# 解密雲端運算的安全

## 談雲端運算的安全維護

錢小山

首席技術顧問

大中華區數據中心事業部

二〇一七年七月

# Perimeter security used to be effective

# By 2020, 92% of global data center traffic will come from the cloud.

Cisco® Global Cloud Index (GCI)

# Customer challenges

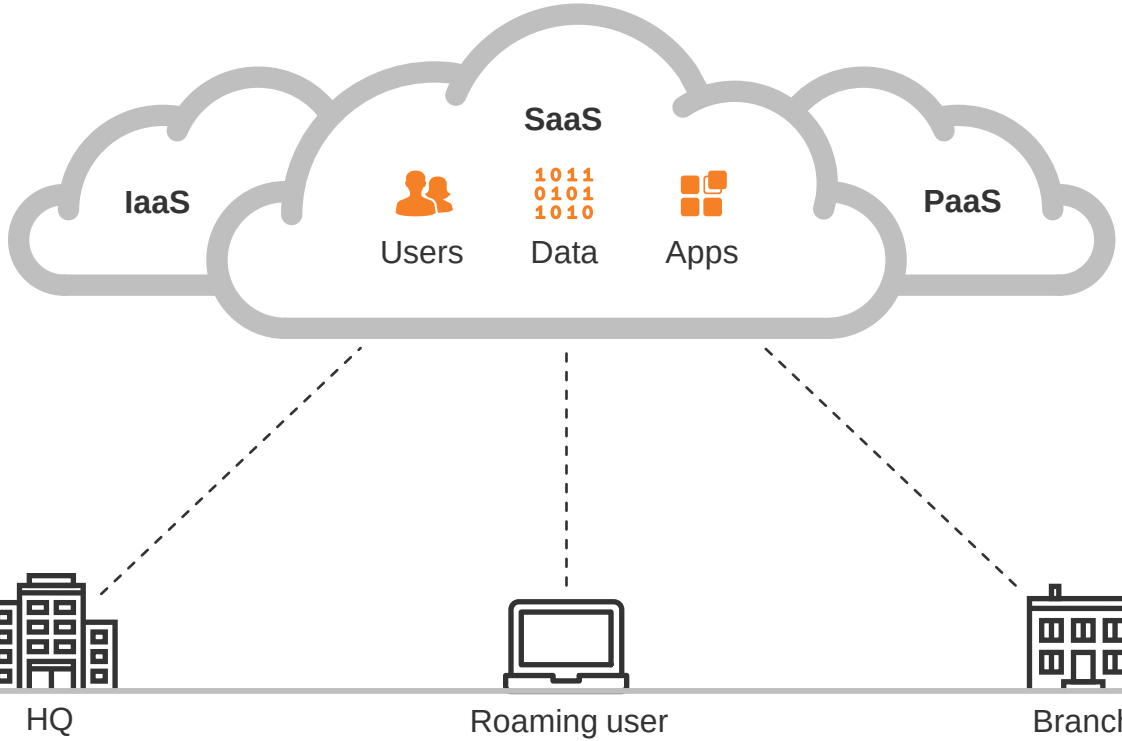
Malware and ransomware

Gaps in visibility and coverage

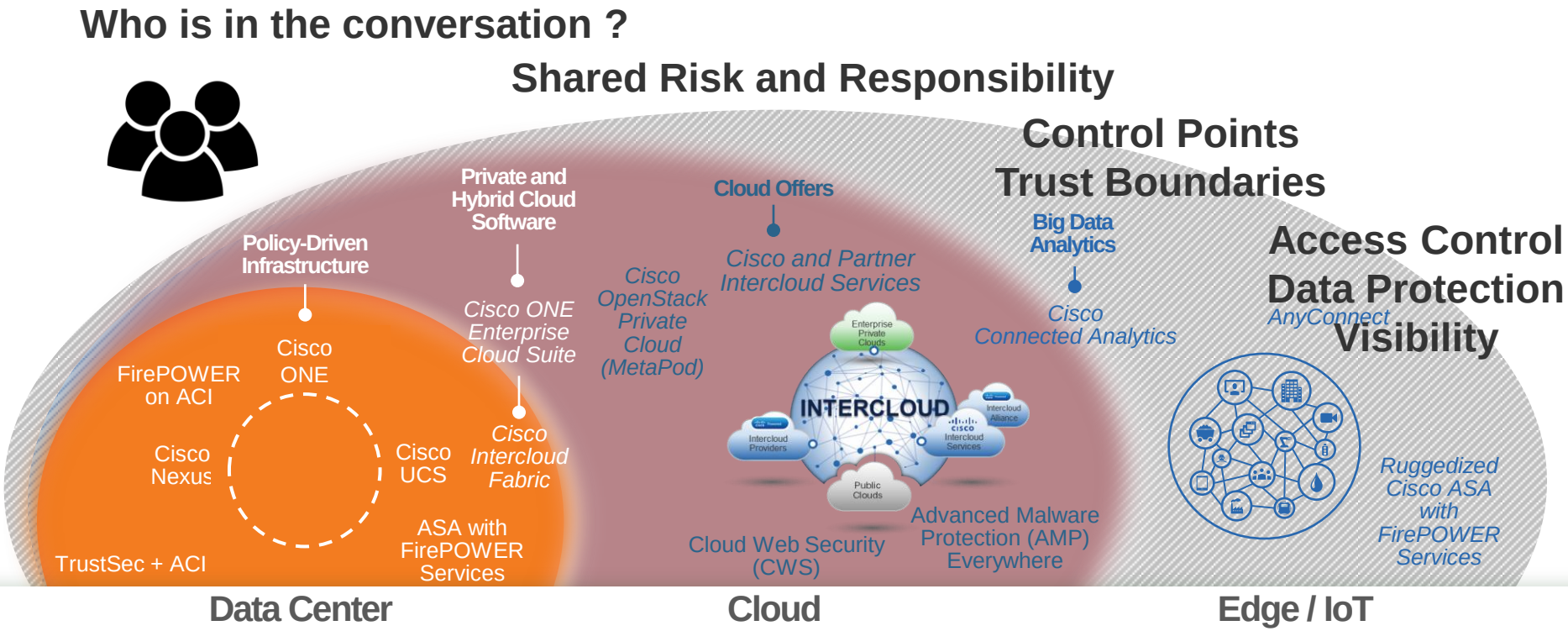
Compromised accounts and malicious insiders

Data breaches and compliance

# Security challenges have evolved



# 揭秘雲安全架構


Who is in the conversation ?
Shared Risk and Responsibility
Control Points
Trust Boundaries
Access Control
Data Protection
Visibility
Policy-Driven Infrastructure
Cisco ONE
FirePOWER on ACI
Cisco Nexus
Cisco UCS
TrustSec + ACI
Private and Hybrid Cloud Software
Cisco ONE Enterprise Cloud Suite
Cisco Intercloud Fabric
ASA with FirePOWER Services
Cisco OpenStack Private Cloud (MetaPod)
Cloud Offers
Cisco and Partner Intercloud Services
INTERCLOUD
Enterprise Private Clouds
Intercloud Providers
Intercloud Services
Intercloud Alliance
Public Clouds
Cloud Web Security (CWS)
Big Data Analytics
Cisco Connected Analytics
Advanced Malware Protection (AMP) Everywhere
AnyConnect
Ruggedized Cisco ASA with FirePOWER Services
Data Center
Cloud
Edge / IoT
Security Everywhere

# Who is in the conversation ?

CIO, CSO, CISO — enable digitization with cloud technologies while satisfying security, compliance, and financial control

Planners

Line of Business Managers — innovate faster; satisfy customer needs and gain better insight; and adapt in real-time

Pioneers/Settlers

IT Managers — get control of cloud, manage infrastructure and deliver new services

Planners/Settlers

Developers — freedom to innovate without asking permission, and use whatever they want, wherever they want, and when they want

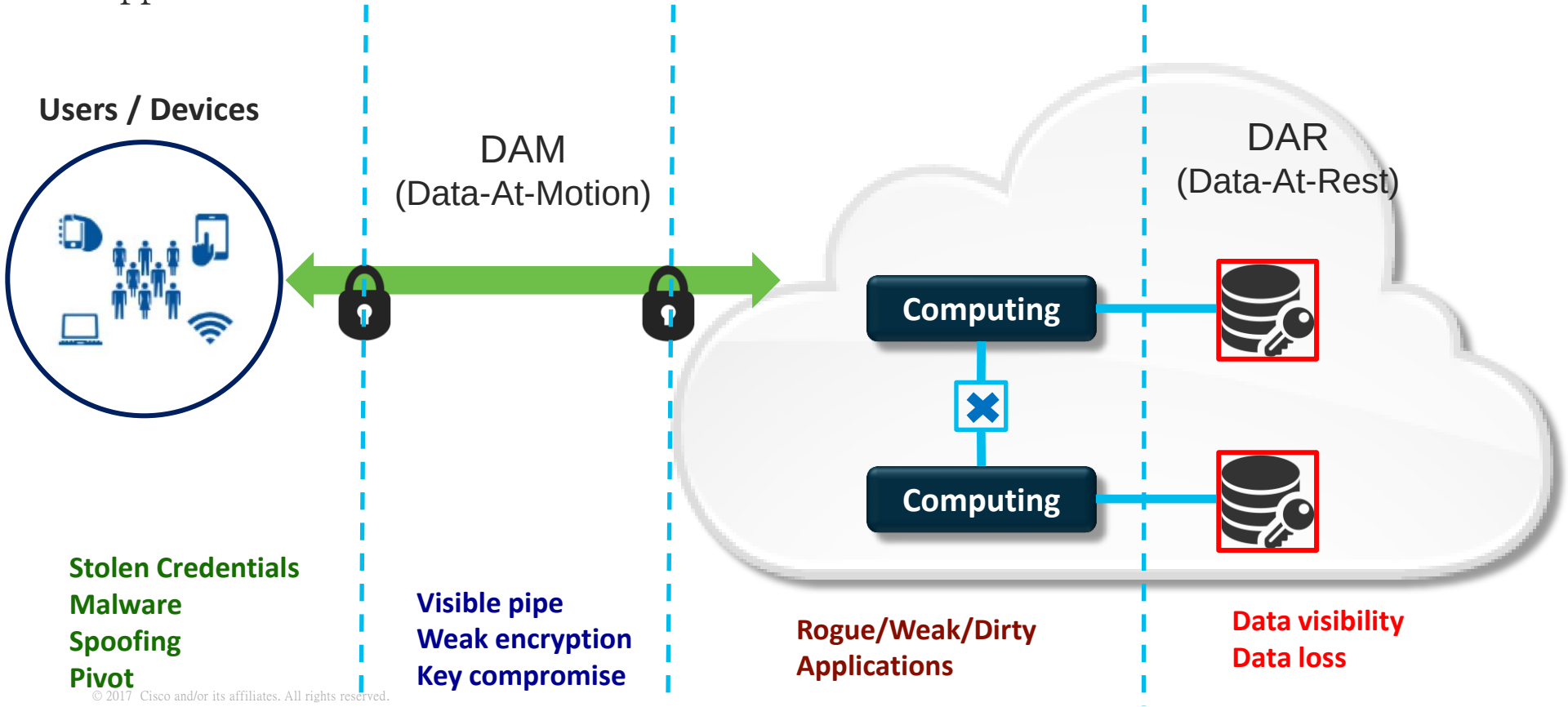
Pioneers

## Trust Boundaries

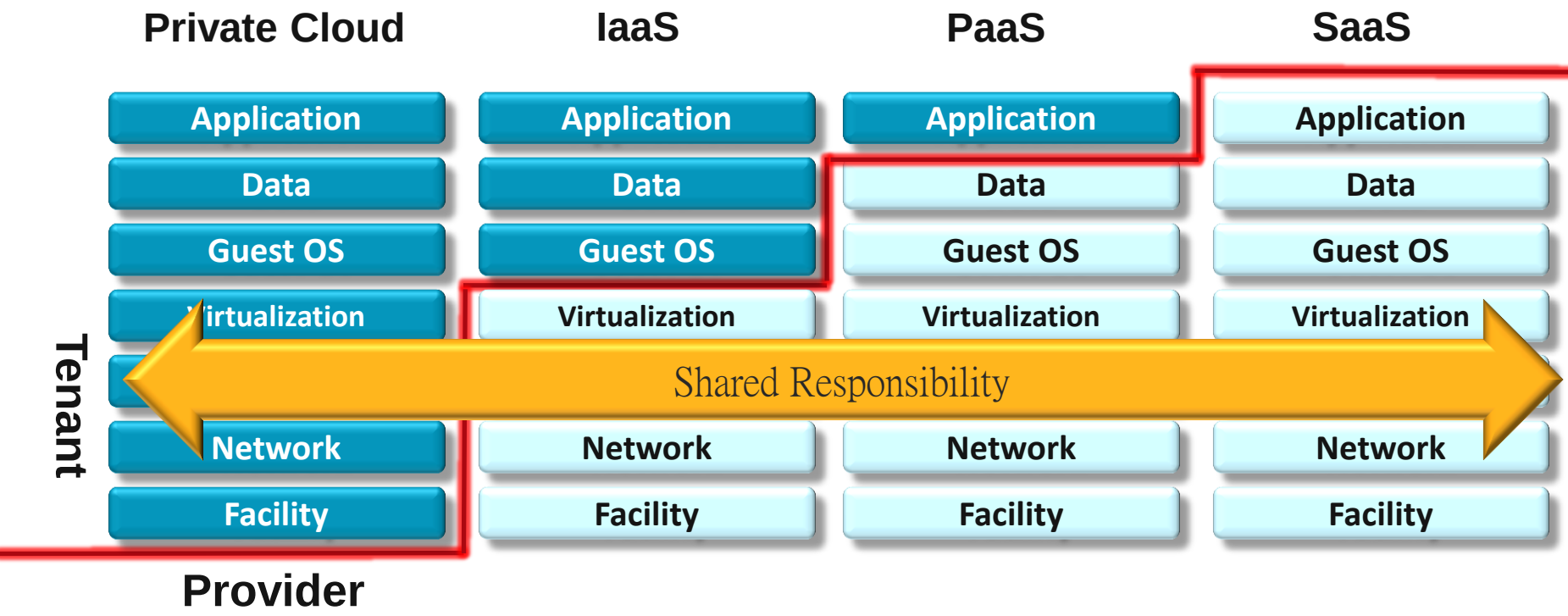
## Control Points

# Control Points / Trust Boundaries

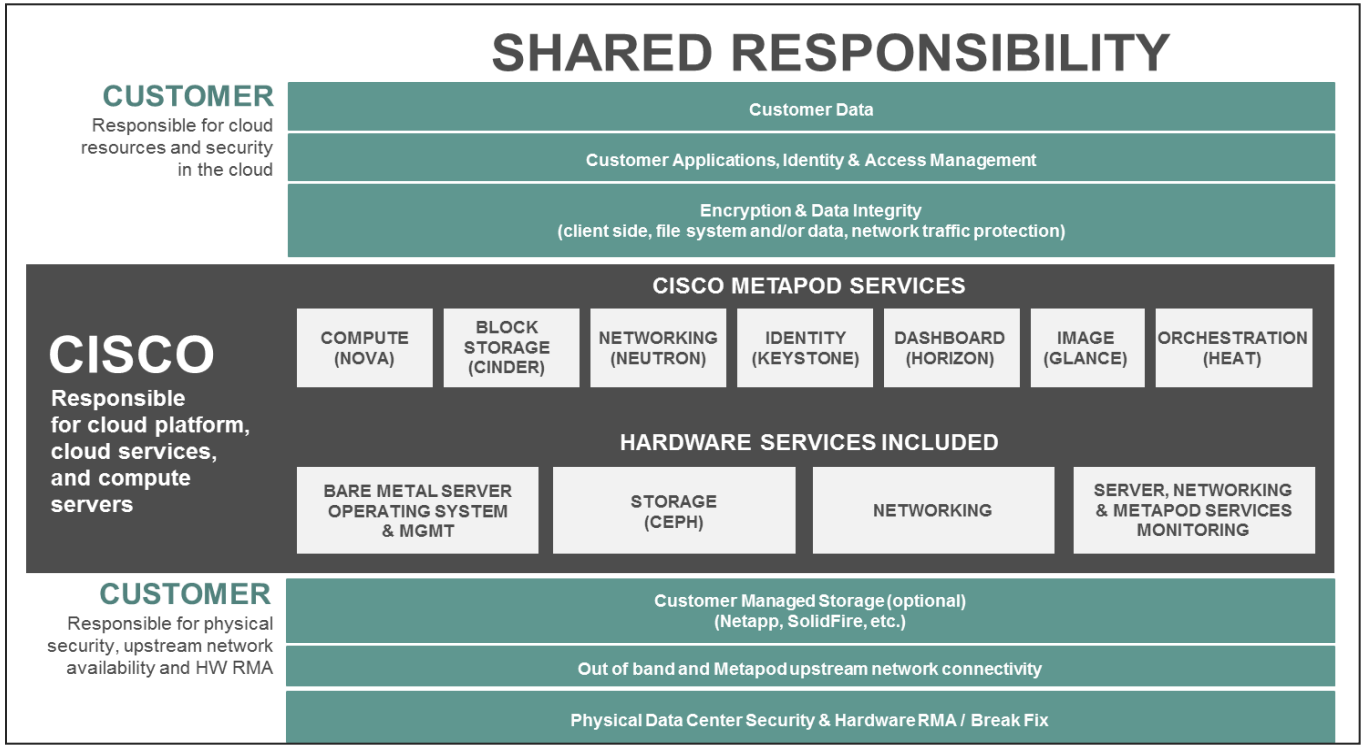
## Application/Data Protection



# Control Points / Trust Boundaries
## Cloud Delivery Models & Security



# Private Cloud – Metapod Shared Risk Model Example



# Who is in the conversation ?

CIO, CSO, CISO — enable digitization with cloud technologies while satisfying security, compliance, and financial control

Planners

Line of Business Managers — innovate faster; satisfy customer needs and gain better insight; and adapt in real-time

Pioneers/Settlers

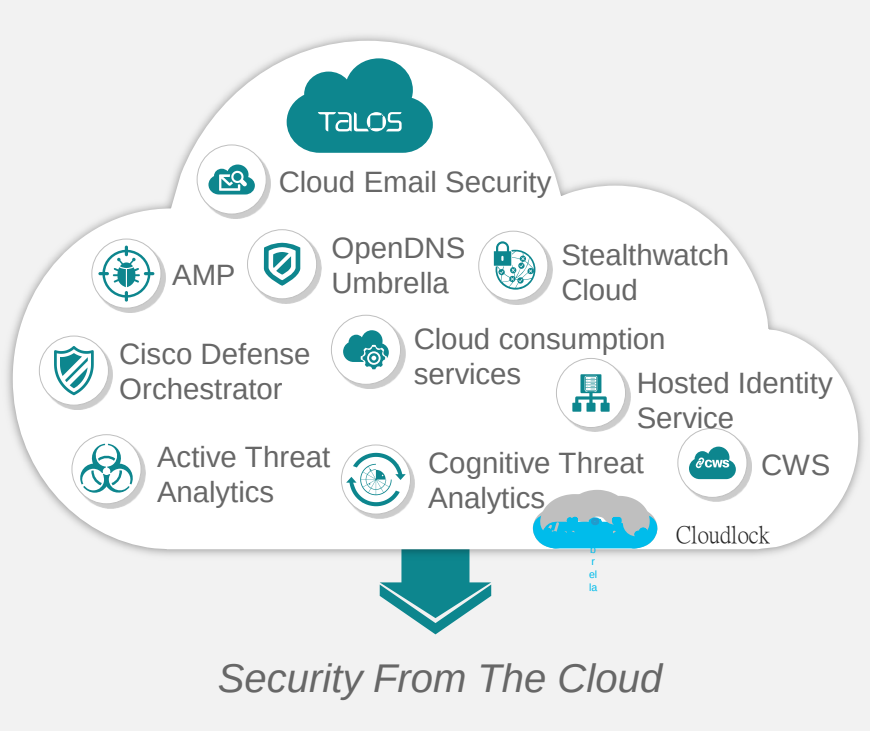
IT Managers — get control of cloud, manage infrastructure and deliver new services

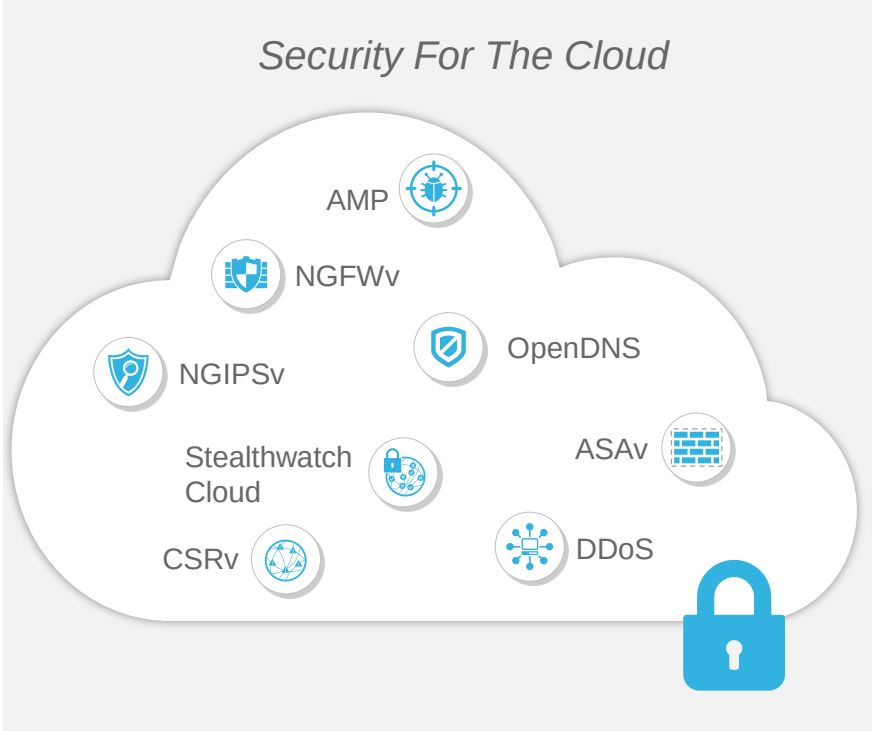
Planners/Settlers

Developers — freedom to innovate without asking permission, and use whatever they want, wherever they want, and when they want

Pioneers

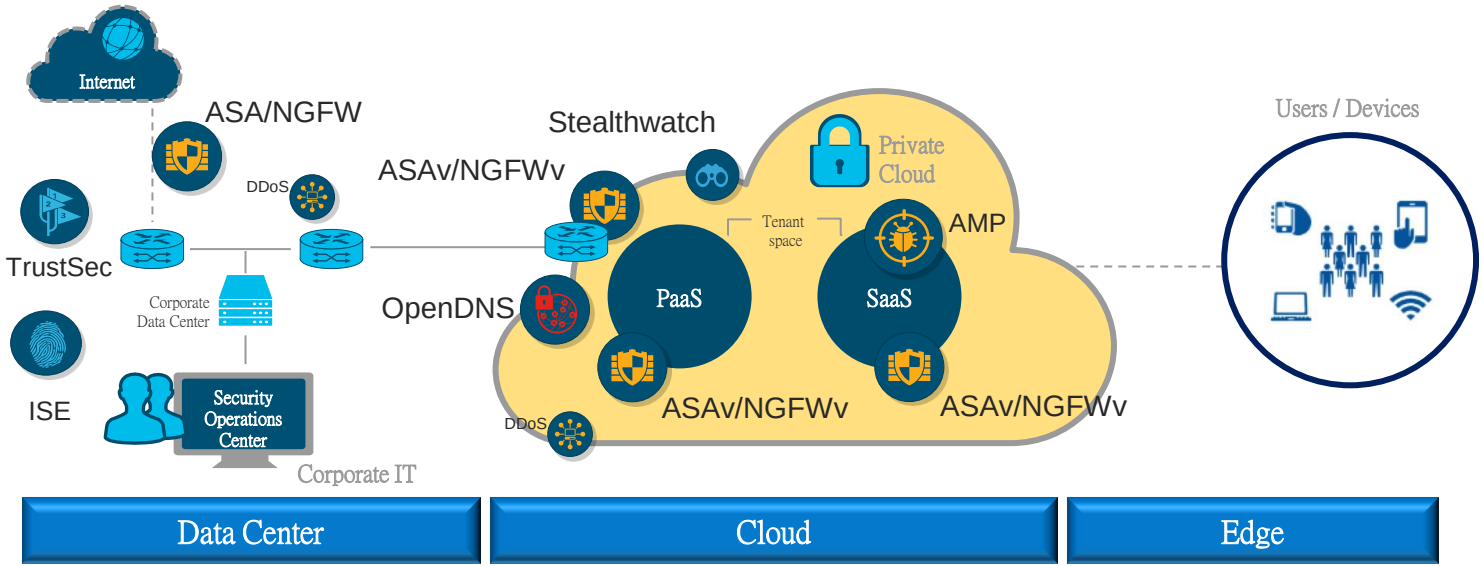
# Security "From The Cloud & For The Cloud"



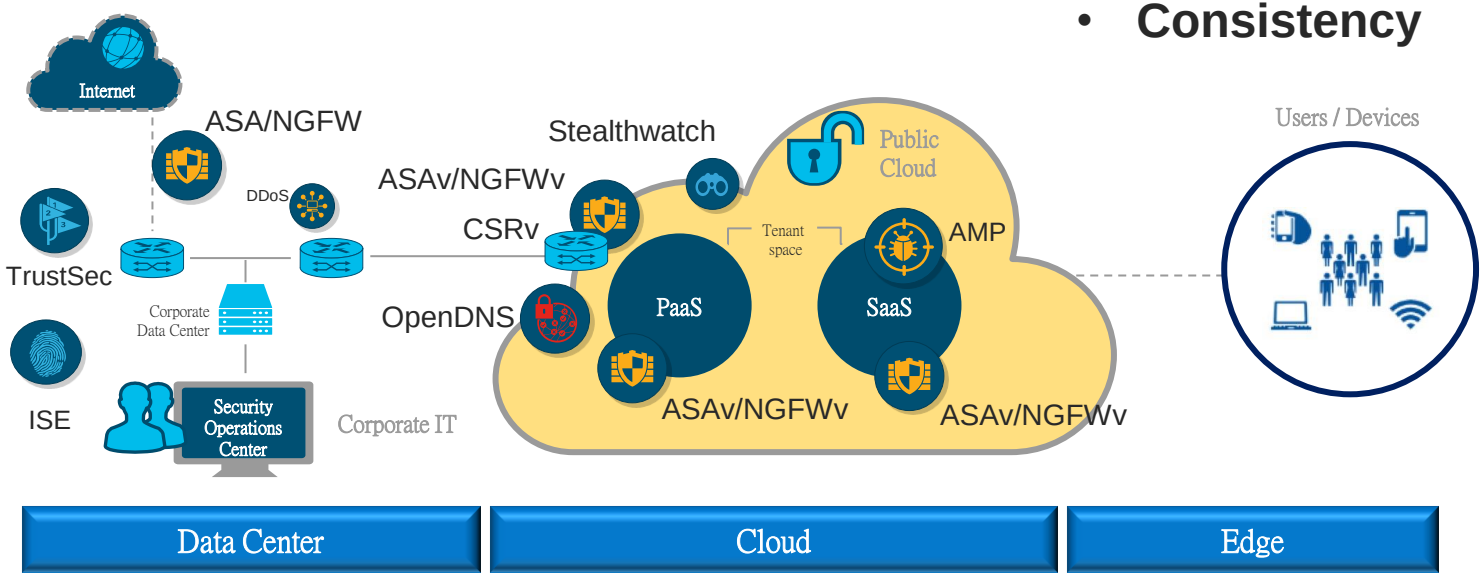
# Private Clouds

- Visibility
- Policy/Compliance
- Control
- Data Protection
- **Shared Risk Model (Managed)**



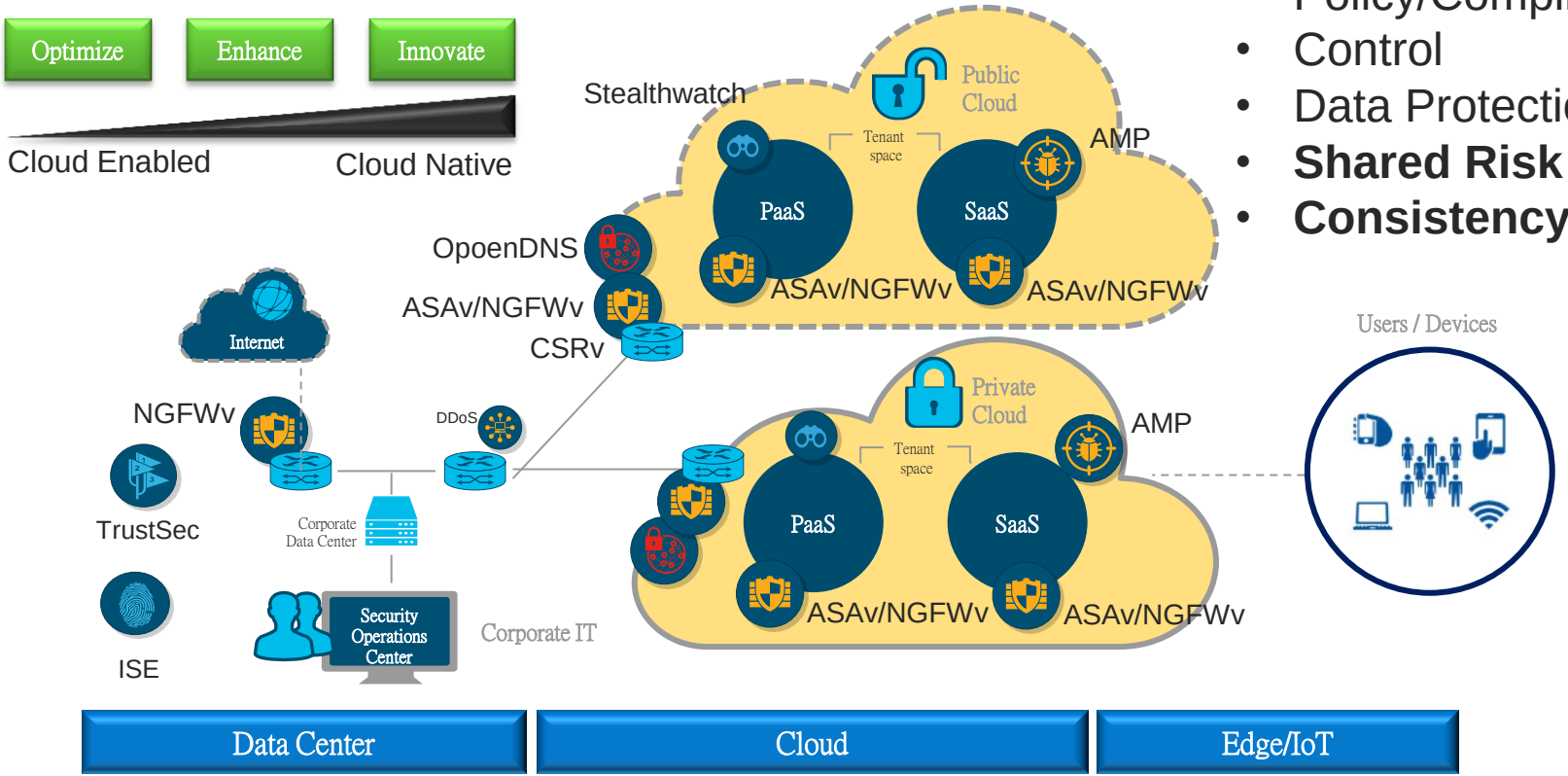
# Public Clouds

- Visibility
- Policy/Compliance
- Control
- Data Protection
- **Shared Risk Model**
- **Consistency**

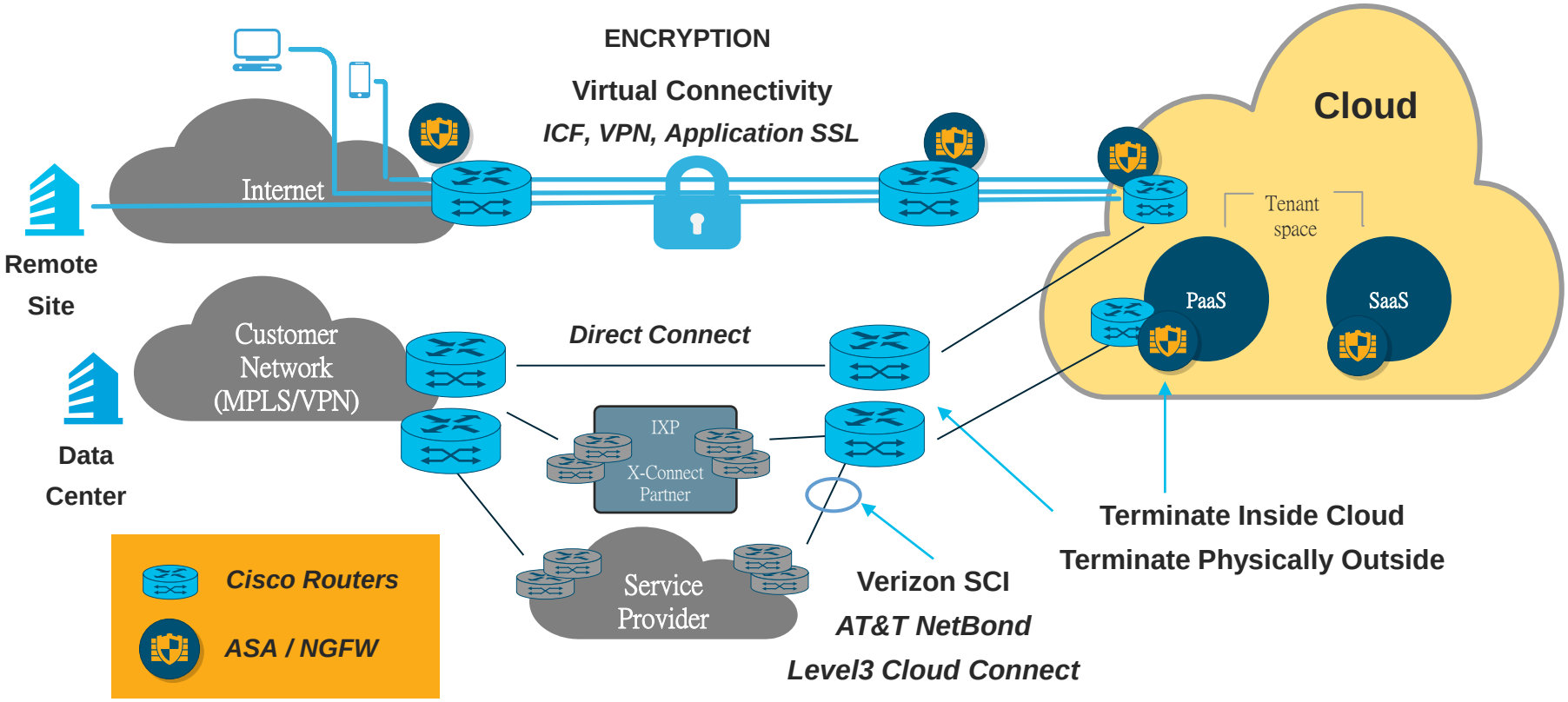


# Hybrid Clouds

- Visibility
- Policy/Compliance
- Control
- Data Protection
- **Shared Risk Model**
- **Consistency**



# Securing the Connectivity to Cloud Platform



# Cisco Security Solutions

## Cloud Service Router

- Built in Security and Application Aware
- Highly secure VPN gateway
- Comprehensive WAN Functionality

## Next-Gen IPS (FirePower)

- Real-time contextual awareness
- Full-stack visibility
- Intelligent security automation

## Next-Gen Firewall (ASA>FTD)

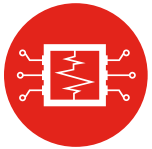
- Prioritizes threats
- Automates response
- Improved malware protection
- Fully integrated management

## AMP

- See a threat once, block it everywhere
- Most effective solution for known and emerging advanced threats

## OpenDNS

- Security from the cloud
- Blocks 95% of threats before they cause damage

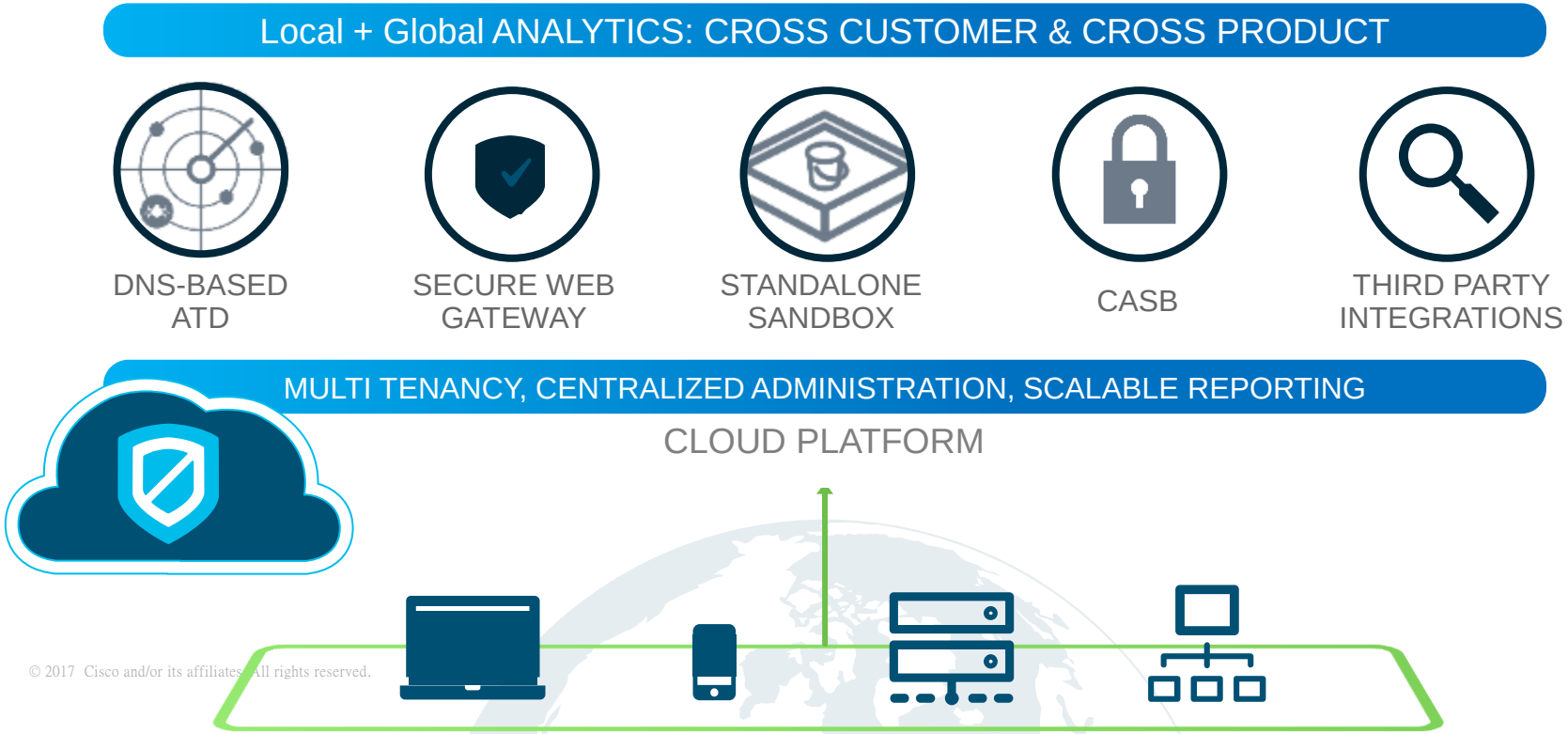


## Stealthwatch

- Alerts attempted communication with an infected host
- Prevents infected host from communication within the network
- Uses Network as a Sensor to contain and minimize threats

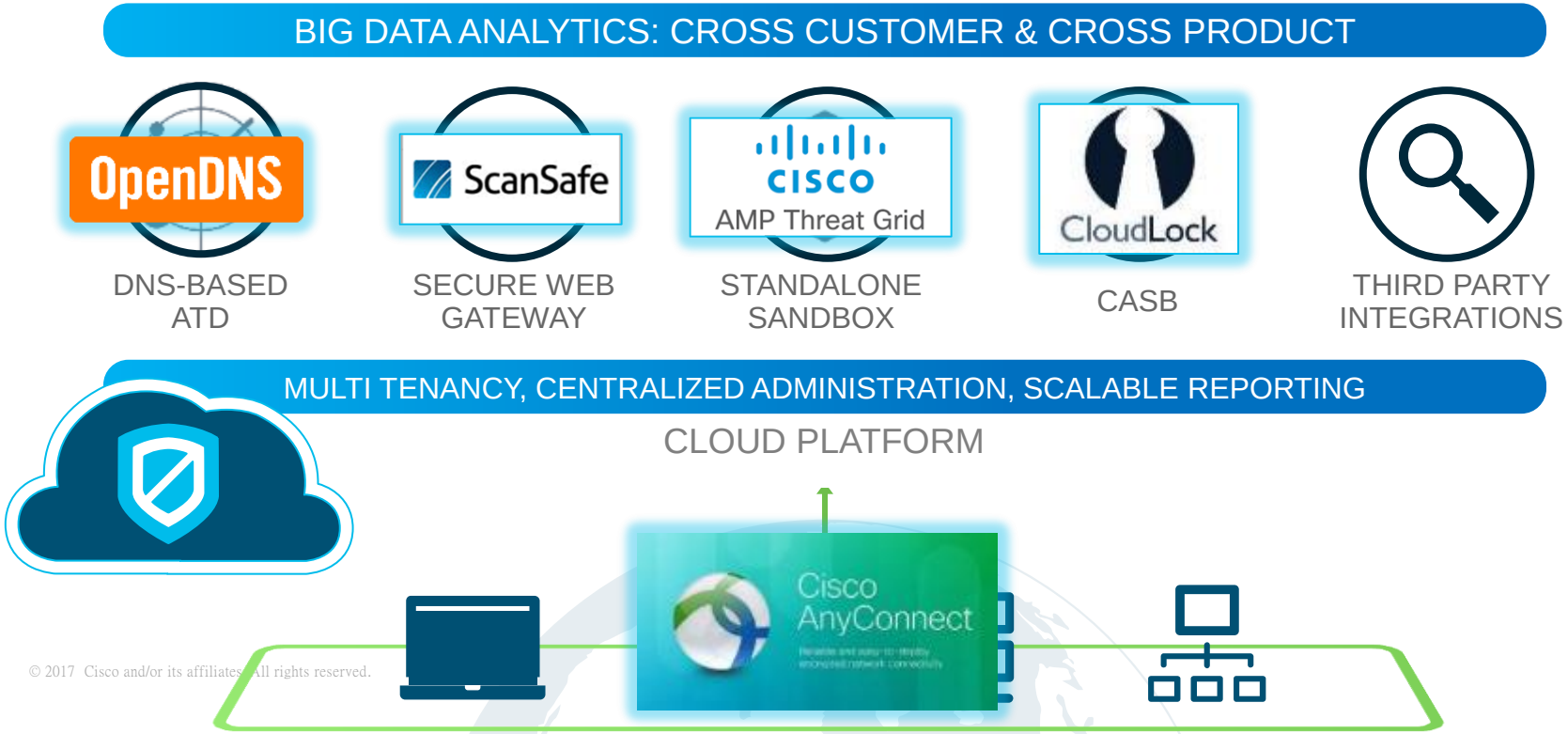
# Building a new Cloud Security Platform

Rebuilding the perimeter with next generation, multi-service, cloud platform…



# Building a new Cloud Security Platform

Rebuilding the perimeter with next generation, multi-service, cloud platform…



# Who is in the conversation ?

CIO, CSO, CISO — enable digitization with cloud technologies while satisfying security, compliance, and financial control

Planners

Line of Business Managers — innovate faster; satisfy customer needs and gain better insight; and adapt in real-time

Pioneers/Settlers

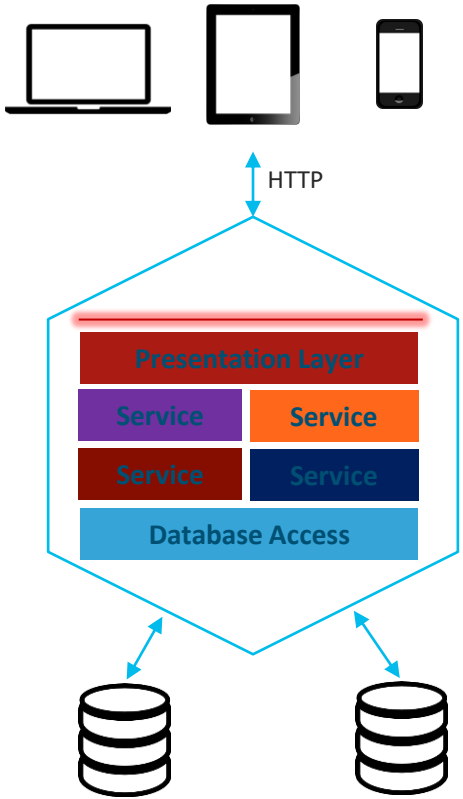
IT Managers — get control of cloud, manage infrastructure and deliver new services

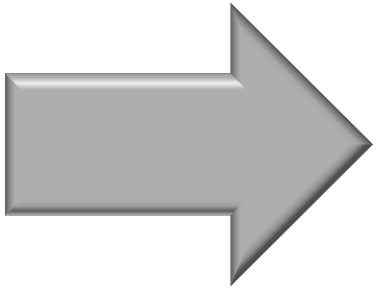
Planners/Settlers

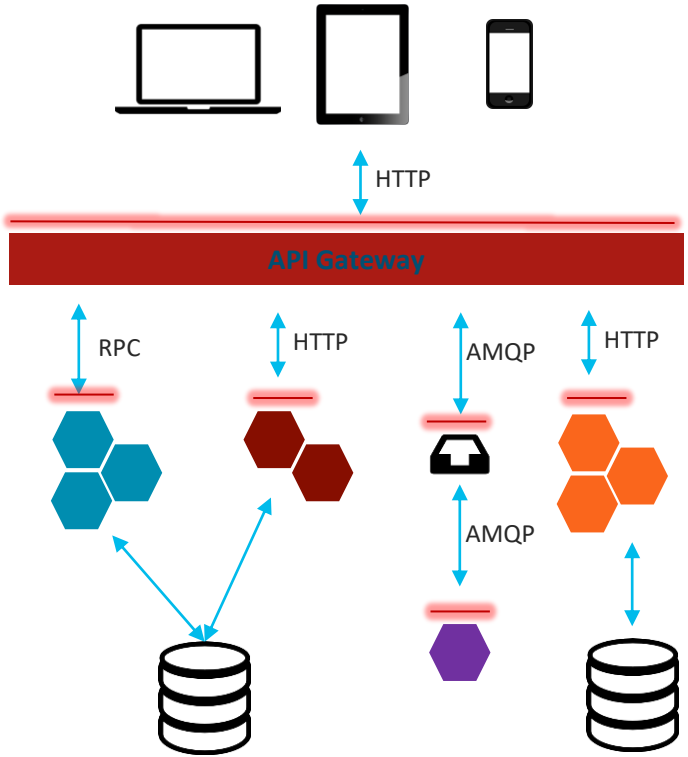
Developers — freedom to innovate without asking permission, and use whatever they want, wherever they want, and when they want

Pioneers

# Application Architecture Evolution



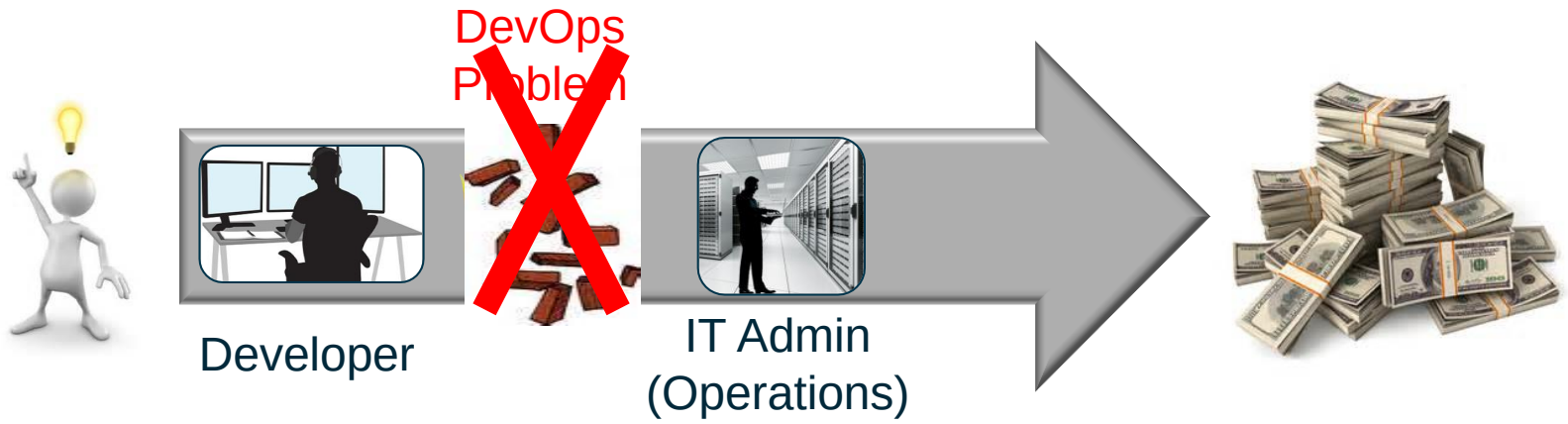





***Monolith***

***Microservice***

# Why Developer and DevOps Love Cloud?





**But what about Security and Compliance**

# Securing the Application Development Lifecycle

- Provide **Security-as-a-Service** within Cloud Models
- IaaS/PaaS clouds must be **Self-Defending** with **Highly Automated** controls like…

**Dynamic Network Access Control**

**Config/Package Security**

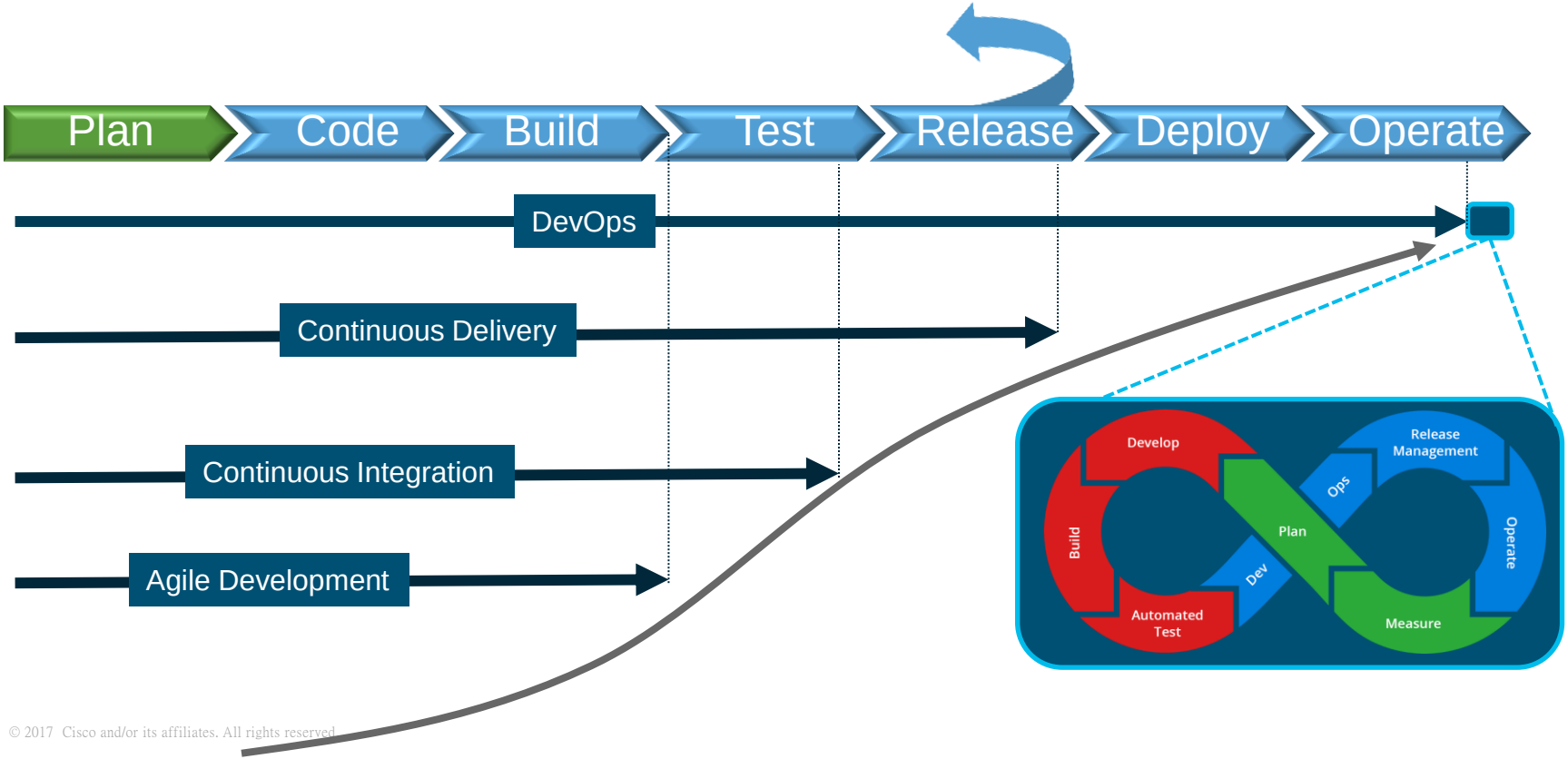
**Visibility / Control**

**Threat / Alerting**

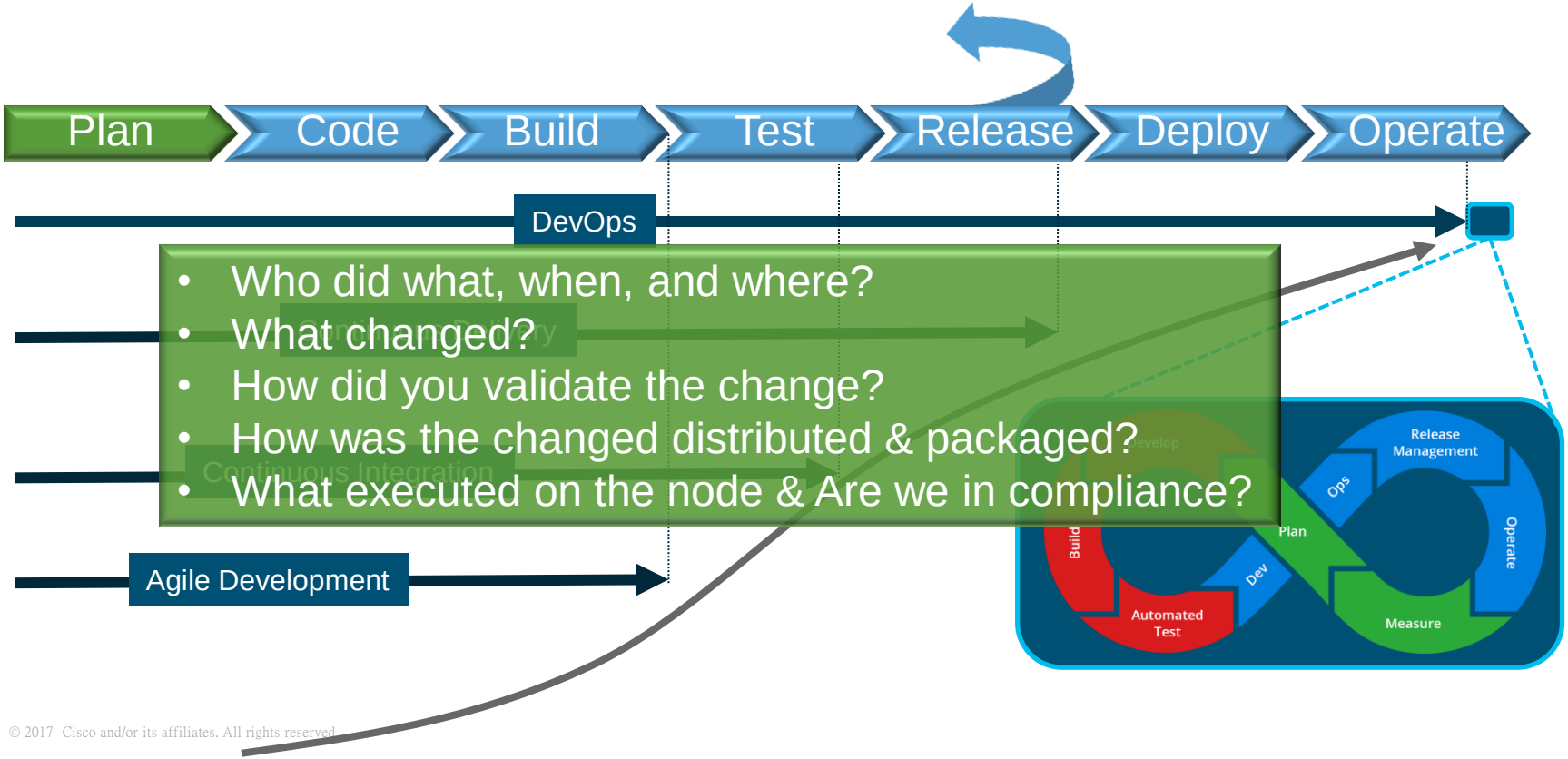
**Forensics / Analytics**

**Integration/Automation**

# Securing the Application Development Lifecycle

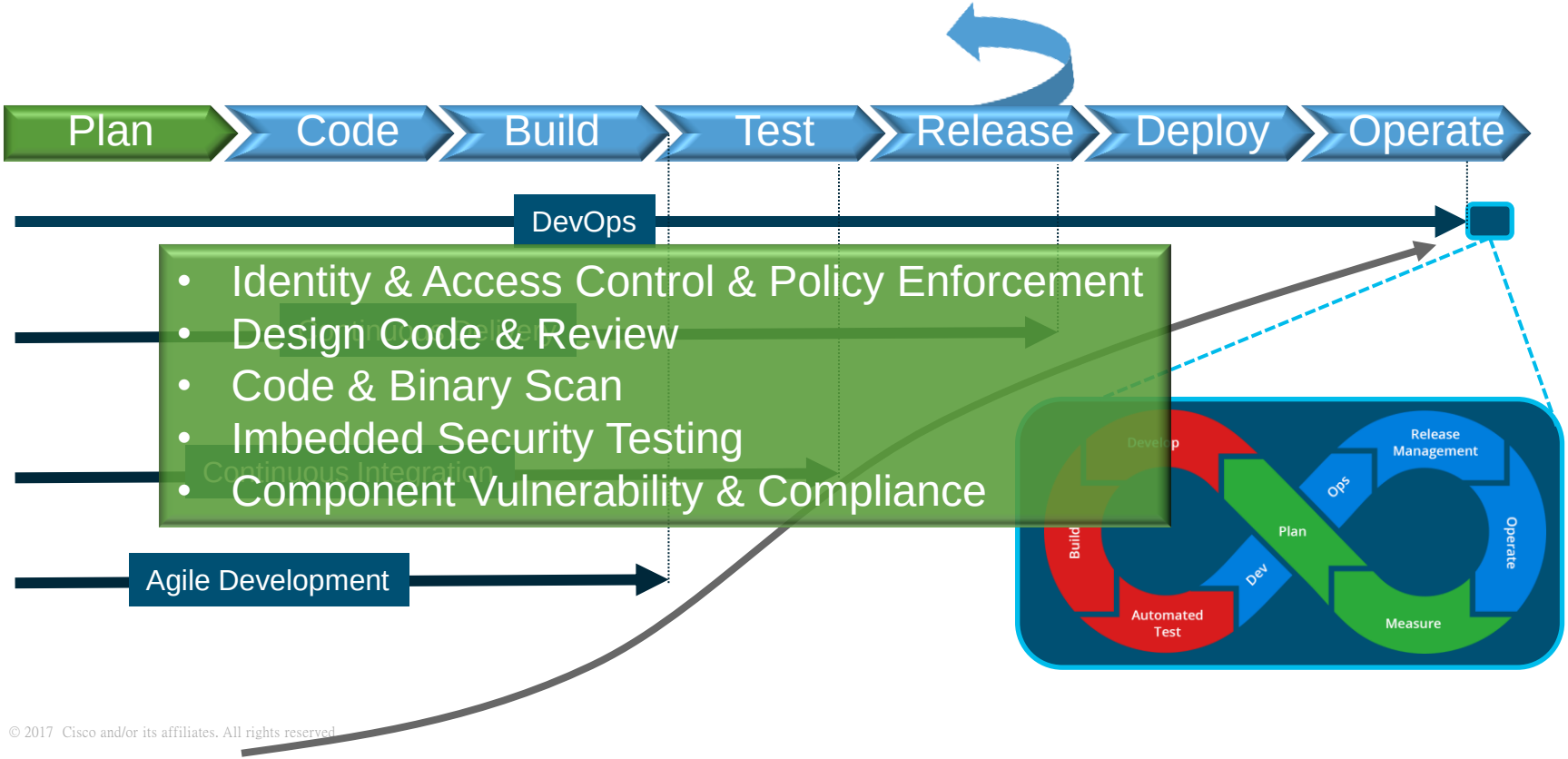


# Securing the Application Development Lifecycle



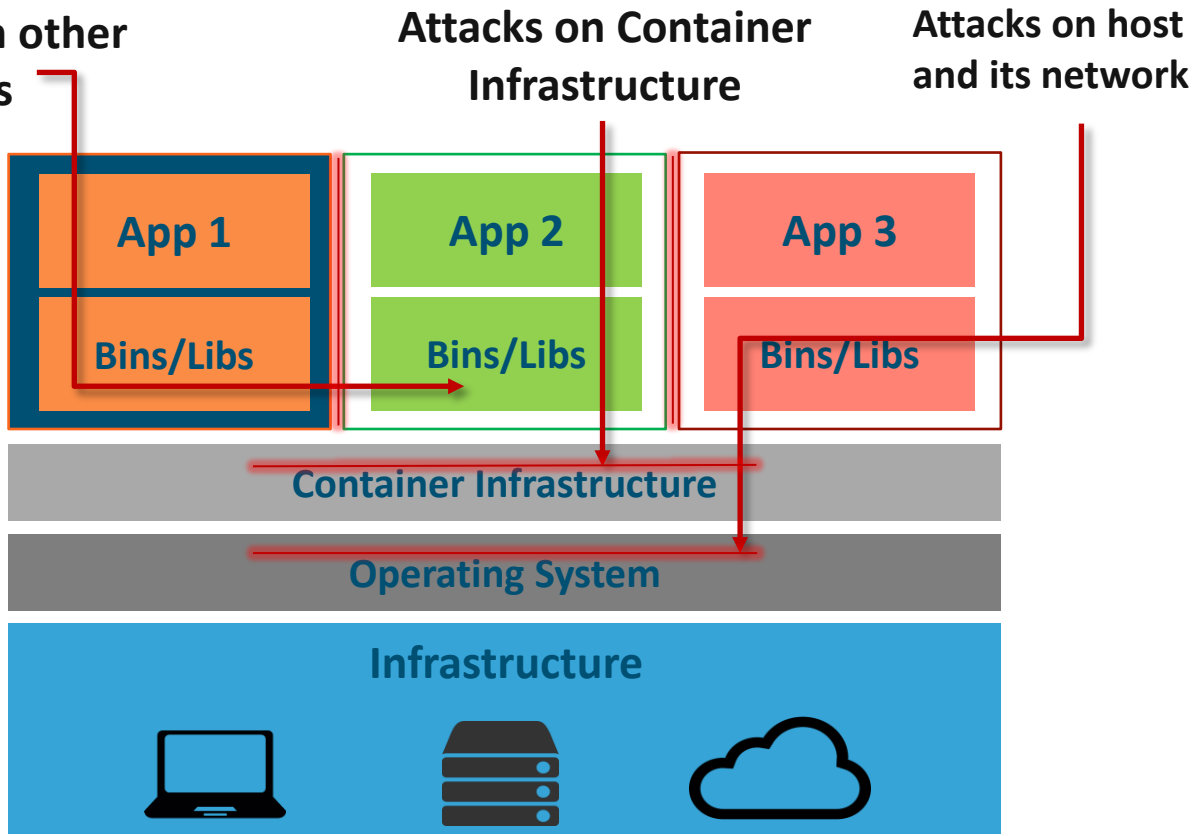

- Who did what, when, and where?
- What changed?
- How did you validate the change?
- How was the changed distributed & packaged?
- What executed on the node & Are we in compliance?

# Securing the Application Development Lifecycle

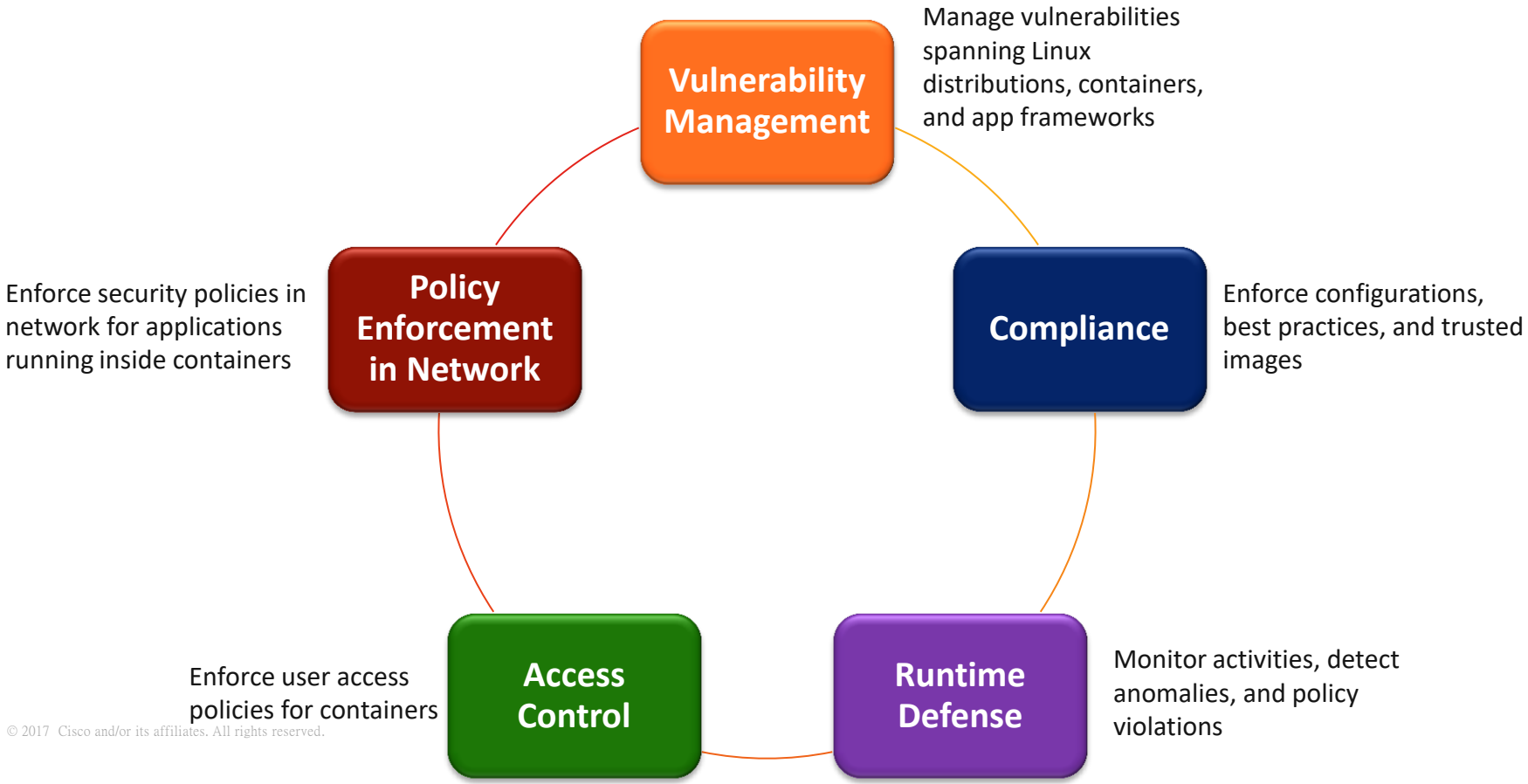


# Container Threats

- Kernel Exploits
- DOS Attacks
- Container breakouts
- Poisoned images
- Compromising secrets

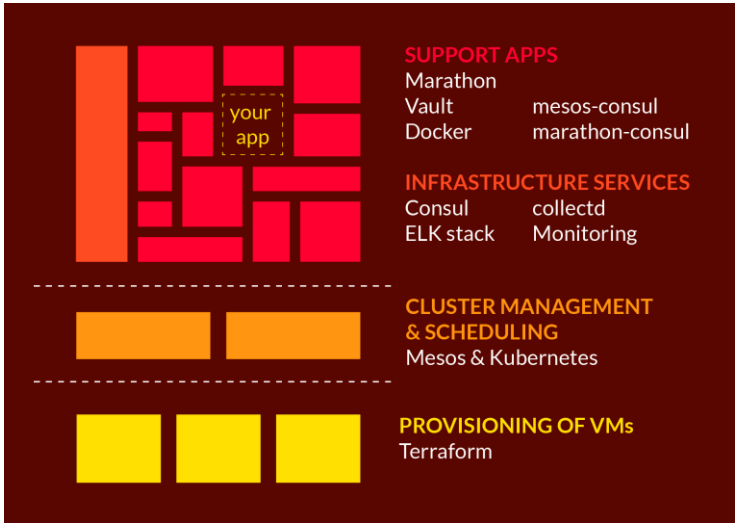


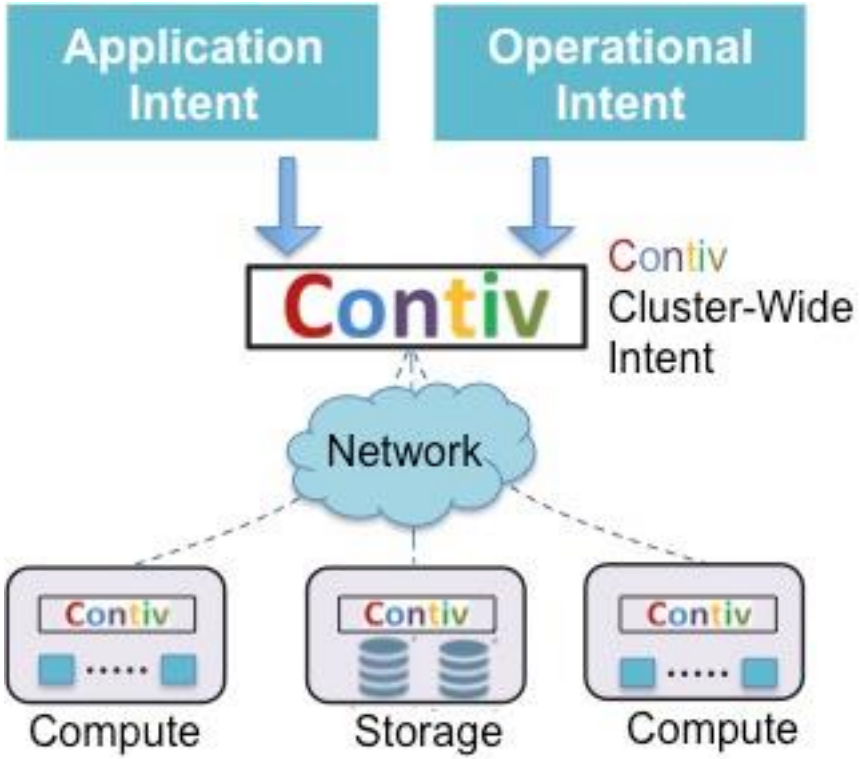
# Essential Steps to Secure Containers



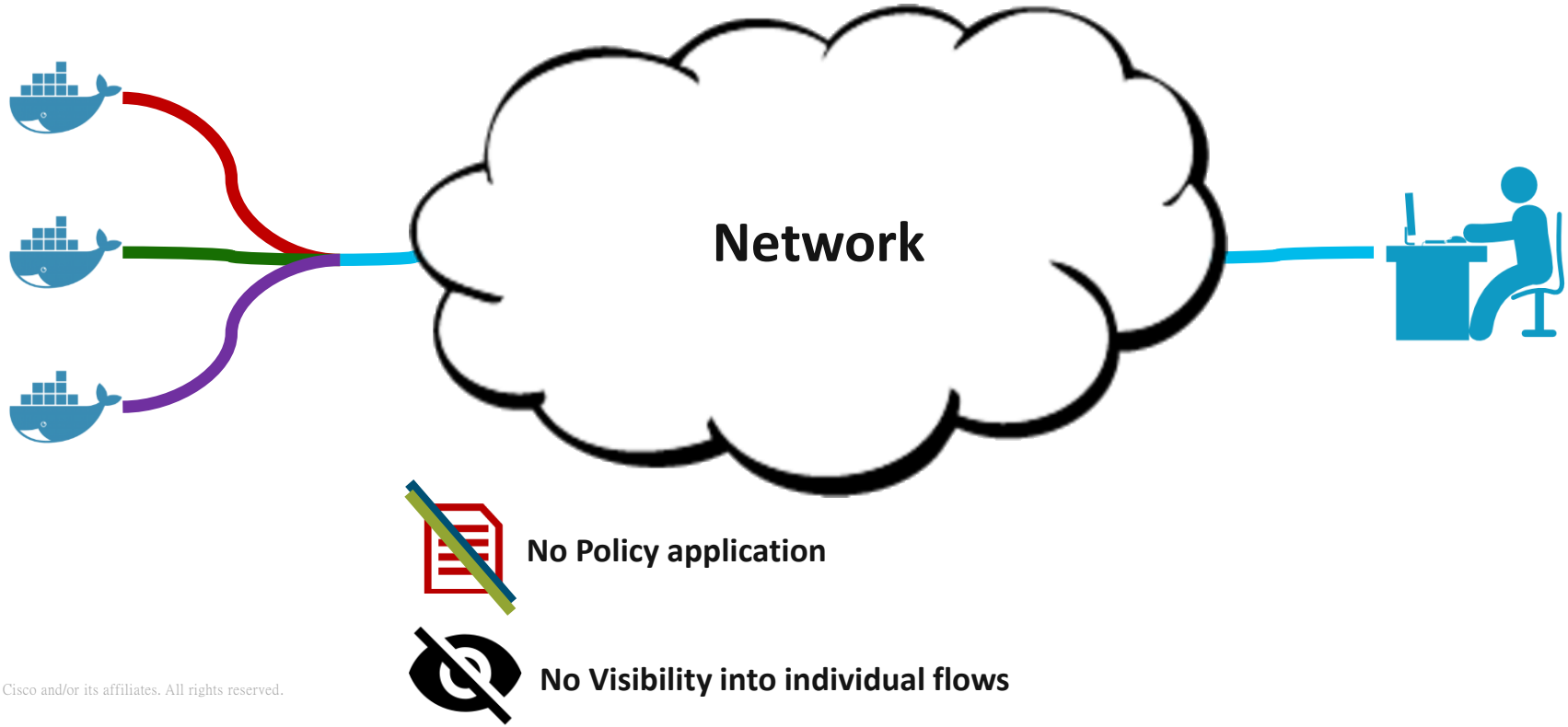
# Microservice Infrastructure Solutions

MANTL



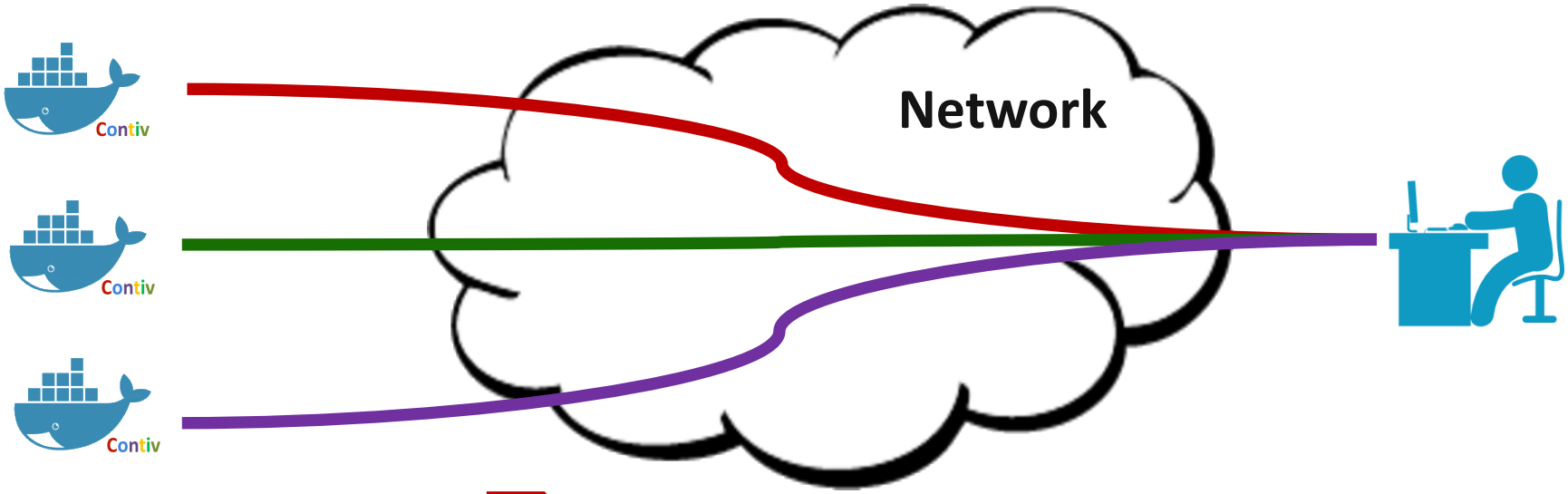



# Network Visibility for Container Workloads



# Network Visibility with Cisco

Contiv




Group Based Policy

Visibility into individual flows

# Cisco Cloud Compliance (REFERENCE)

European Court of Justice's Decision Regarding EU-US Safe Harbor

Cloud Security: Trust Cisco to Protect Your Data Whitepaper

Cloud Security: Trust Cisco to Protect Your Data At-a-Glance

Cisco End User Licensing and Cloud Terms

Cisco Metapod - Secure the Private Cloud

Cisco Metapod Service Description

Cisco Cloud Services EU DPA

Cloud Acceptable Use Policy

# Public Cloud Compliance and Certifications **(REFERENCE)**

- AWS Compliance
- Microsoft Azure Compliance
- Google Compliance
- IBM SoftLayer Compliance

# Compliance and Certifications **(REFERENCE)**

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- SSAE 16 / SOC1 / SOC2
- Payment Card Industry (PCI) Data Security Standard (DSS)
- Cloud Security Alliance
- DMTF Cloud Audit Data Federation (CADF)
- HIPAA

# Q & A

# Thank You


CISCO