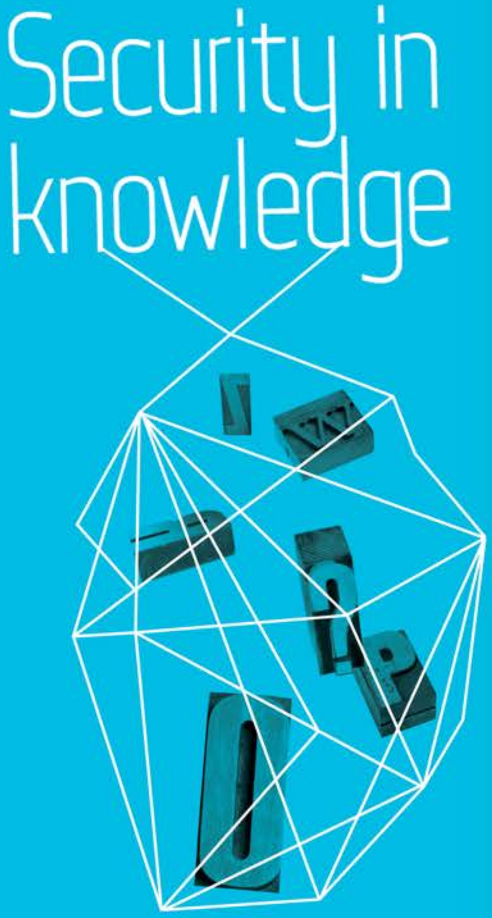
RSA CONFERENCE 2013



MAKING THE CLOUD A SECURE EXTENSION OF YOUR DATACENTER

Bret Hartman

Cisco / Security & Government Group

Session ID: SPO1-W25

Session Classification: General Interest

Mobility

Cloud

Threat

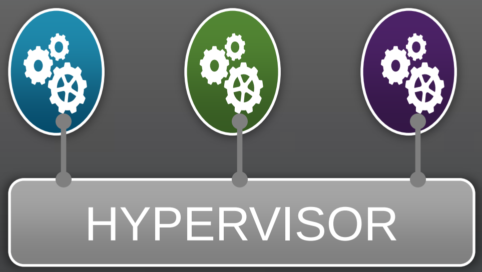
Customer centric market dynamics require an end to end security architecture

Physical | Virtual | Cloud Journey

PHYSICAL WORKLOAD

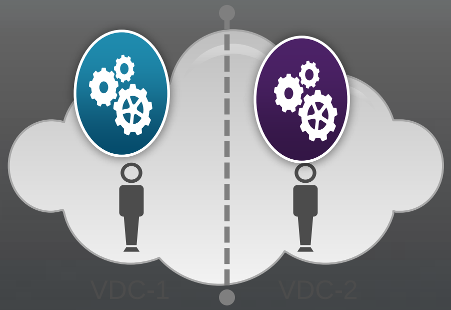
- One app per Server
- Static
- Manual provisioning

VIRTUAL WORKLOAD



- Many apps per Server
- Mobile
- Dynamic provisioning

CLOUD WORKLOAD

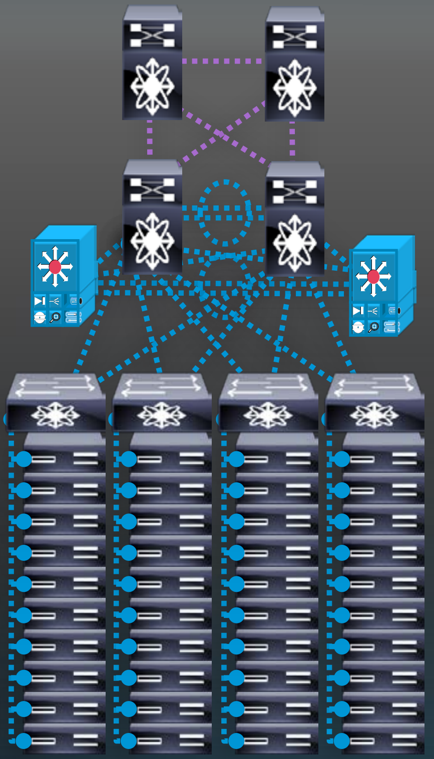


- Multi-tenant per Server
- Elastic
- Automated Scaling

CONSISTENCY: Policy, Features, Security, Management, Separation of Duties

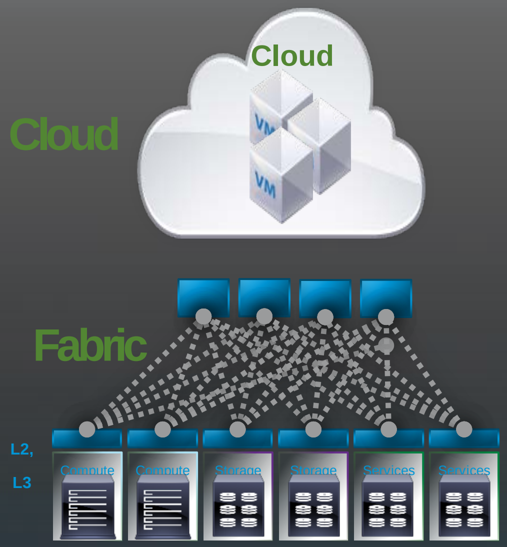
Evolution of Data Center

Distributed



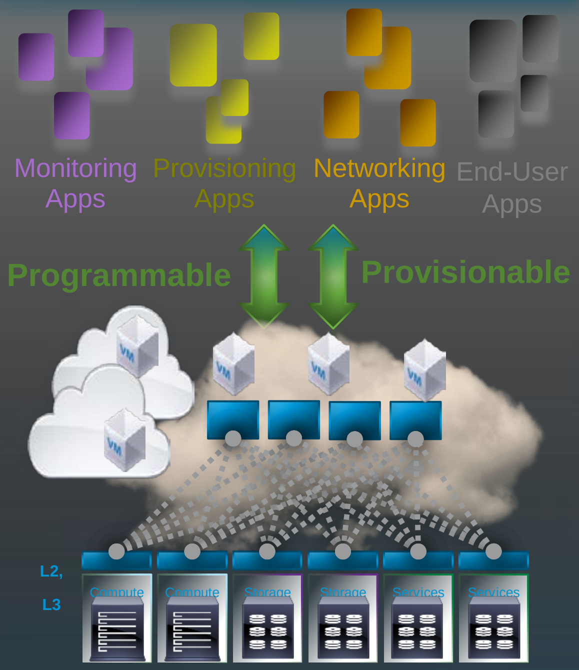
- Manual Provisioning
- Limited scaling
- Rack-wide VM mobility

Fabric Based



- Policy-based Provisioning
- Scale Physical & Virtual/Cloud
- DC-wide/Cross-DC VM Mobility

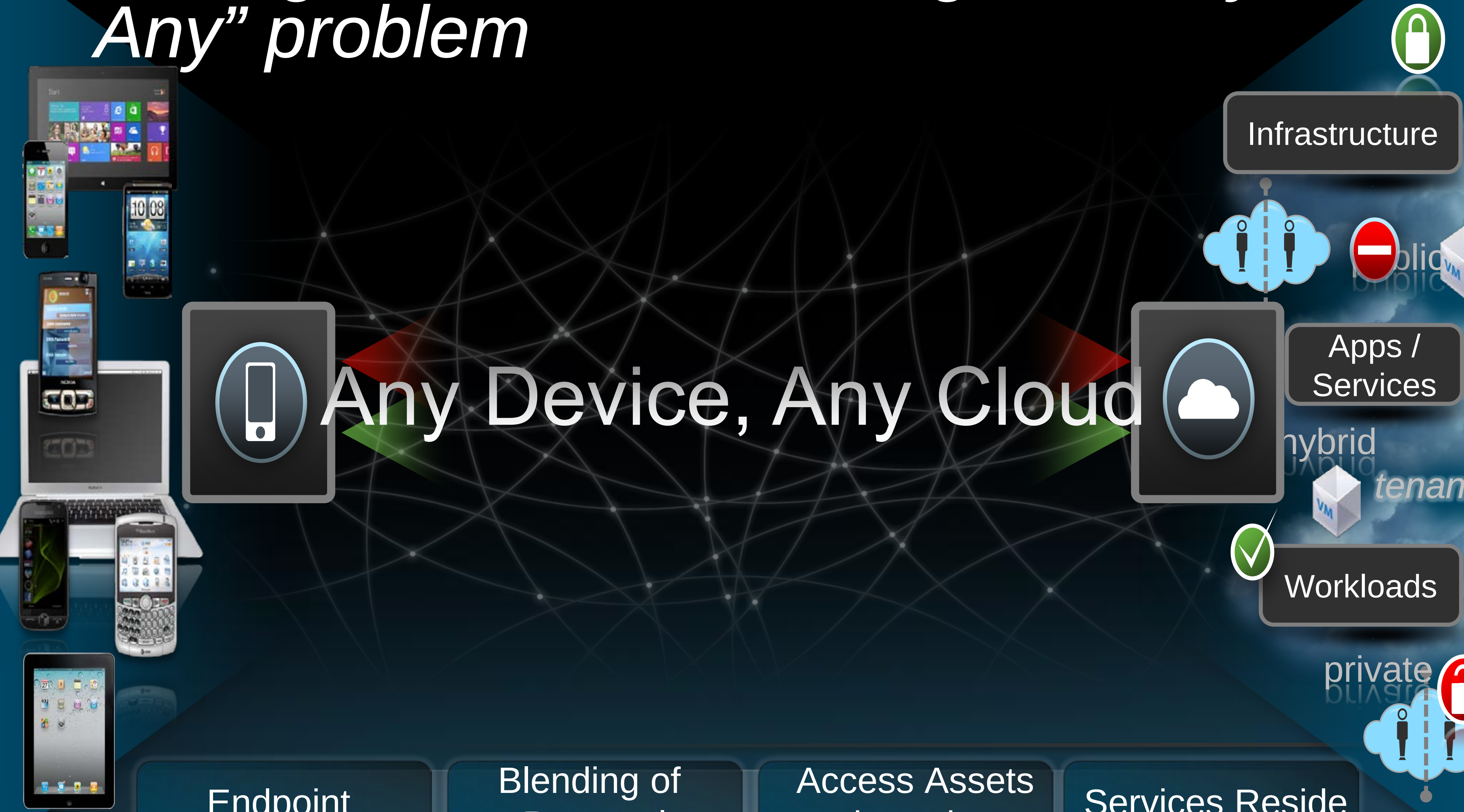
Application Driven



Integrated Fabric & Cloud
World of Many Clouds

- Service-centric Provisioning
- Flexible – Anywhere, Anytime
- Cross-cloud VM Mobility

IT Megatrends are creating the "Any to Any" problem



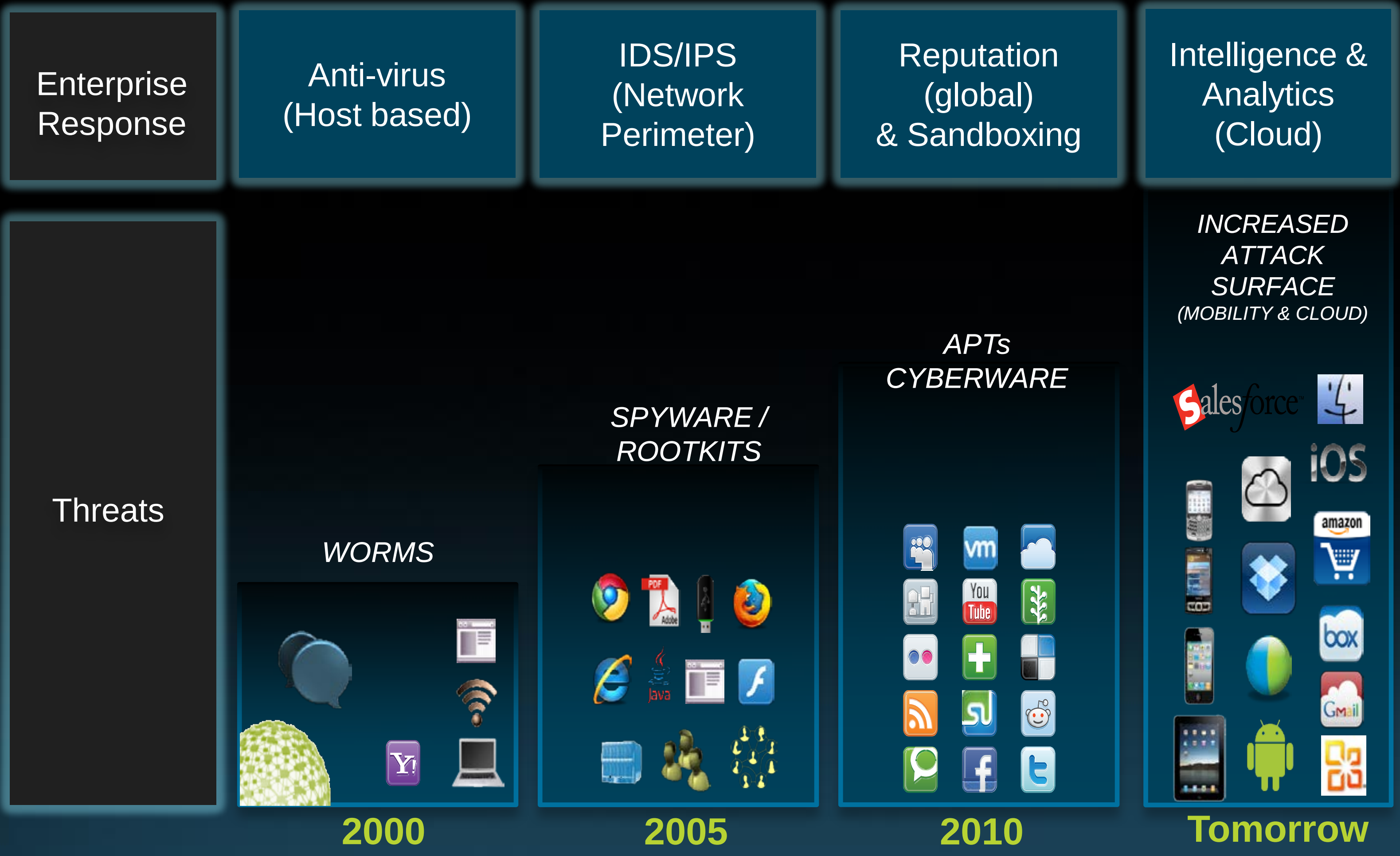
Endpoint Proliferation

Blending of Personal & Business Use

Access Assets through Multiple Medians

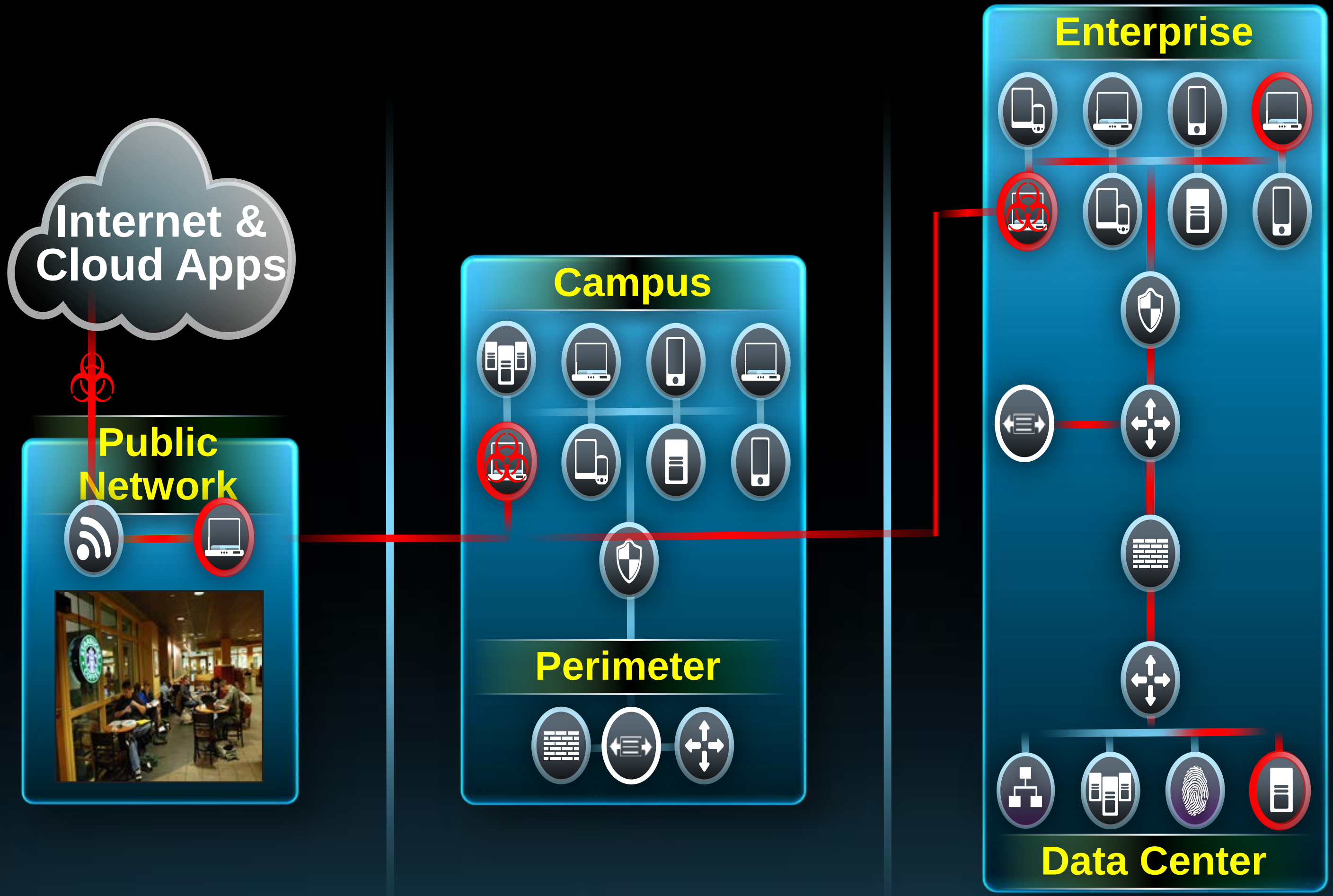
Services Reside In Many Clouds

The Threat Evolution



	2000	2005	2010	Tomorrow
Enterprise Response	Anti-virus (Host based)	IDS/IPS (Network Perimeter)	Reputation (global) & Sandboxing	Intelligence & Analytics (Cloud)
Threats	*WORMS*	*SPYWARE / ROOTKITS*	*APTs CYBERWARE*	*INCREASED ATTACK SURFACE (MOBILITY & CLOUD)*

Anatomy of a Modern Threat



Infection entry point occurs outside of the enterprise

Advanced cyber threat bypasses perimeter defense

Threat spreads & attempts to exfiltrate valuable data

WE'RE ALL MOVING TO THE CLOUD – BUT. . .

- Securing the cloud is a massive transition
  - Diminishing effectiveness of device and data center security
  - Protection burden is shifting to service providers
  - Service providers may not be able to deal with the threats
- Increased risks in the cloud
  - Centralized services are consolidated targets
  - Challenges with isolation and multi-tenancy
  - Expansion of DDoS as a component of a multi-pronged attack

Implications for Security

Functions need to work as a system

Defend

Policy & Access Control

Blocking

Quarantine

Re-routing Traffic

Discover

Increased Content Inspection

Behavior Anomaly Detection

Advanced Threats

Inside the Network

Remediate

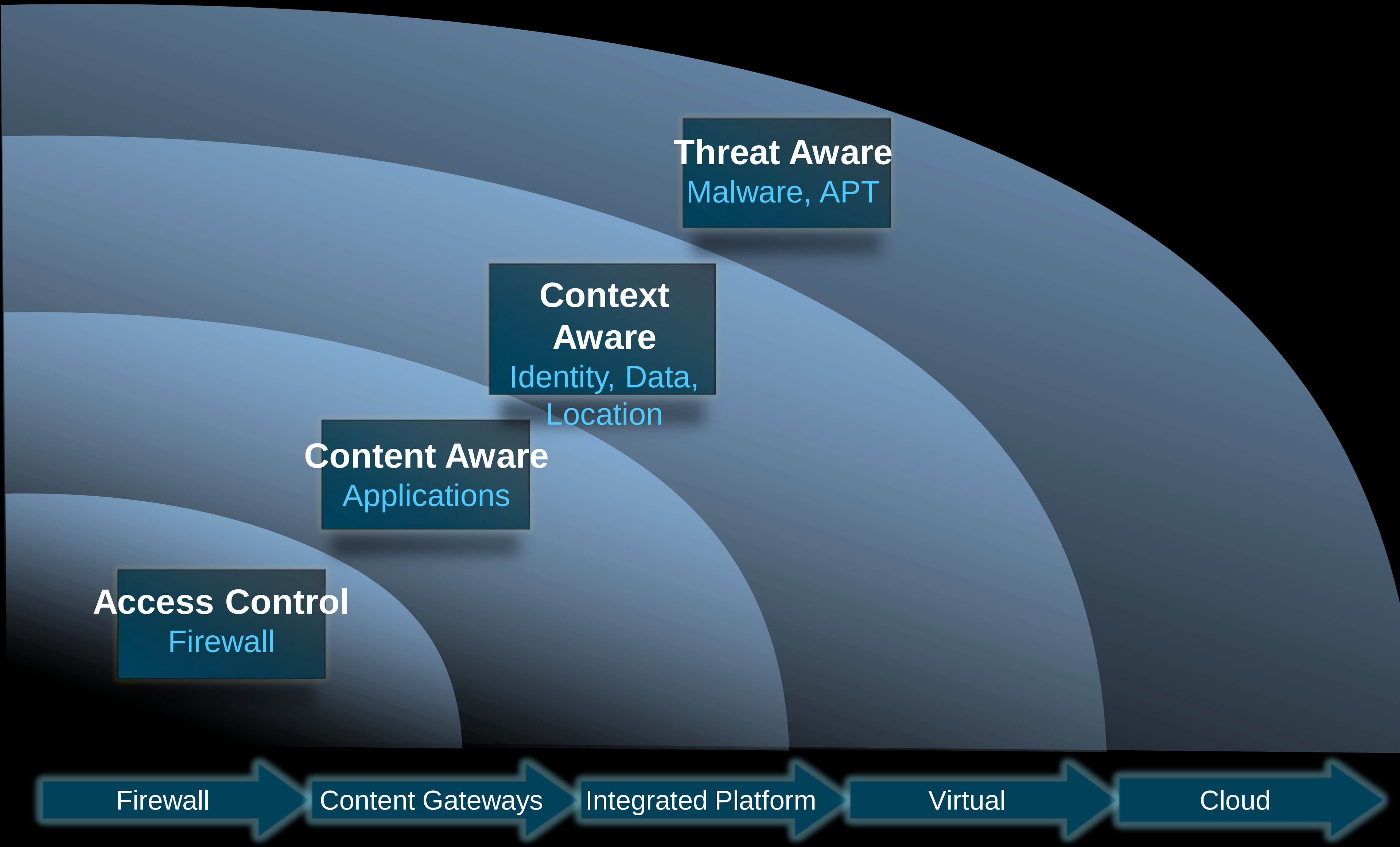
Assess Environment & Threat

Advanced Forensics

Contain

Fix

Integrated Platform for Defense, Discovery and Remediation



Threat Aware
Malware, APT

Context Aware
Identity, Data, Location

Content Aware
Applications

Access Control
Firewall

Firewall

Content Gateways

Integrated Platform

Virtual

Cloud

CLOUD-BASED THREAT INTEL & DEFENSE

ATTACKS | APPLICATION REPUTATION | SITE REPUTATION | MALWARE

GLOBAL | LOCAL | PARTNER API

COMMON POLICY, MANAGEMENT & CONTEXT

COMMON MANAGEMENT | SHARED POLICY | ANALYTICS | COMPLIANCE | PARTNER API

IDENTITY | APPLICATION | DEVICE | LOCATION | TIME

NETWORK ENFORCED POLICY

ACCESS | FW | IPS | VPN | WEB | EMAIL

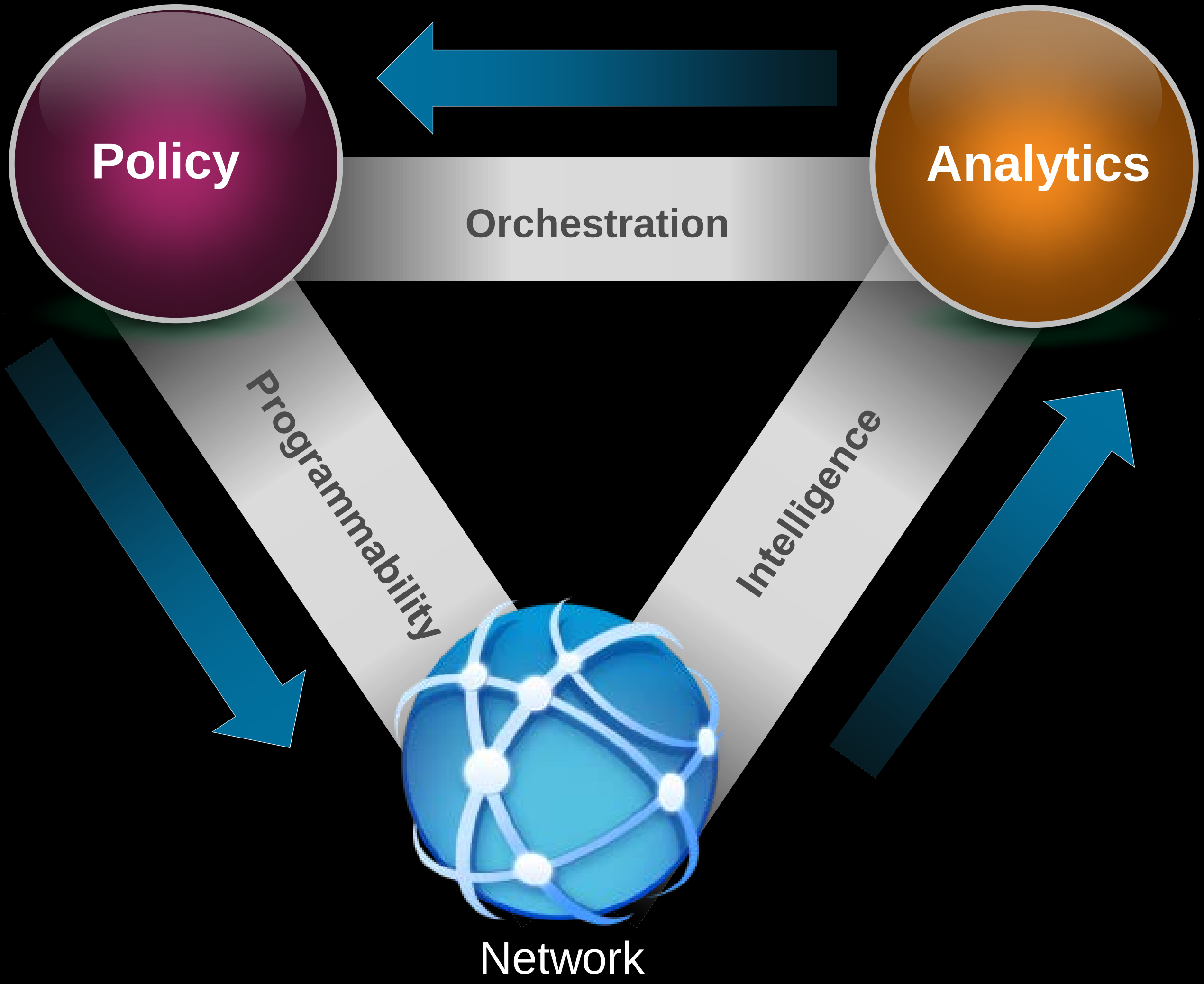
APPLIANCES | ROUTERS | SWITCHES | WIRELESS | VIRTUAL

Infrastructure
public
VM
Apps / Services
hybrid
tenants
VM
Workloads
private

A MORE INTEGRATED APPROACH

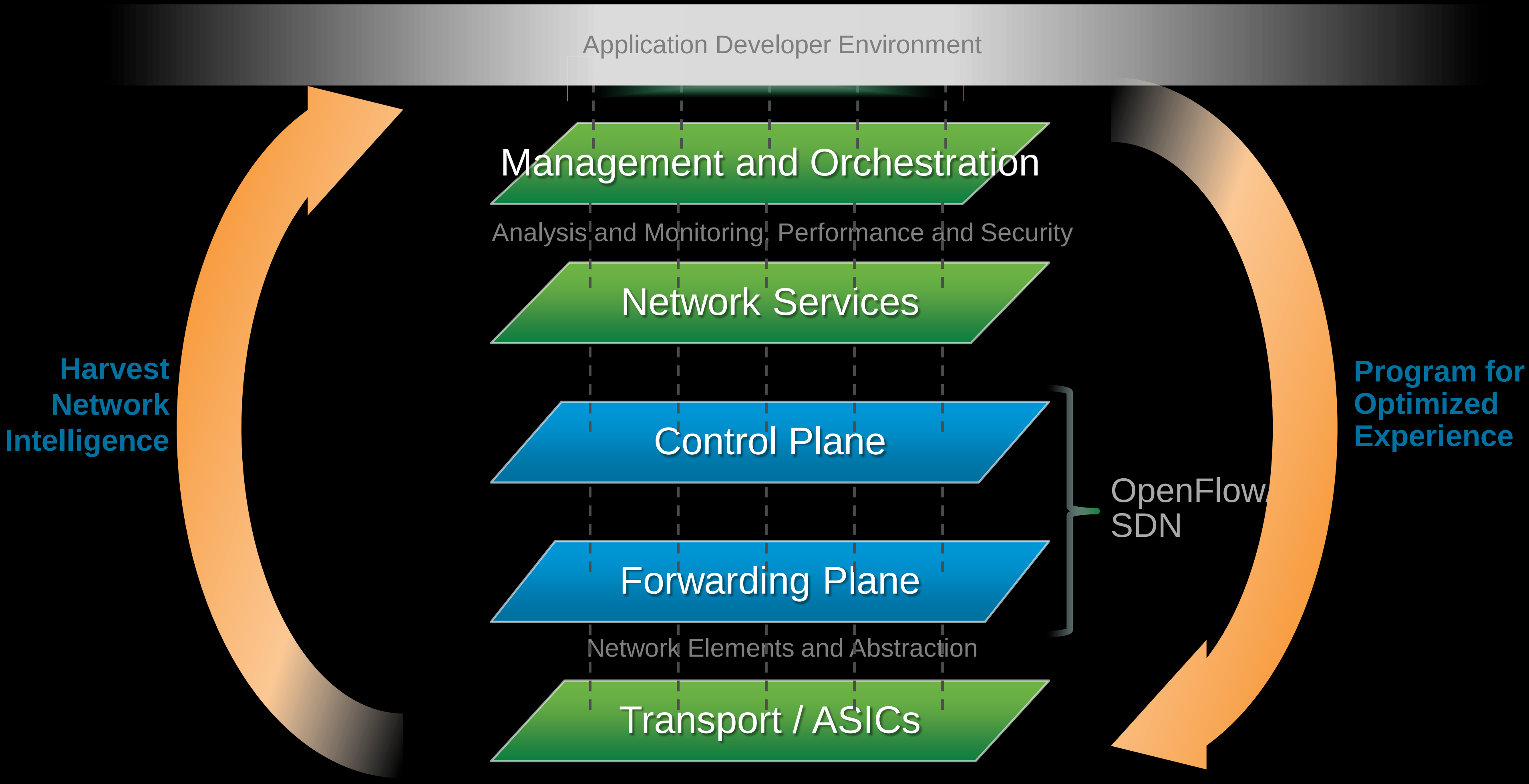
Software-Defined Networking

Leverage Network Value

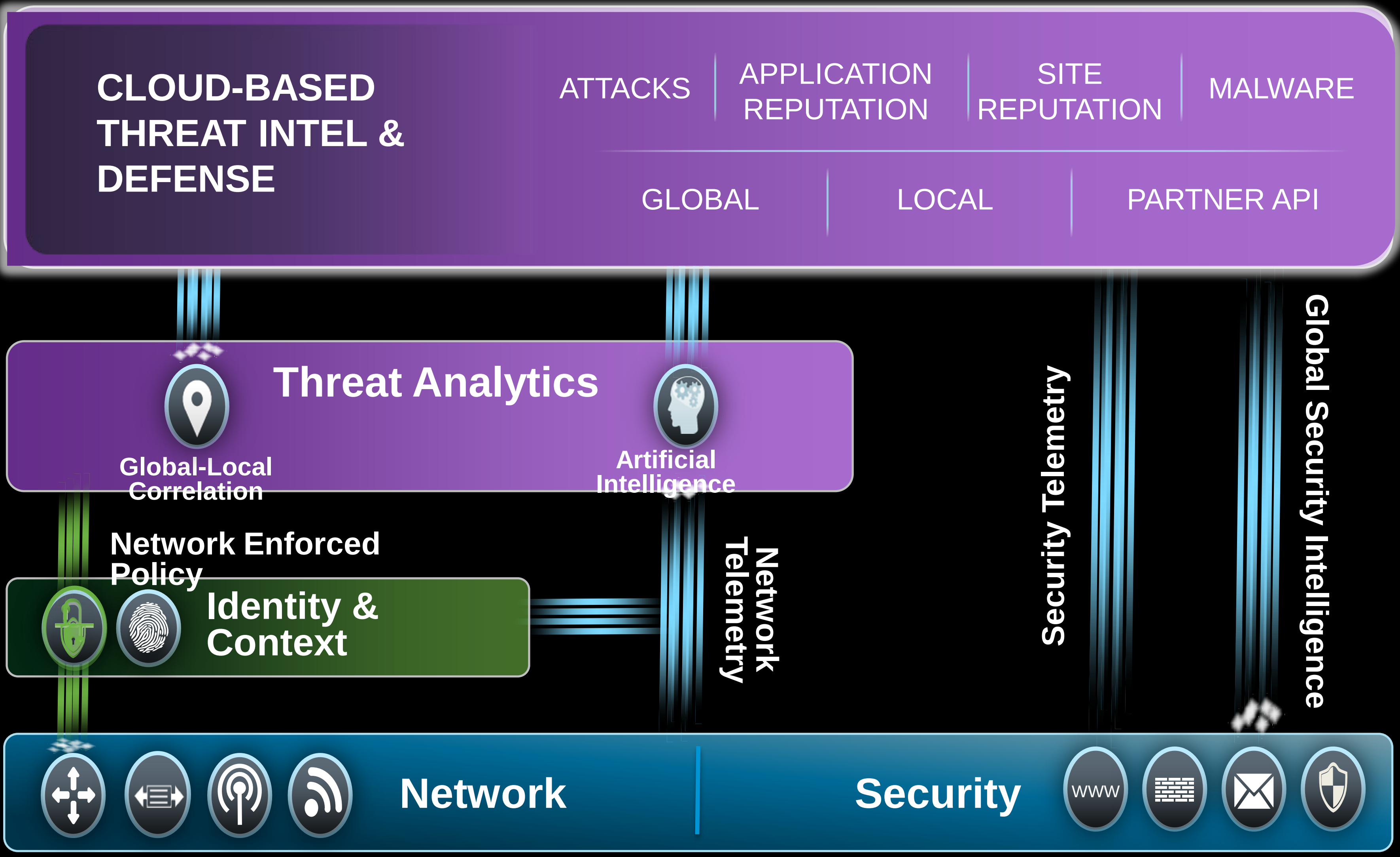


Programmability at Multiple Layers of the Network

Flexibility in Deriving Abstractions


Application Developer Environment
Management and Orchestration
Analysis and Monitoring, Performance and Security
Network Services
Control Plane
Forwarding Plane
Network Elements and Abstraction
Transport / ASICs
OpenFlow/
SDN
Harvest
Network
Intelligence
Program for
Optimized
Experience

Threat Defense and Intelligence



MOVING TO THE CLOUD: RISKS AND OPPORTUNITIES

- Risk – New attack surface
  - Build chain of trust for network devices, controllers, and applications
  - Create standards for security policies across multiple vendors
- Opportunities – Improved visibility and control
  - Unprecedented potential for intelligence analytics
  - Embedded network enforcement end-to-end