RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: BAS-M03

Innovation In Network Security

Michael Geller

Principal Engineer
Cisco Systems, Inc.
@michaelge11er

#RSAC

Innovation In Network Security Is …

- Visibility & Control
- The application of people, process and tools delivered as a service and as a set of products Threats are mitigated as close to the source as possible
- Security services are dynamically chained together and instantiated to form a service chain to mitigate a specific threat and/or to provide a managed security service on distributed compute resources
- Threat defense provides a distributed capability to mitigate threats – targeted at the network, the Data Center, the Cloud and the applications that they serve

Stuff To Think About

- What do we do as encryption becomes more and more pervasive? If it's about visibility …
- When it comes to NfV and SDN, do I go open source or build it myself?
- How do I securely have an application connect to the network to deliver a customer outcome?

Security Imperatives

Visibility-Driven

Network-Integrated, Broad Sensor Base, Context and Automation

Threat-Focused

Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

Platform-Based

Agile and Open Platforms, Built for Scale, Consistent Control, Management

Network

Endpoint

Mobile

Virtual

Cloud

What The Network Does For You

Visibility

End to End Network Visibility From Endpoint to Cloud

Agile Control

Consistent Policies Across Network and Data Center

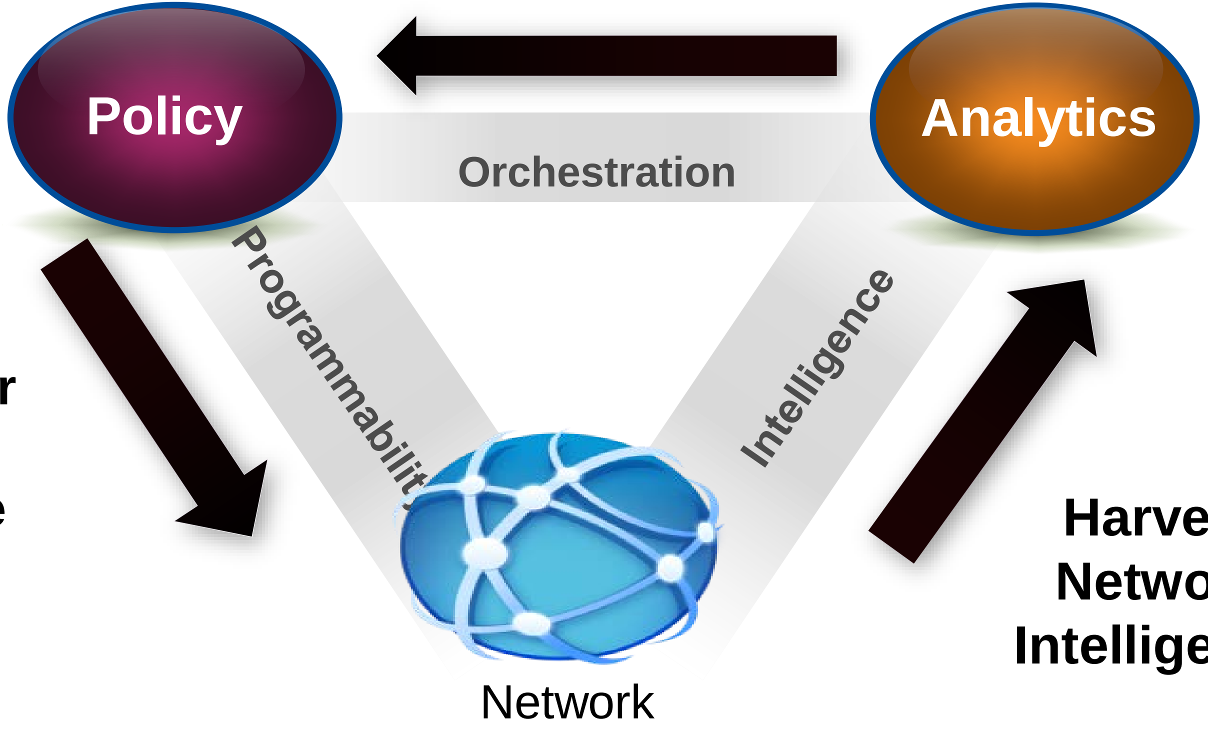
Advanced Threat Protection

Detects and Stops Advanced Threats across CPE, Cloud, and Network

Complexity Reduction

Fits and Adapts to Changing Business Models

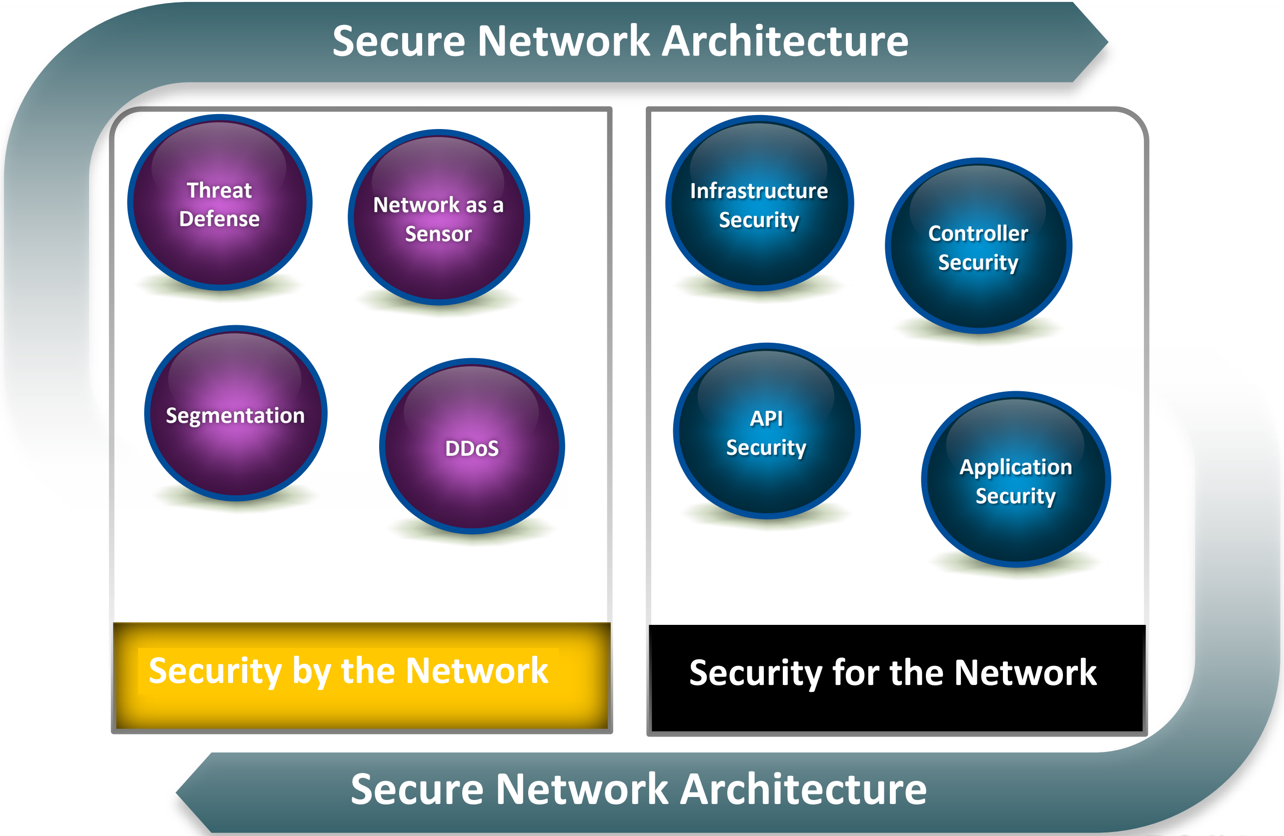
Using Information Better



Program for Optimized Experience

Harvest Network Intelligence

A Secure Network Architecture



Secure Network Architecture

Threat Defense

Network as a Sensor

Segmentation

DDoS

Security by the Network

Infrastructure Security

Controller Security

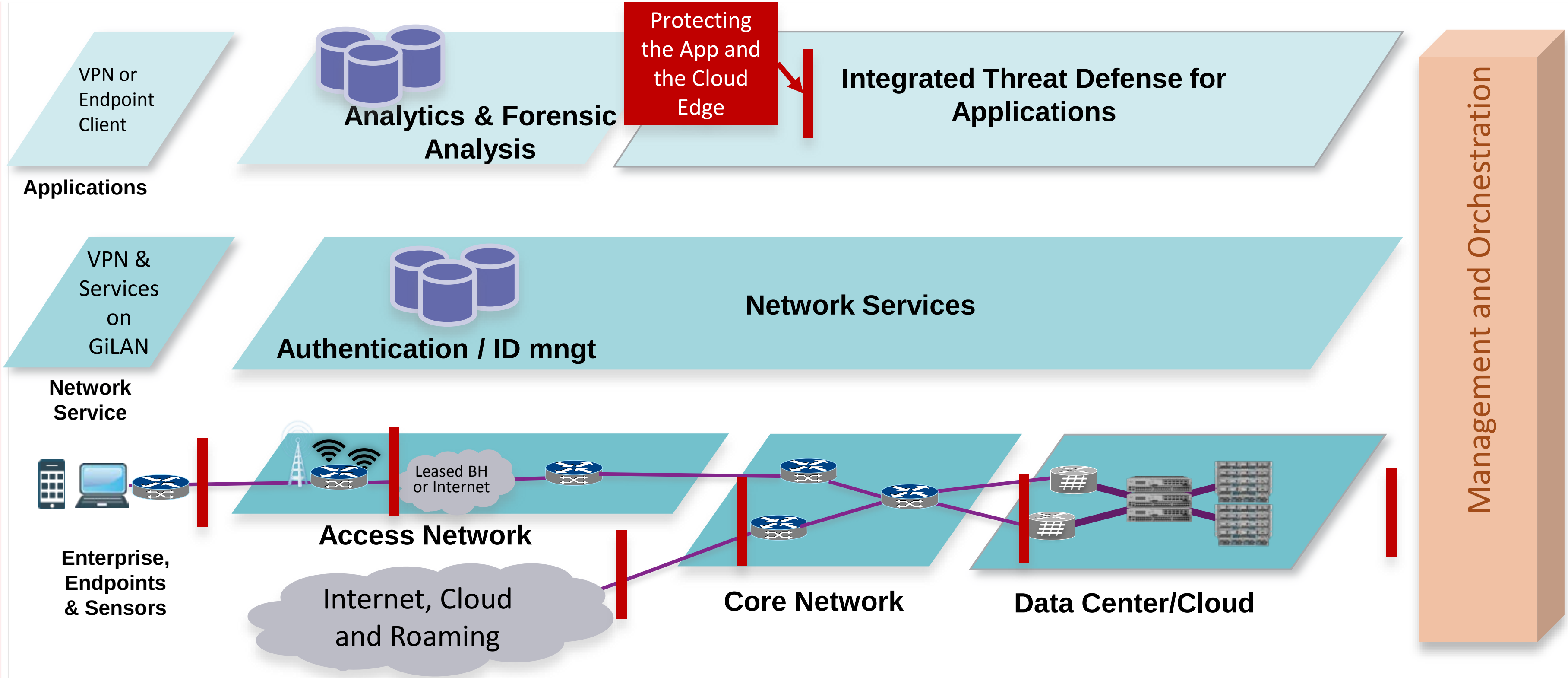
API Security

Application Security

Security for the Network

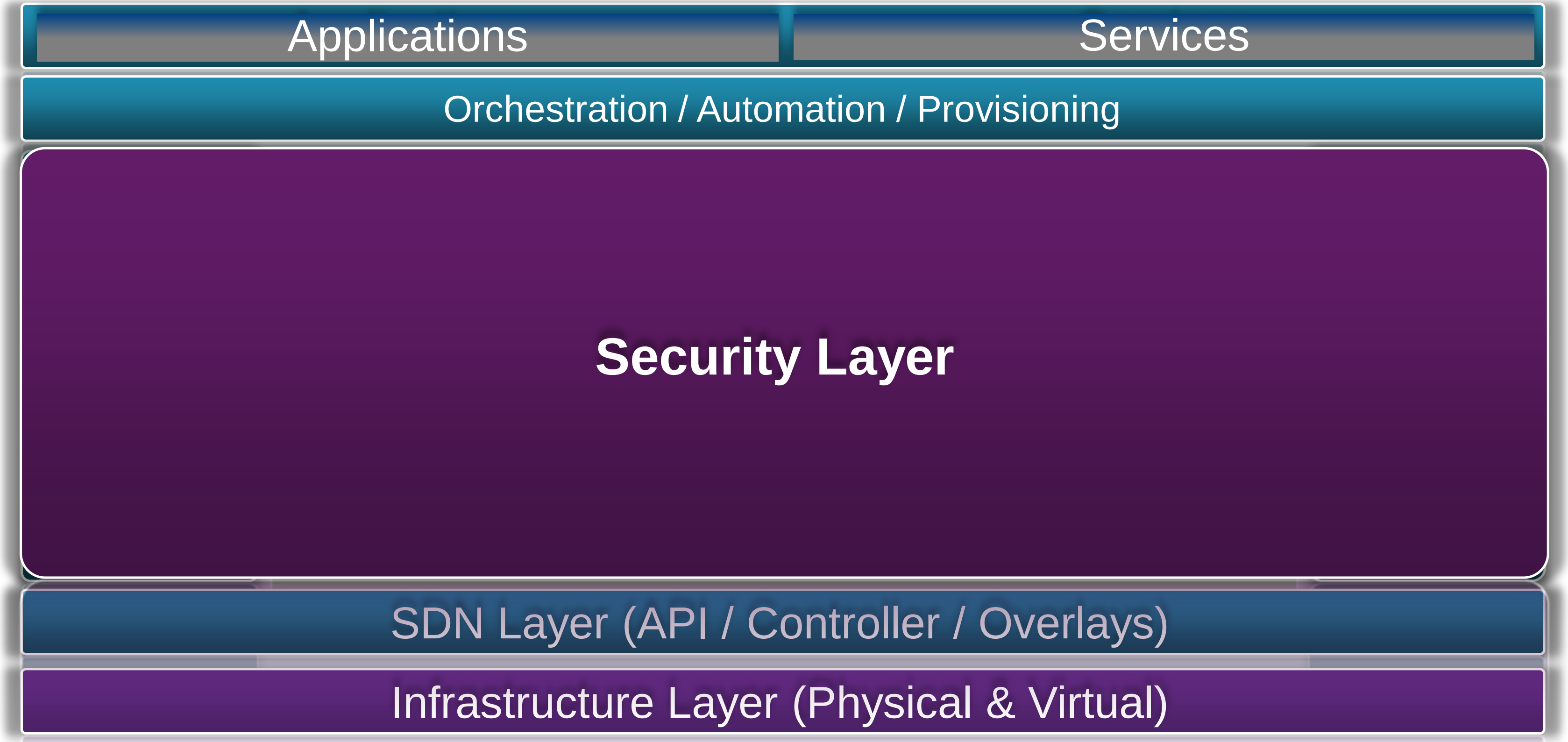
Secure Network Architecture

Protecting Trust Boundaries


VPN or Endpoint Client
Applications
Analytics & Forensic Analysis
Protecting the App and the Cloud Edge
Integrated Threat Defense for Applications
VPN & Services on GiLAN
Network Service
Authentication / ID mngt
Network Services
Leased BH or Internet
Access Network
Enterprise, Endpoints & Sensors
Internet, Cloud and Roaming
Core Network
Data Center/Cloud
Management and Orchestration

🟥 =Trust Boundary

Architectural Approach To Innovation



Applications

Services

Orchestration / Automation / Provisioning

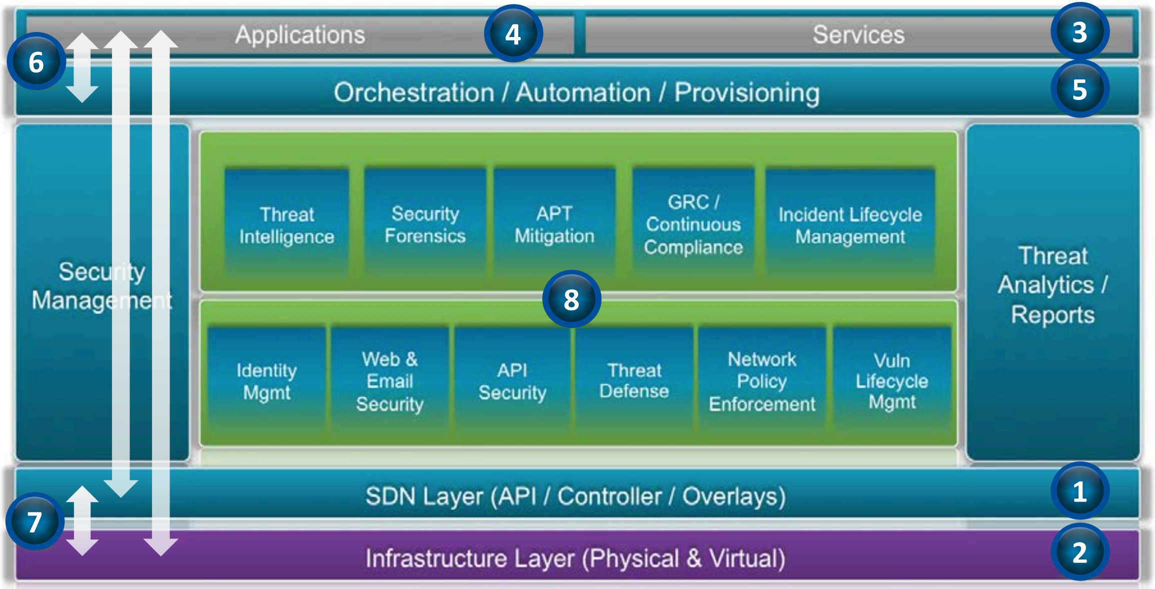
Security Layer

SDN Layer (API / Controller / Overlays)

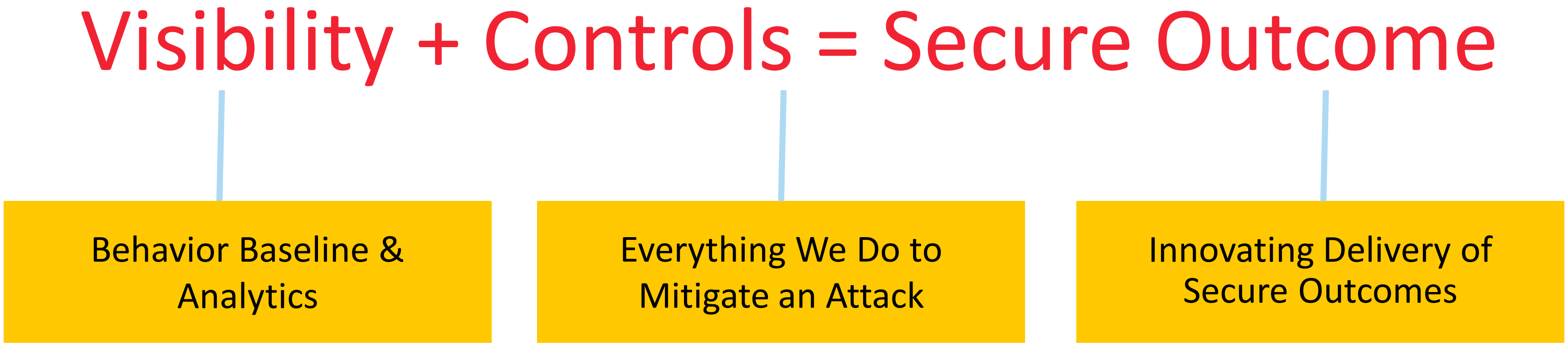
Infrastructure Layer (Physical & Virtual)

Securely Adding NfV and SDN

1. Securing Controller
2. Securing Infrastructure
3. Securing Network Services
4. Securing Application
5. Securing Management & Orchestration
6. Securing API
7. Securing Communication
8. Security Technologies


Applications
4
Services
3
6
Orchestration / Automation / Provisioning
5
Security Management
Threat Intelligence
Security Forensics
APT Mitigation
GRC / Continuous Compliance
Incident Lifecycle Management
8
Identity Mgmt
Web & Email Security
API Security
Threat Defense
Network Policy Enforcement
Vuln Lifecycle Mgmt
Threat Analytics / Reports
SDN Layer (API / Controller / Overlays)
1
7
Infrastructure Layer (Physical & Virtual)
2

Let’s “Apply” What We’ve Learned



Visibility + Controls = Secure Outcome

Behavior Baseline & Analytics

Everything We Do to Mitigate an Attack

Innovating Delivery of Secure Outcomes

Security Innovation = {People, Process & Tools}

What Should You Do Now?

- When you leave today, you should ask yourself:
  - What can you see on the network, what you know and how you can validate it
  - Once you have a good working baseline, do you have a policy that defines acceptable behavior and business priority
  - How quickly can you get the mitigation controls in place?
  - Applications want to talk to your network… Are you ready?
  - How thorough is your capability to learn after the attack?
  - Am I prepared to be innovative in Security?

Questions?

Thank you!