Securing the business in the digital era

Sujata Ramamoorthy
Director, Cloud Platform Security
September 14, 2017

Agenda


The digital world

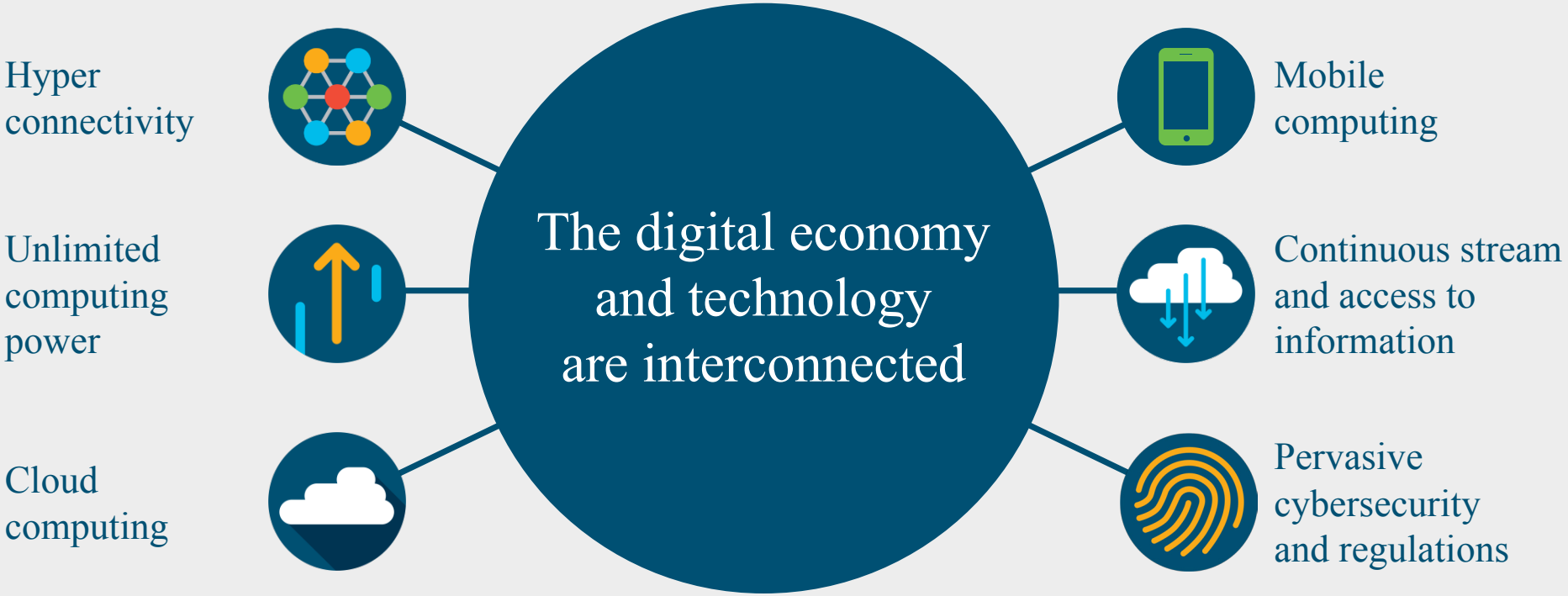

Security landscape


Cloud trends and challenges


Cisco practices – Cloud, data and threats


Summary

An irreversible digital economy



Source: IDC 2016

Fitness going digital
from active wear to digital coaching

Living in the cloud
Companies today are born digital

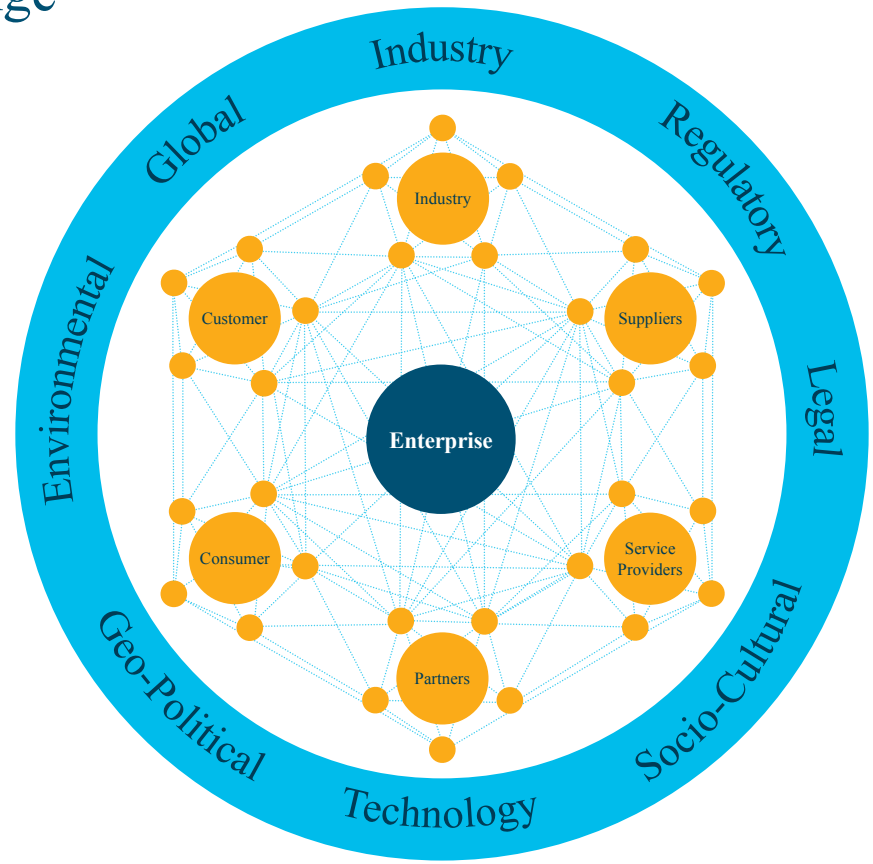
Taxi

Retail store

Music

The global digital economy has come of age

An era of rapid change



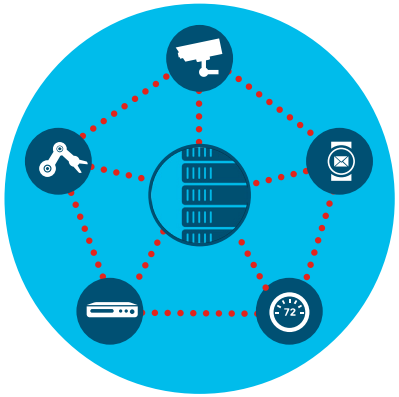
Source: Price Waterhouse Coopers

Threat landscape

Exploit kits fade into the shadows

Adversaries focus on other attacks

Exploit Kits



DDoS

Email

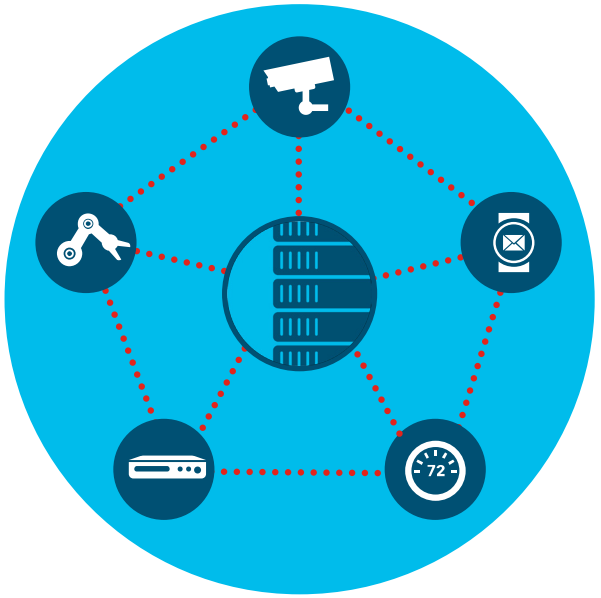
Ransomware

Exploit Kits

DDoS

Botnets compete to control IoT and have the ability to clog up the Internet

- IoT DDoS attacks propelled us into the 1TBps DDoS era
- Set up can be completed within an hour
- Distribution is rapid. Perpetrators can have a botnet of 100,000+ infected devices in 24 hours
- The malware has a low detection rate.
  It is very difficult to retrieve samples because the malicious code lives in the device's memory and is wiped out once the device is restarted



Source: Radware

Business email compromise

Social engineering problem that could be bigger than ransomware

Ransomware

Business email compromise

Source: Flashpoint

Emerging ransomware tactics

- Using ransomware codebases to their advantage
- Ransomware-as-a-Service (RaaS) platforms are growing fast
- Ransom Denial of Service (RDoS)

Dark cloud

As cloud systems become more leveraged in the organizations, it also presents a new level of risk for security teams

Organizations

- Cloud apps expand rapidly in organizations
- Millions of employees leverage cloud apps
- The app risk levels are rising
- OAuth grants access to organization backbone
- Excessive number of privileged users
- Percentage of DevOps servers left wide open are creating a huge ransomware risk

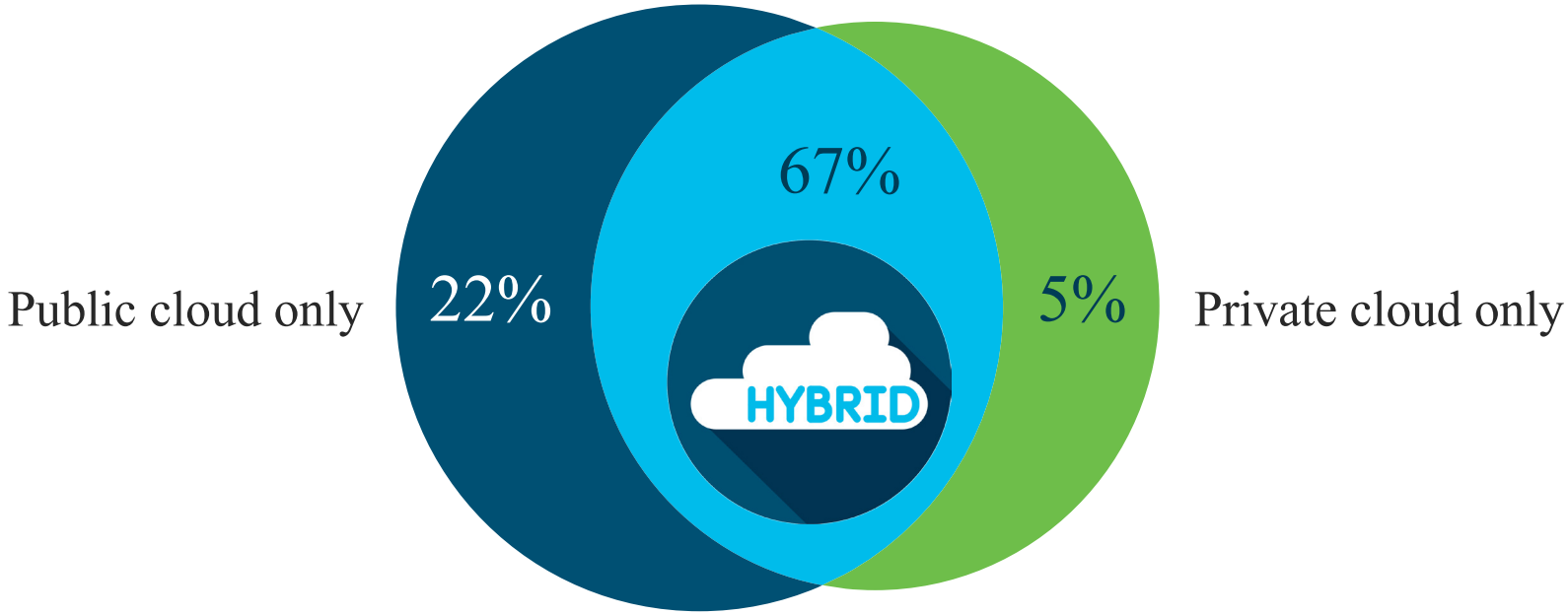
Adversaries

- Target privileged users to steal credentials
- Access to the entire network
- Leverage previously breached credentials

Cloud trends

The trend toward cloud

95% of Respondents are using cloud

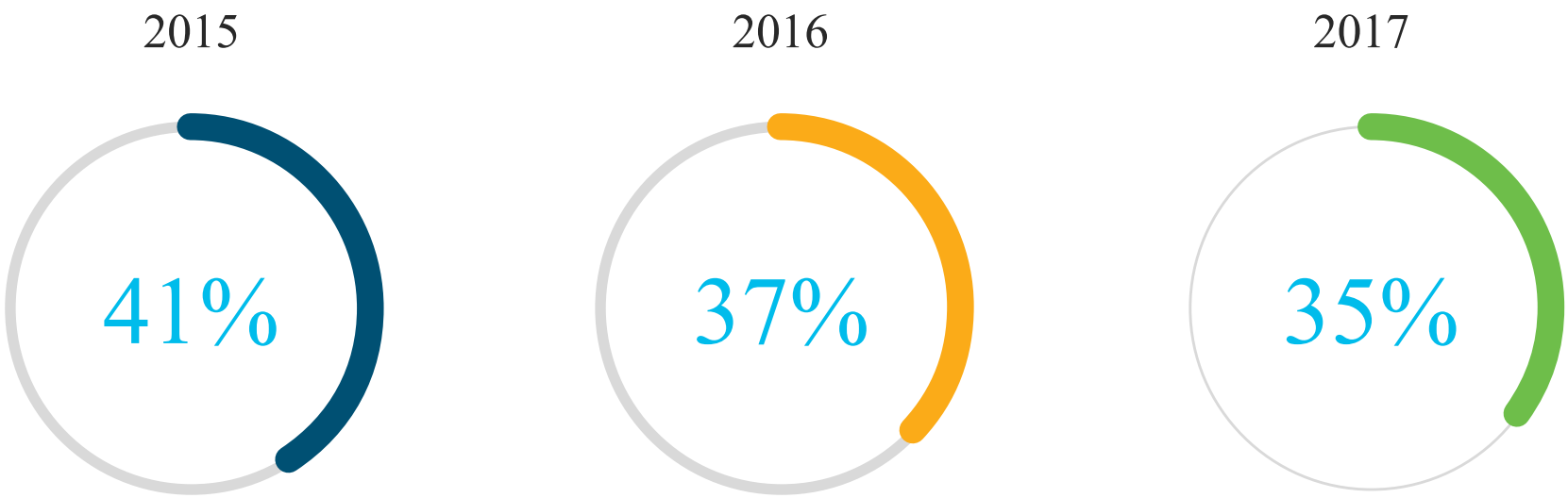


Public= 89%

Private = 72%

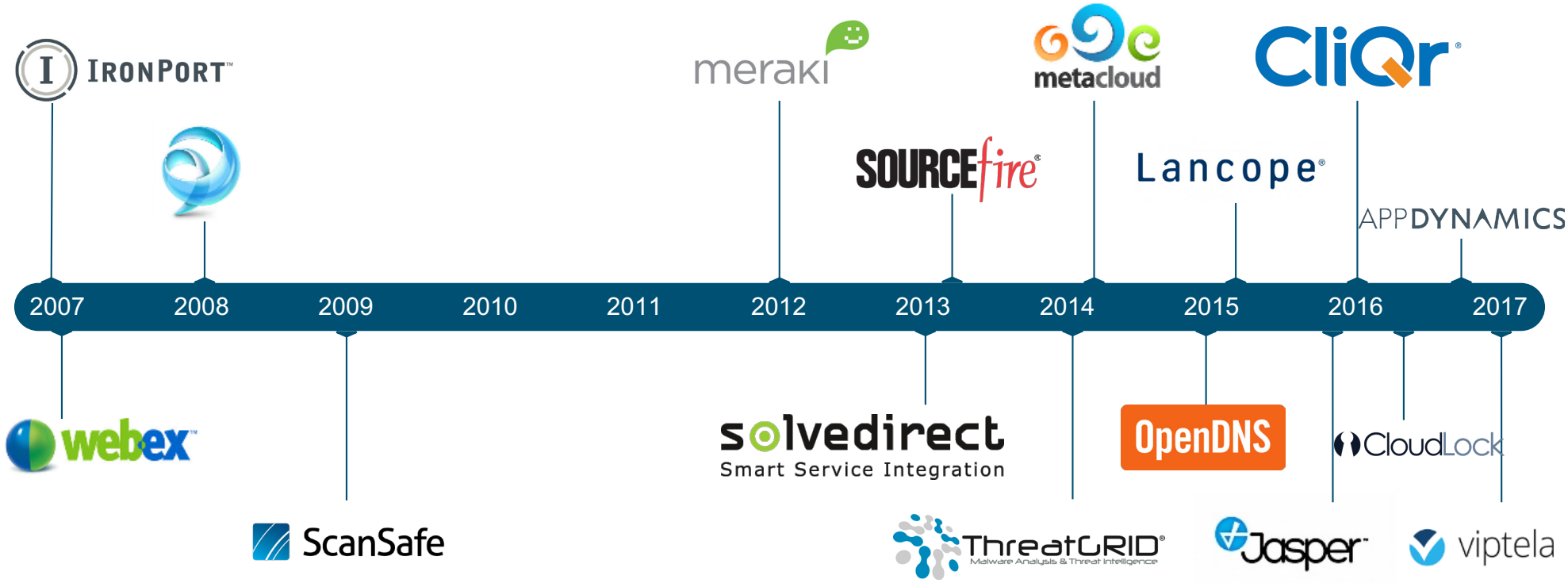
Source: RightSca/e 2017 State of the Cloud Report

Enterprises rating cloud security as a significant challenge



Source: RightSca/e 2017 State of the Cloud Report

Cisco's growing cloud presence



Digitization fundamentally changes security landscape

Speed of business

New richer targets

Emergence of cybercrime as-a-service

Increased impact/loss

Cisco Security practices

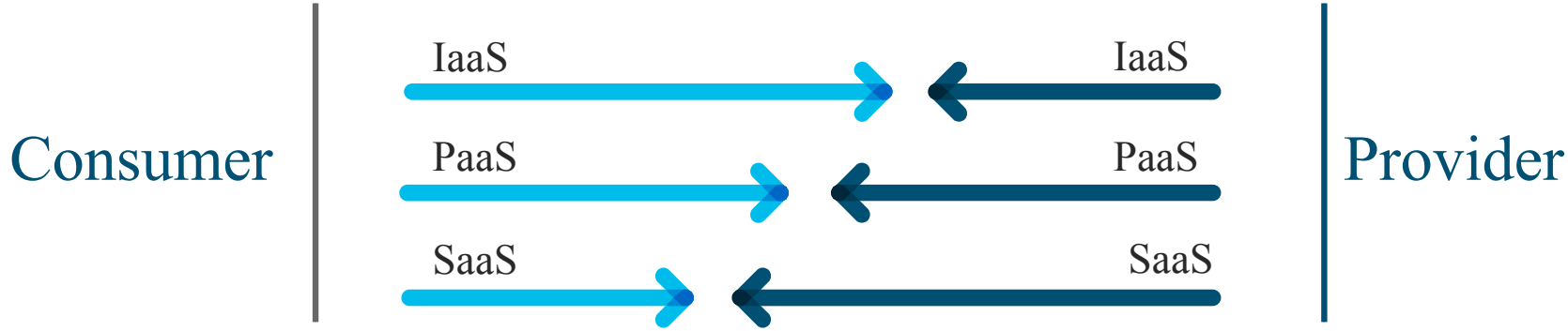
Cloud

Data

Threat detection/ containment

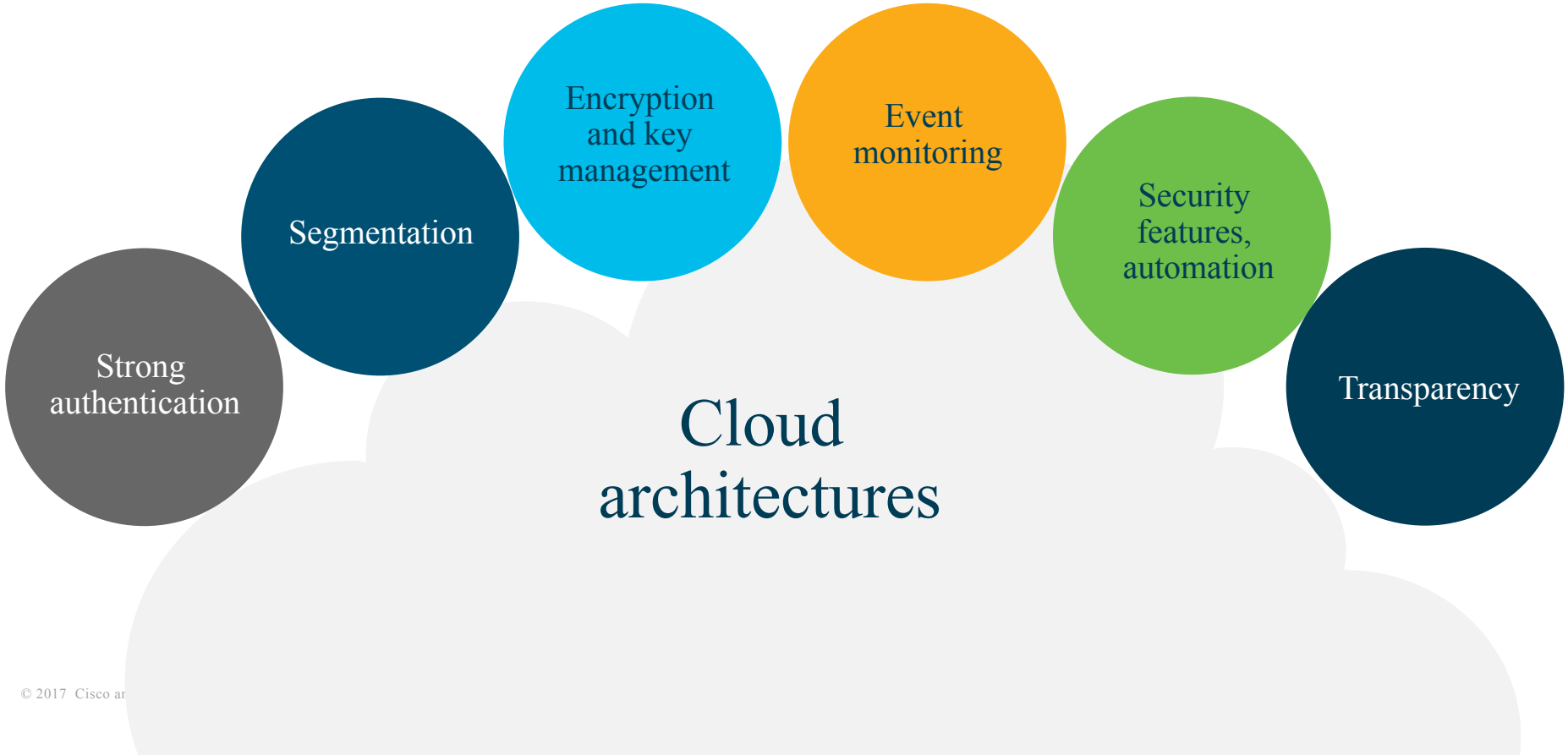
Cloud Security

Security responsibilities
Cloud providers vs. consumers



What is the providers role?

Cloud security models will leverage…



What is the consumer's role?

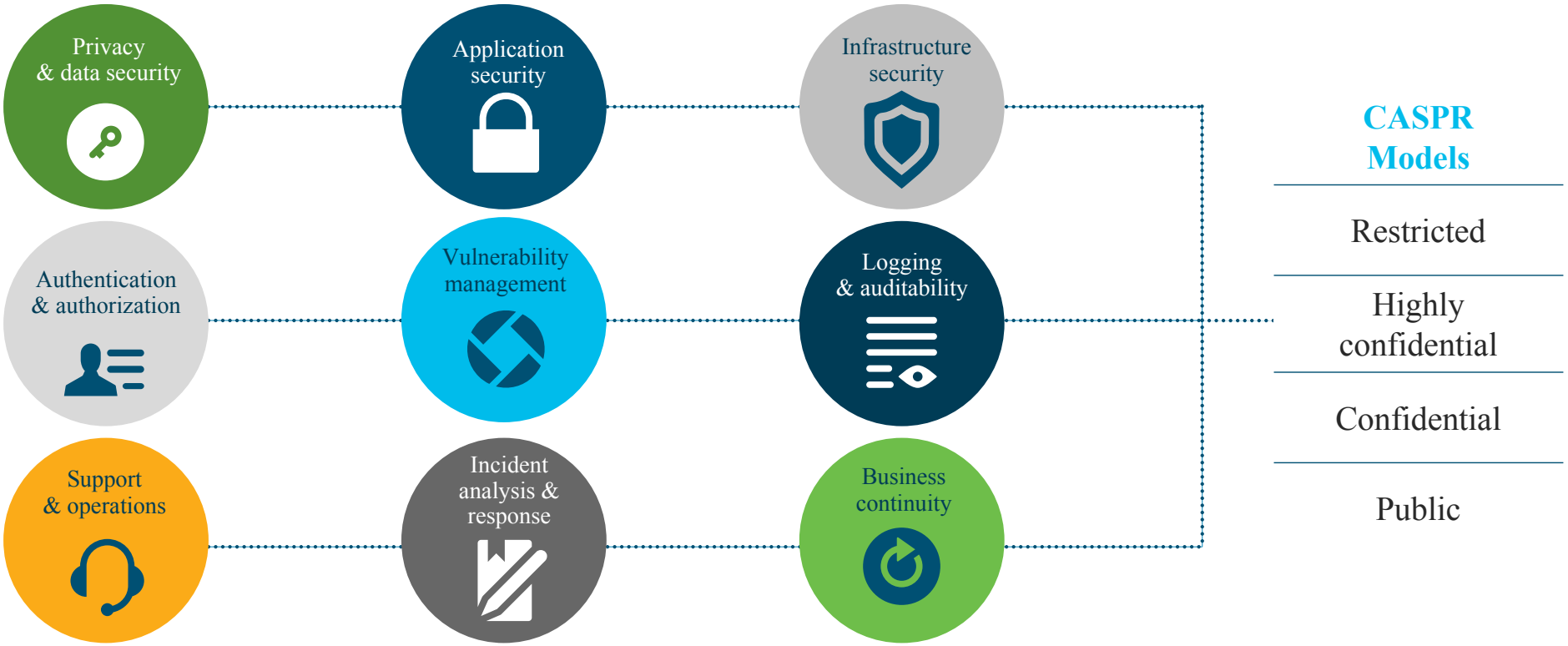
Policy

Engagement

Monitoring

Integration

Security of the procured Cloud Services
(Cloud assessment and service provider remediation)



Security in our cloud offers
Model to drive trust

Build

- Security standards and architectures
- Threat analysis and protection
- Quality management
- Common secure services

Operate

- Data encryption and protection
- Assessment activities
- Intrusion detection and prevention systems
- Security governance

Monitor

- Policy and compliance
- Transparency to enable customers
- Secure cloud value chain
- Application layer data and event monitoring

Data protection

Key elements of a data protection program

Policy, standards and taxonomy

Identification and classification

Data risk and organizational maturity

Awareness and education

Oversight and enforcement

Privacy and international privacy policy

Security and data loss prevention

Incident management

Foundational

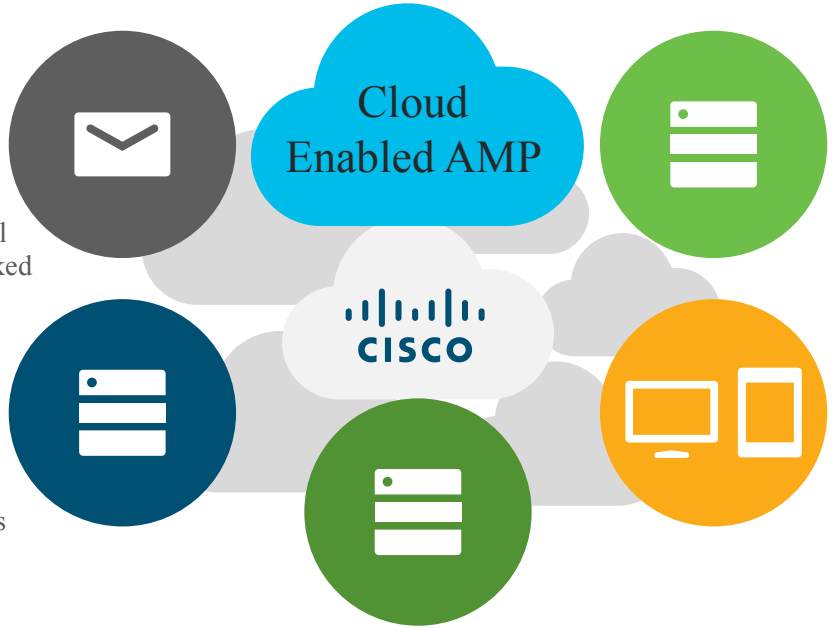
Preparing for General Data Protection Regulation (GDPR) – May 2018

- Policy and process updates
- Data inventory/risk assessments
- Data impact assessments
- Vendor management

Threat detection and response

Integrated threat defense

13 iPOPs globally



AMP'd web and email

1% of all WSA transactions blocked

80 WSAs/ 30 ESA Deployed

3K+ email files blocked by AMP monthly

AMP for Networks

Passive and inline capabilities

25K+ quarterly alerts

NG-IPS 83xx and VM series deployed

Threat Grid/AMP

On-Prem sandboxing

10K+ files analyzed every 24hrs.

14 TG appliances deployed

AMP for Endpoints

Machine learning engine

10K+ agents deployed

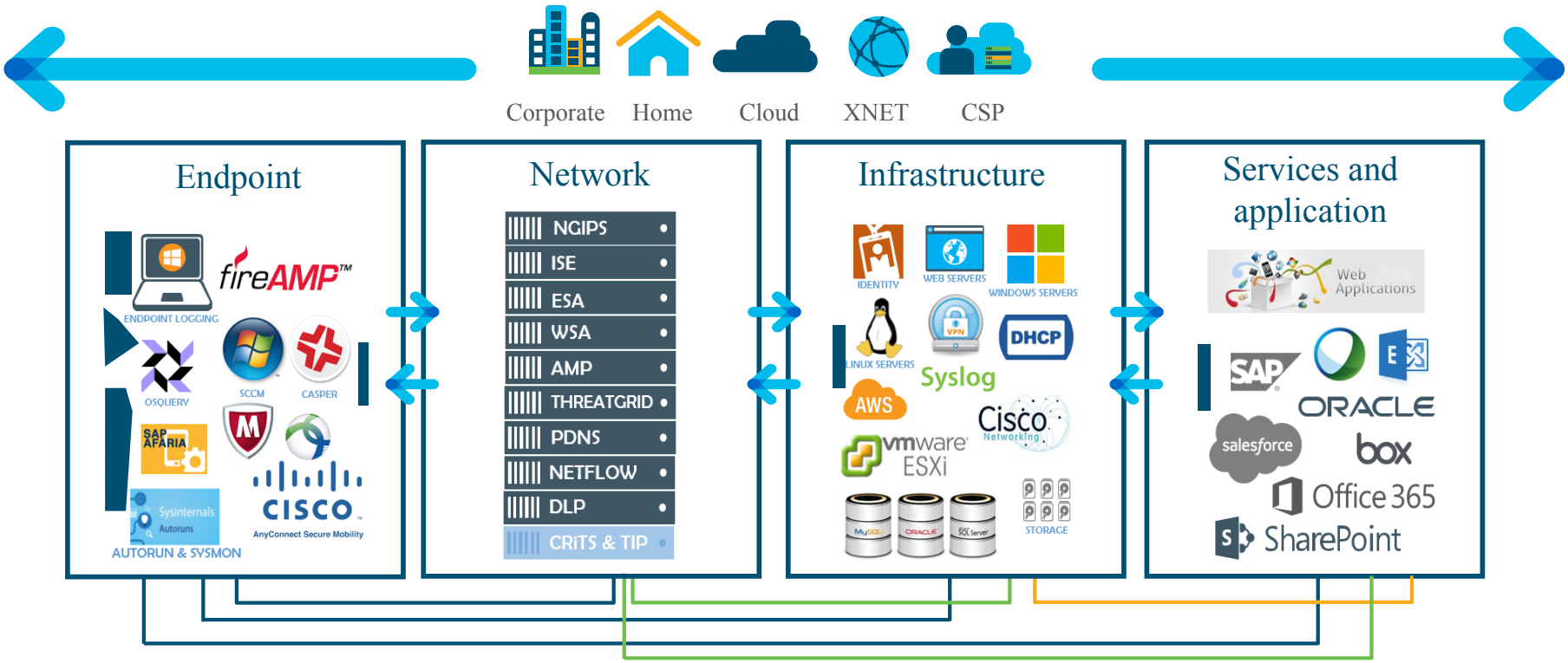
Analytics engine

FireSIGHT Management Center

Eight global appliances deployed

Expecting the unexpected

Incident detection and containment – circa 2017

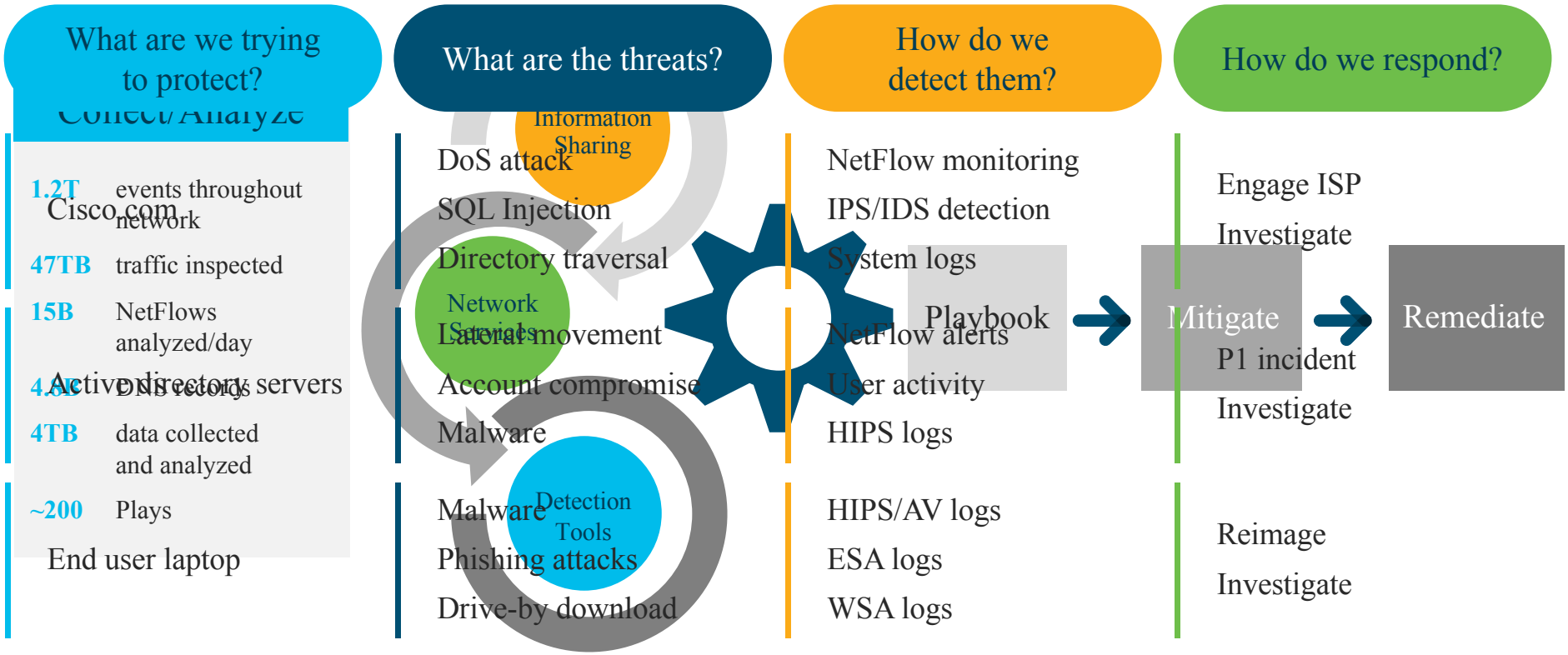


Integrated protection – advanced correlation

47TB Traffic inspected p/day * 1.2T Events monitored * 14 Incidents p/day

Playbook defensive response to threats

Enabling active response to threats



Actionable steps to sleep better at night

Get educated

Business landscape, threat landscape, security programs and what you can do better continuously

Overwhelmed defenders

Simplify, integrate, automate (vendors, solutions)

Executive leadership

Engage early on (IT/OT, risk/ rewards, fiscal impact, budget, train personnel)

Balance defense with active response

Don’t set and forget, establish business continuity/disaster recovery plan


CISCO