RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO3-T09

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

David Ulevitch

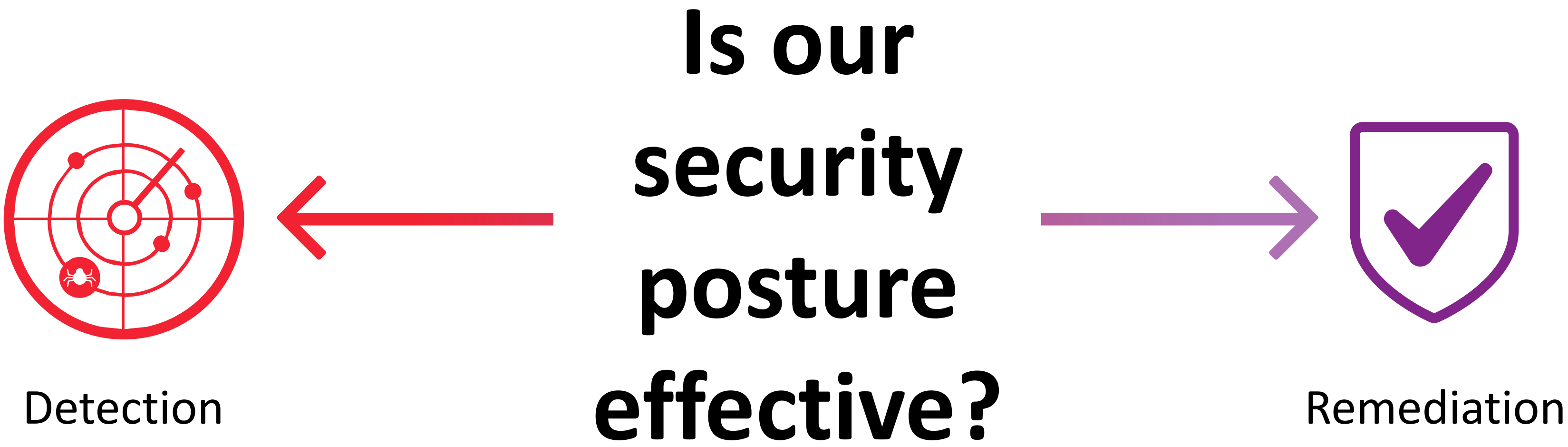
VP for Cisco's Security
Business Group
tweet @davidu
email d@cisco.com

#RSAC

Discussion Topics

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

Are we secure?



Is our security posture effective?

Detection

Remediation

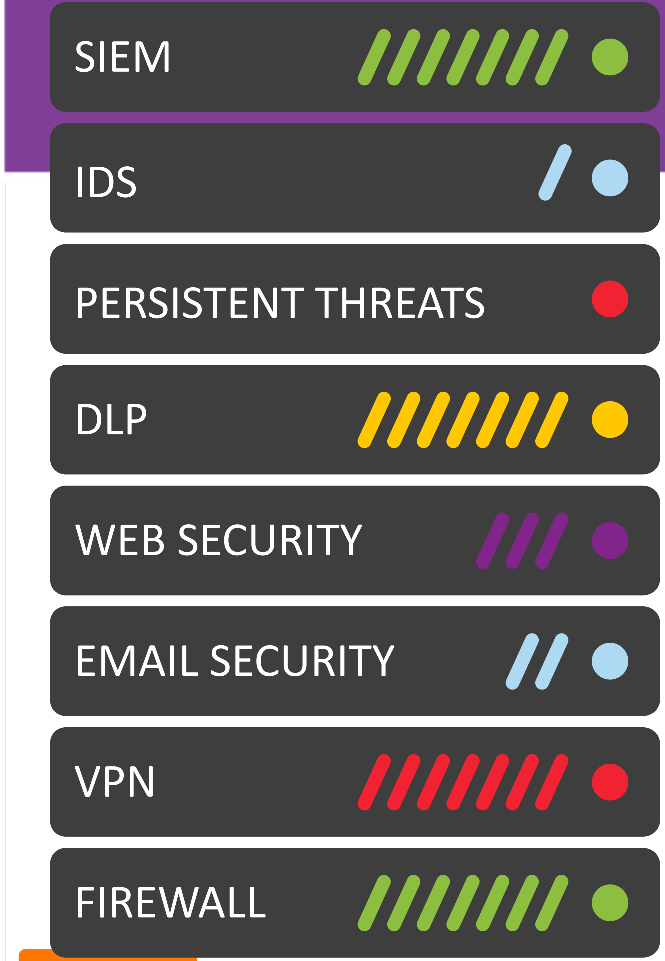
Can we predict attacks?

Not there yet.

Last 20 years of security:

Got a problem?

BUY A BOX



SIEM

IDS

PERSISTENT THREATS

DLP

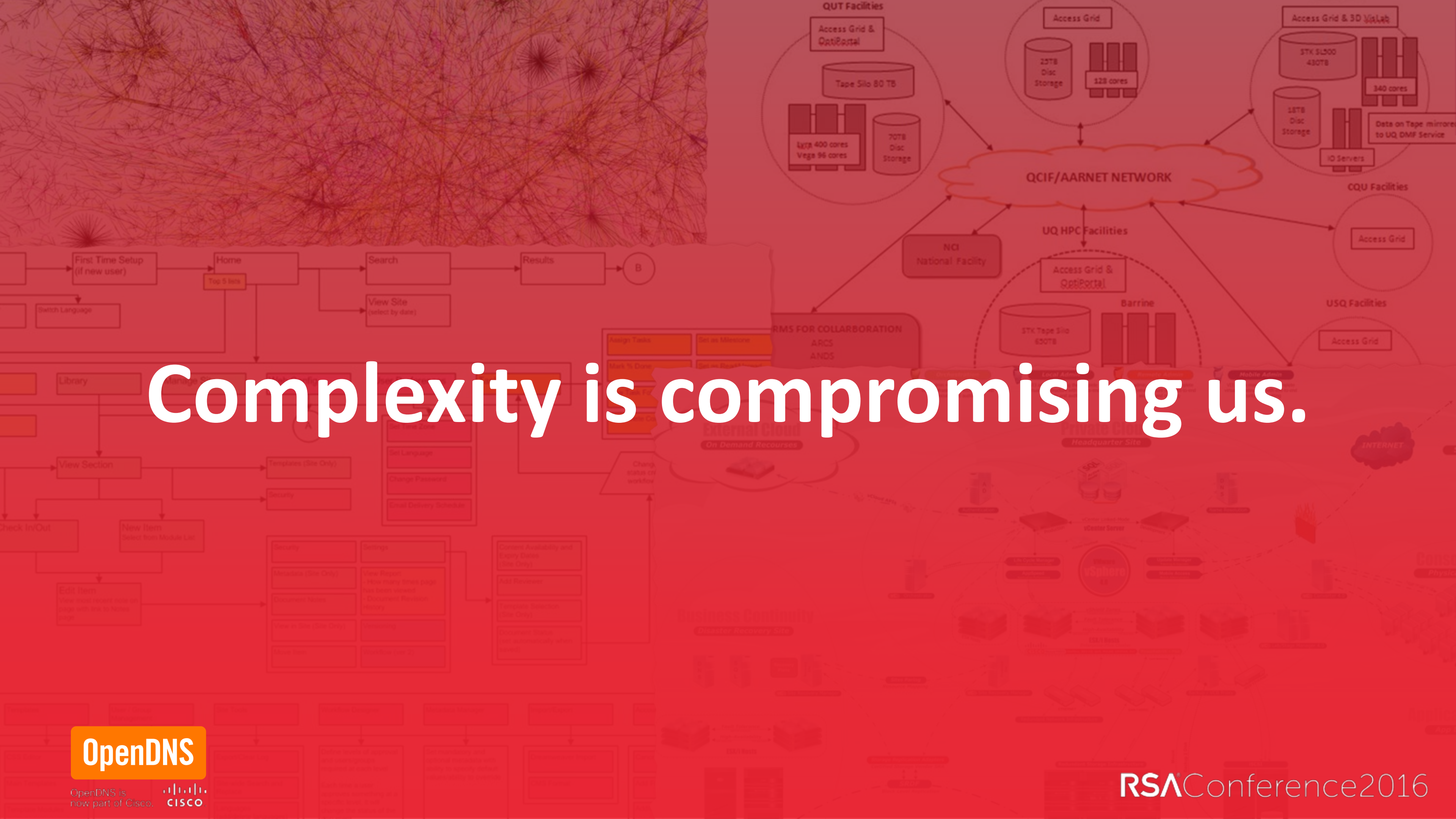
WEB SECURITY

EMAIL SECURITY

VPN

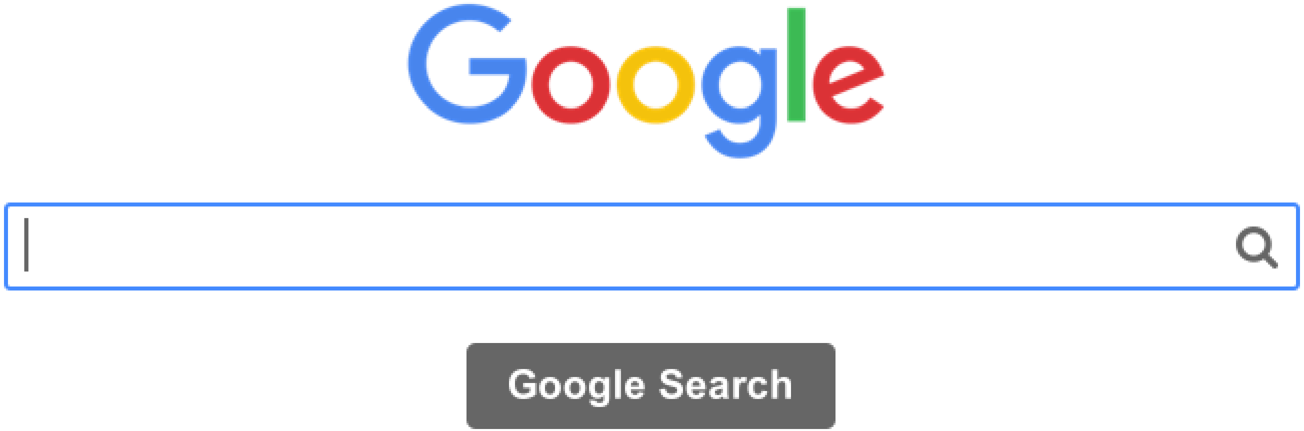
FIREWALL

The OLD security stack...



Complexity is compromising us.

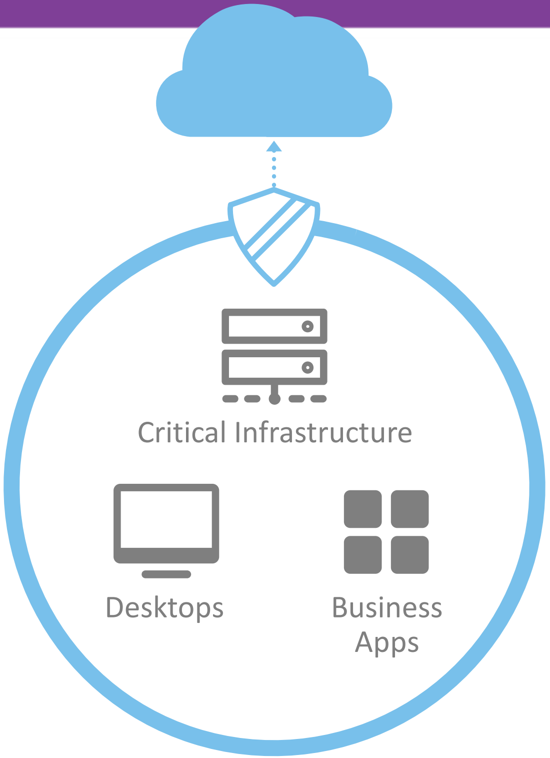
We need simplicity



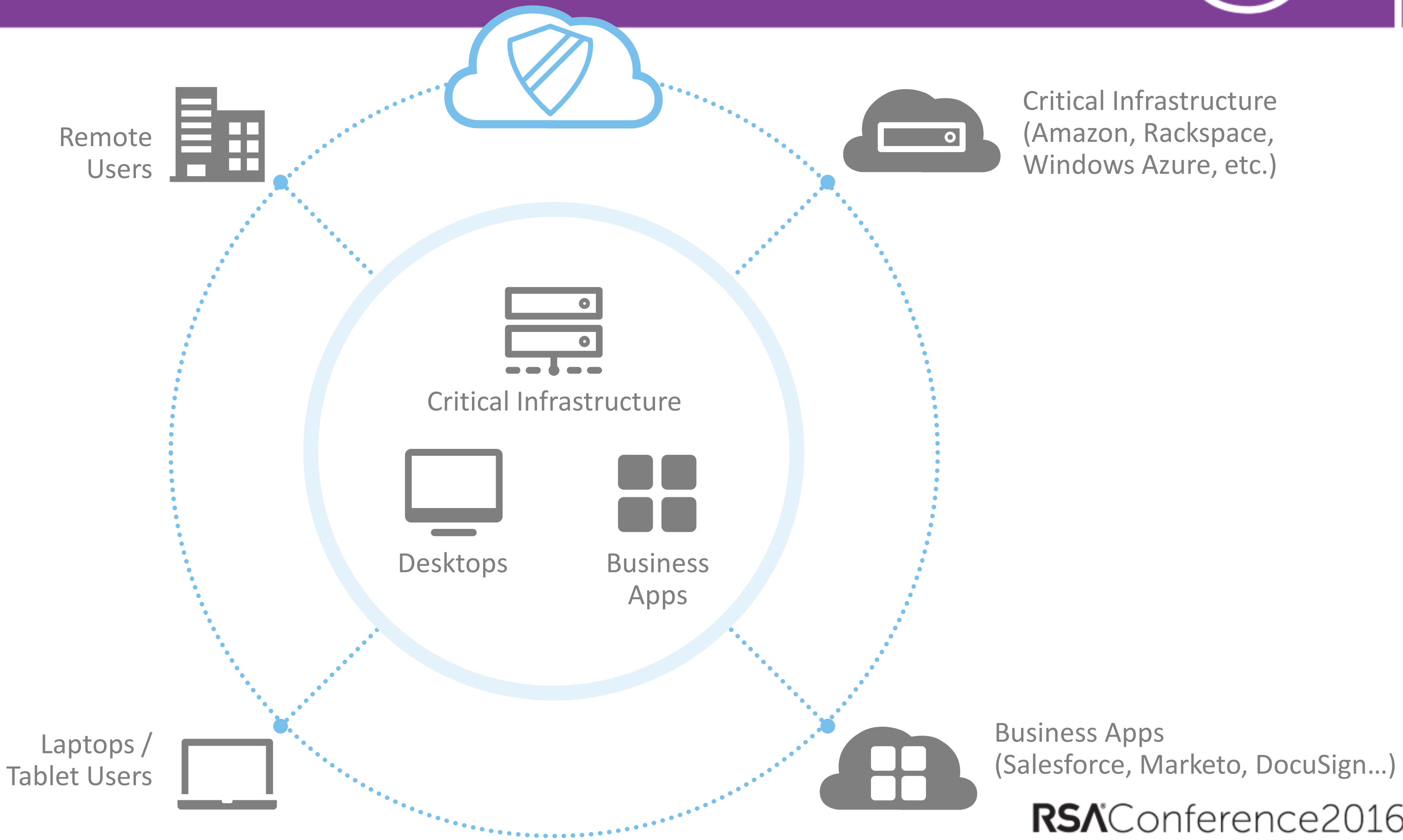
But simple isn’t easy

Where Do We Enforce Security?

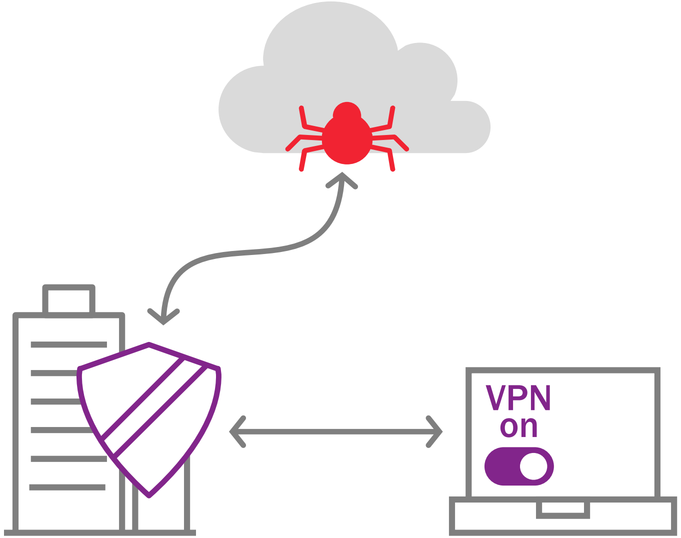
The Shift from Old to New



The Shift from Old to New


Remote Users
Critical Infrastructure (Amazon, Rackspace, Windows Azure, etc.)
Critical Infrastructure
Desktops
Business Apps
Laptops / Tablet Users
Business Apps (Salesforce, Marketo, DocuSign…)

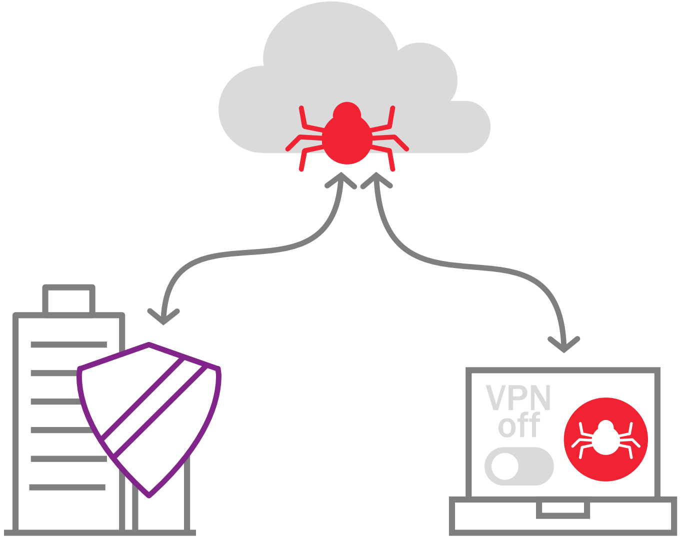
You Cannot Rely on the VPN



Last 20 years of
off-network security:

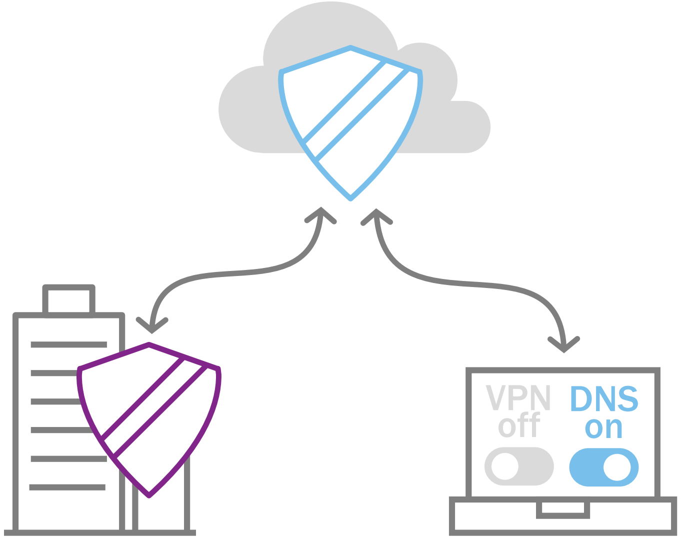
REMOTE ACCESS

You Need a New 24x7 Security Landscape



But the VPN is not on 24x7…

You Need DNS-Layer Network Security



DNS is the Internet's control plane

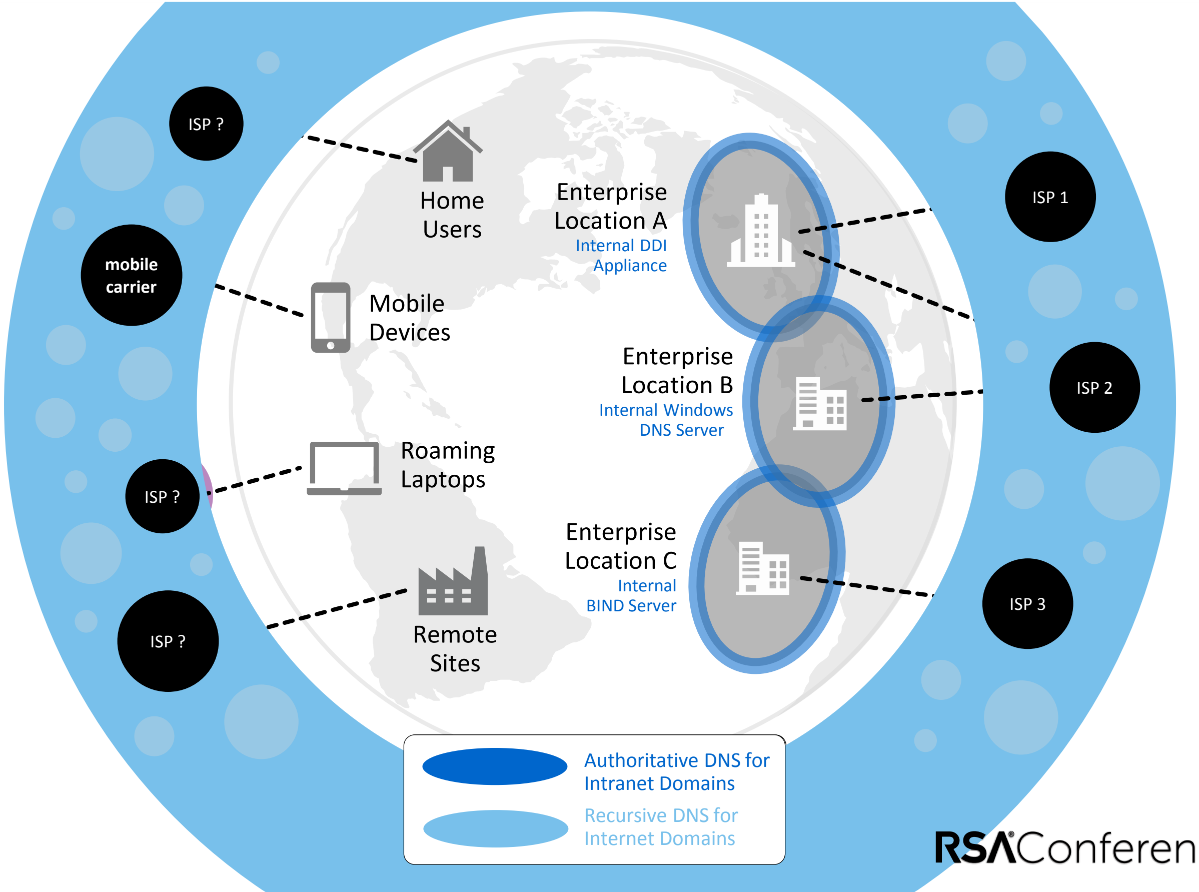
DNS Works on Any Device, Anywhere

BENEFITS

Global Internet Activity Visibility

Network Security w/o Adding Latency

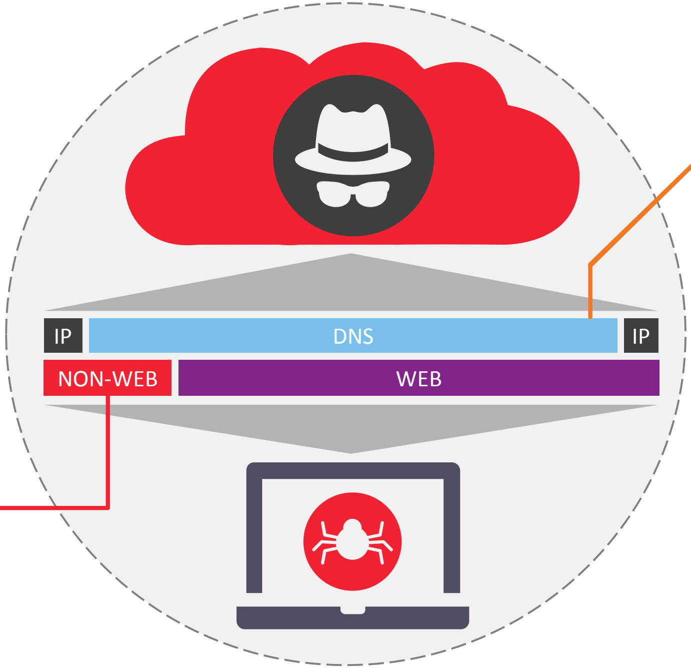
Consistent Policy Enforcement



OpenDNS

OpenDNS is now part of Cisco. cisco

DNS Blocks Threats That Others Miss



91%

of C2 can be blocked at the DNS layer

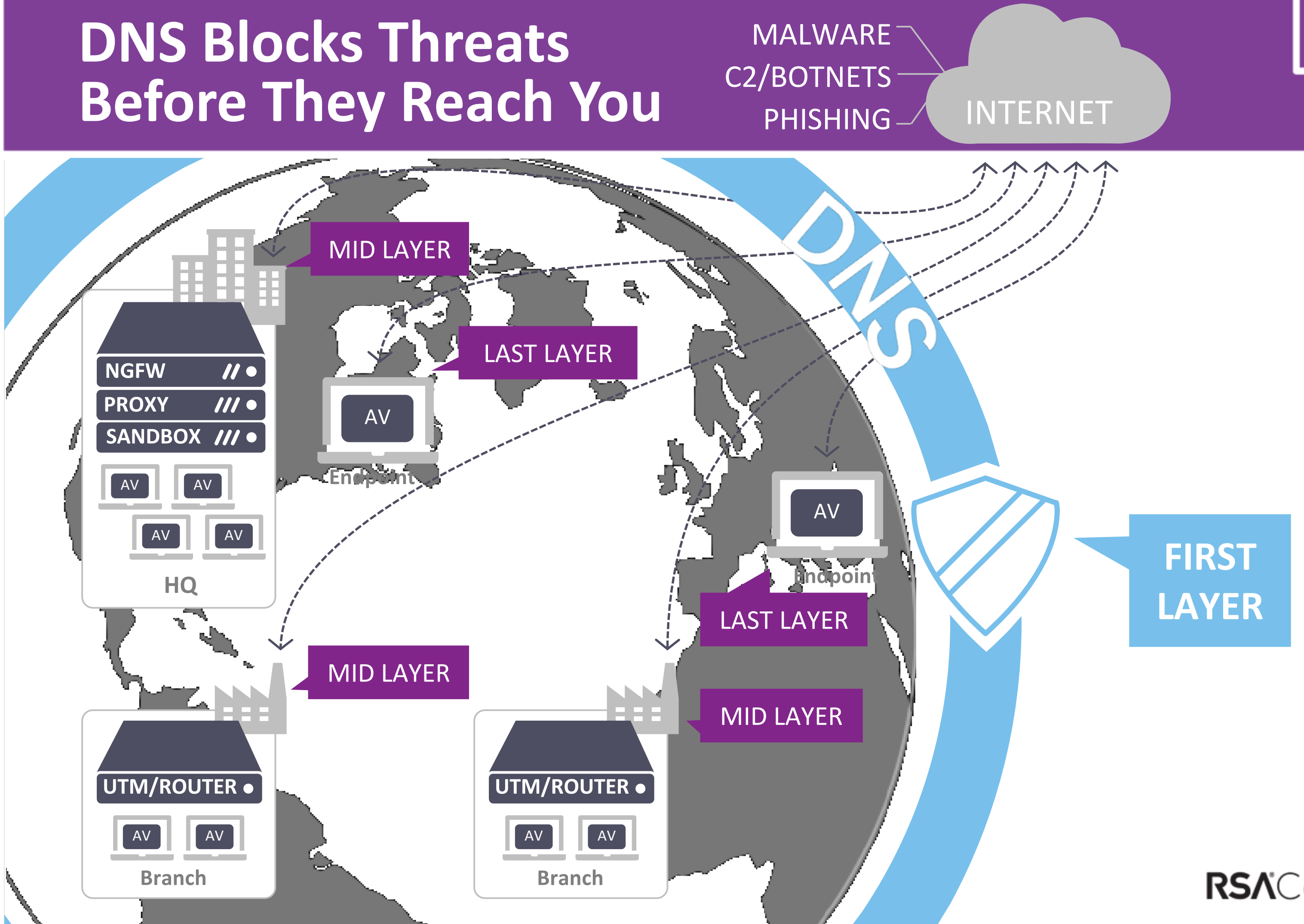
15%

of C2 bypasses Web ports 80 & 443

OpenDNS

OpenDNS is now part of Cisco. CISCO

DNS Blocks Threats Before They Reach You



BENEFITS

Reduce alerts by 2-10x

Block malware before it hits the enterprise

Contain malware if already inside

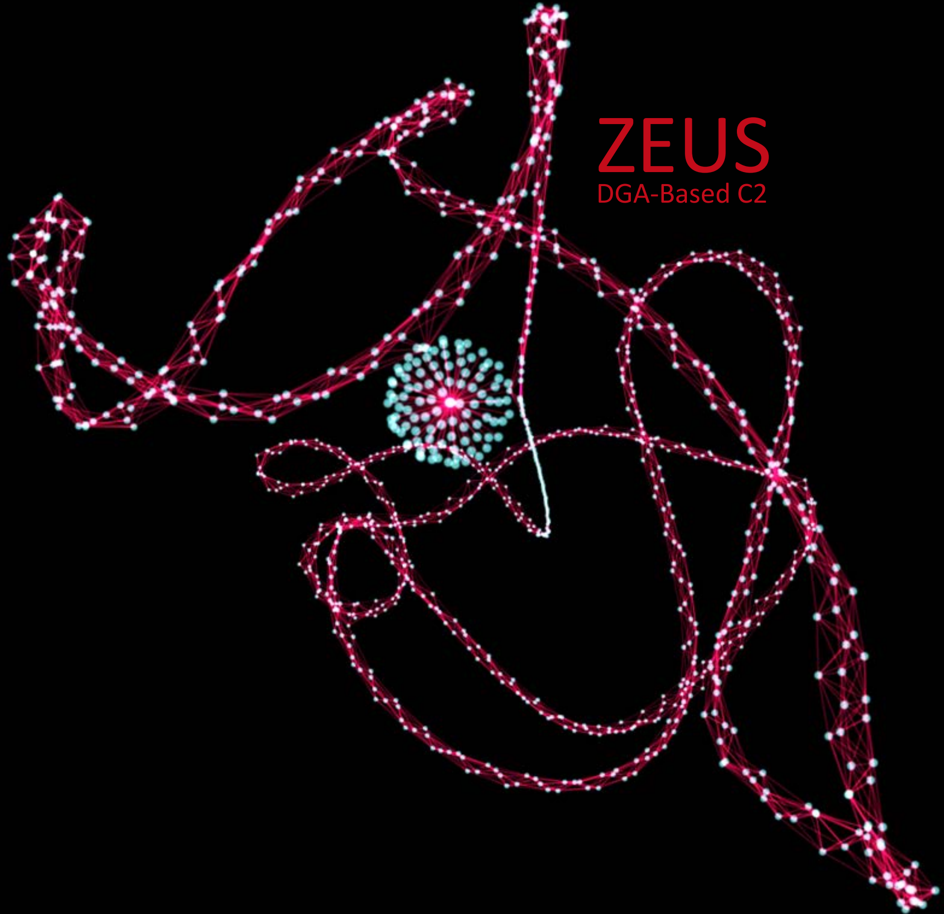
DNS is the Easiest and Fastest way to Establish a 24x7 Security Landscape

Can We Get Ahead of Attacks?

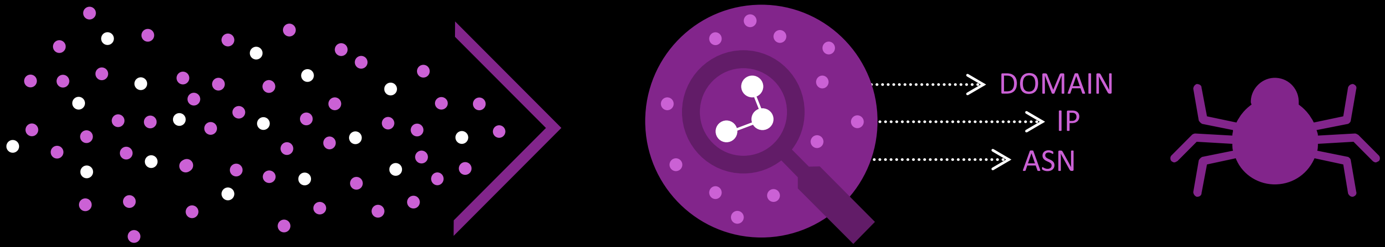
Yes. But It Requires Internet-Wide Visibility.

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

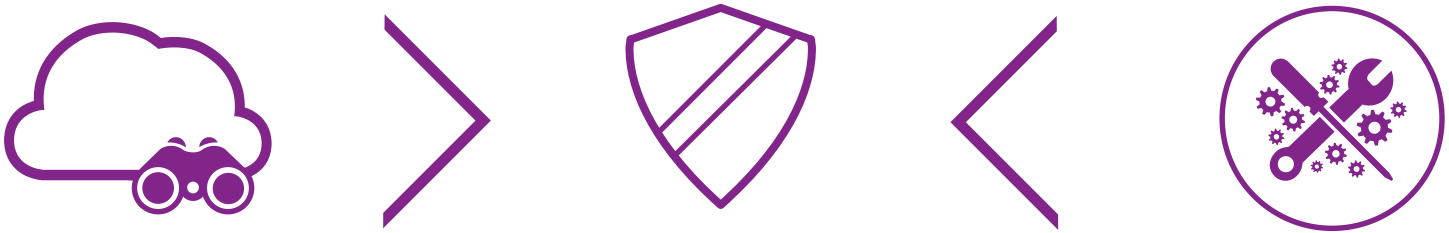
Second, Identify New Patterns by Applying Human Intelligence to Data Visualizations



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



Apply what you have learned today



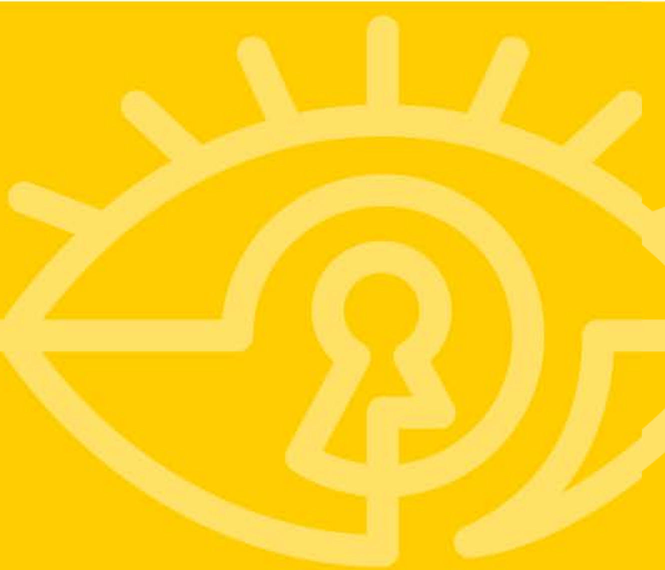
VISIBILITY
see all the traffic

ENFORCEMENT
24x7 security landscape

MANAGEABILITY
consistently adapt

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



Thank You

David Ulevitch
tweet @davidu
email d@cisco.com