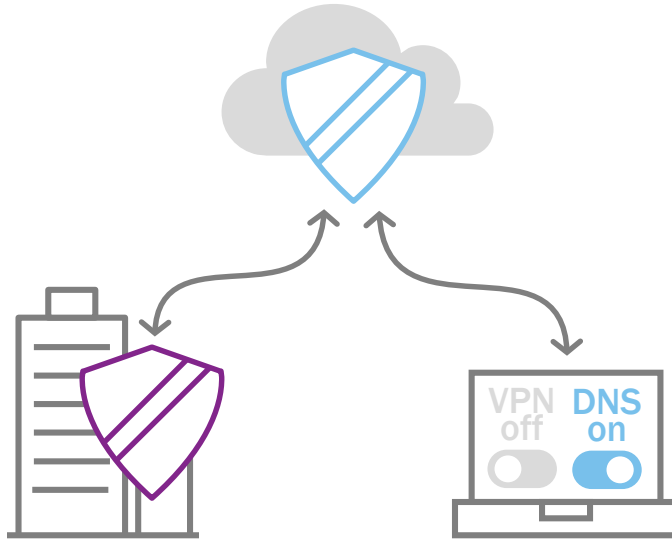
RSA<sup>®</sup>Conference2016



# You Need DNS-Layer Network Security



#RSAC



DNS is the  
Internet's  
control plane

OpenDNS

OpenDNS is  
now part of Cisco.



RSA<sup>®</sup>Conference2016

# DNS Works on Any Device, Anywhere



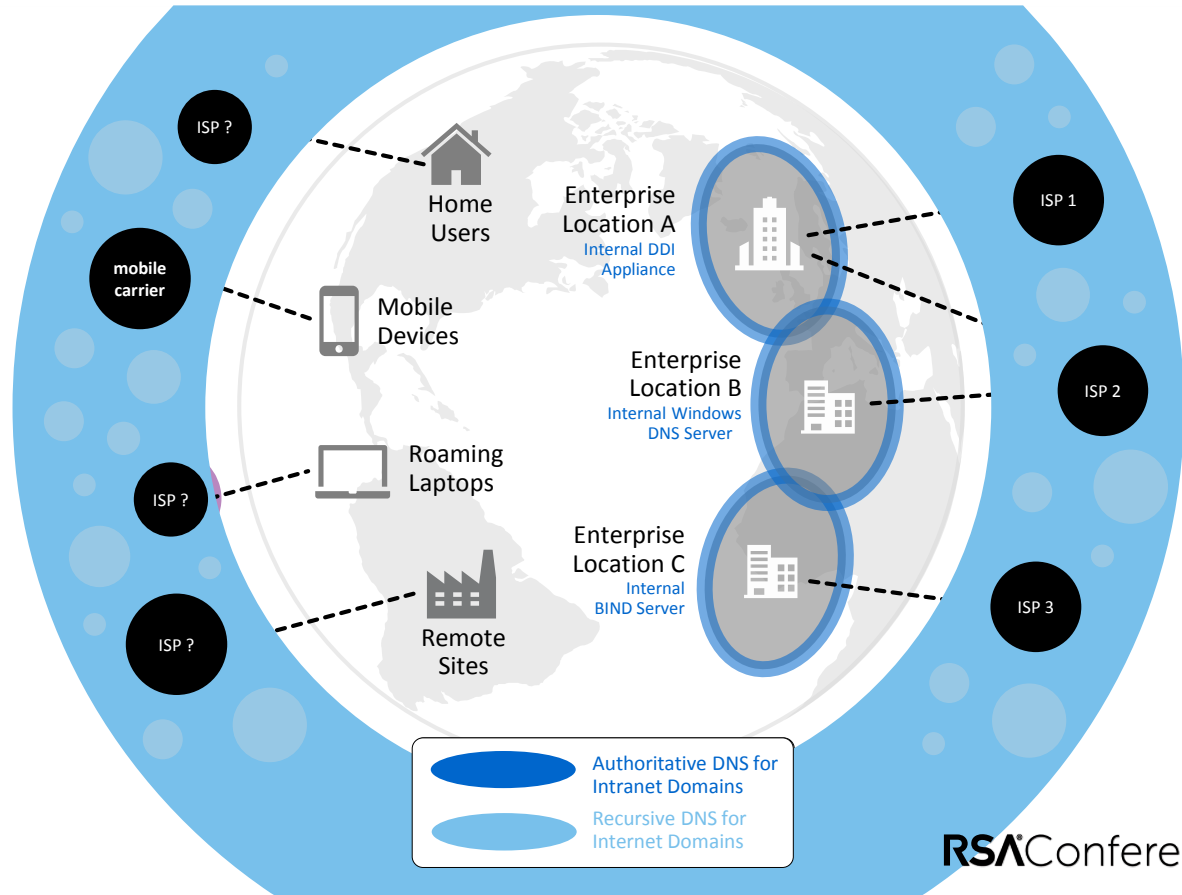
#RSAC

## BENEFITS

Global Internet  
Activity Visibility

Network Security  
w/o Adding Latency

Consistent Policy  
Enforcement



OpenDNS

OpenDNS is  
now part of Cisco.



RSA Conference 2016

# DNS Blocks Threats That Others Miss



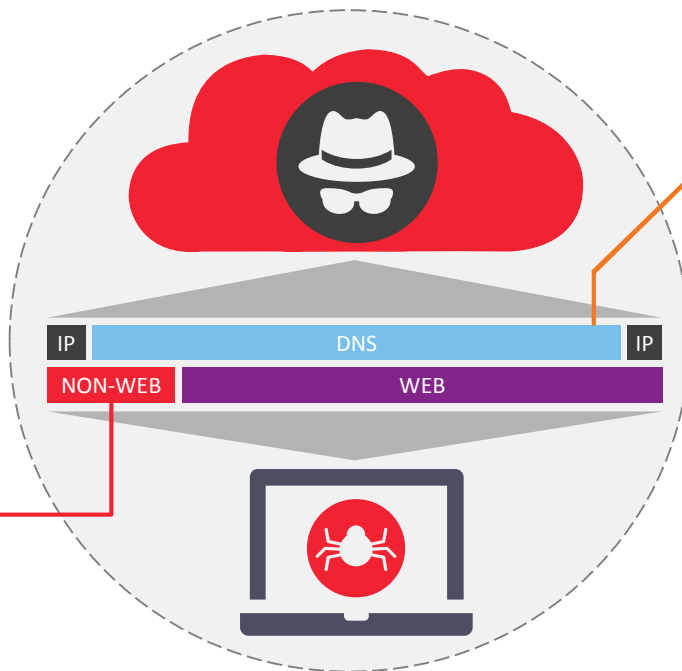
#RSAC

91%

of C2 can be blocked  
at the DNS layer

15%

of C2 bypasses  
Web ports 80 & 443



OpenDNS

OpenDNS is  
now part of Cisco.



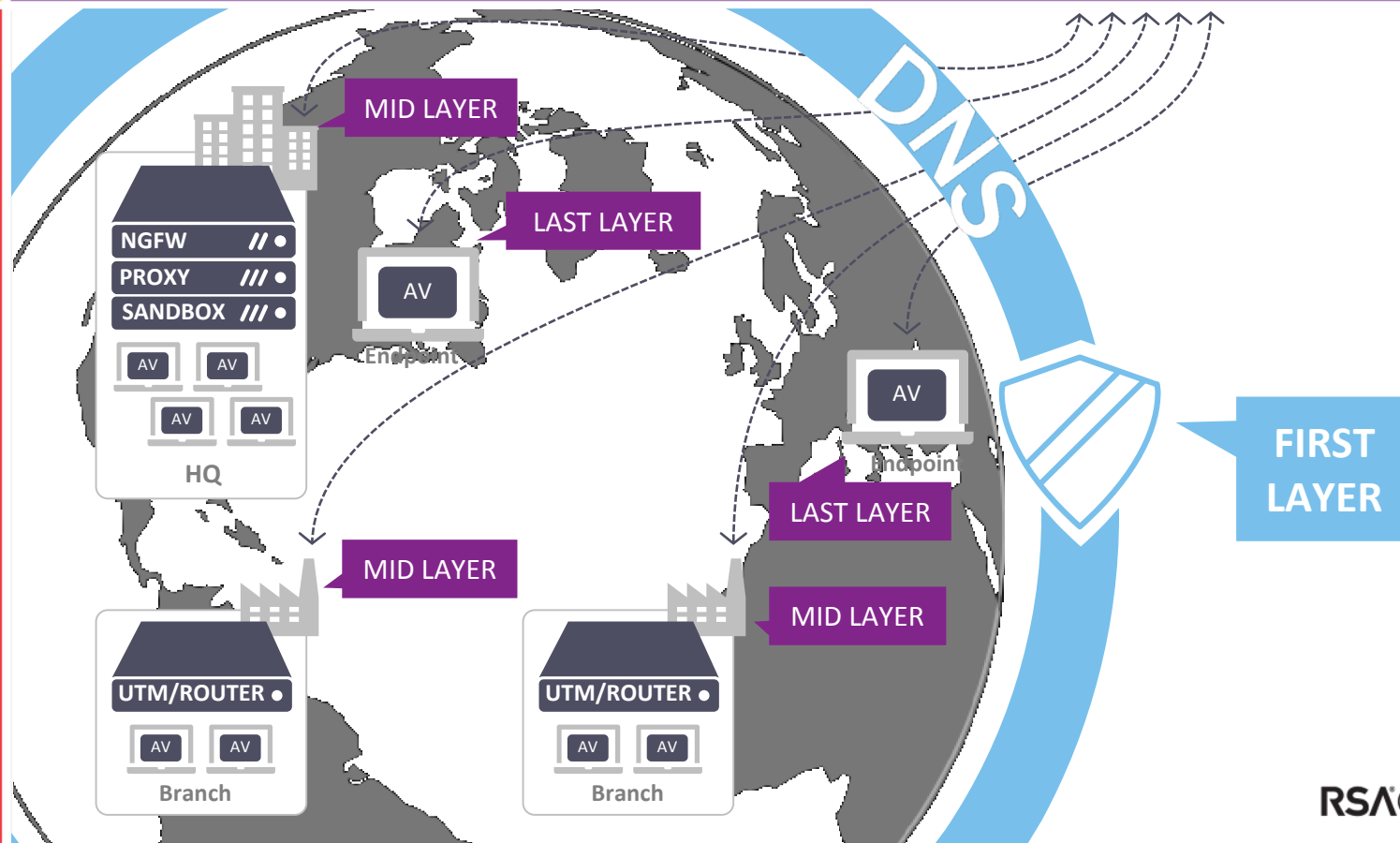
RSA Conference 2016

# DNS Blocks Threats Before They Reach You

MALWARE  
C2/BOTNETS  
PHISHING

INTERNET

#RSAC



## BENEFITS

Reduce alerts  
by 2-10x

Block malware  
before it hits  
the enterprise

Contain  
malware if  
already inside



# DNS is the Easiest and Fastest way to Establish a 24x7 Security Landscape



**OpenDNS**

OpenDNS is  
now part of Cisco



RSAConference2016



## **Can We Get Ahead of Attacks?**





Yes. But It Requires  
Internet-Wide Visibility.



OpenDNS is  
now part of Cisco.



RSAConference2016



# First, Gather a Significant Percentage of All Internet Activity in Real-Time



**OpenDNS**

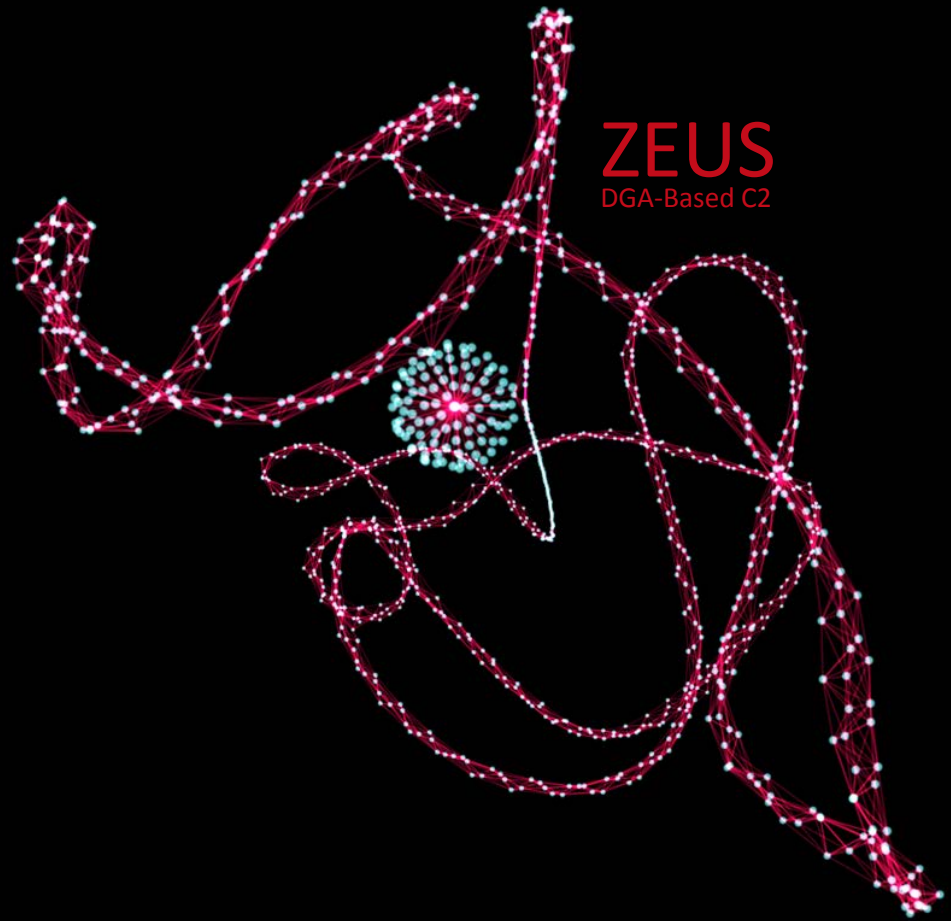
OpenDNS is  
now part of Cisco.



**RSA**Conference2016



# Second, Identify New Patterns by Applying Human Intelligence to Data Visualizations



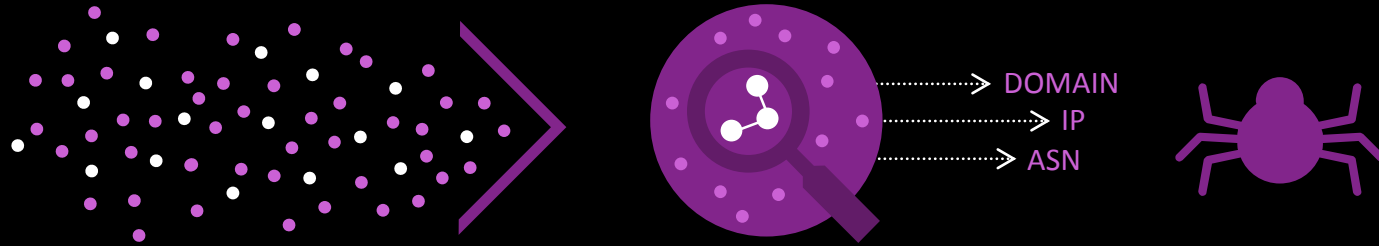
OpenDNS

OpenDNS is  
now part of Cisco.



RSAConference2016

# Third, Automatically Identify Where Attacks Are Staged by Applying Statistical Models to The Data



# Apply what you have learned today

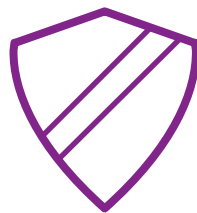


#RSAC



## VISIBILITY

see all the traffic



## ENFORCEMENT

24x7 security landscape



## MANAGEABILITY

consistently adapt

OpenDNS

OpenDNS is  
now part of Cisco.



RSA<sup>®</sup>Conference2016

# Apply what you have learned today



## ■ Next week...

- start gathering your DNS logs for visibility
- evaluate how often laptops connect off-network

## ■ Next month...

- find a non-VPN/proxy solution to extend network security beyond the perimeter

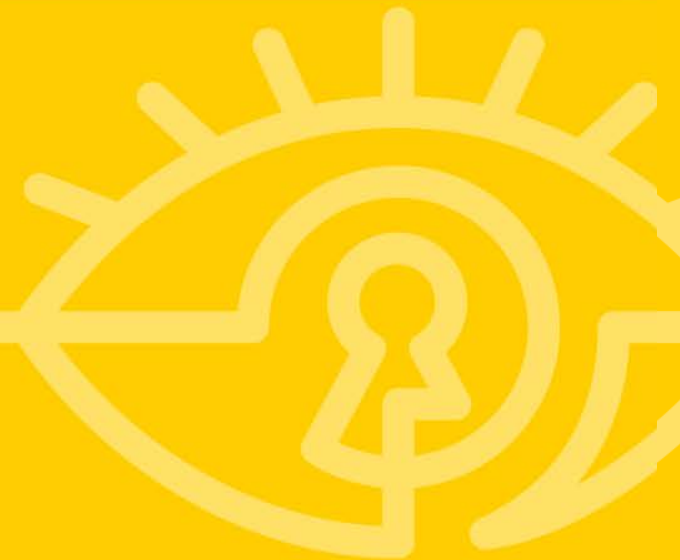
## ■ Next quarter...

- start analyzing your DNS logs for threat intelligence



OpenDNS is  
now part of Cisco.





## Thank You

David Ulevitch  
tweet @davidu  
email d@cisco.com