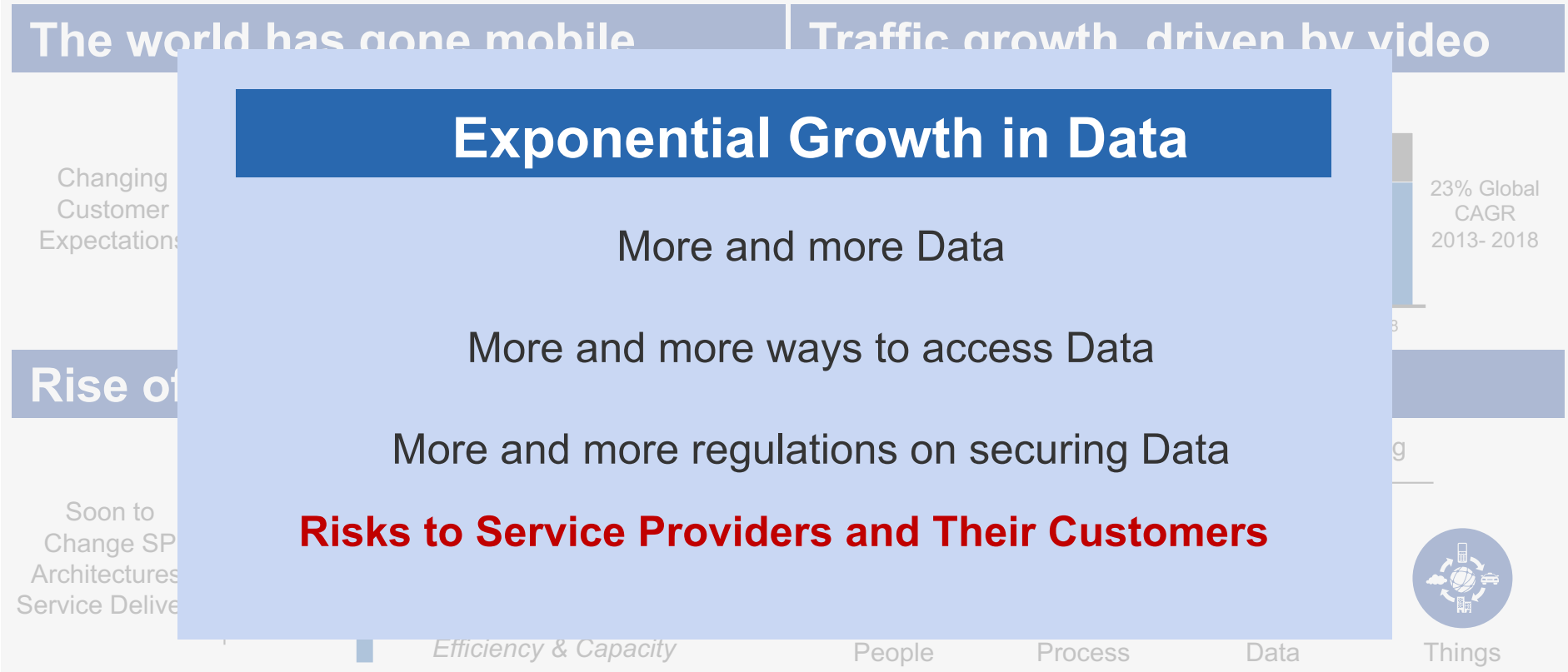
Service Provider Security Architecture

Andrew Turner
Technical Marketing, Security Business Group
April 12th 2017

Digitization is disrupting the SP business



Exponential Growth in Data

More and more Data

More and more ways to access Data

More and more regulations on securing Data

Risks to Service Providers and Their Customers

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

All Data has Monetary Value

Welcome to the Hackers' Economy

Source: CNBC

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

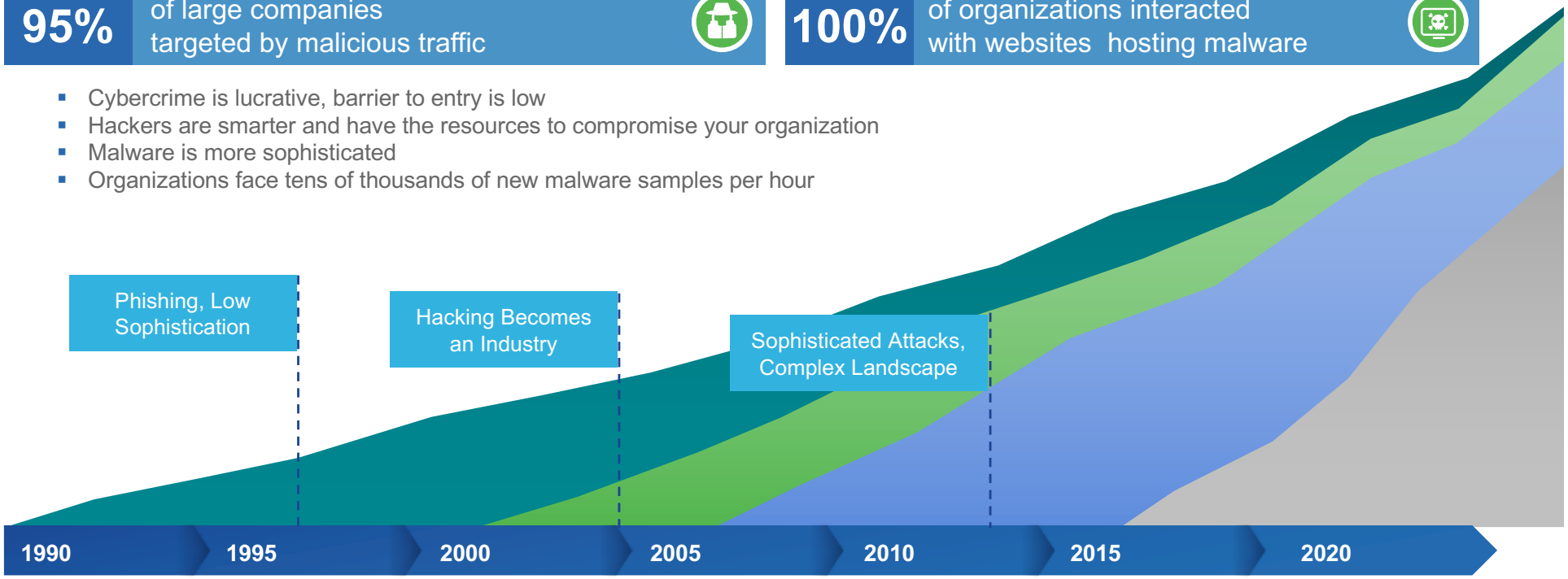
Money Motivates Attackers

Organizations Are Under Attack and Malware Is Getting in

95% of large companies targeted by malicious traffic

100% of organizations interacted with websites hosting malware

- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new malware samples per hour



Viruses 1990-2000

Worms 2000-2005

Spyware and Rootkits 2005-Today

APTs Cyberware Today +

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Being Breached Costs Dollars and Reputation

[1]Verizon – 2015 Data Breach Investigations Report
[2] Ponemon Institute - 2015 Cost of Data Breach Study: Global Analysis
[3]Verizon – 2014 Data Breach Investigations Report
[4]Verizon – 2014 Data Breach Investigations Report

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

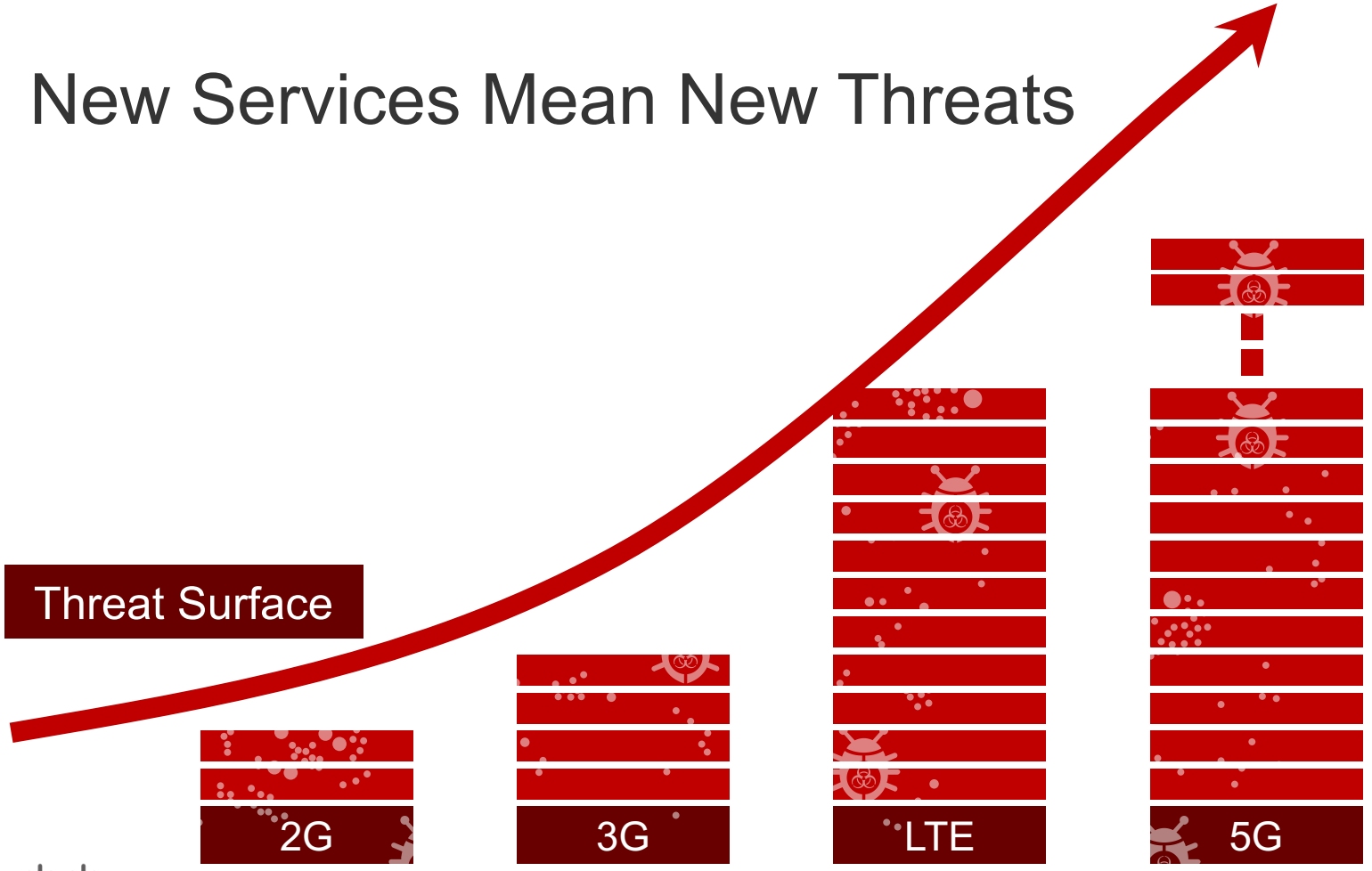
Shift to 5G Will Be Led by New Services

- **Ultra Reliability** (Wherever + Whenever)
- **Ultra Capacity and Coverage**
- **Ultra High-Speed** (up to 10 Gbps to cell site)
- **Ultra Low Latency** (1 ms End-to-End)
- **Massive Device Connectivity**

Broadband access in dense areas	Broadband access everywhere	Higher user mobility	Massive Internet of Things	
Pervasive Video	Average 1 Gbps per device	High Speed Train	Sensor Networks	
Extreme real-time communications	Lifeline communications	Ultra-reliable communications	Broadcast-like services	
Tactile Internet	Natural Disaster	E-Health Services	Broadcast Services	

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

New Services Mean New Threats

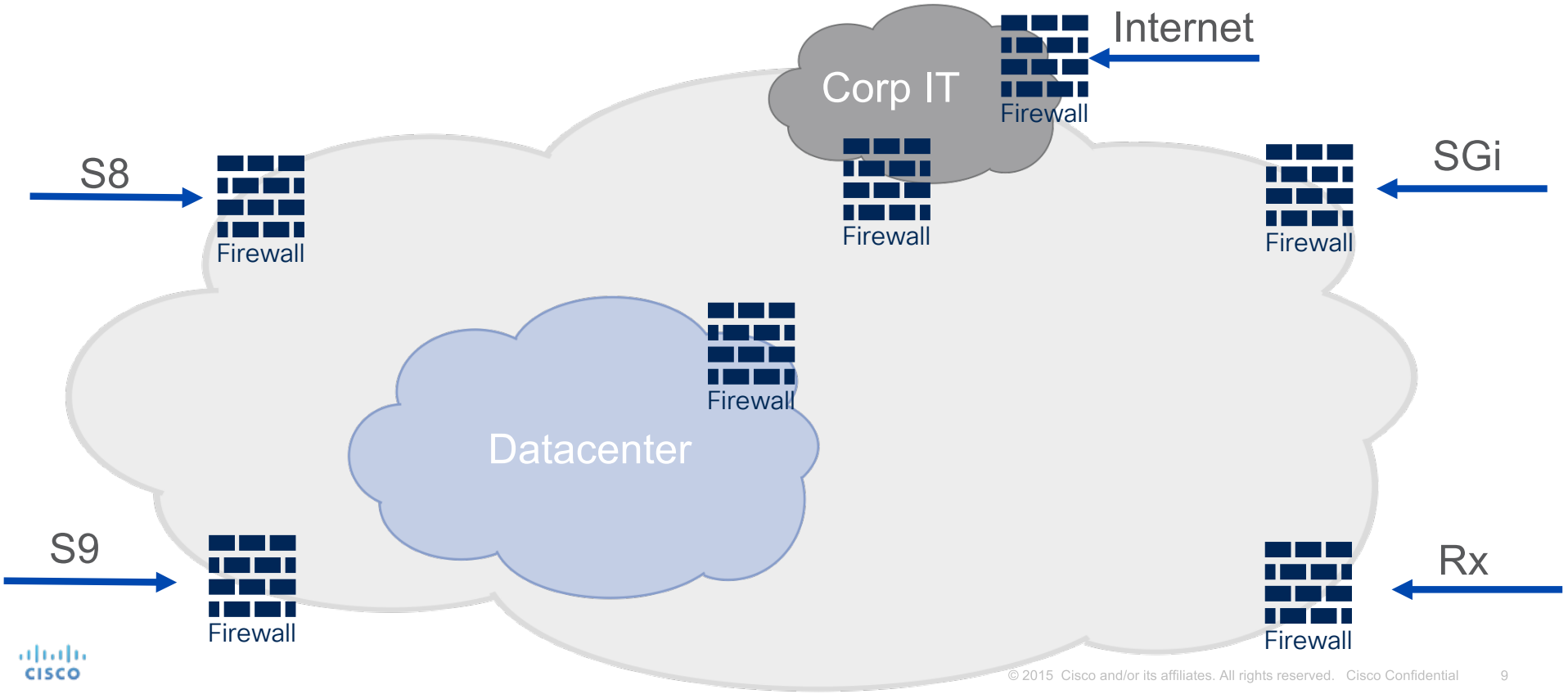


© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco: Committed to Security

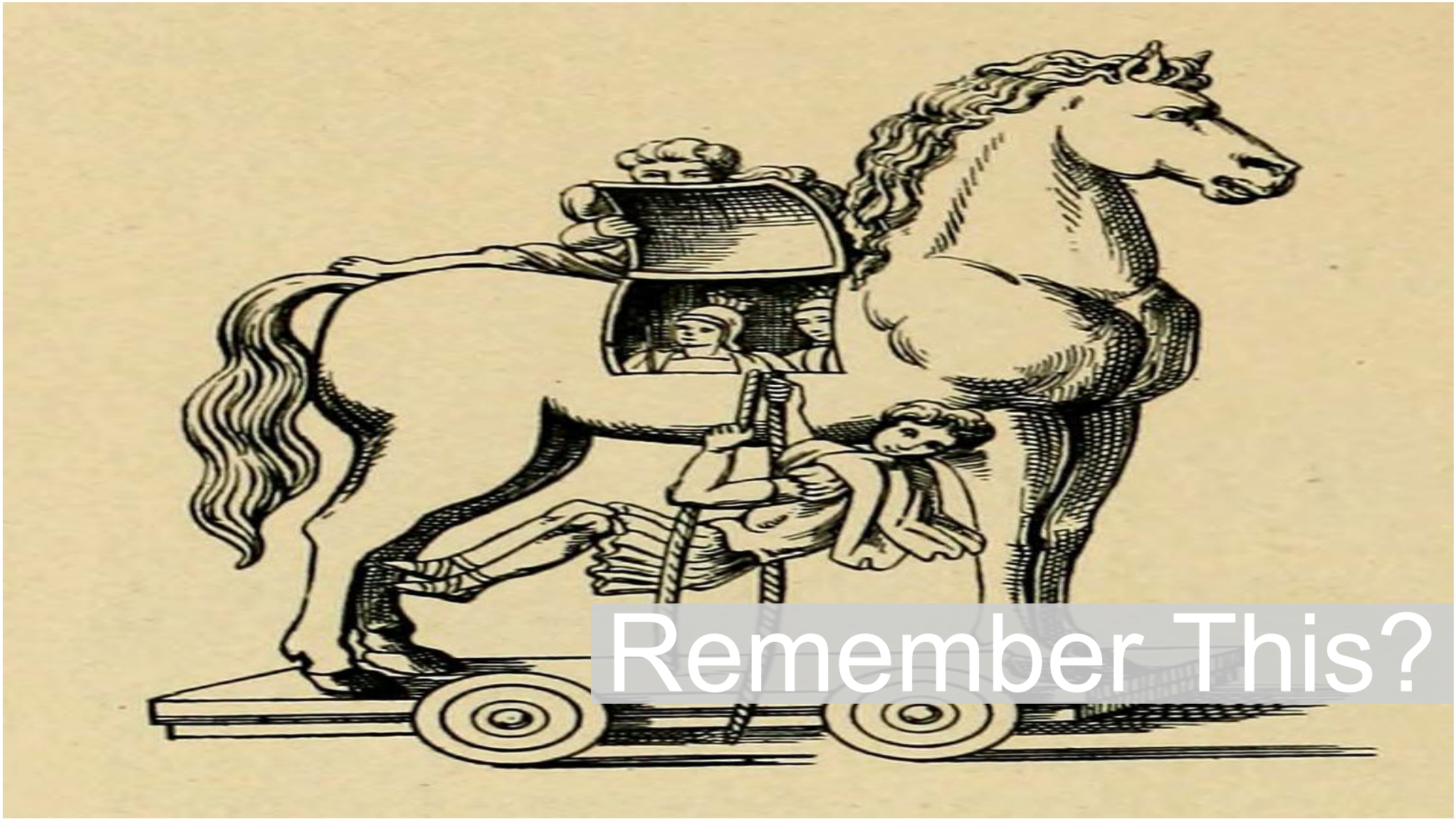
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Security Needs to Keep Pace



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

Security


Remember This?

Look Inside

Or Maybe Not

Traditional Security Needs to Keep Pace

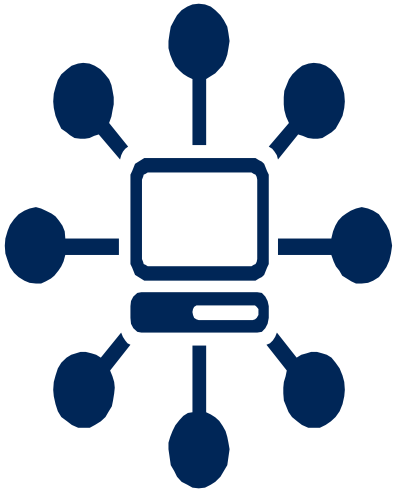
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Security Needs to Keep Pace

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

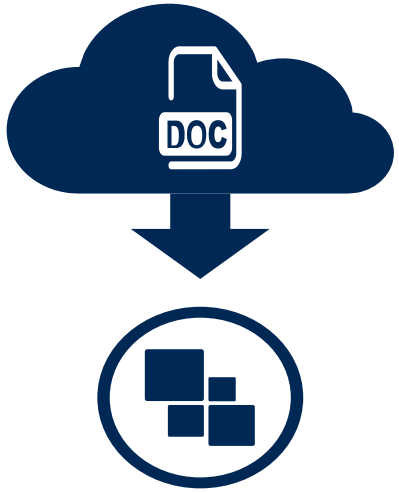
Example Threats inside the Perimeter

Insider



Internal
DoS

Interception
and
Exploitation



Exfiltration

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

Security begins with visibility

Who is on the Network?

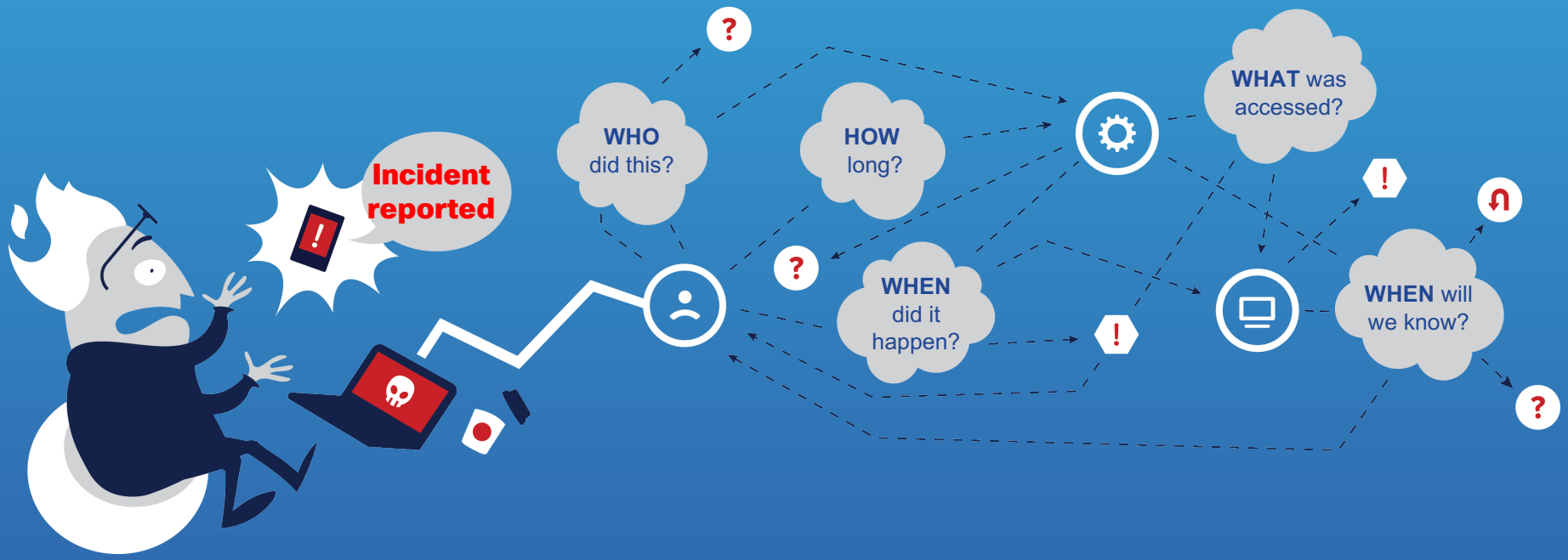
You can’t protect

what you can’t see

And what are they up to?

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

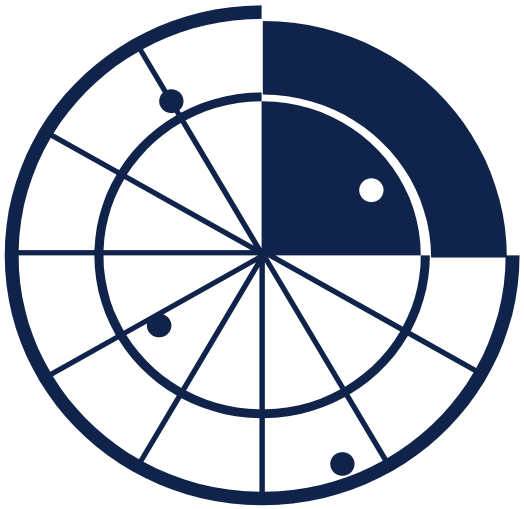
Because when it happens…..



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

Evolution of Firewalls

How to increase visibility at the Firewall?



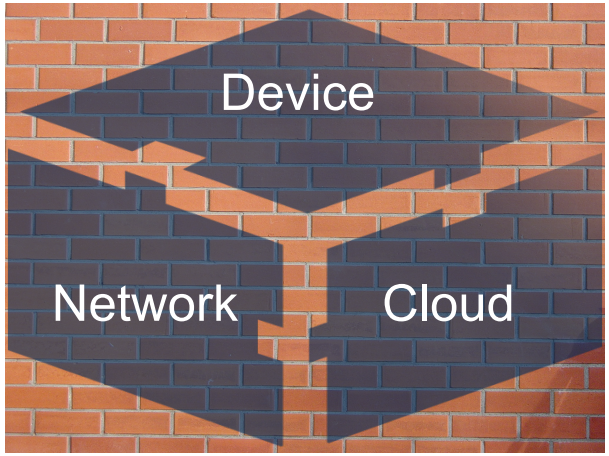
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Evolution of Security

Firewall

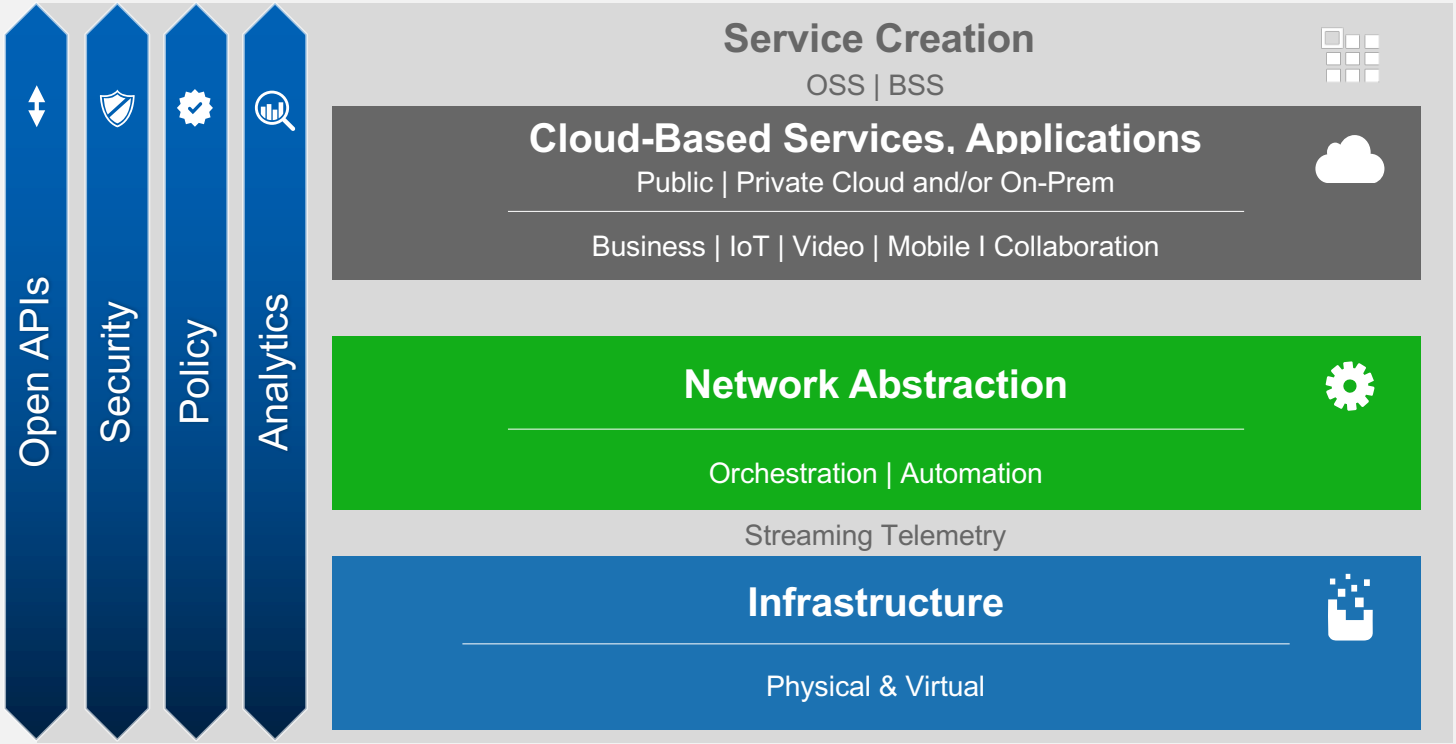
NGFW

Architecture including NGFW



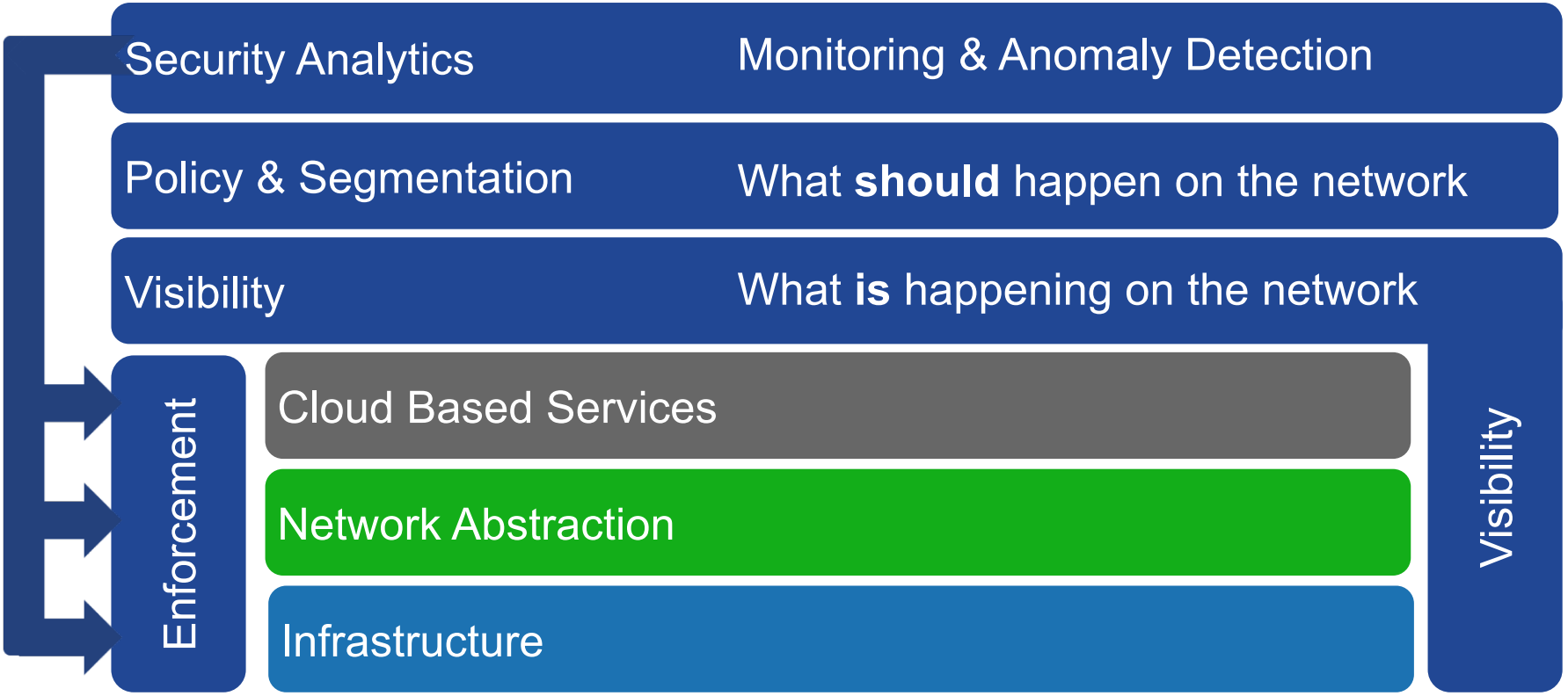
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Open Network Architecture for 5G, IoT, Beyond



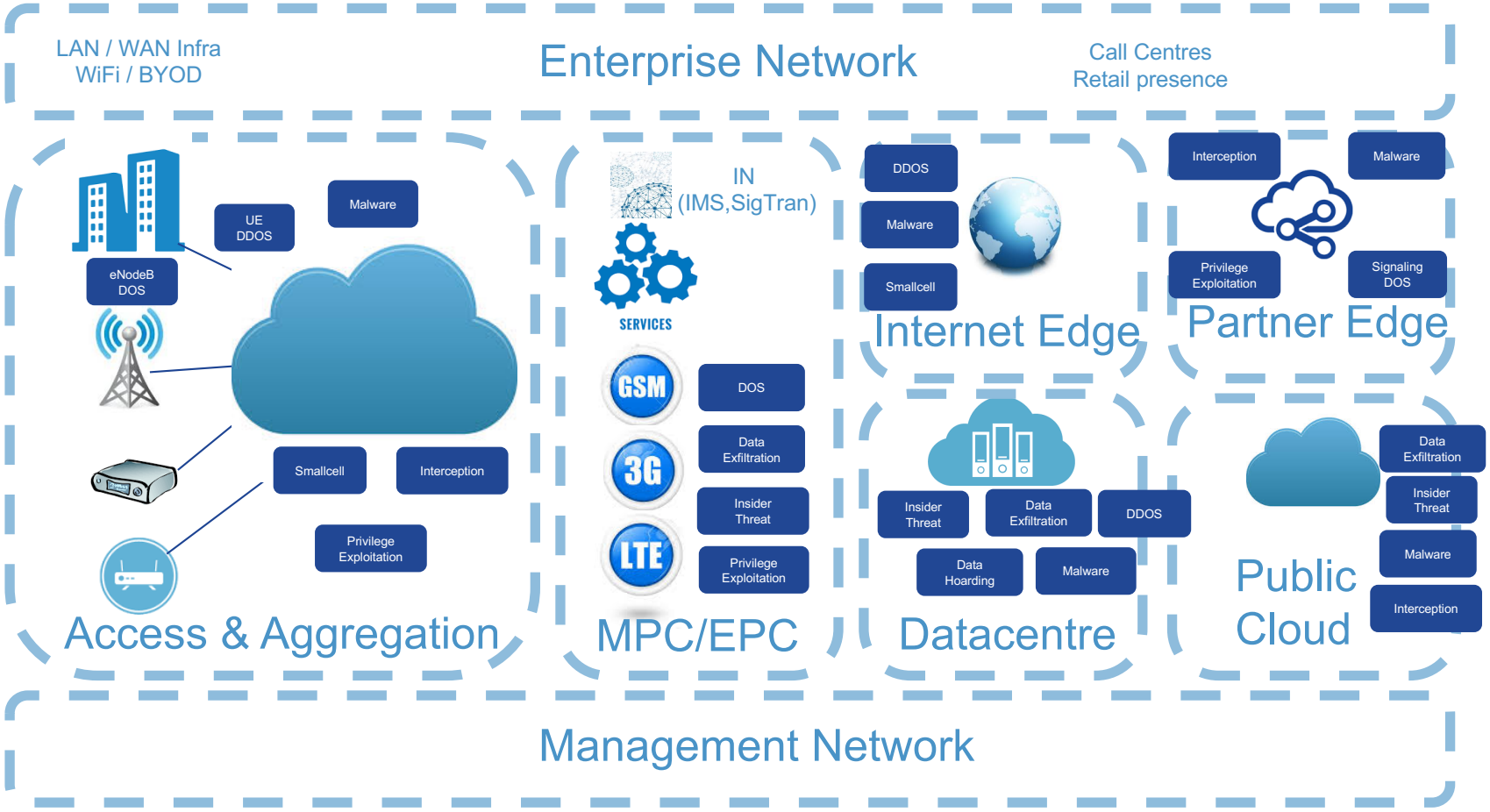
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security in the Open Network Architecture



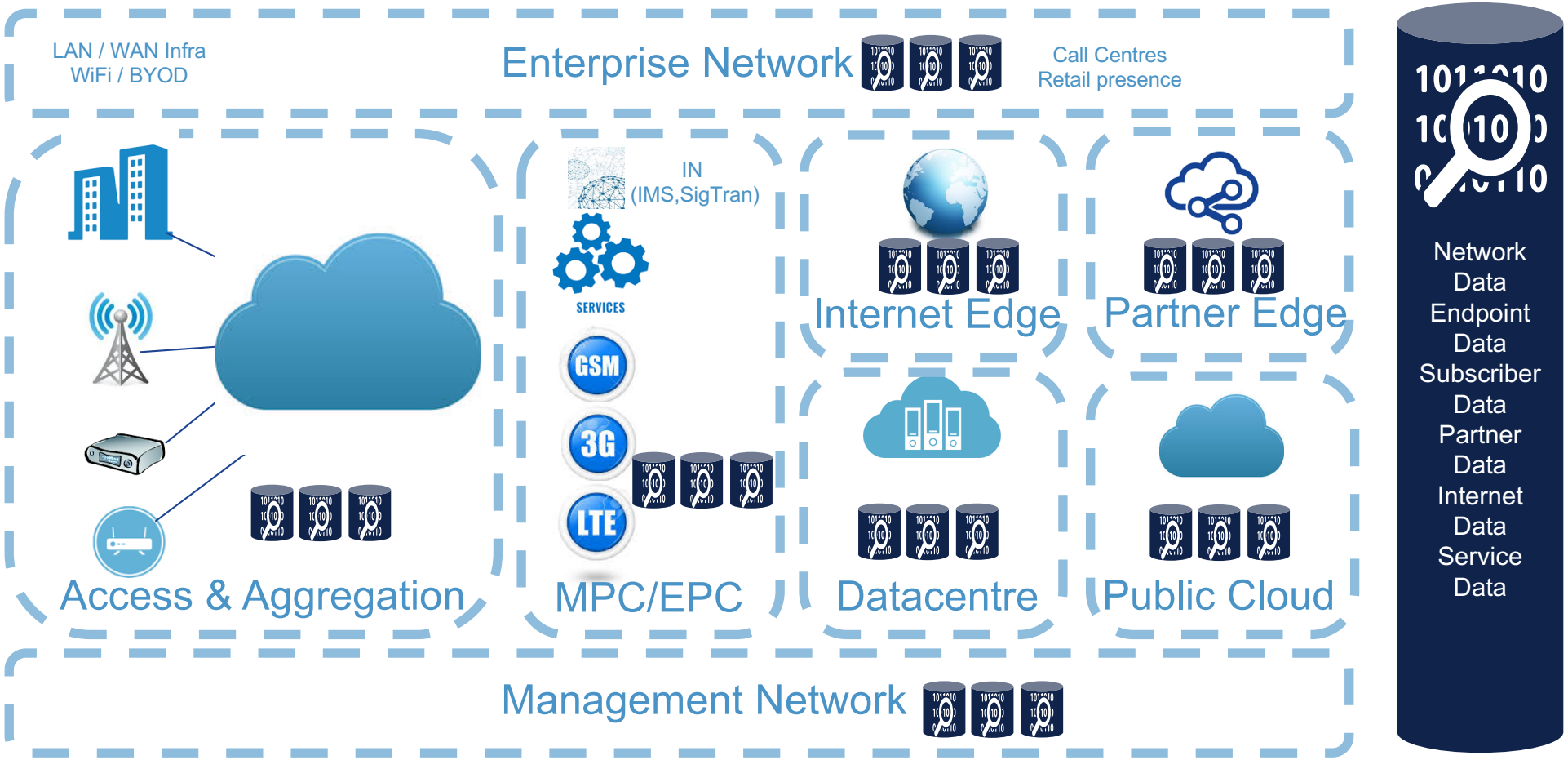
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Architecture



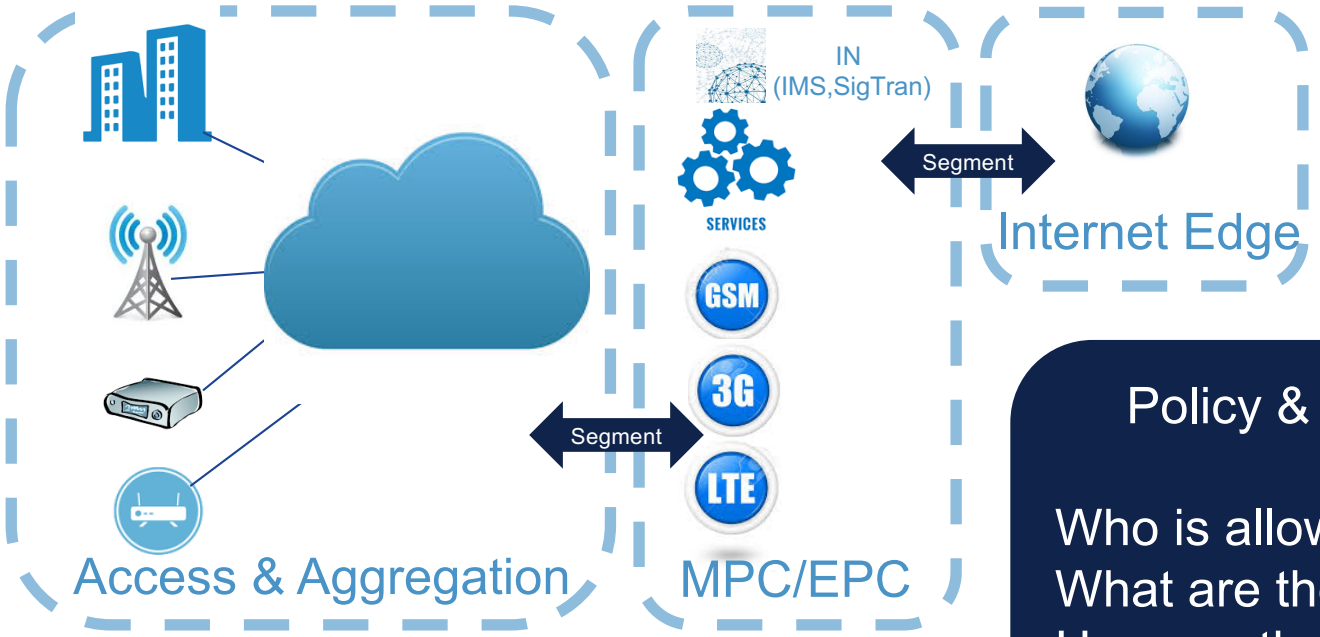
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobility Security Architecture - Visibility



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

Mobility Security Architecture – Policy & Segmentation

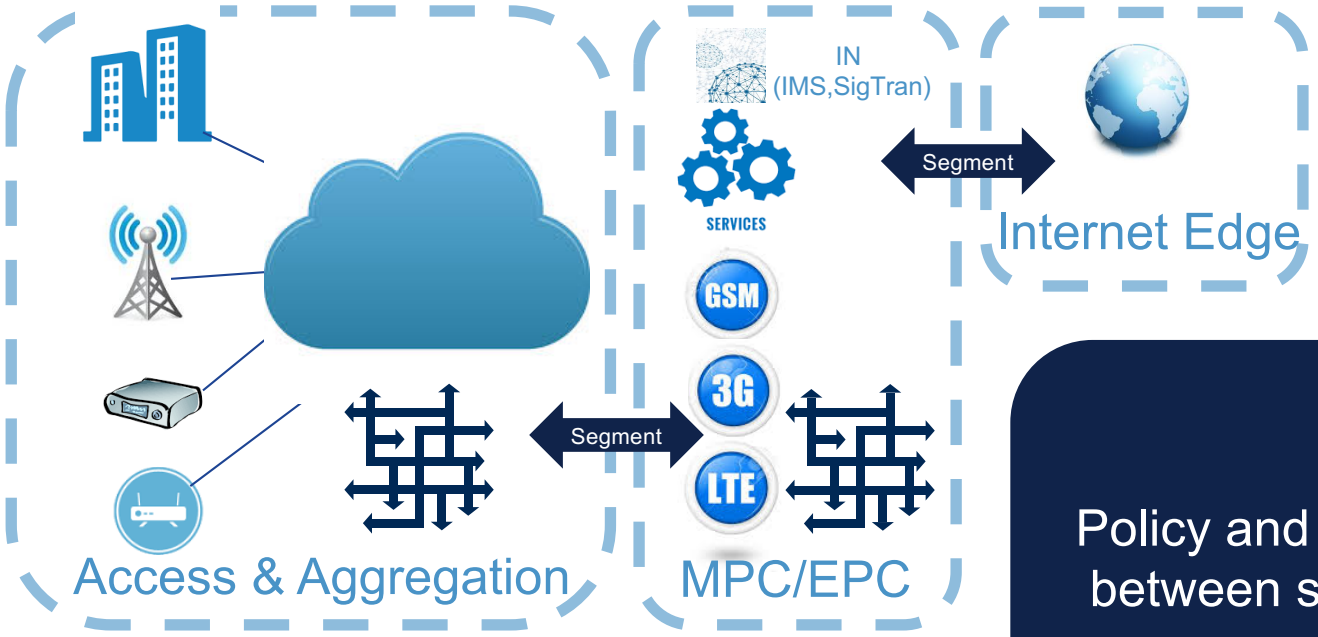


Policy & Segmentation defines

Who is allowed to talk to Who?
What are they allowed to talk about?
How are they allowed to talk?
When are they allowed to talk?

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

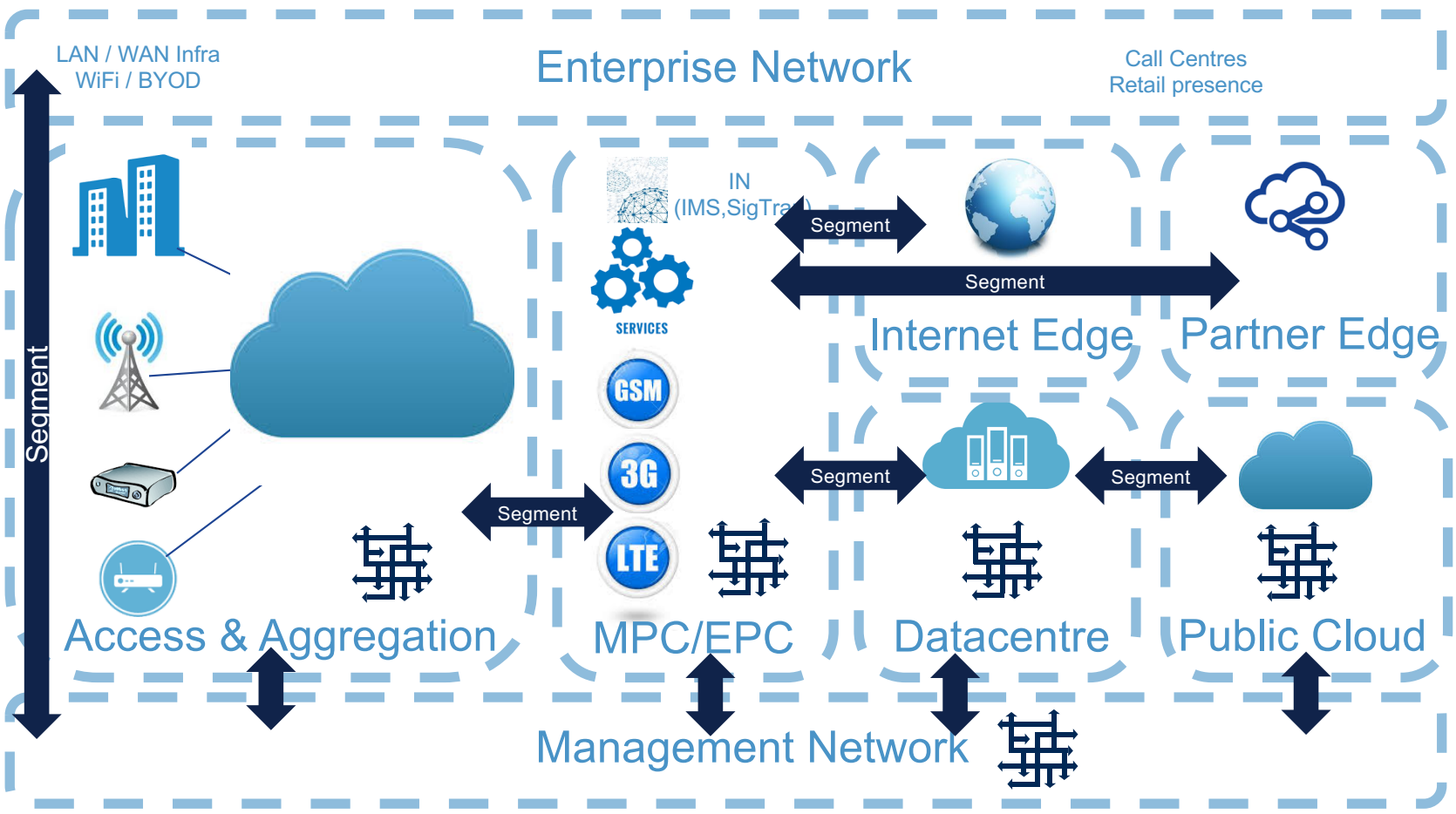
Mobility Security Architecture – Policy & Segmentation



Policy and Segmentation is not just between segments but also within segments

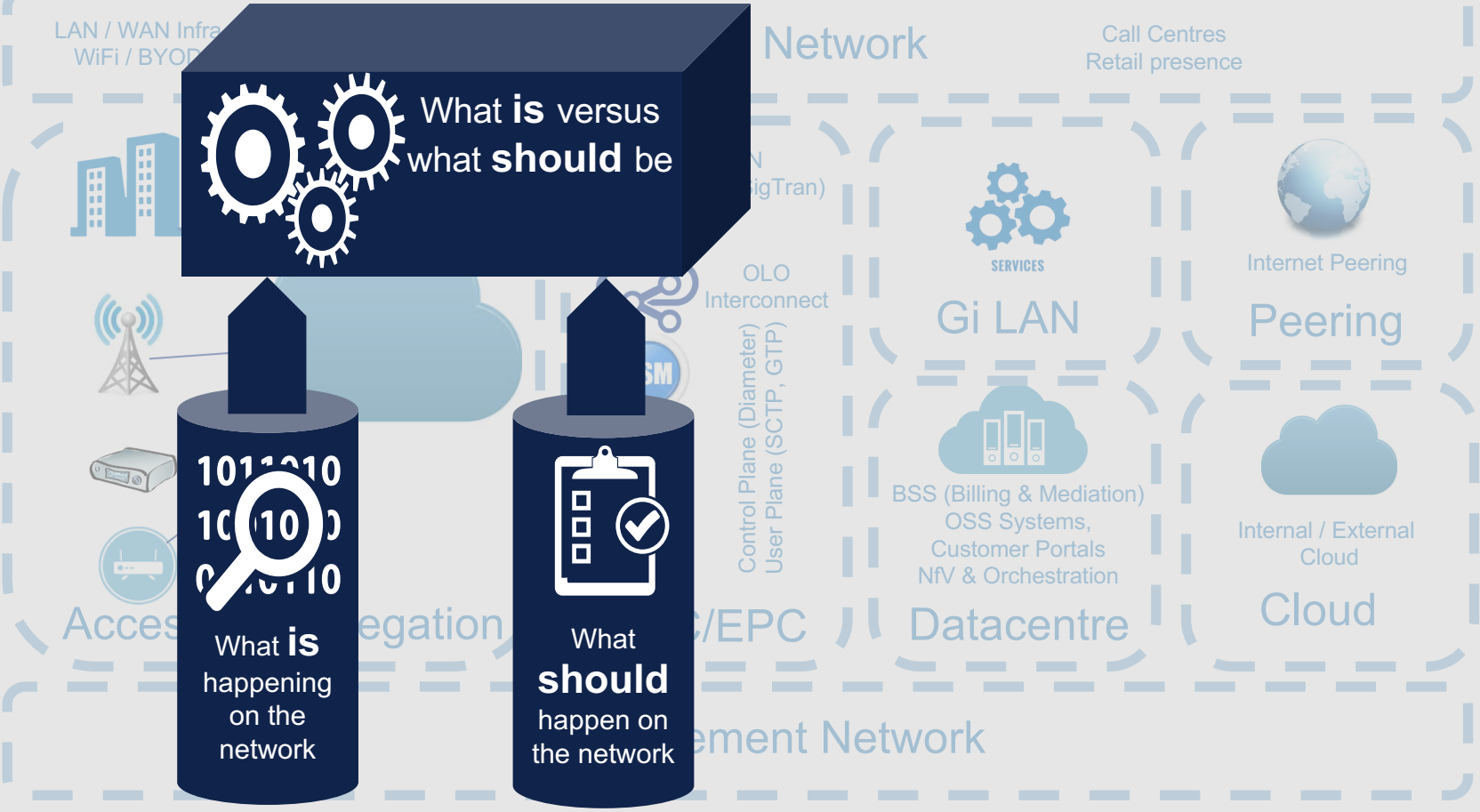
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobility Security Architecture – Policy & Segmentation



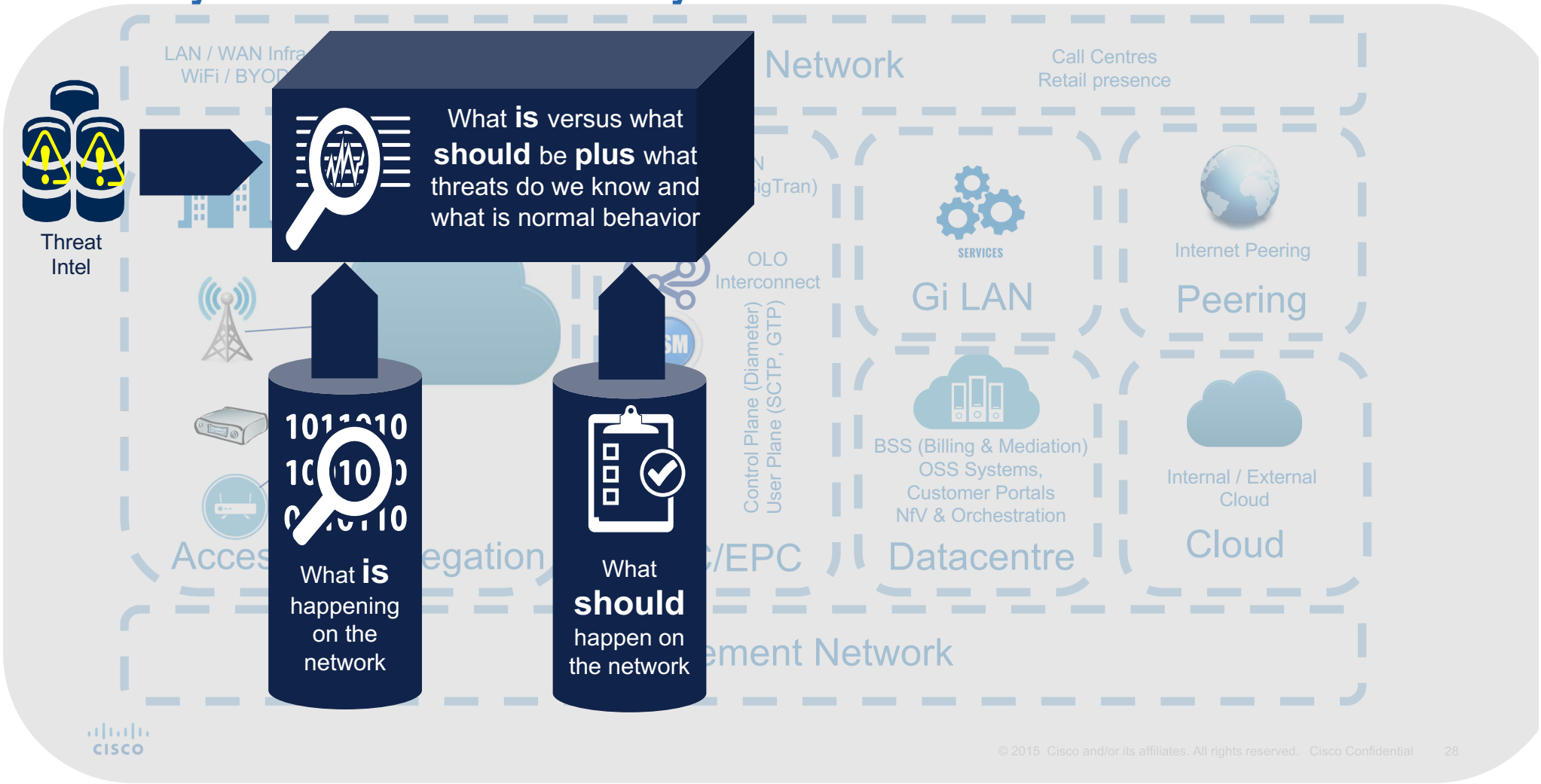
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Architecture - Analytics



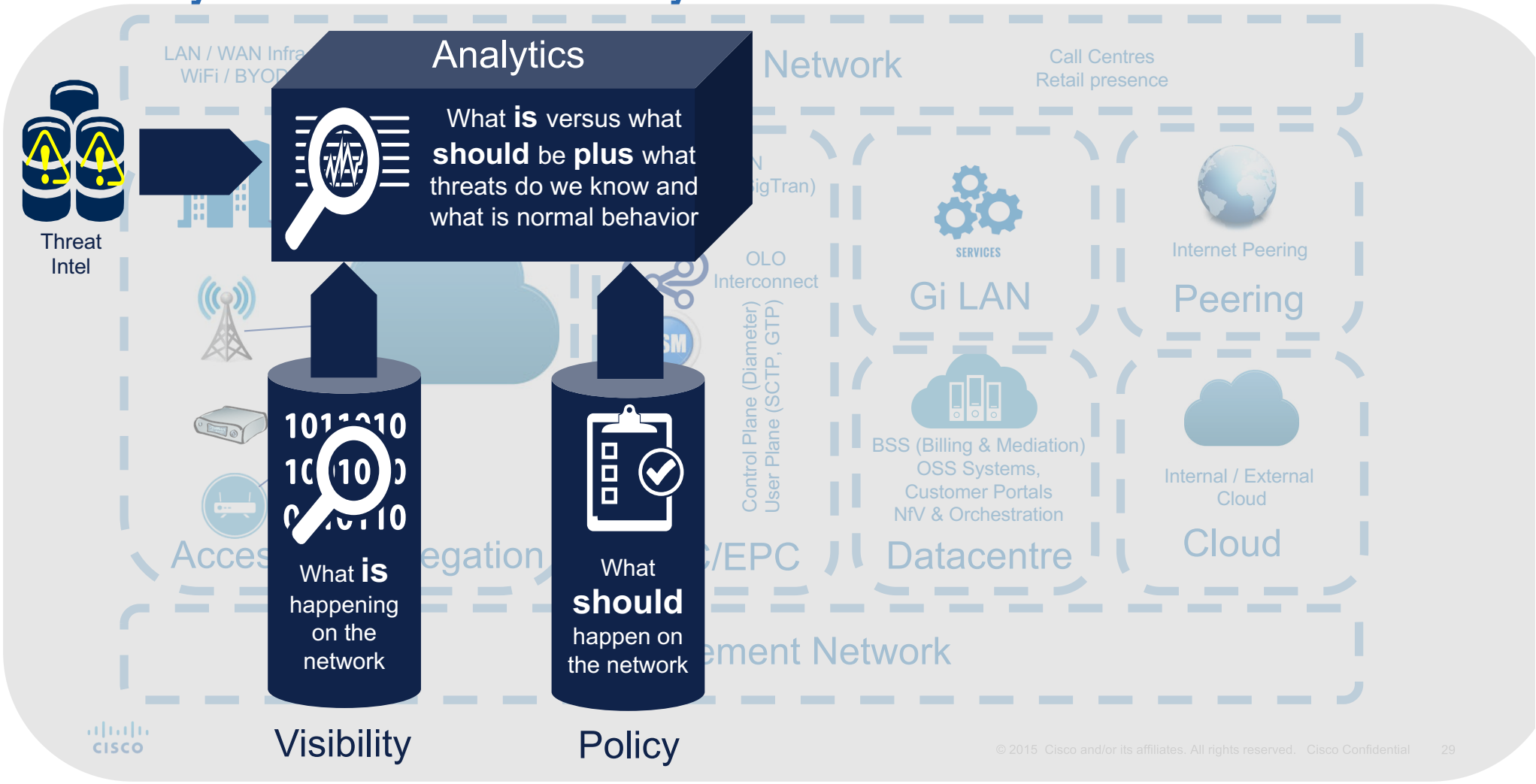
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Architecture - Analytics



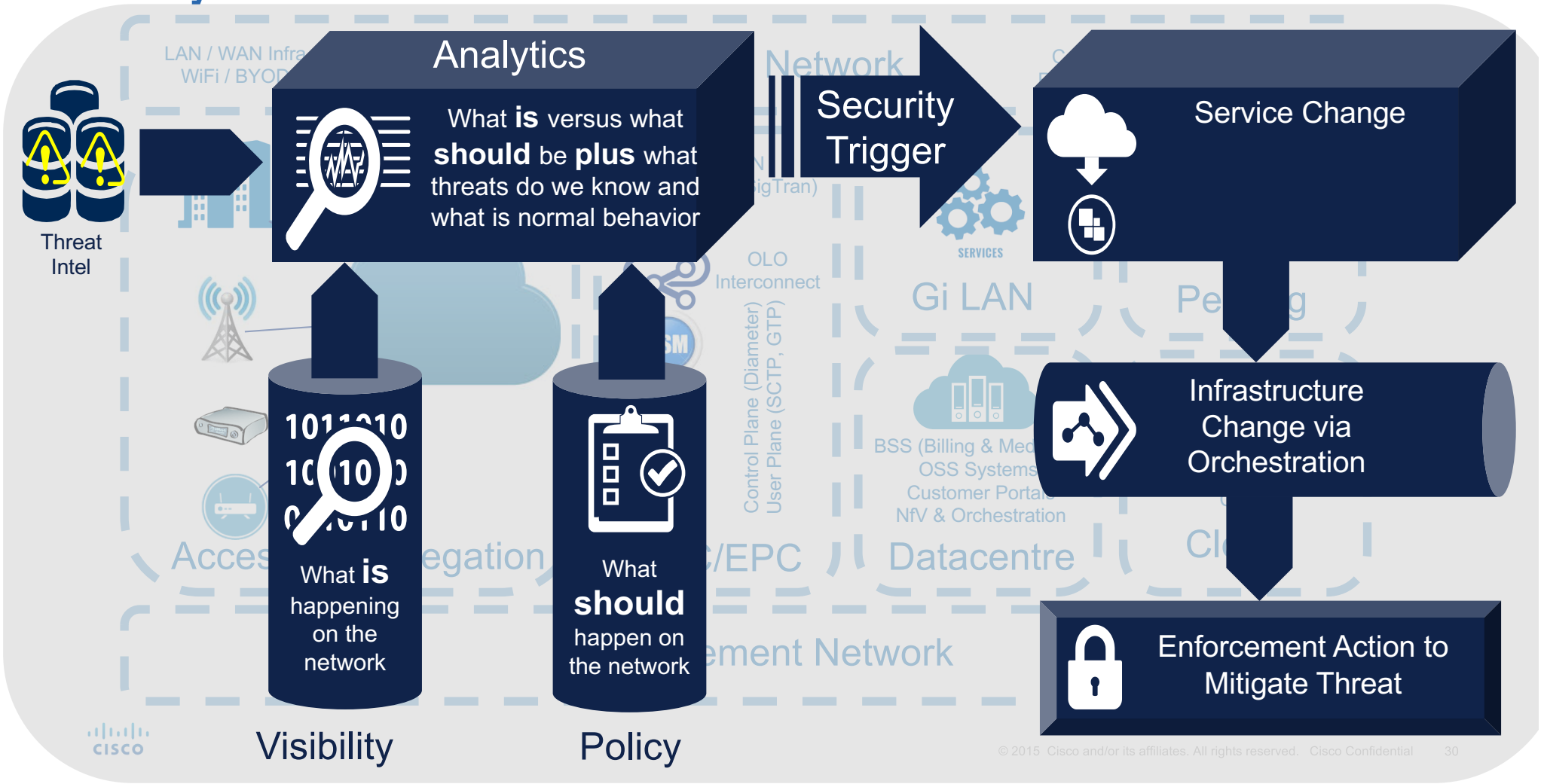
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Architecture - Analytics



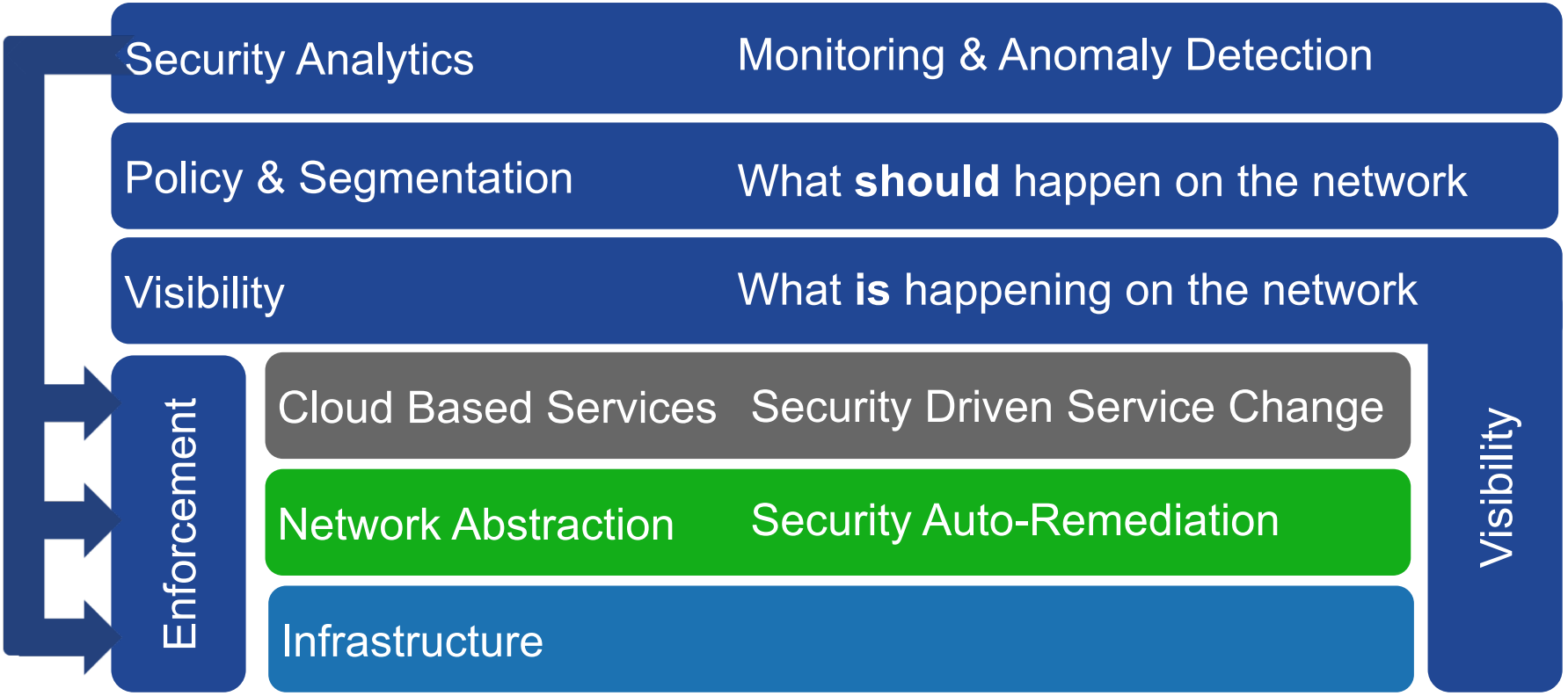
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Architecture



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

Security in the Open Network Architecture



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

Example

Enforcement

Firewall Rules

Source		Destination			Action
IP	SGT	IP	SGT	Service	Action
Any	Employee	Any	**DC Server**	HTTPS	Allow
Any	Suspicious	Any	**DC Server**	Any	Deny

Device is quarantined for remediation or mitigation – access is denied per security policy

Based on the new policy, network enforcers automatically restrict access

Device is compromised
Tries to breach datacenter

Rapid Threat Containment

Visibility

User Activity and File Activity monitored, aggregated and analyzed.

Analytics

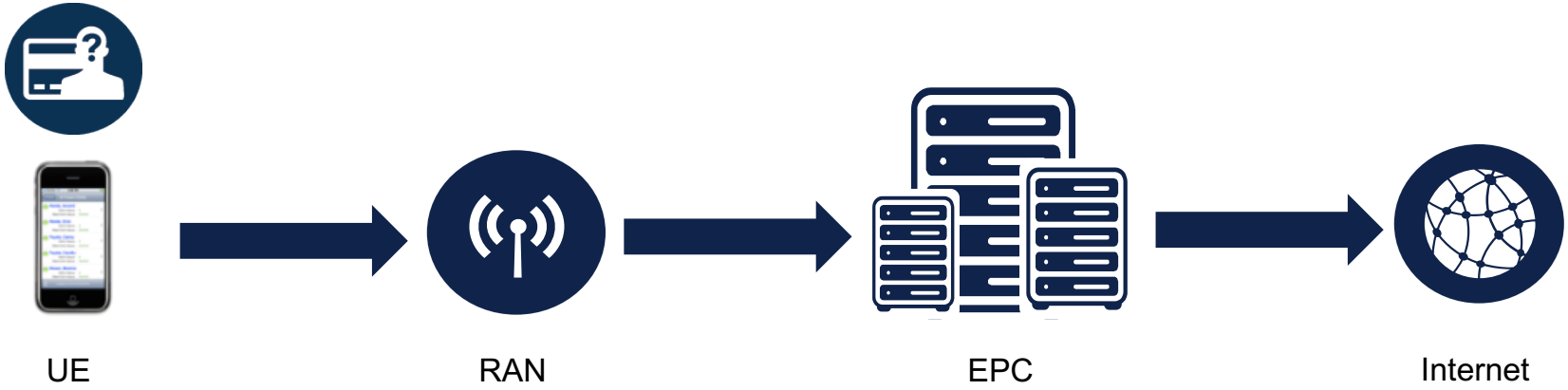
Analytics detect suspicious behavior and inform policy server.

Policy server changes policy for device

Policy

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

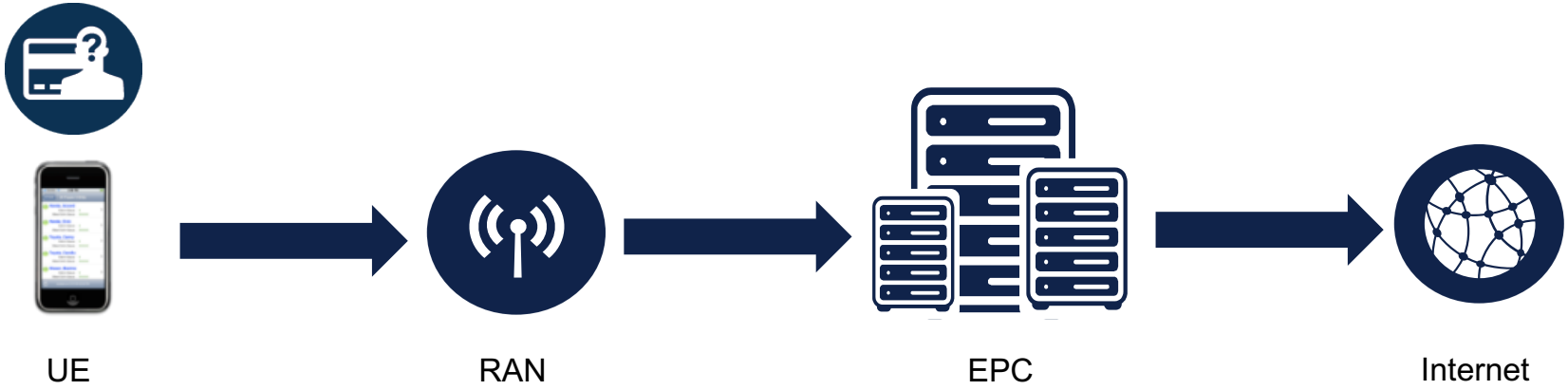
Visibility



Which User Accessed a URL at any particular time?

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

Visibility



URL
Date/Time of Connection
Duration of the Connection

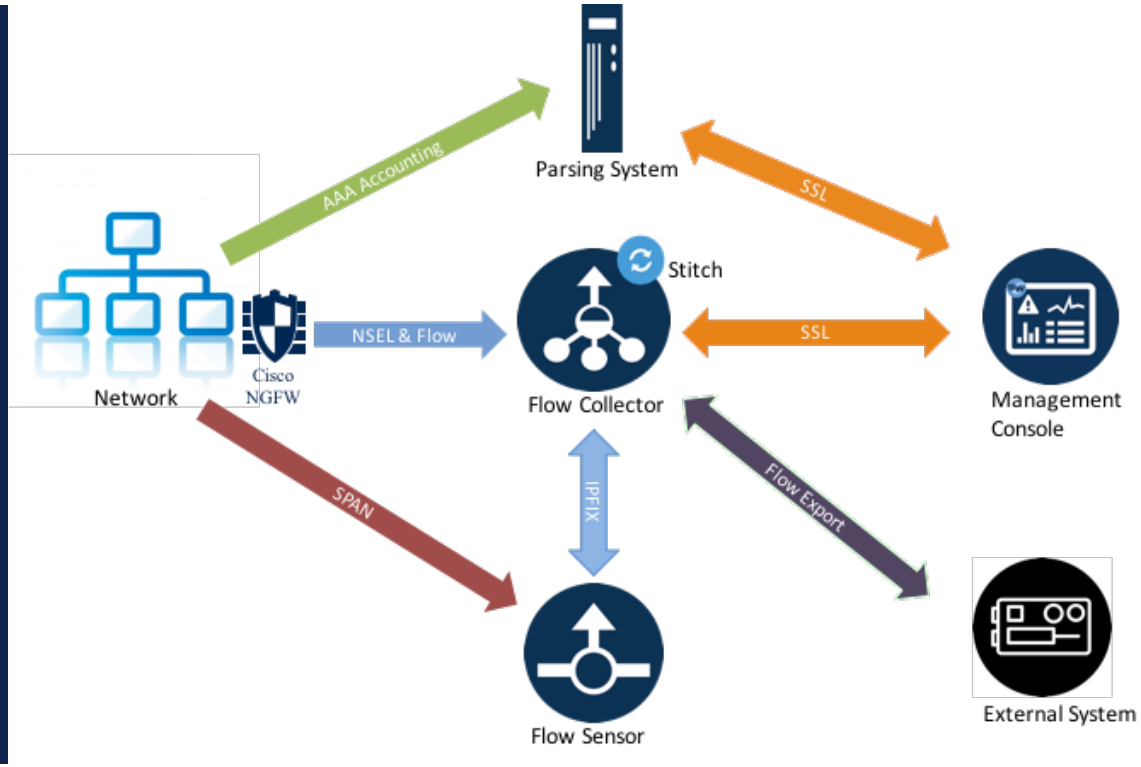
NAT IP Address
Source IP Address
IMSI/MSISDN

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

Visibility

Cisco Stealthwatch

Correlates multiple data types and sources to provide traffic details, subscriber info and application context for every traffic flow passing through the network



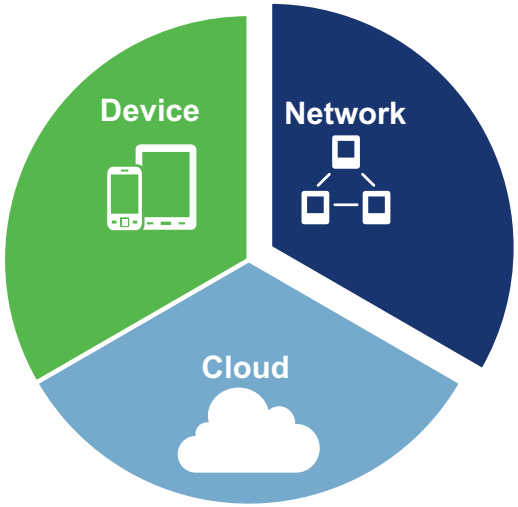
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

See Once, Enforce Everywhere

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

Protecting Network, Cloud, Device for 5G, IoT, Beyond

Security Gateway (SecGW) Solutions for Secure Mobile Backhaul



Centralized SecGW

Firepower 9300

Firepower 4100 Series

ASAv

Distributed SecGW

ASR 900 Series

ASAv

Superior Performance and Scale

High throughput IPsec VPN and Security Gateway processing

Exceptional Flexibility

Right sized with pay-as-you-grow options; unique clustering technology on Firepower to optimize performance while reducing rack space, power and cooling costs

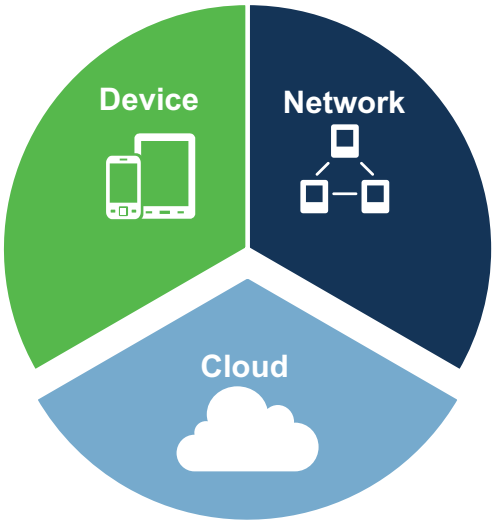
Future Proof

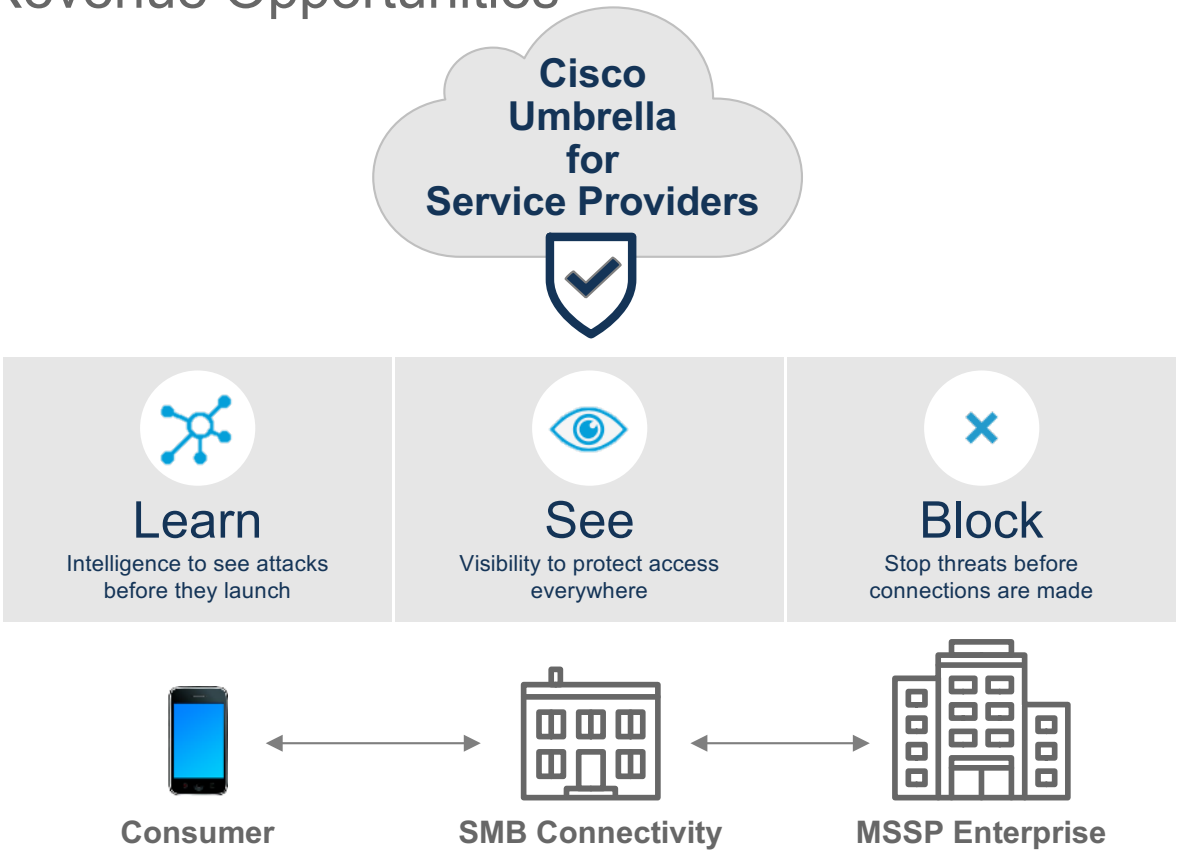
Physical and virtual options to address architectural requirements

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

Protecting Network, Cloud, Device for 5G, IoT, Beyond

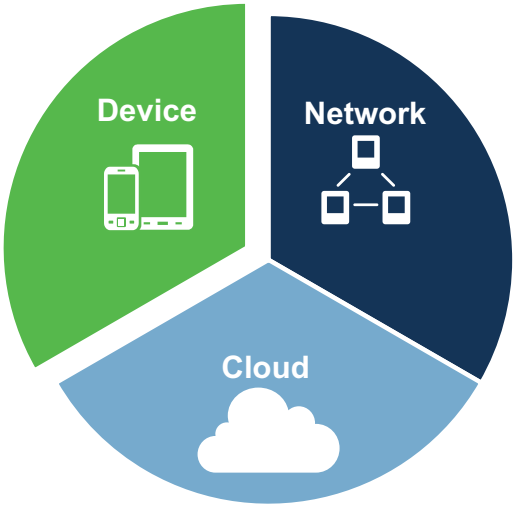
Cisco Umbrella for New Revenue Opportunities

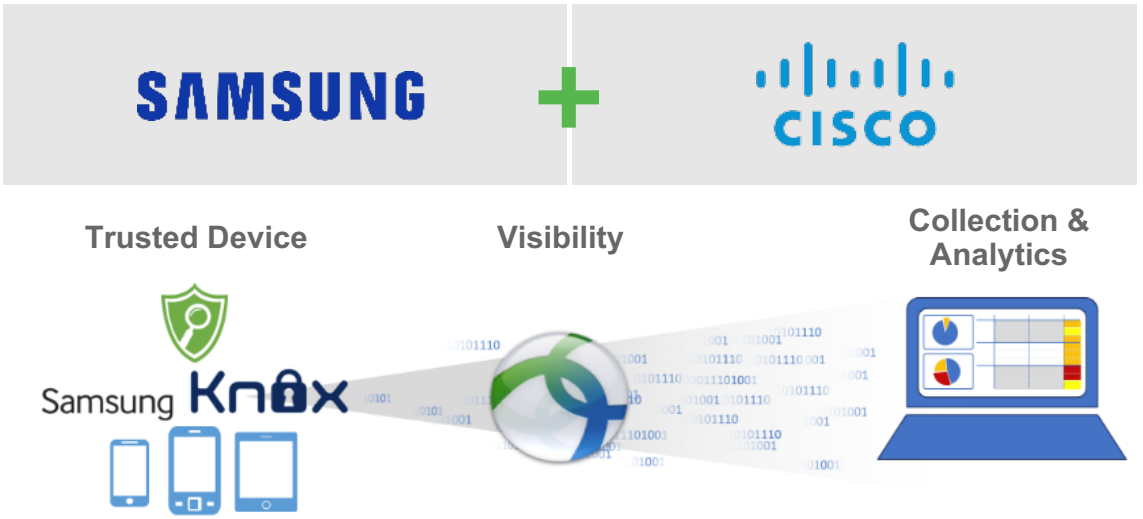




© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protecting Network, Cloud, Device for 5G, IoT, Beyond
Secure Enterprise Mobility





Samsung and Cisco are partnering to provide the most secure mobile device platform with unmatched visibility for the enterprise

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

Thank You

Security Business Group

“There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.”

John Chambers

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential