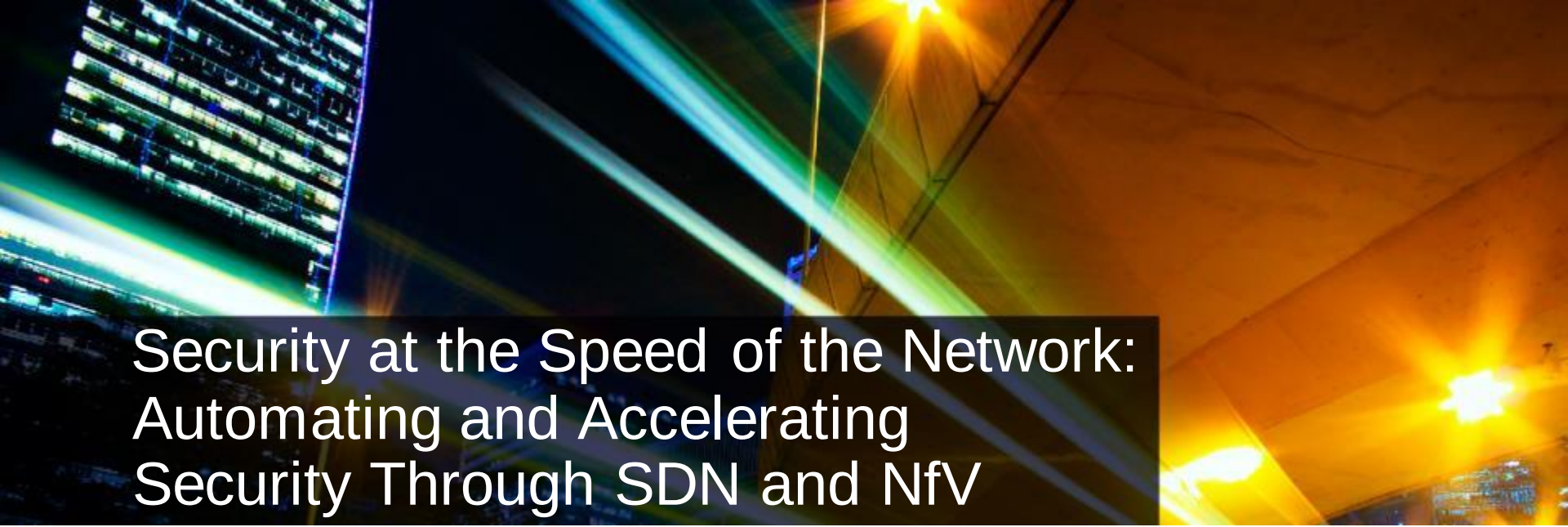

TOMORROW
starts here.
CISCO
Cisco live!



Security at the Speed of the Network: Automating and Accelerating Security Through SDN and NfV

BRKSEC-2760

Stefan Avgoustakis

Consulting Systems Engineer – Security Architecture

#clmel

Cisco live!

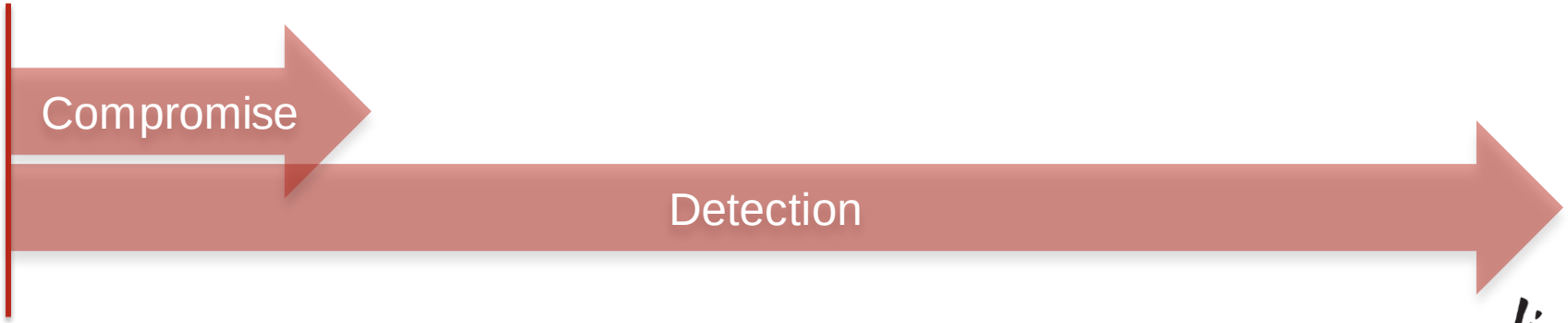

Automating The Security Cycle

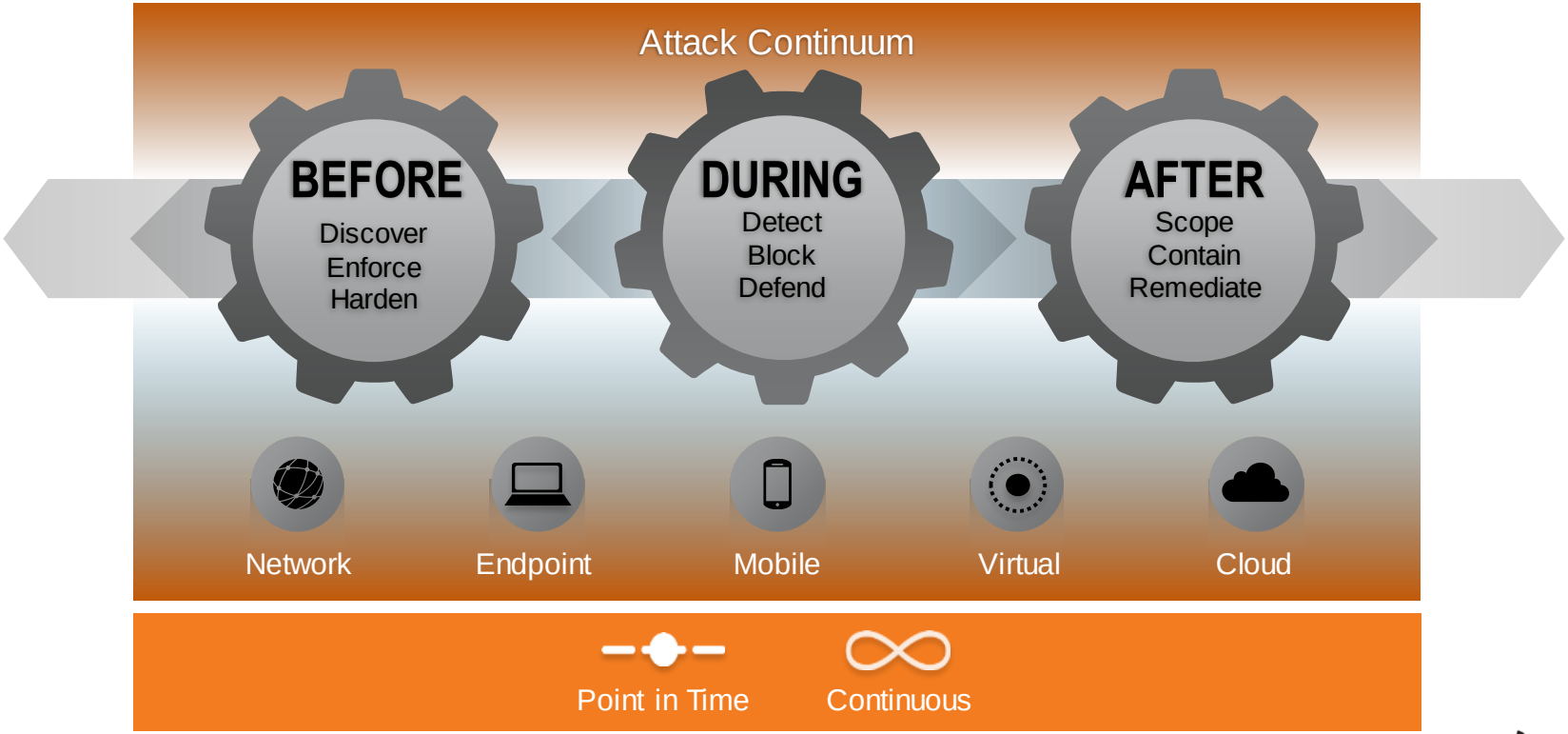
2013 Verison Data

Breach Investigations Report

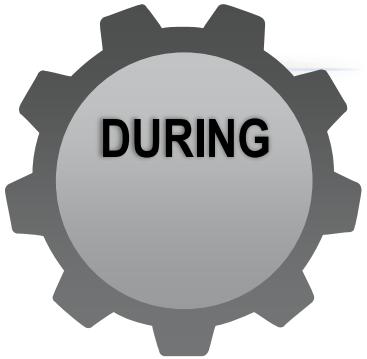
84% of initial compromises completed within hours

66% of compromises undetected for months



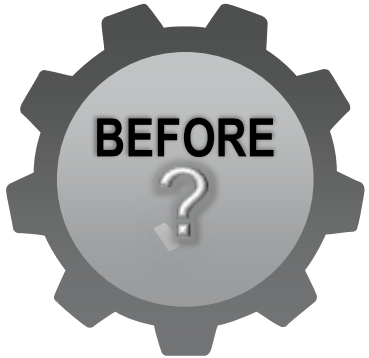


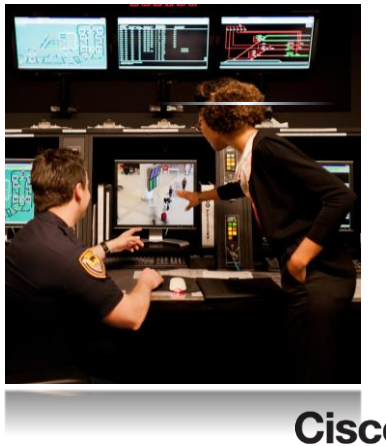
Manual Security Processes



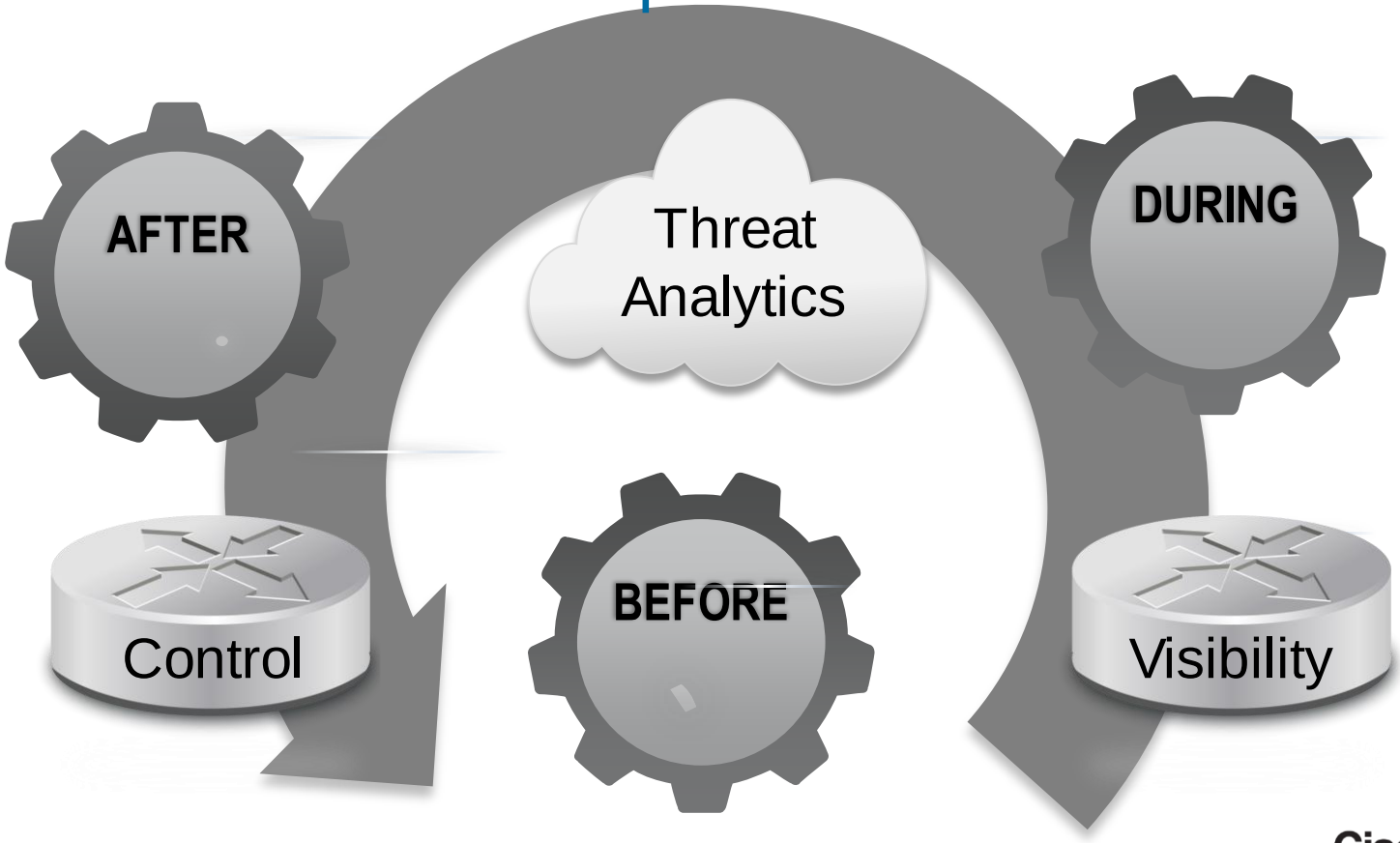

```
Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            rtp-mcgrew-891.cis UGSc           19        0     en0
10.117.10.224/28   link#4             UCS             1        0     en0
rtp-mcgrew-891.cis 28:94:f:e8:b7:2c   UHLWIir        20       24     en0   1103
rtp-mcgrew-0912.ci localhost          UHS             0        0     lo0
127                localhost          UCS             0        0     lo0
localhost          localhost          UH              2      550     lo0
169.254            link#4             UCS             0        0     en0

Internet6:
Destination        Gateway            Flags      Netif Expire
localhost          link#1             UHL           lo0
fe80::%lo0         localhost          UcI           lo0
localhost          link#1             UHLI          lo0
fe80::%en0         link#4             UCI           en0
darkstar-2.local   20:cf:e9:10:ef:6d  UHLI          lo0
fe80::8a53:95ff:fe 88:53:95:7b:7b:94  UHLWI         en0
ff01::%lo0         localhost          UmCI          lo0
ff01::%en0         link#4             UmCI          en0
ff02::%lo0         localhost          UmCI          lo0
ff02::%en0         link#4             UmCI          en0
darkstar-2:~ mcgrew$
```

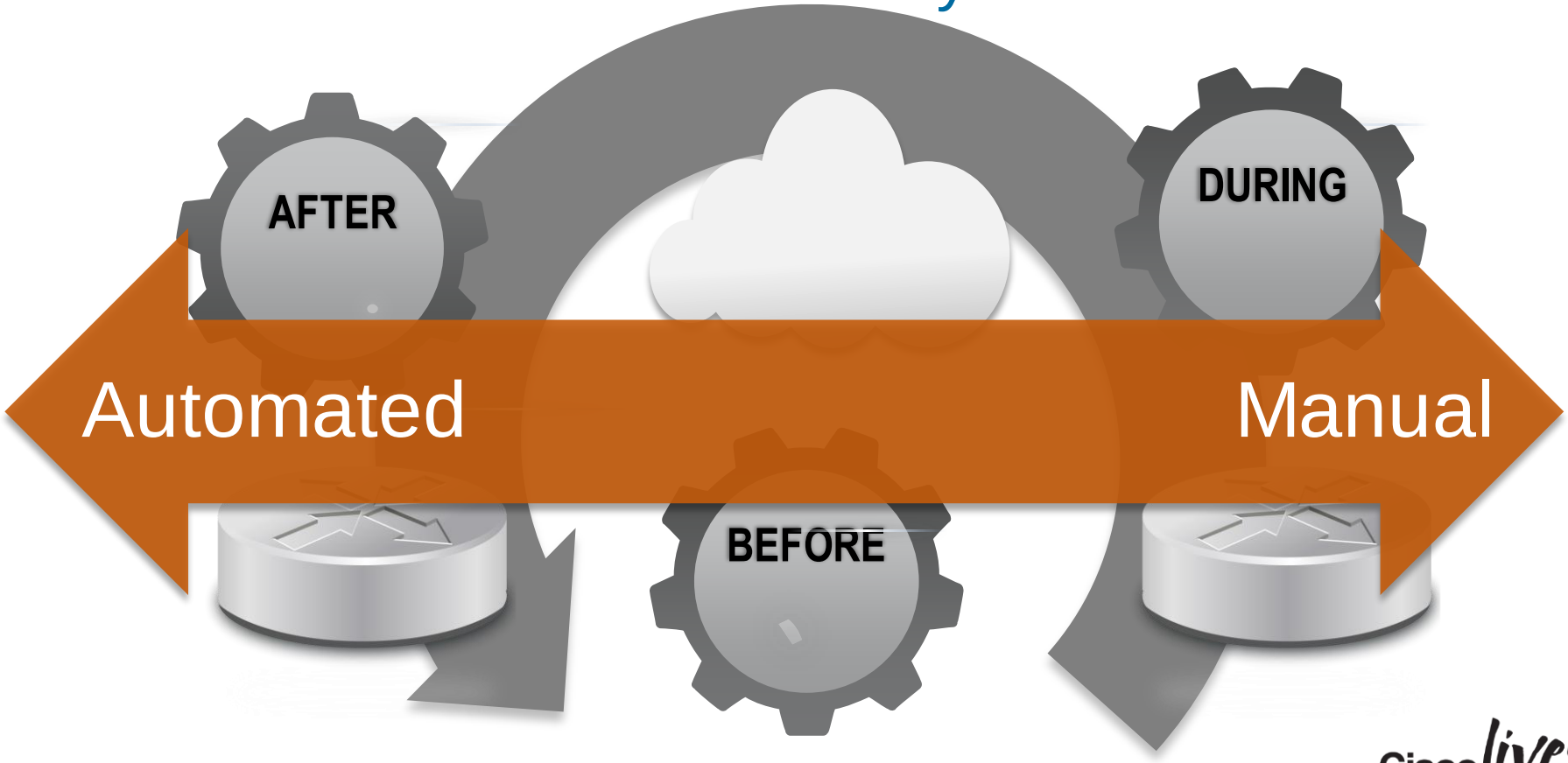




SDN Automation: The Speed of The Network



How Automated Are You Today?



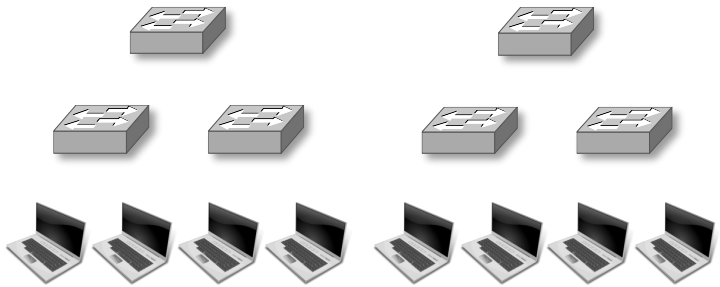
Software Defined Networking

Network Programmability

Network Monitoring

Bandwidth Management

Load Balancing



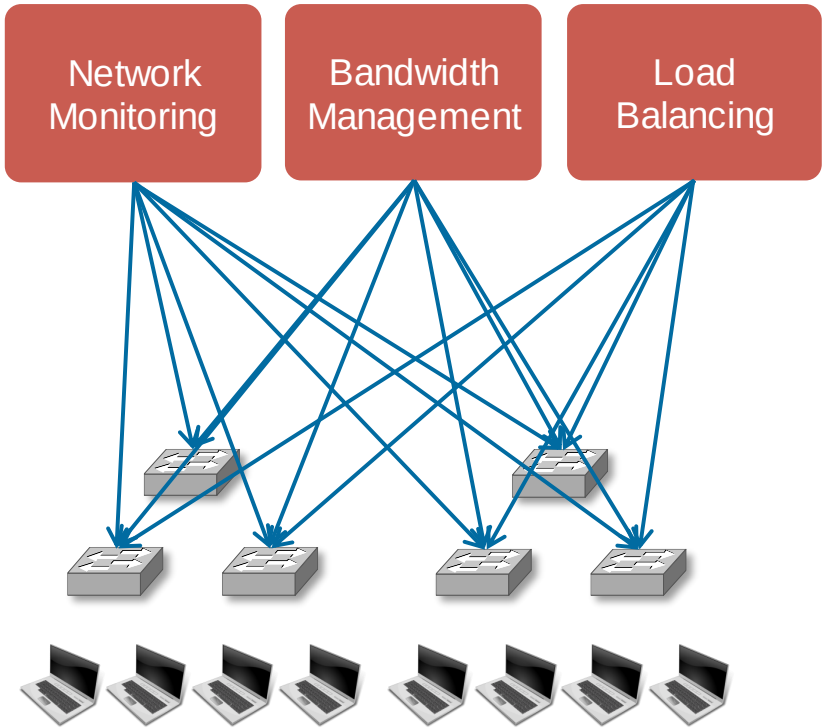
Cisco live!

Network Programmability

SNMP

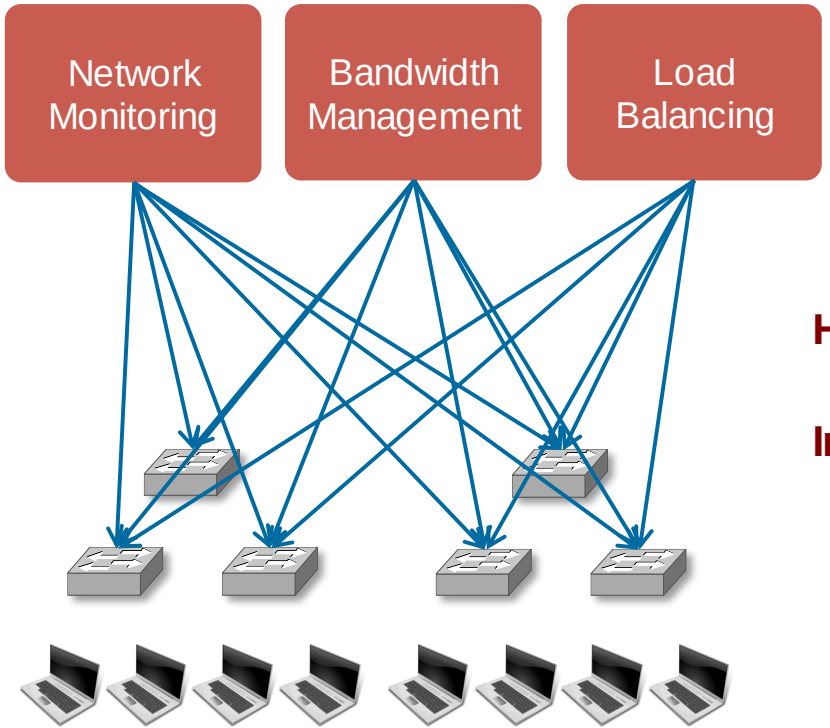
CLI

NetFlow



Cisco live!

Network Programmability



SNMP

CLI

NetFlow

Heterogeneous devices

Inconsistent data models

☹

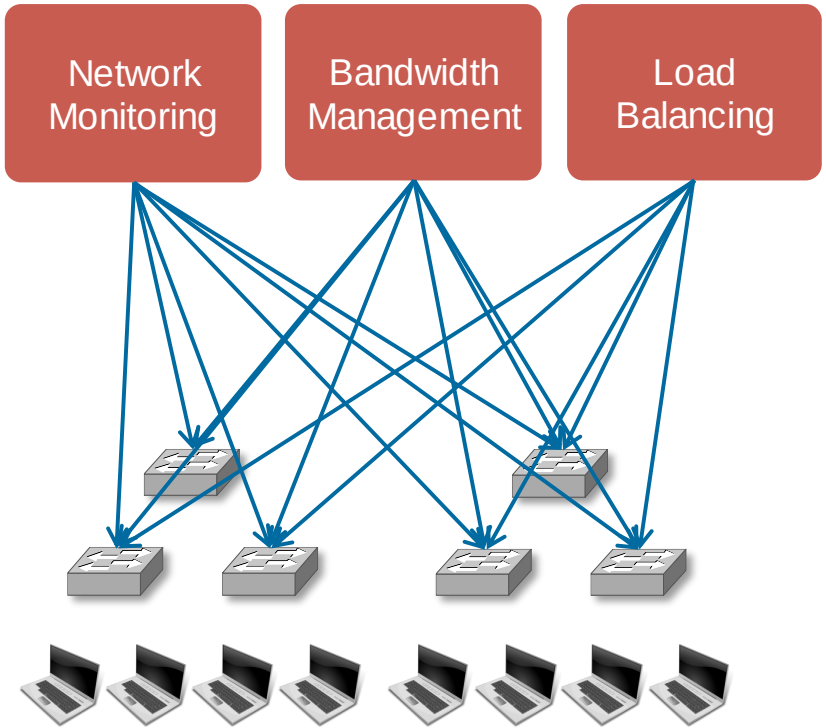
Cisco live!

Network Programmability

Programmatic Interfaces

onePK

OpenFlow

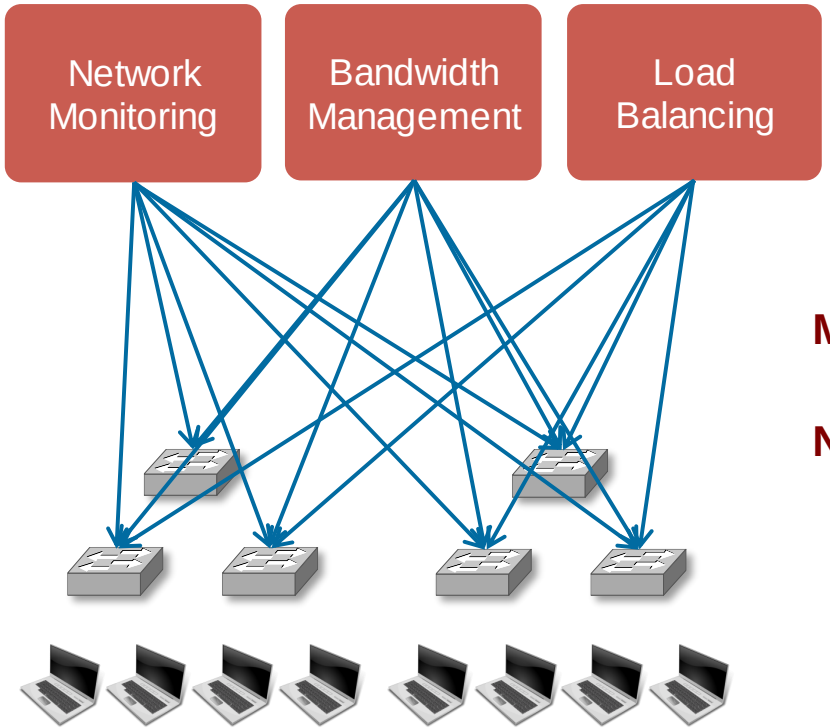


Network Programmability

Programmatic Interfaces

onePK

OpenFlow



Multiple topology models

No policy resolution

☹

Cisco live!

Network Programmability

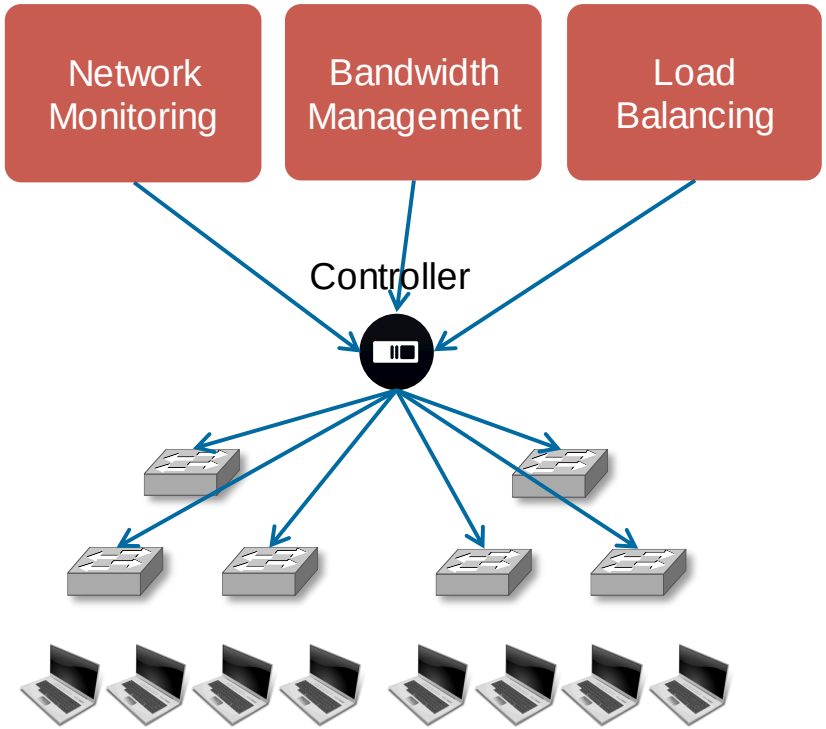
Programmatic Interface

CLI

onePK

OpenFlow

REST APIs



Network Programmability

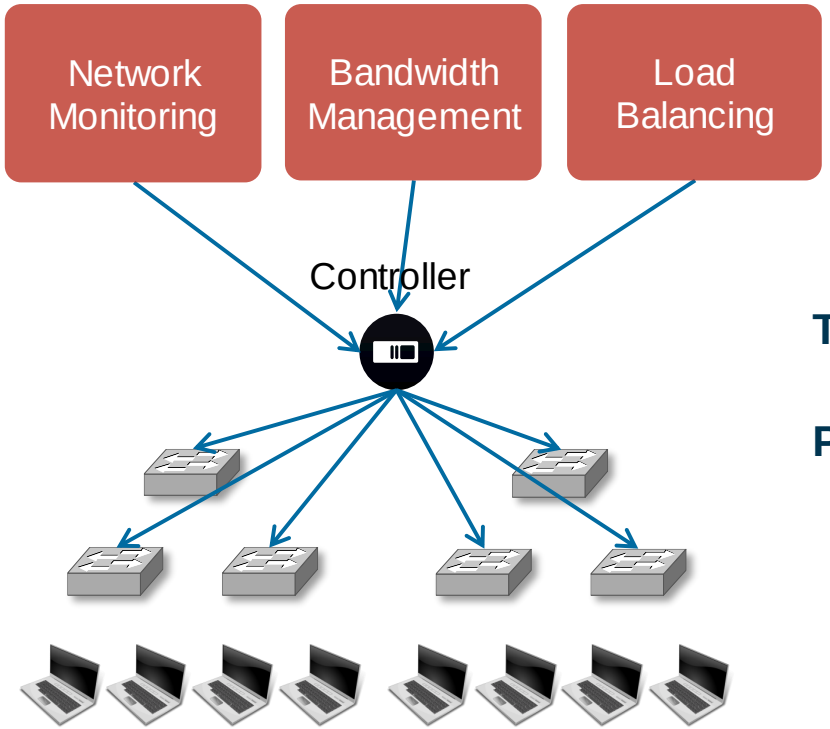
Programmatic Interface

CLI

onePK

OpenFlow

REST APIs



Topological awareness

Policy resolution

Cisco Controllers

Application Policy Infrastructure Controller (APIC)

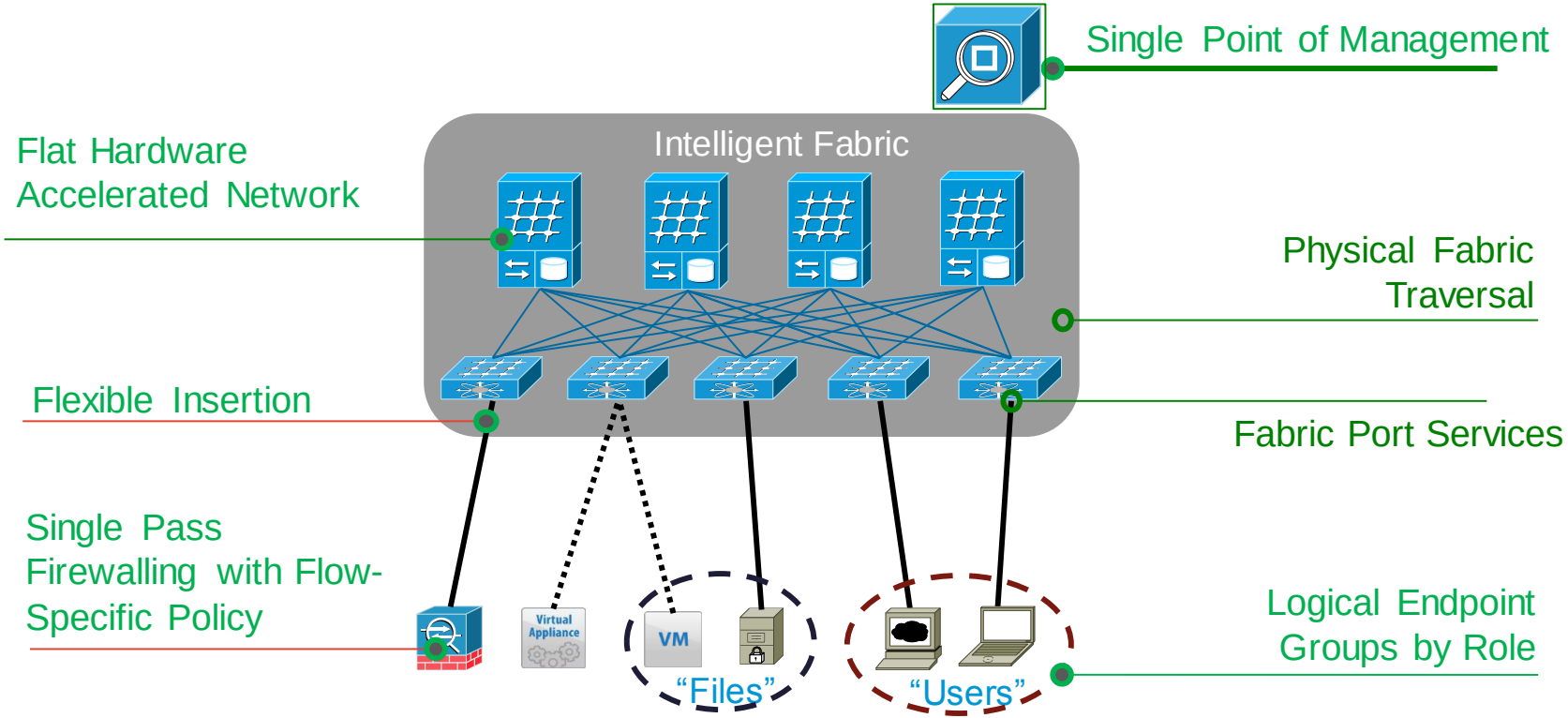
Application Centric Infrastructure Fabric

Physical, Virtual, and Cloud

Open APIs

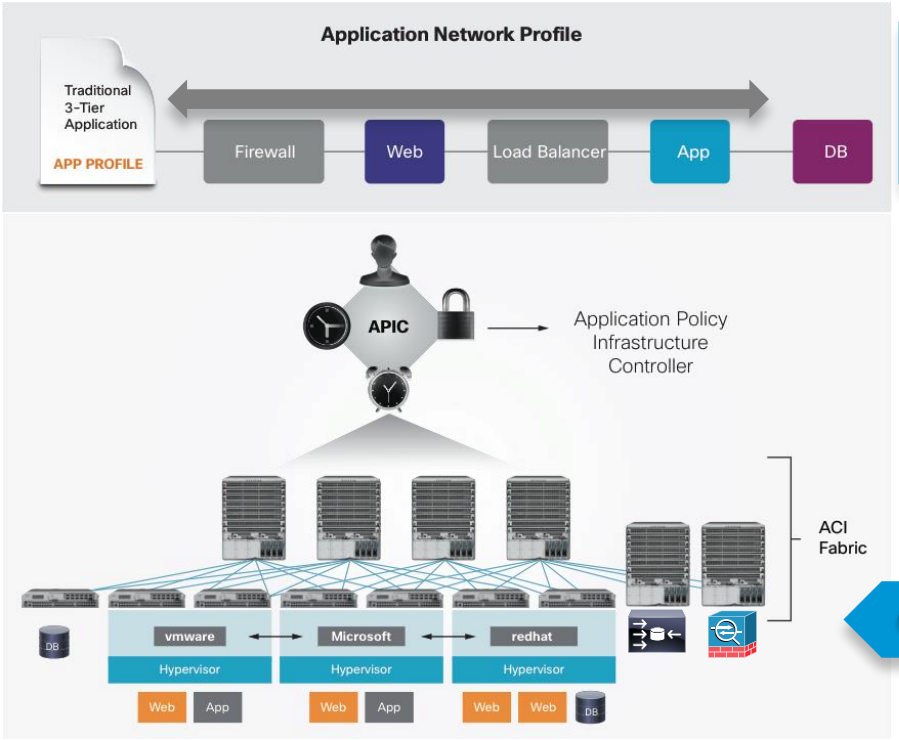
OpenStack

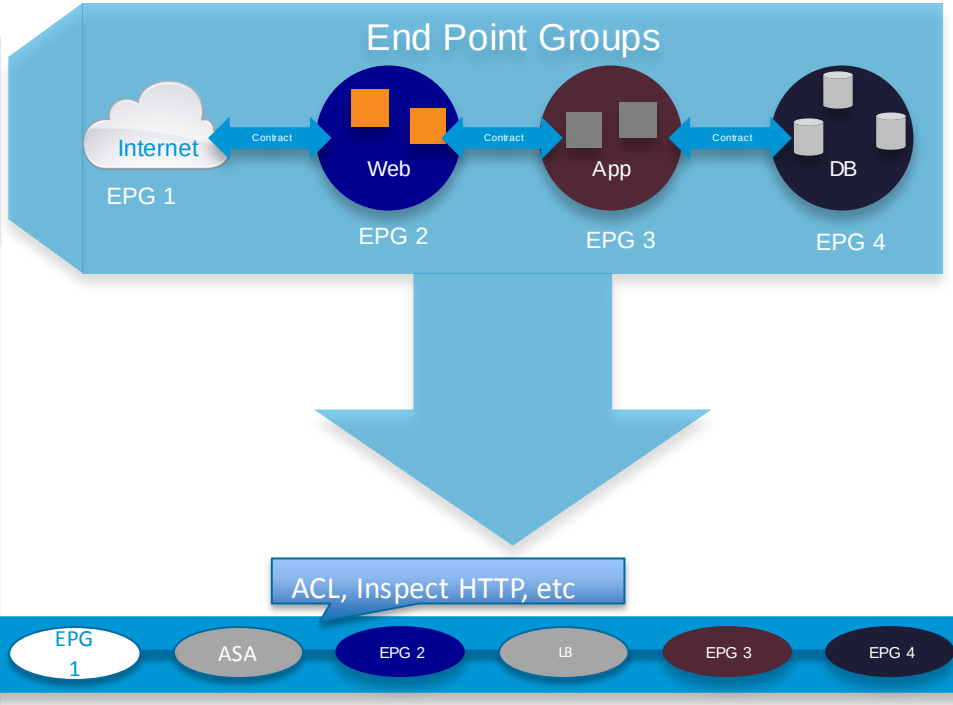
Application Centric Infrastructure Fabric



End Point Groups and Contracts Simplify Policy

Service Insertion and ACI





Cisco Controllers

Application Policy Infrastructure Controller (APIC)

Application Centric Infrastructure Fabric

Physical, Virtual, and Cloud

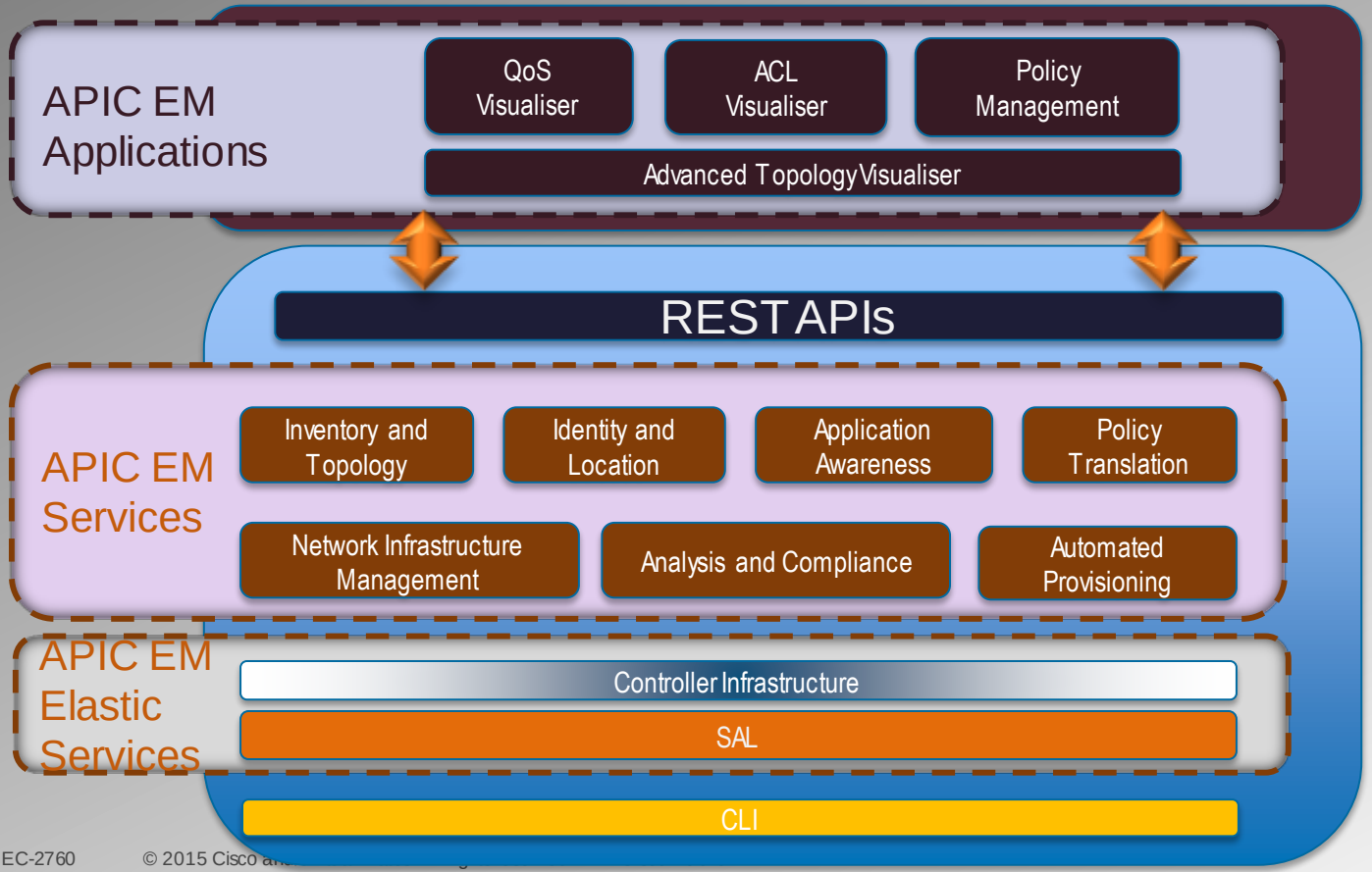
Open APIs

OpenStack

APIC-EM

CLI

API Controller Enterprise Module – Architecture (Release1.0)



Cisco Controllers

Application Policy Infrastructure Controller (APIC)

Application Centric Infrastructure Fabric

Physical, Virtual, and Cloud

Open APIs

OpenStack

APIC-EM

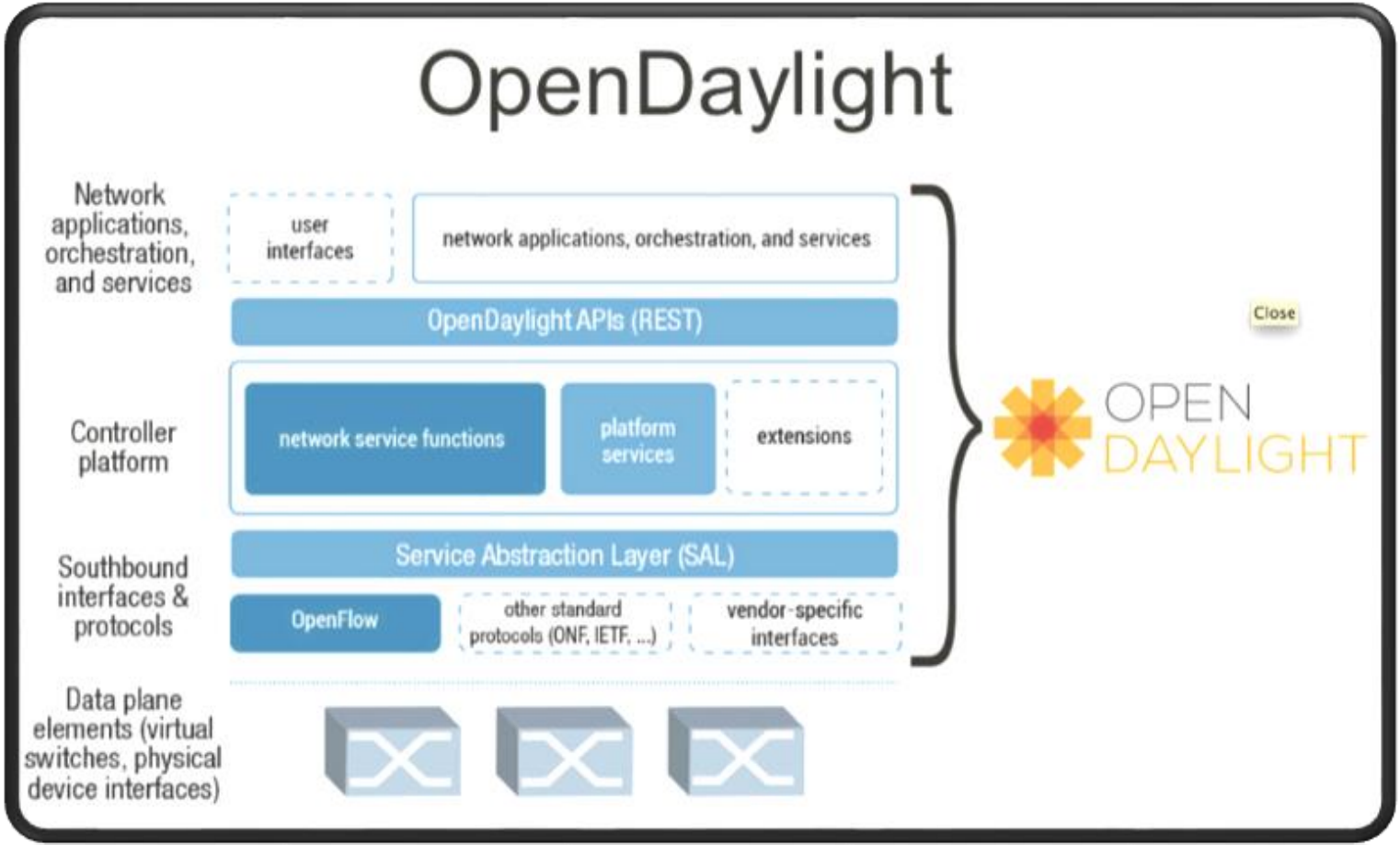
CLI

Open Day Light (ODL)

Open Source

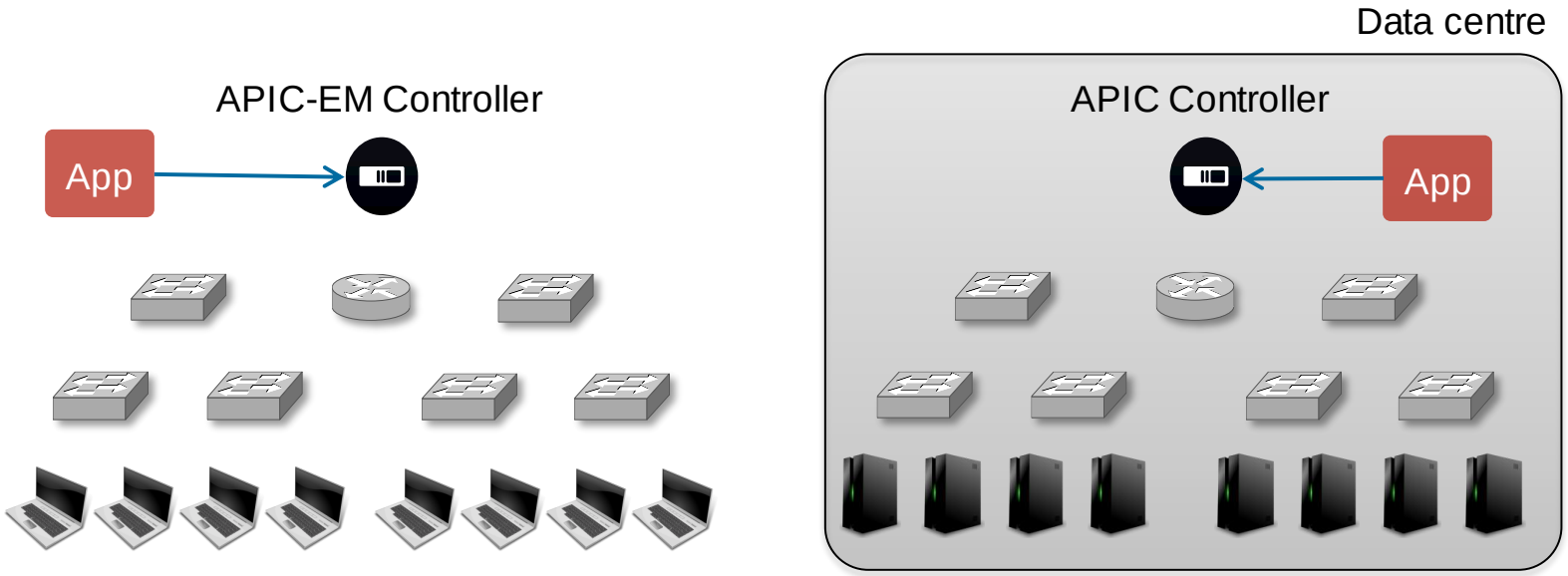
OpenFlow

onePK

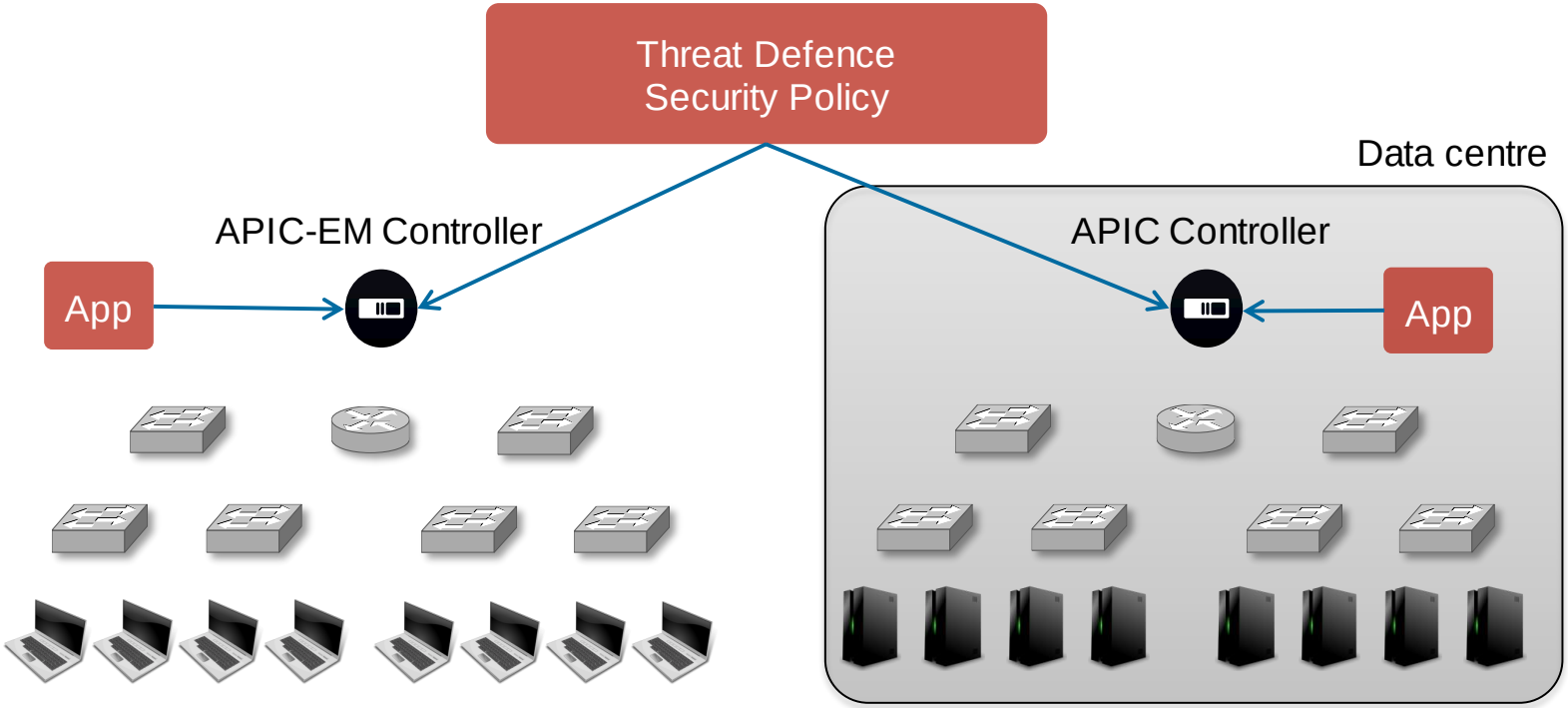


Credit: The Open DayLight Project, Inc.

Programmability Across Multiple Controllers

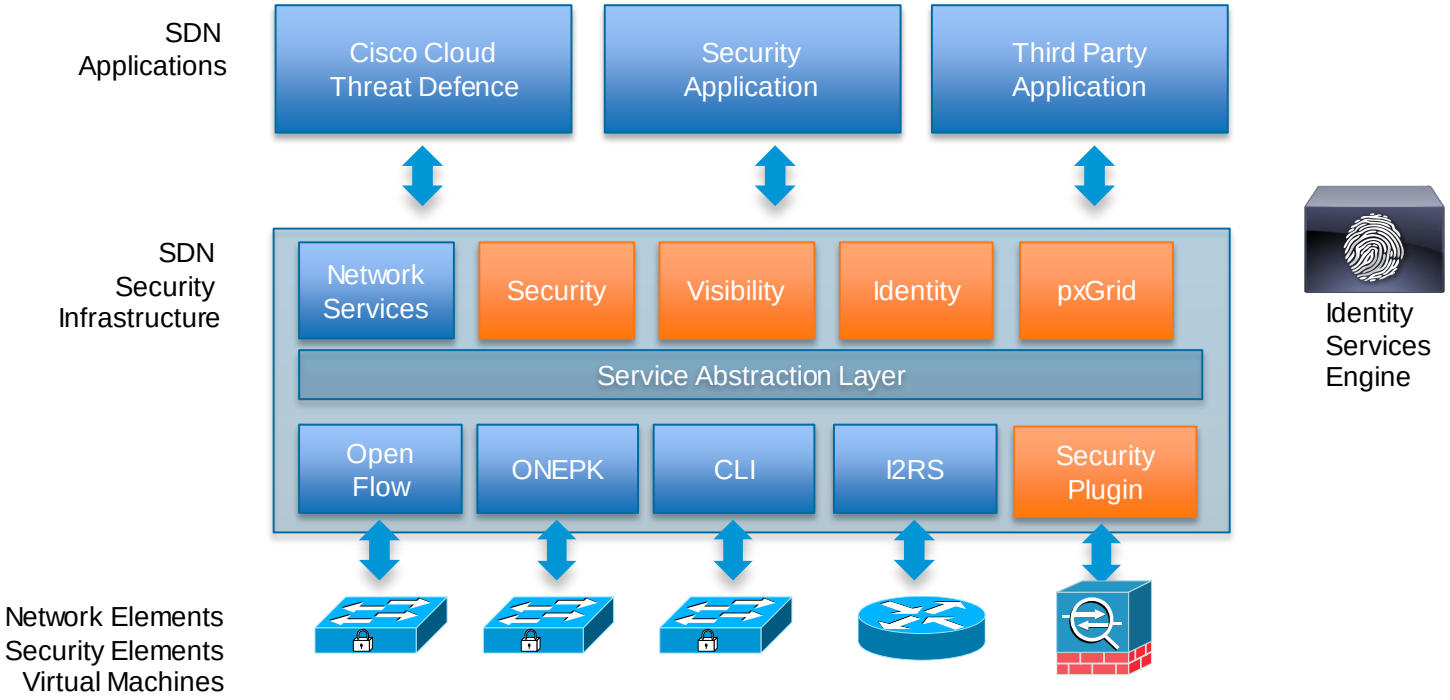


Programmability Across Multiple Controllers

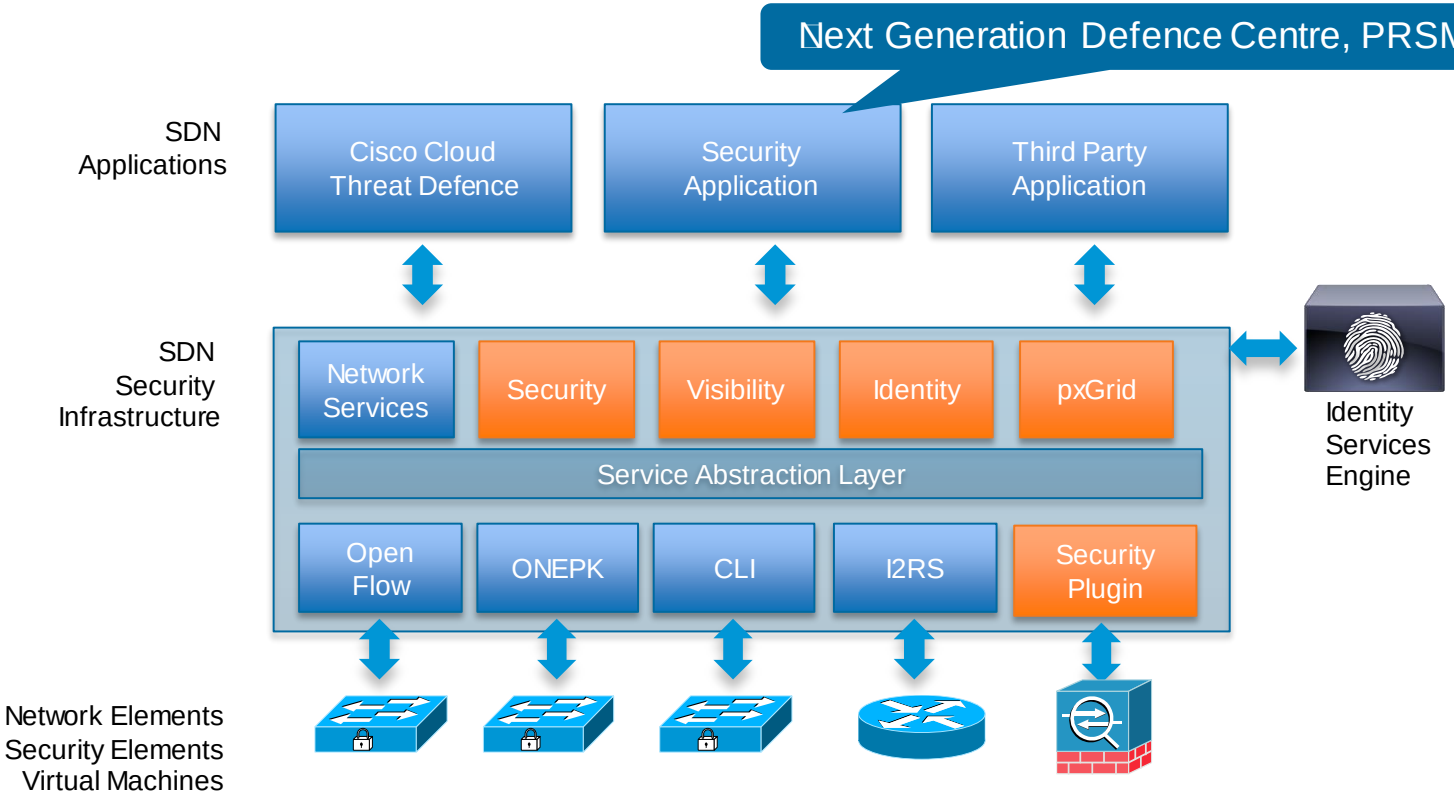


SDN Security Components

SDN Security Components

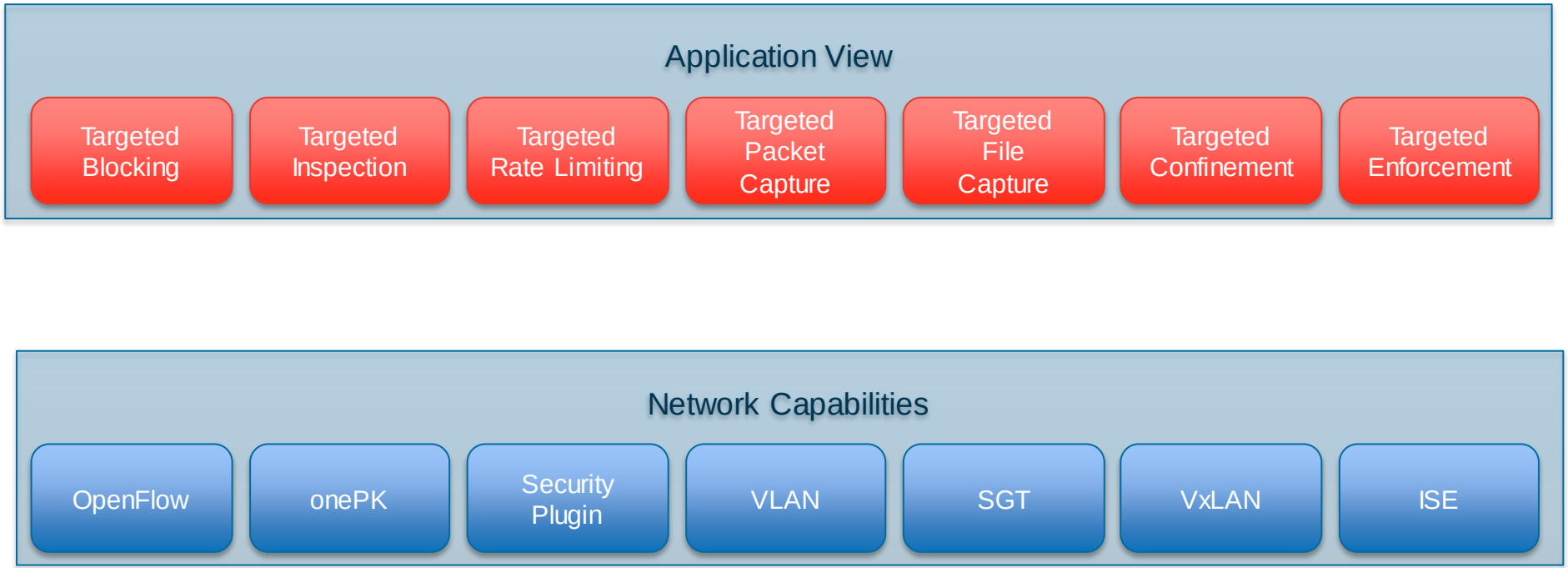


SDN Security Components



Threat Defence Services

Threat Defence Services



Security Services Through SDN

Audit

Recording

Monitoring

Inspection

Rate Limiting

DDoS Scrubbing

Quarantine

Active Web Firewall

Blocking

Security Services Through SDN

Audit

Recording

Monitoring

Inspection

Rate Limiting

DDoS Scrubbing

Quarantine

Active Web Firewall

Blocking

Security Services Through SDN

Effective
Timely

Audit

Recording

Monitoring

Inspection

Rate Limiting

DDoS Scrubbing

Quarantine

Active Web Firewall

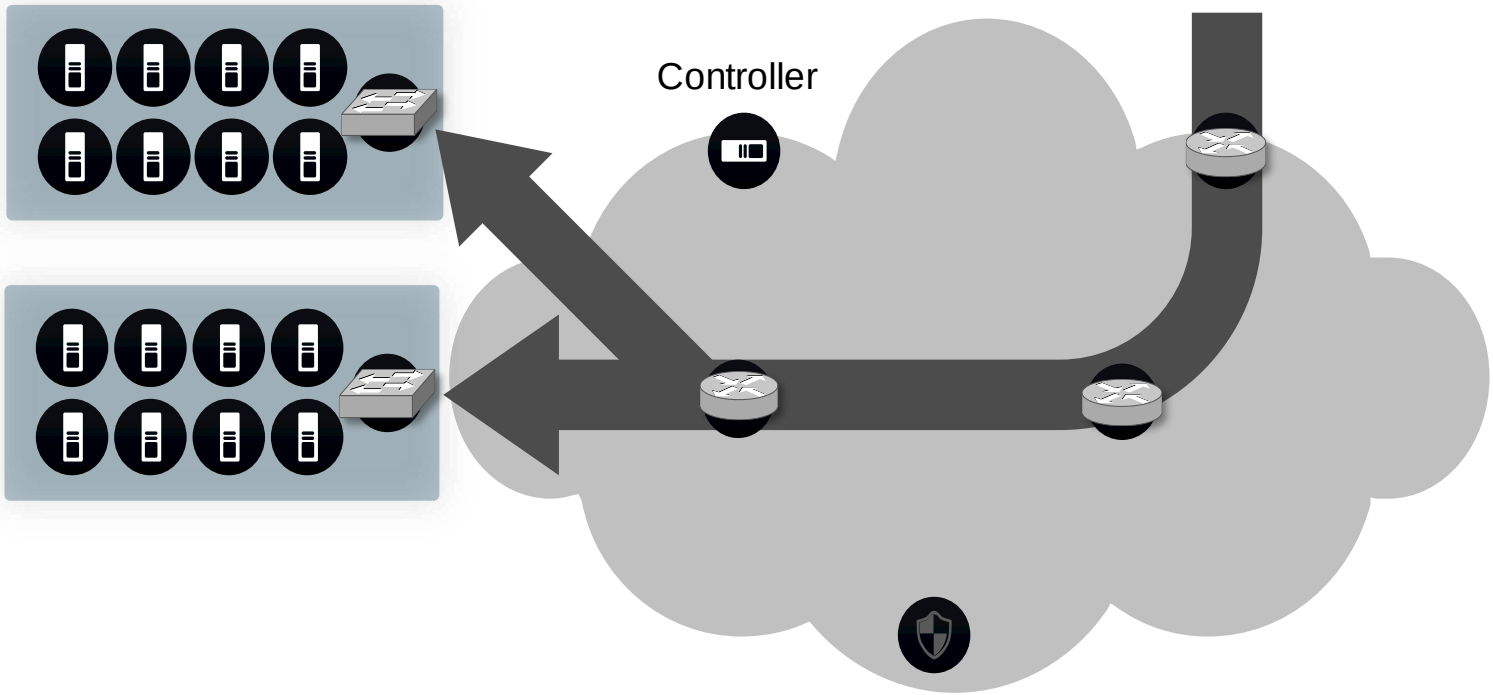
Blocking

Non-invasive

Network Controller Reconciles Mitigations Against The Needs of Mission-critical Applications

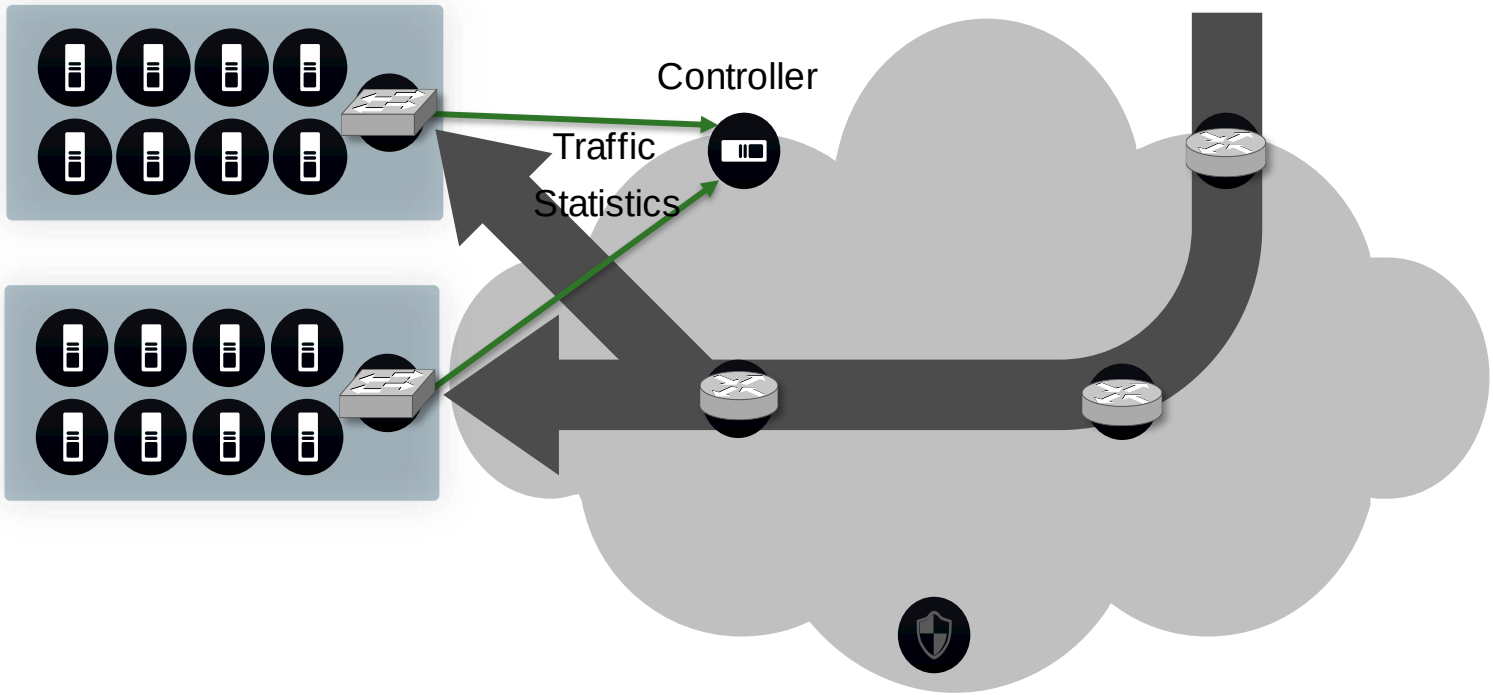
Putting SDN to Work: SDN DDoS Mitigation

Distributed Denial of Service Attack Mitigation

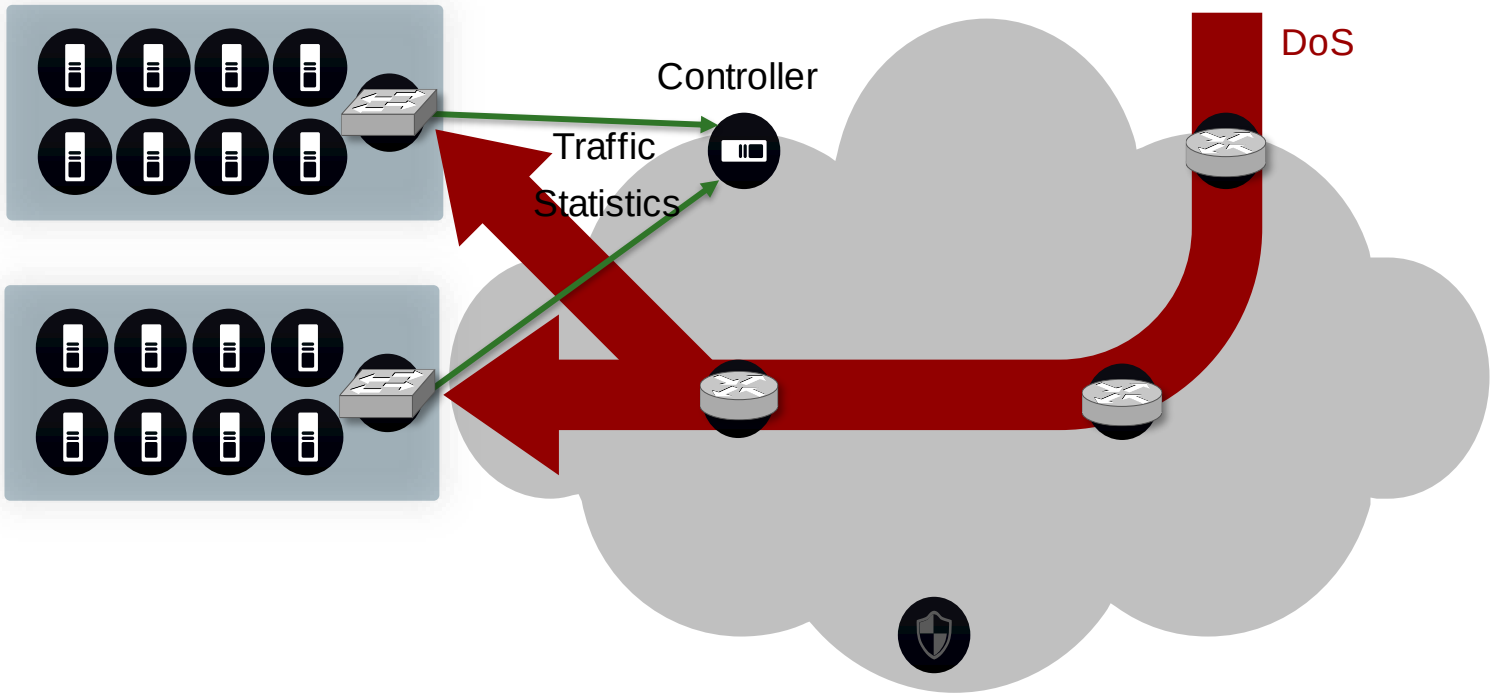


Cisco live!

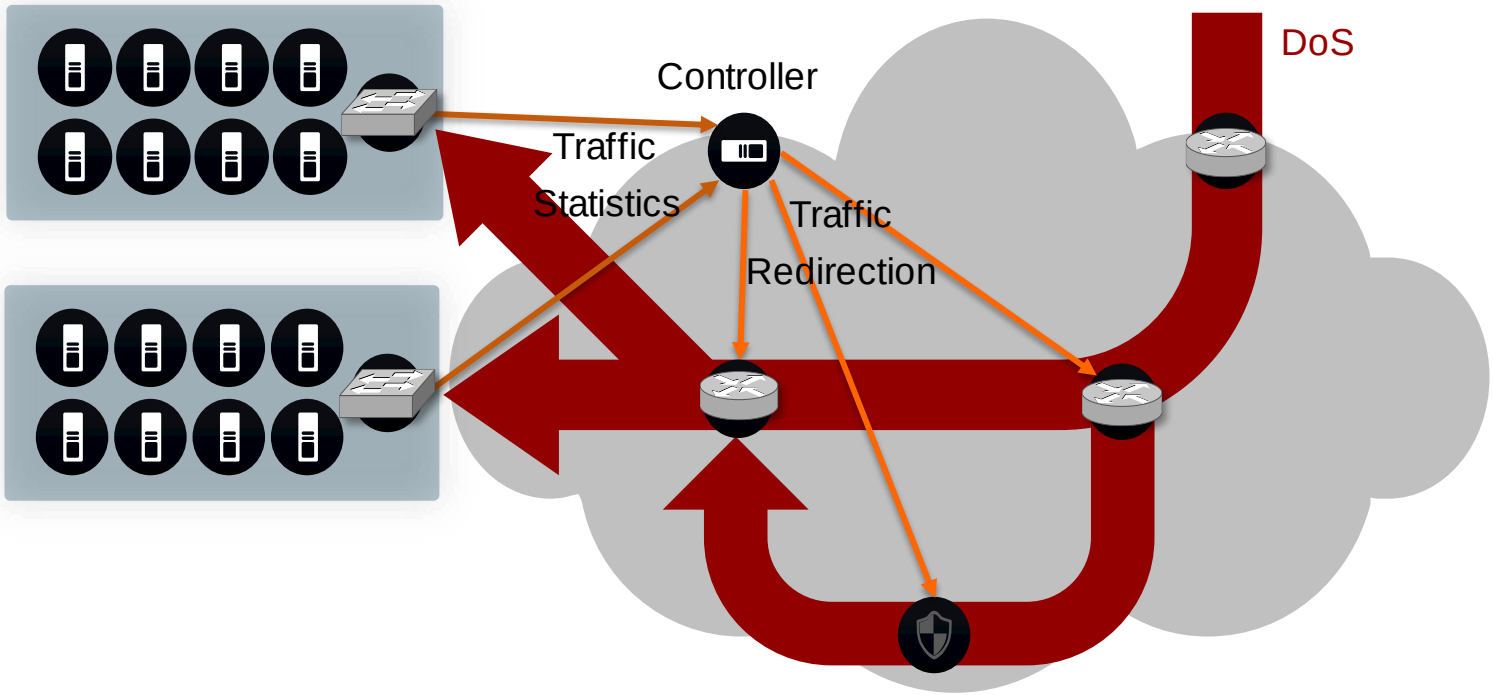
Distributed Denial of Service Attack Mitigation



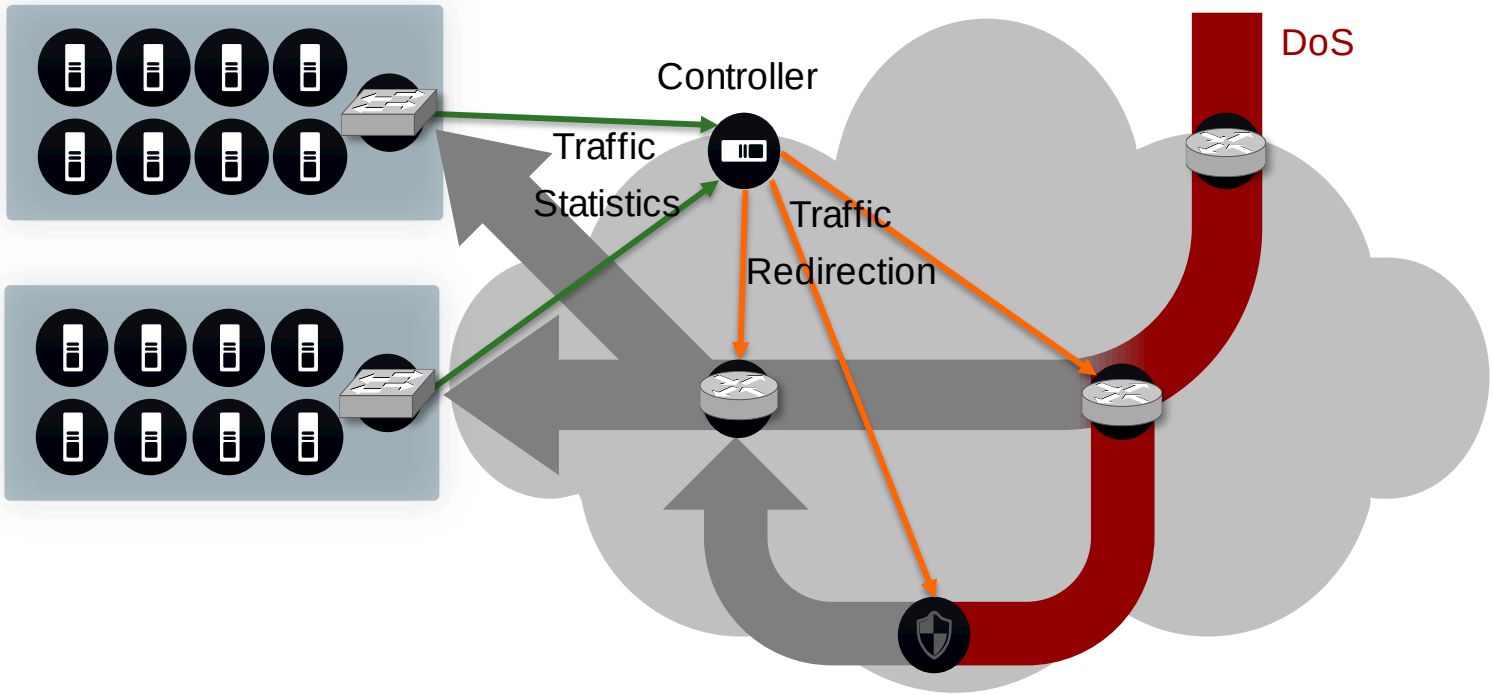
Distributed Denial of Service Attack Mitigation

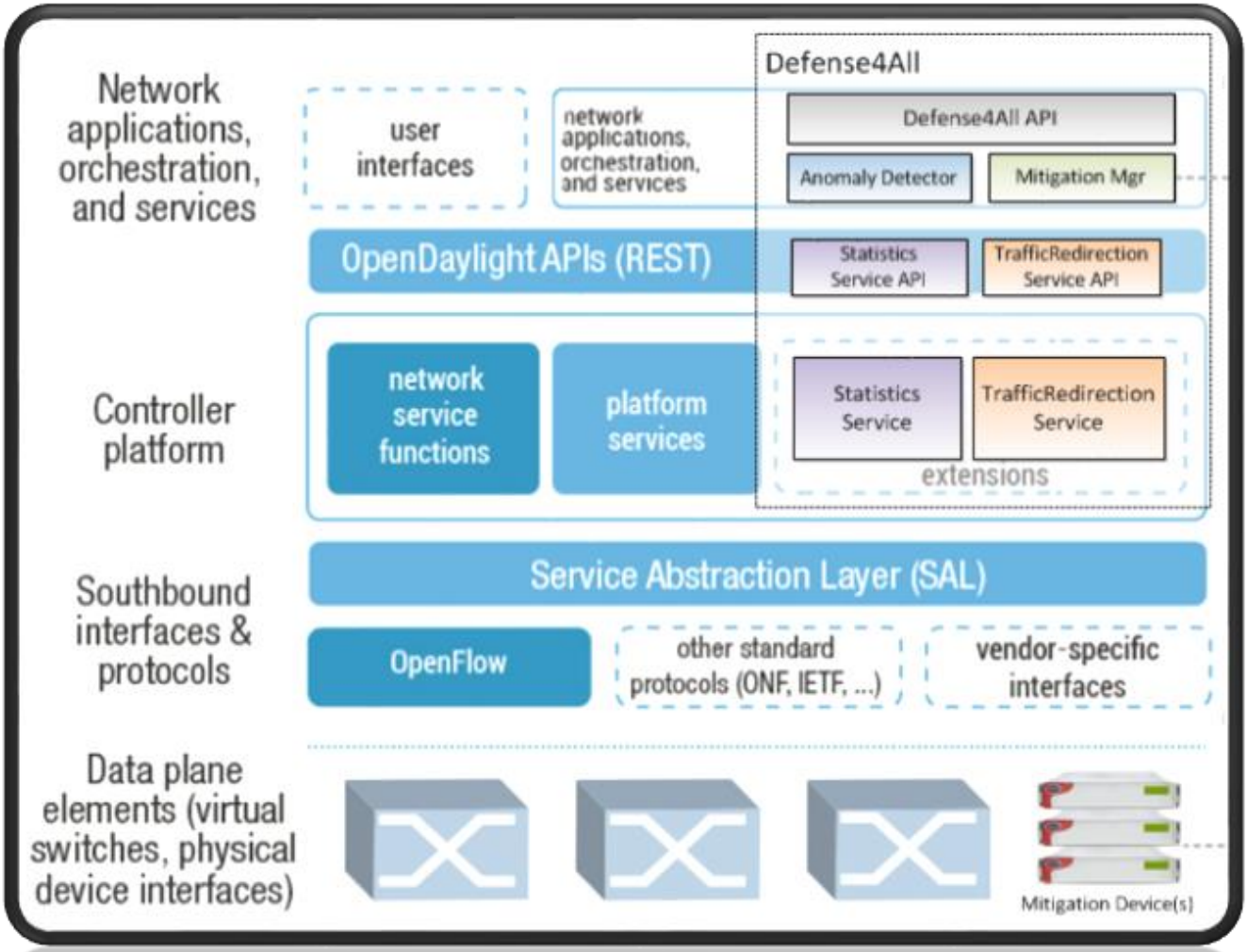


Distributed Denial of Service Attack Mitigation



Distributed Denial of Service Attack Mitigation

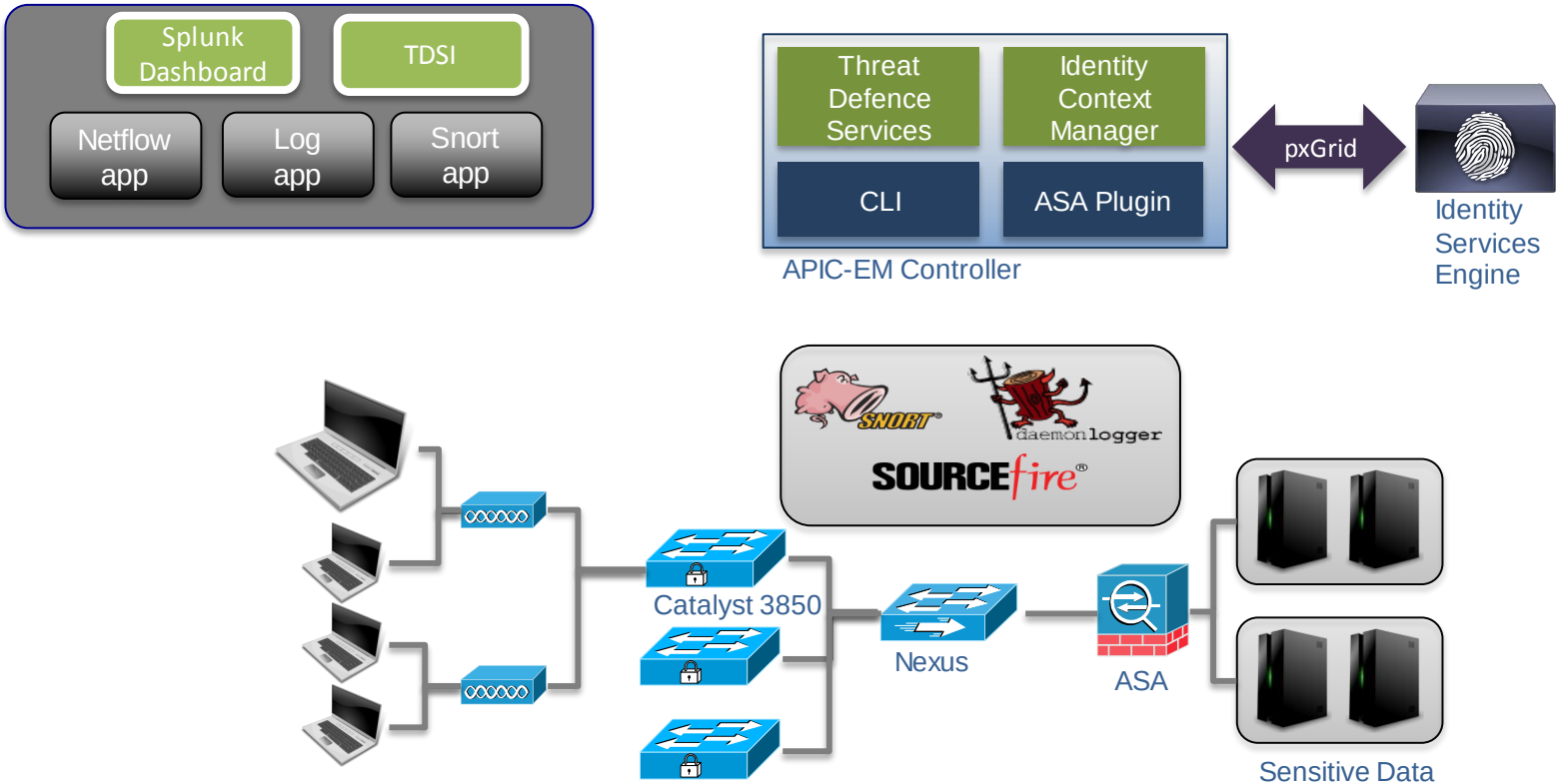




Putting SDN to Work: SDN Threat Defence

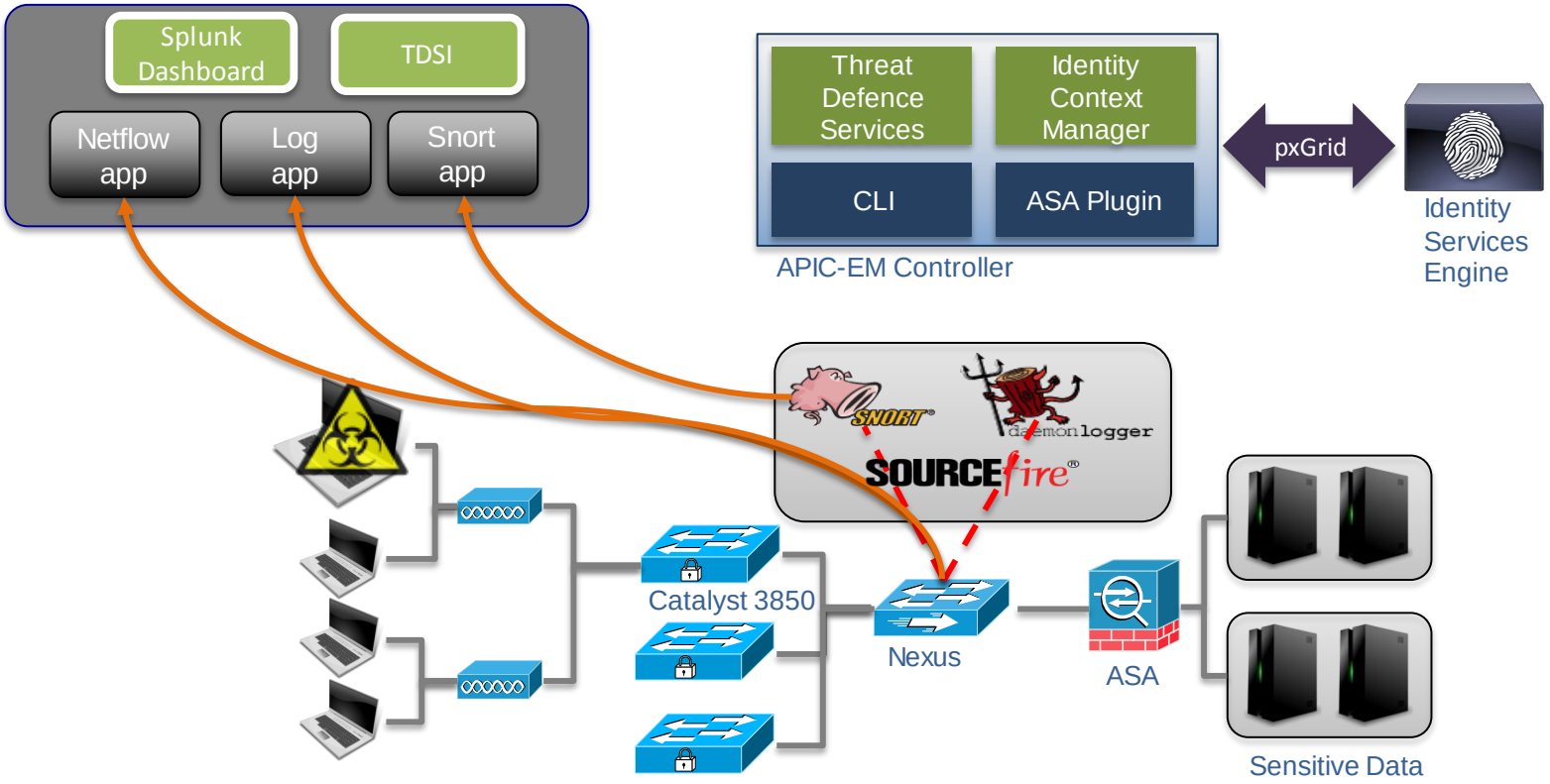
Cisco live!

SDN Threat Defence

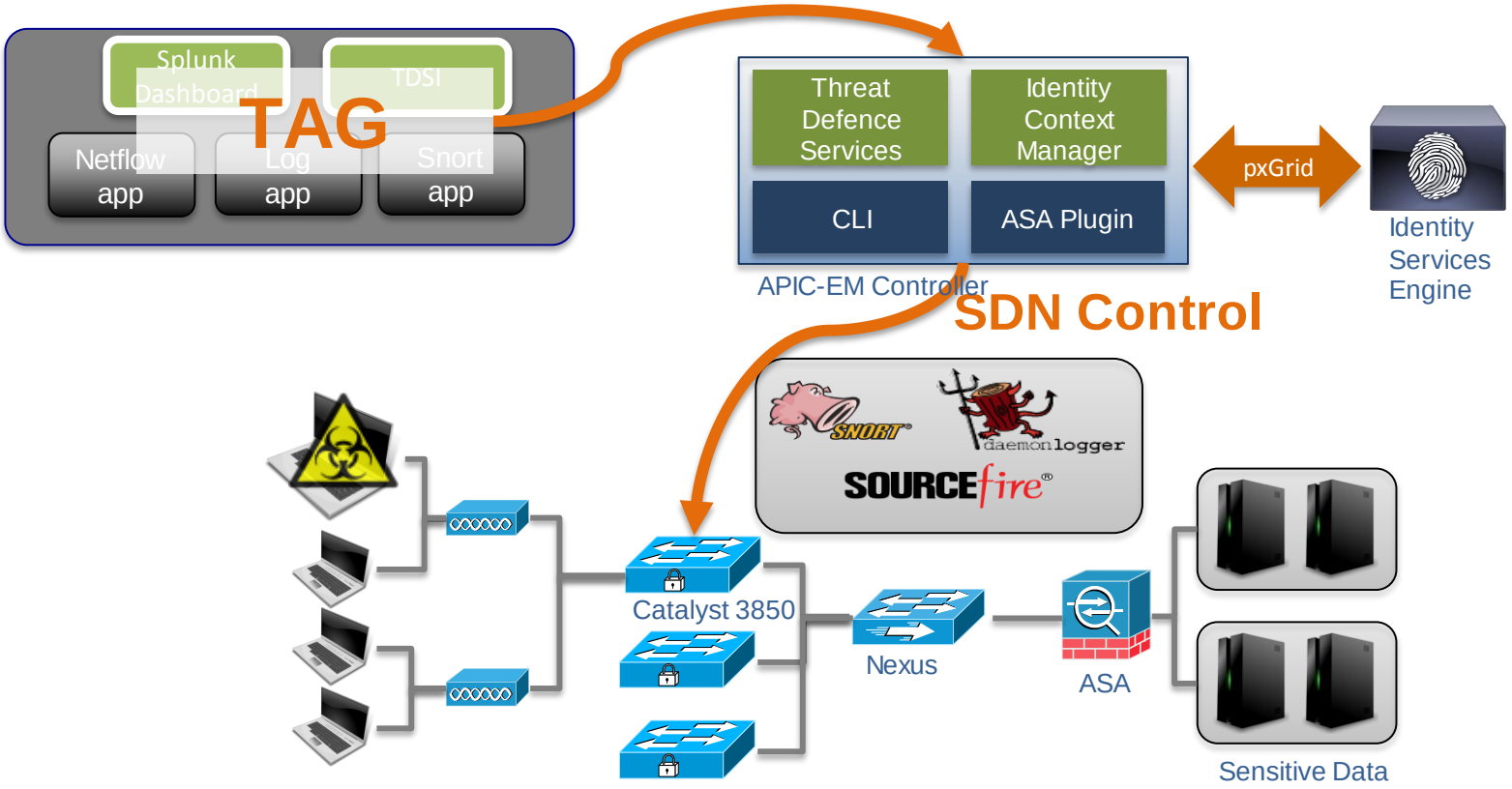


SDN Threat Defence

SDN Threat Defence

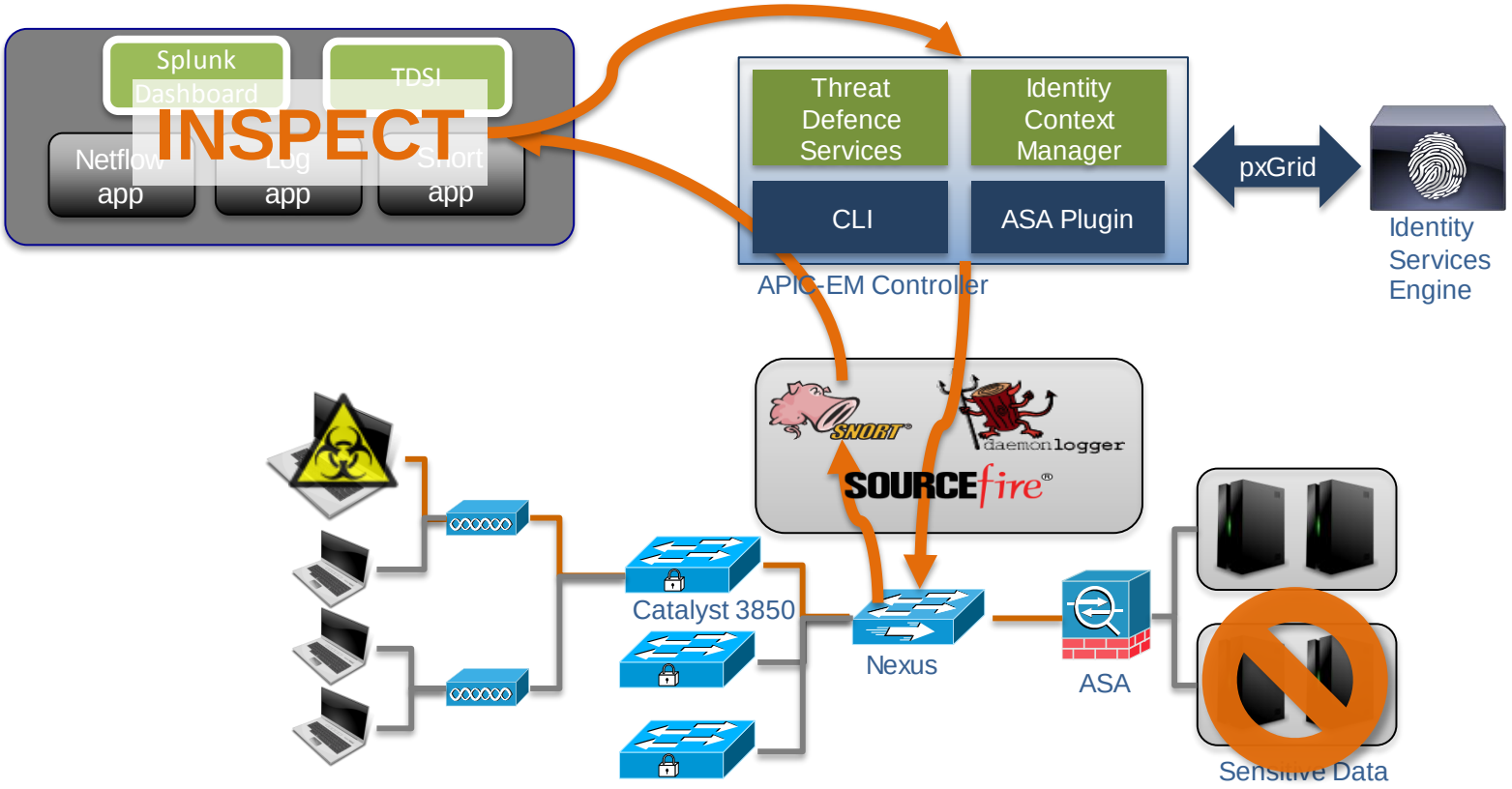


SDN Threat Defence

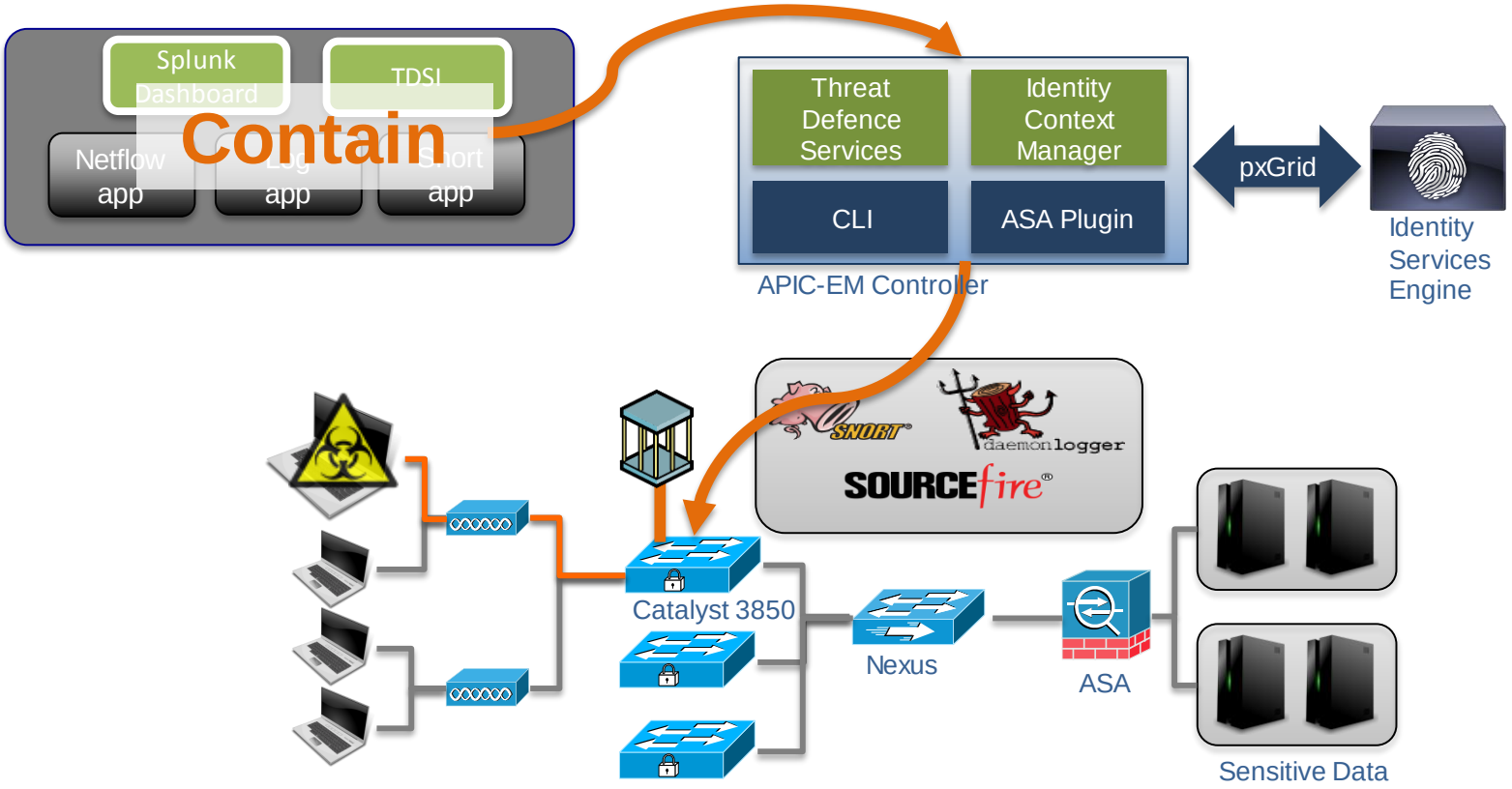


SDN Threat Defence

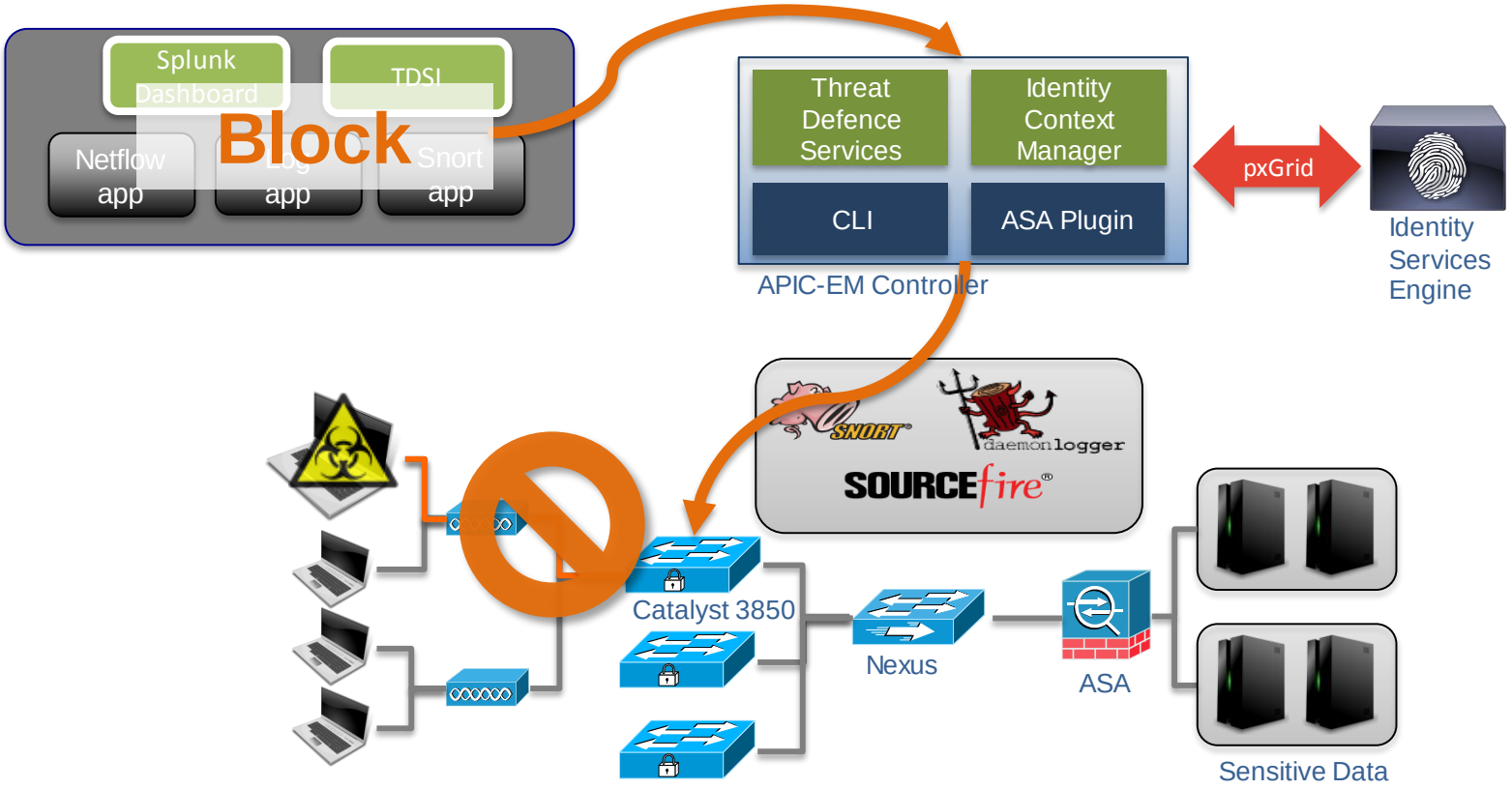
SDN Threat Defence



SDN Threat Defence

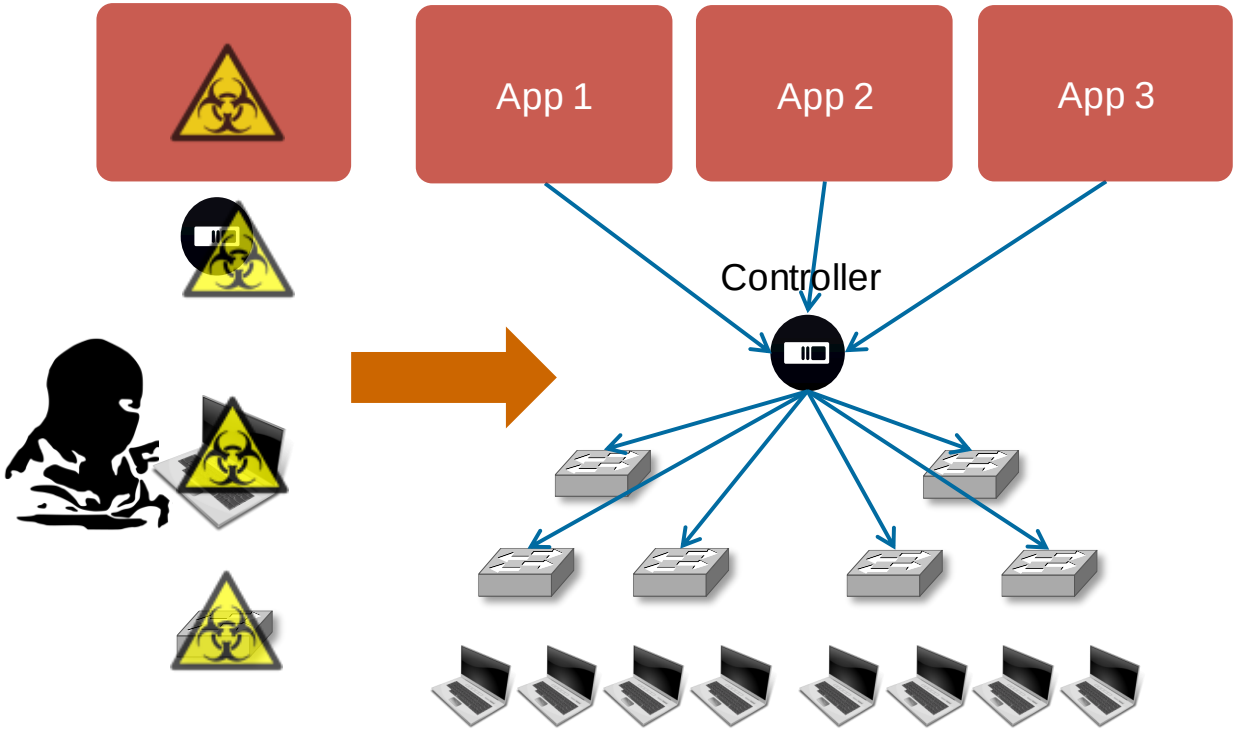


SDN Threat Defence



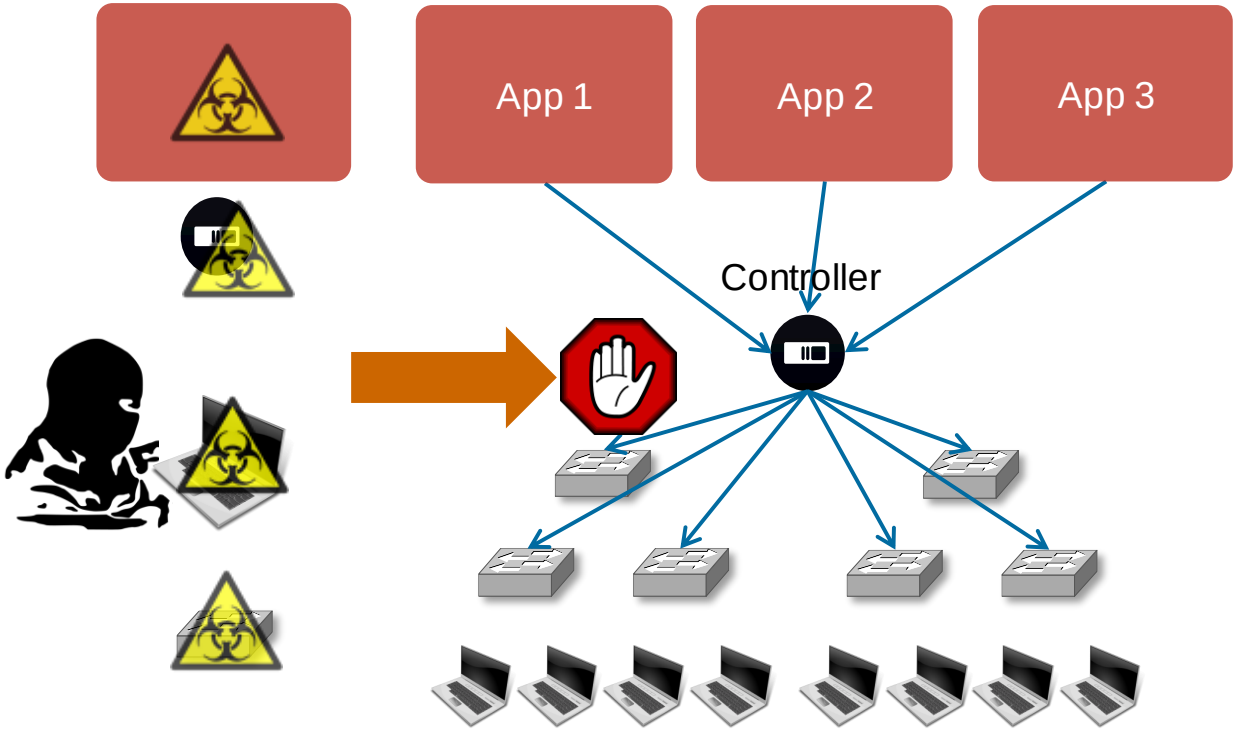

Securing SDN

Threats to an SDN System



Spoofing
Rogue
DoS Attacks

Threats to an SDN System



Hardening
Secure Provisioning
Authentication
Authorisation/RBAC
Integrity
Secure Storage
Audit

Considerations

Considerations

Detection

- How automated is your telemetry capture?
- How automated is your threat analysis?
- Are you limited by privacy considerations?

Considerations

Detection

- How automated is your telemetry capture?
- How automated is your threat analysis?
- Are you limited by privacy considerations?

Response

- What actions are you willing to take in real time?
- What actions should be one-click for a security analyst?

Considerations

Detection

- How automated is your telemetry capture?
- How automated is your threat analysis?
- Are you limited by privacy considerations?

Response

- What actions are you willing to take in real time?
- What actions should be one-click for a security analyst?

SDN

- What type of SDN can you use?
- How SDN-ready is your network?
- SDN security?

Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings


Q & A
Cisco live!

Complete Your Online Session Evaluation

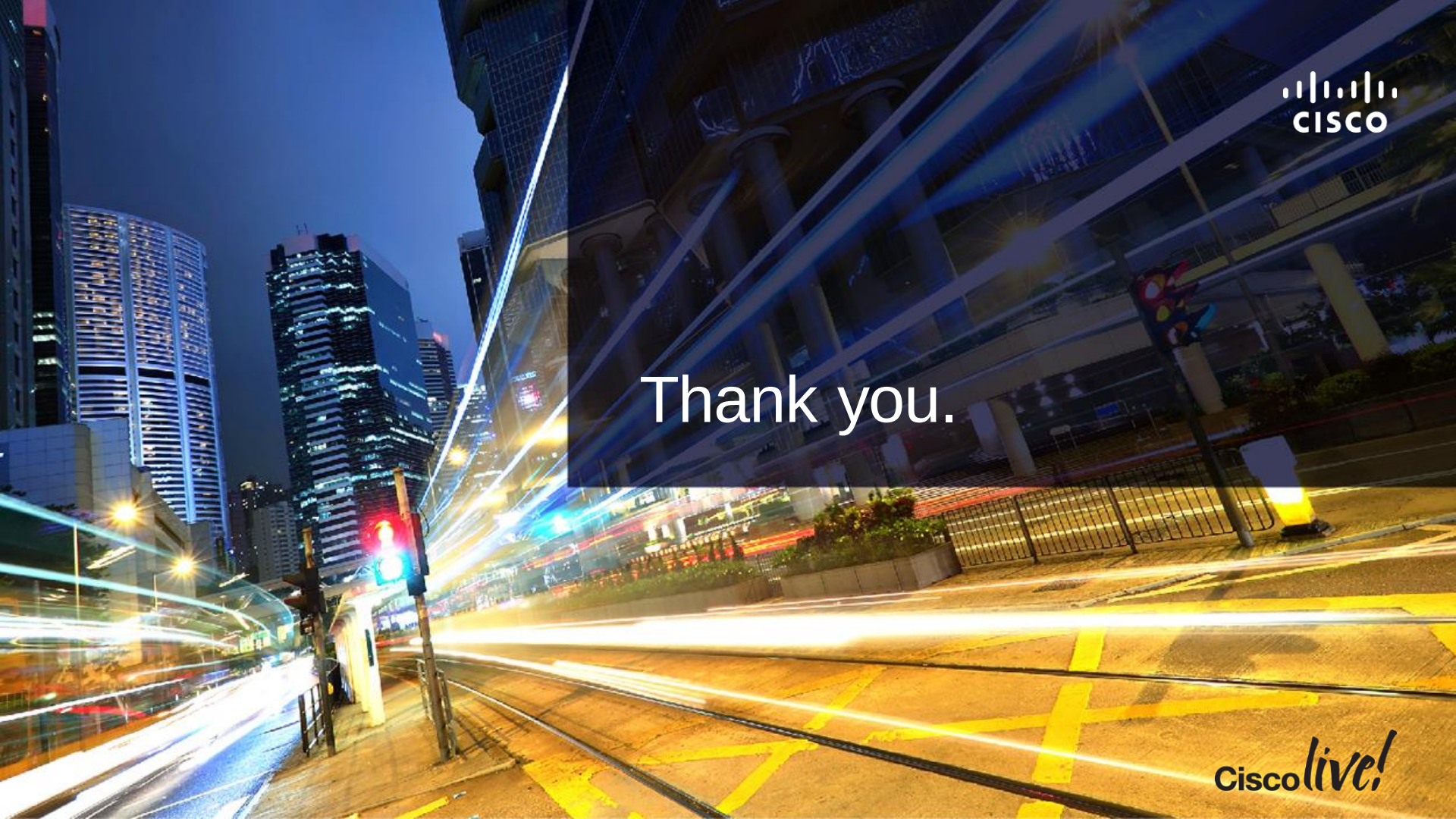
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com


Thank you.
CISCO
Cisco live!


CISCO