
TOMORROW
starts here.
CISCO
Cisco live!

Introduction to Data Centre Security

BRKSEC-1205

Sohaib Ahmed – Systems Engineer

#clmel

Cisco live!

Session Abstract

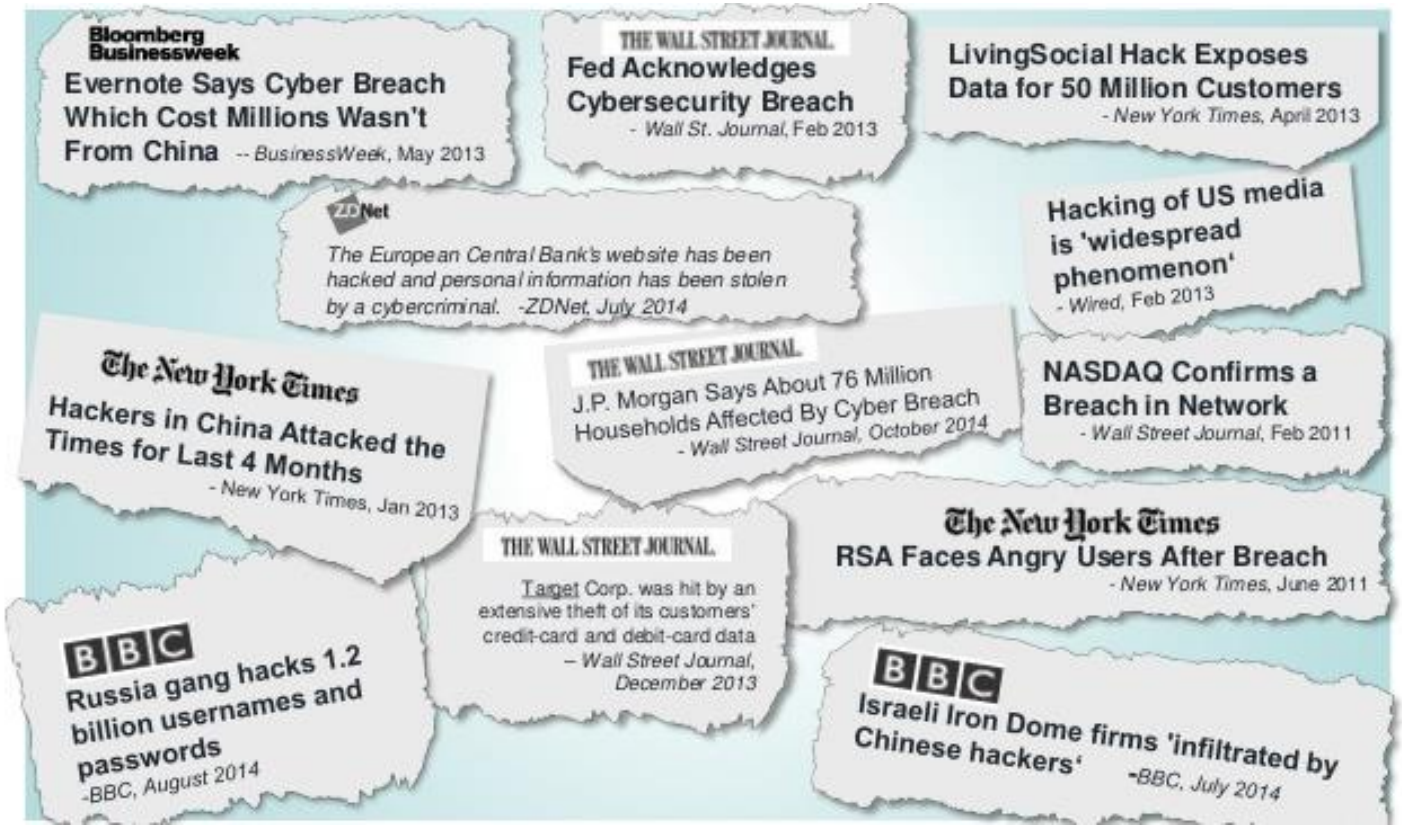
This session will outline how security can be propagated throughout the Data Centre and define how these technologies can work together to build a secure Data Centre and Cloud strategy for the enterprise. Topics covered will include Current Threats, Security Hardware and Software, Network Segmentation, Cloud Connectivity, Software Defined Networks, Security Architectures and more. This session will provide an **overview** to anyone interested in how Security can be inserted in their Data Centre.

Agenda

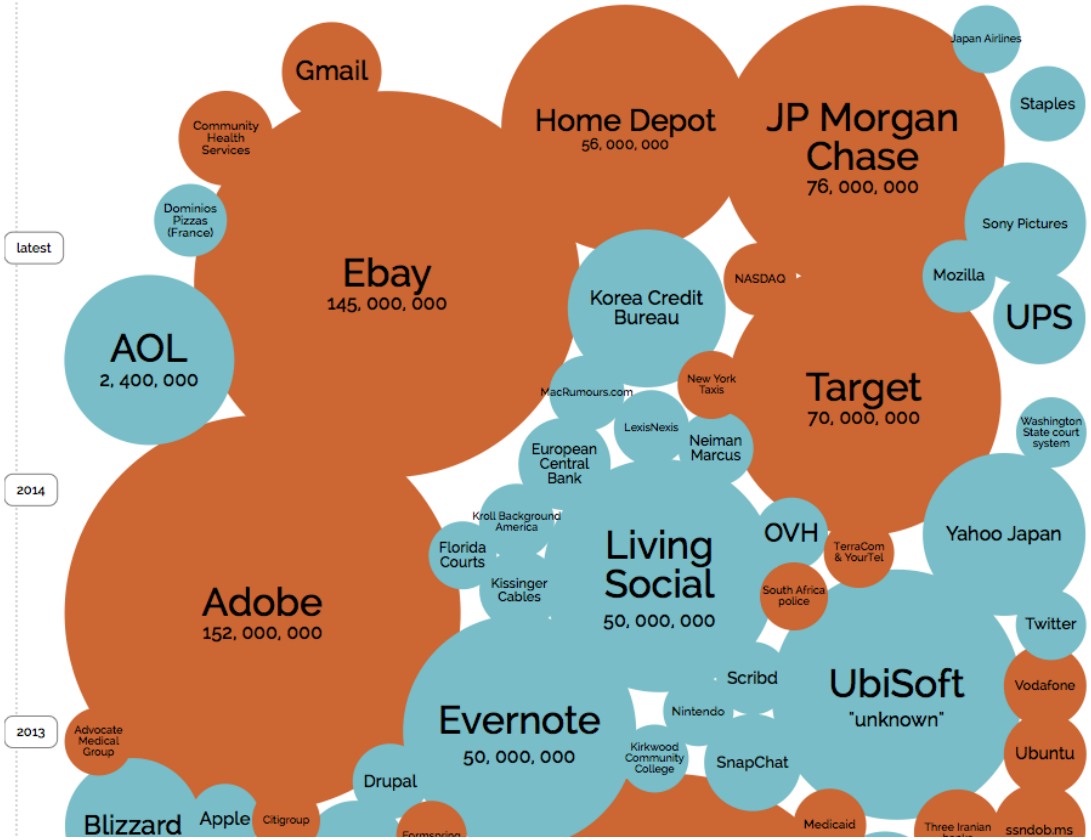
- **Introduction**
  - **The Security Challenge**
  - **Trends Impacting the Data Centre**
  - **New Security Model**
- Security in the Data Centre
- Data Centre Design
- Data Centre Security with Application Centric Infrastructure
- Conclusion

Myth Buster – Data Centre Edition

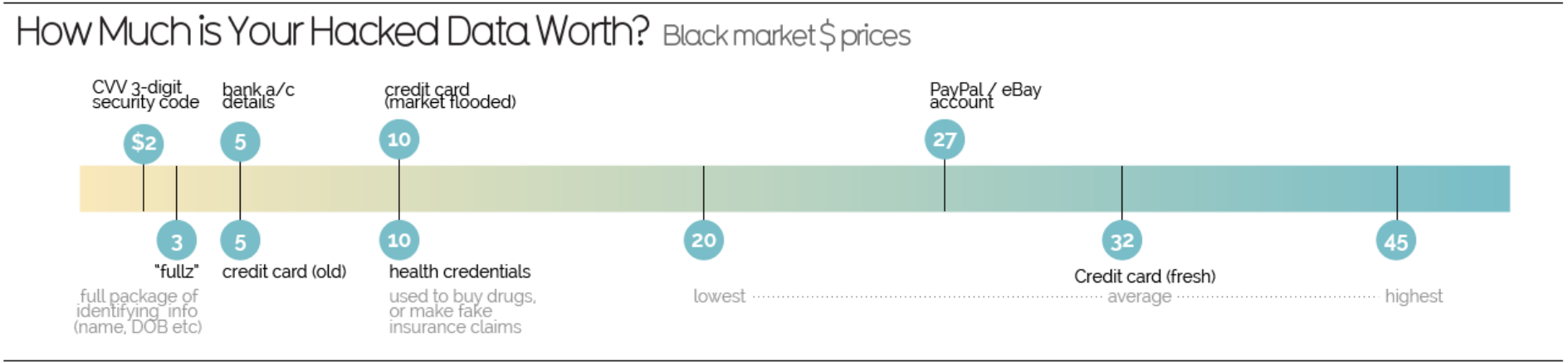
We Live the Headlines



World's Biggest Data Breaches



Source: Information is beautiful – World's Biggest Data Breaches



Source: Information is beautiful – World's Biggest Data Breaches

Your Biggest Security Challenges

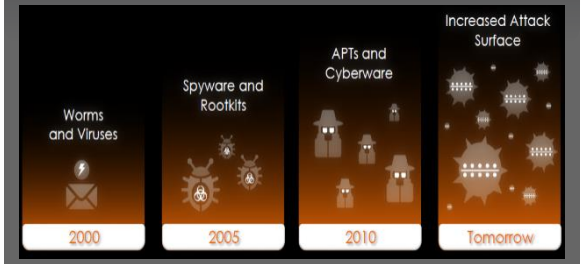
Maintain Security and Compliance as business models change (Agility)

Stay ahead of the threat landscape

Reduce complexity and fragmentation of security solutions

Trends Impacting Data Centre Security

EVOLVING THREATS



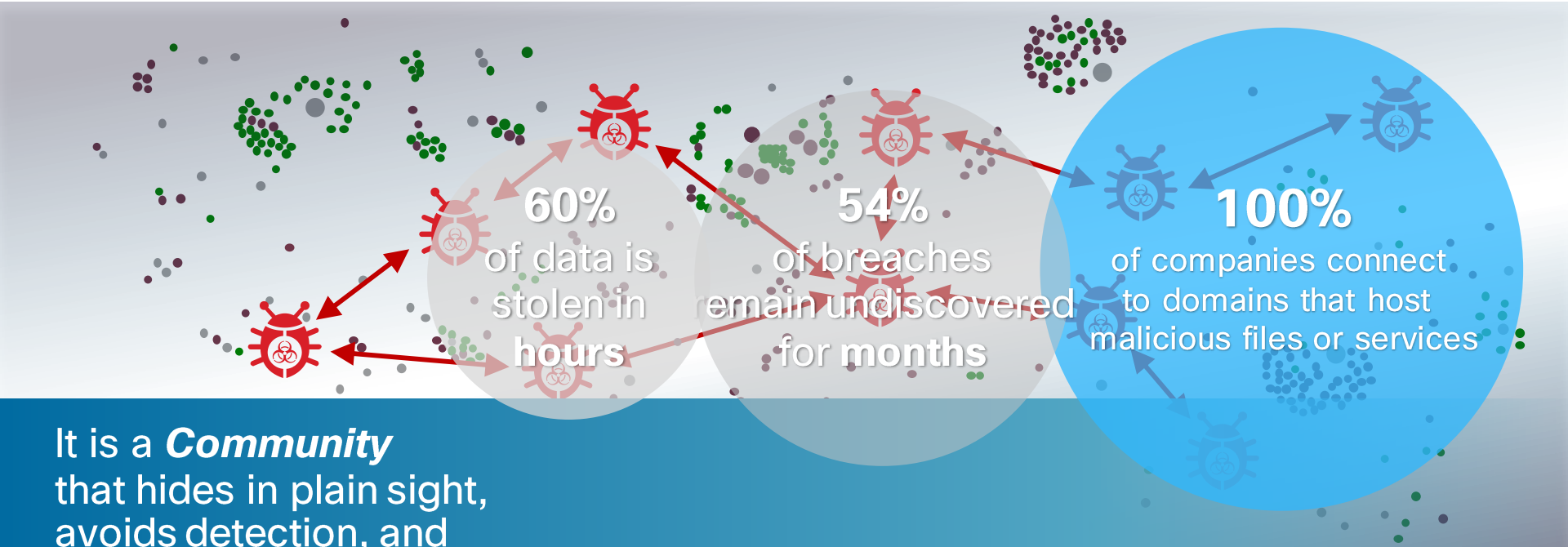
NEW APPLICATIONS (PHYSICAL, VIRTUAL AND CLOUD)

NEW TRAFFIC TRENDS

Source: Cisco Global Cloud Index, 2012

Trends Impacting the Data Centre

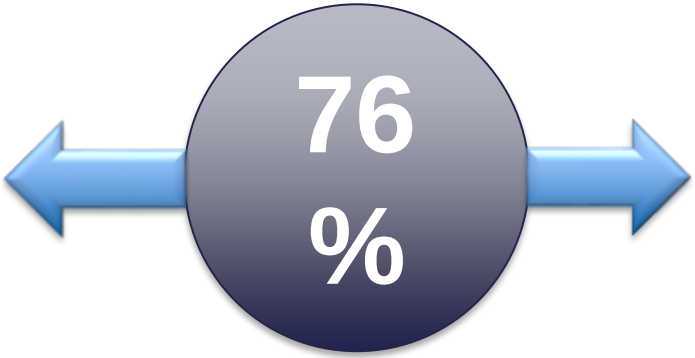
Evolving Threat Landscape



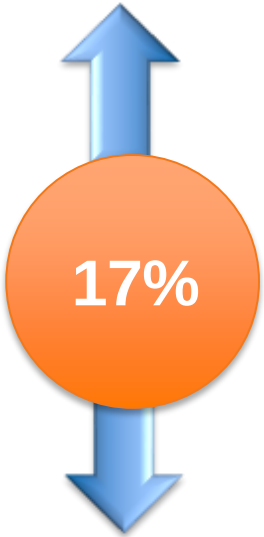
It is a ***Community*** that hides in plain sight, avoids detection, and attacks swiftly

Trends Impacting the Data Centre

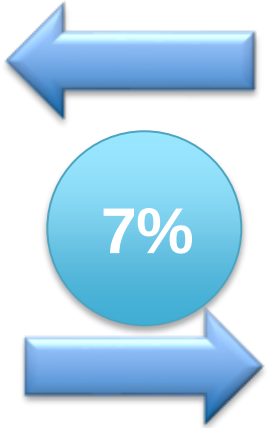
Traffic Patterns in the Data Centre



East – West Traffic



North – South Traffic

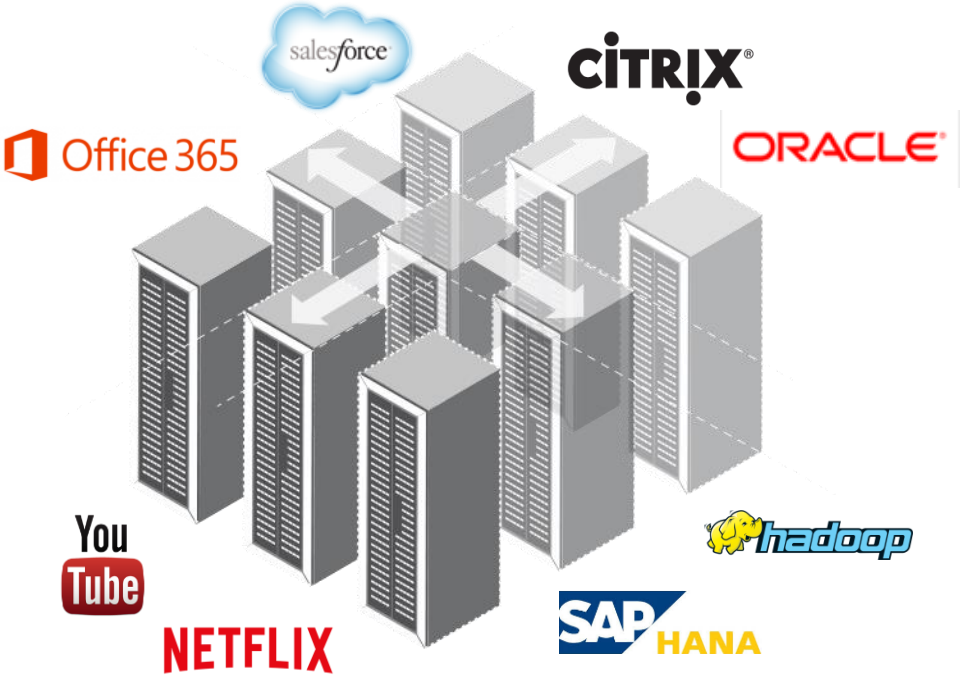


Inter-DC Traffic

Source: Cisco Cloud Index 2012

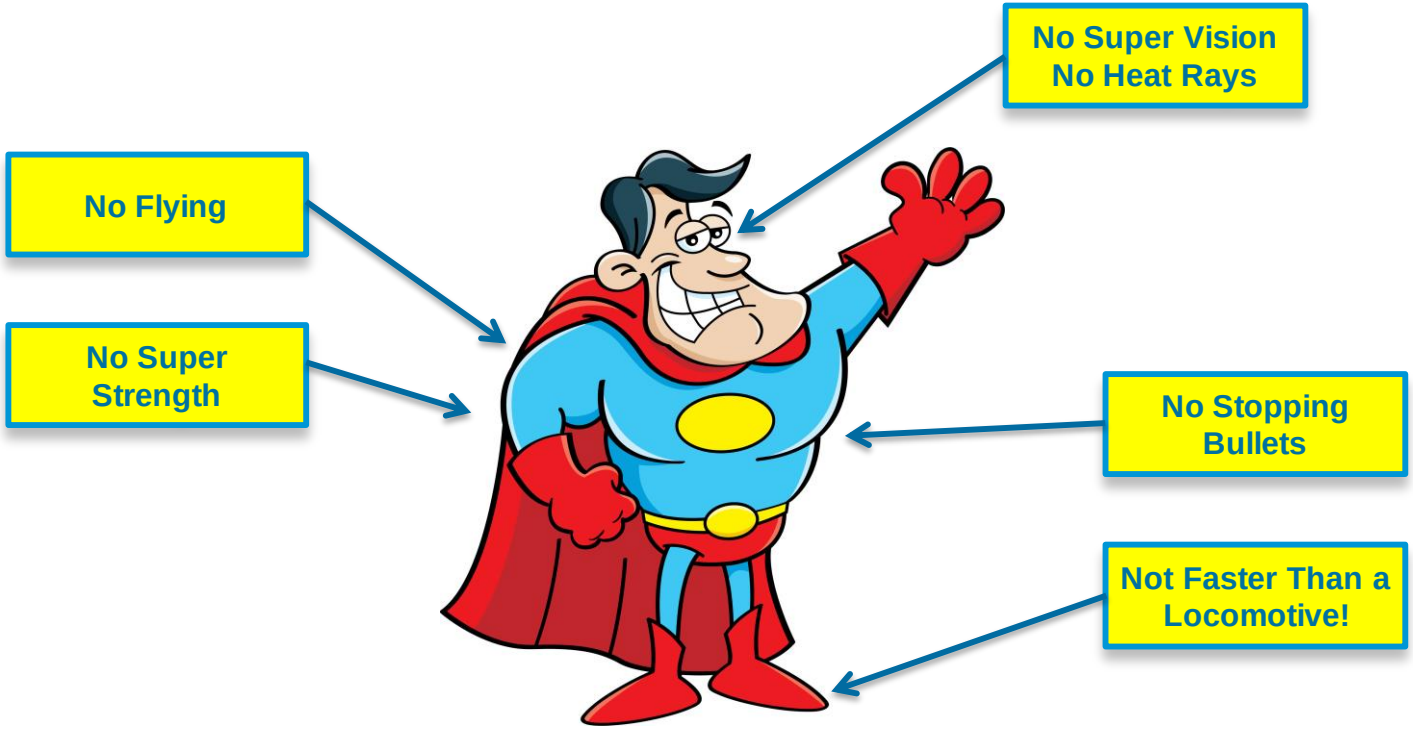
Trends Impacting the Data Centre

Physical, Virtual and Cloud Applications



Capabilities Enables Us to Do Incredible Things….

What if Superman did not have capabilities?



Without Capabilities…

All you have left is hope!

We MUST give our Cyber Defenders capabilities beyond access controls!

Myth Buster – Data Centre Edition

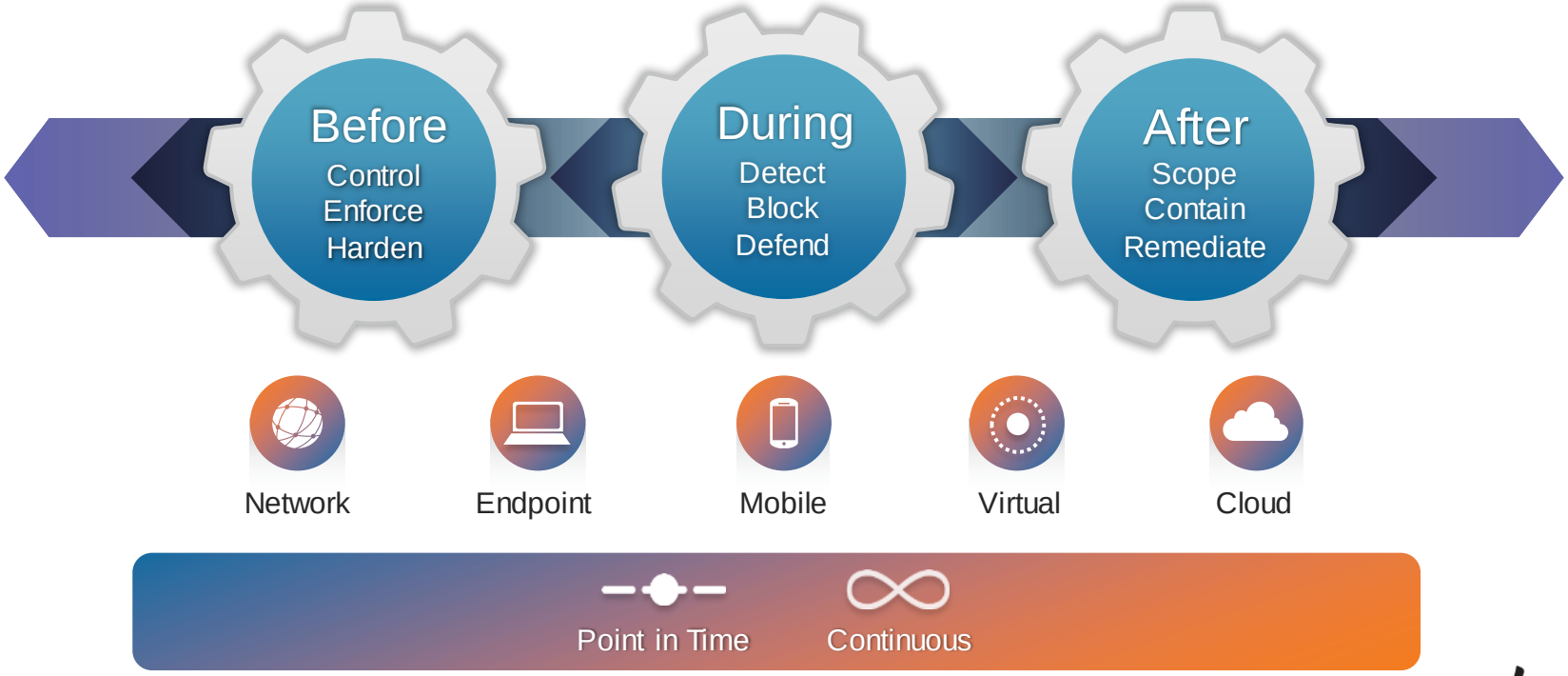
Myth # 1

Security in the Data Centre is not my responsibility

FACT: Security should be a collective thought process from all stakeholders i.e. Application, Security or Network teams. Security should be a design requirement from Day

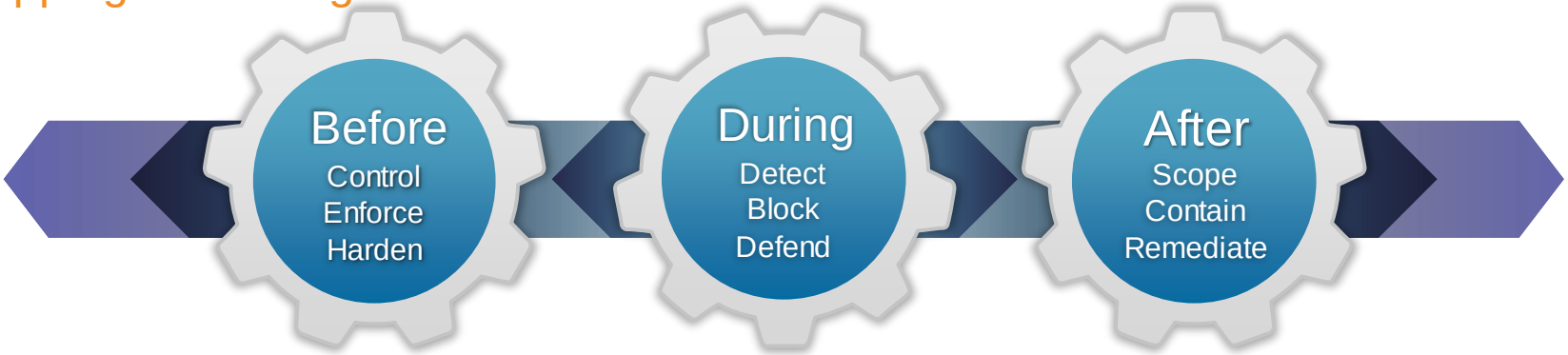
The Security Model

The Attack Continuum



Attack Continuum

Mapping Technologies to the Model



Firewall	Patch Mgmt	IPS	IDS	AMD
App Control	Vuln Mgmt	Anti-Virus	FPC	Log Mgmt
VPN	IAM/NAC	Email/Web	Forensics	SIEM

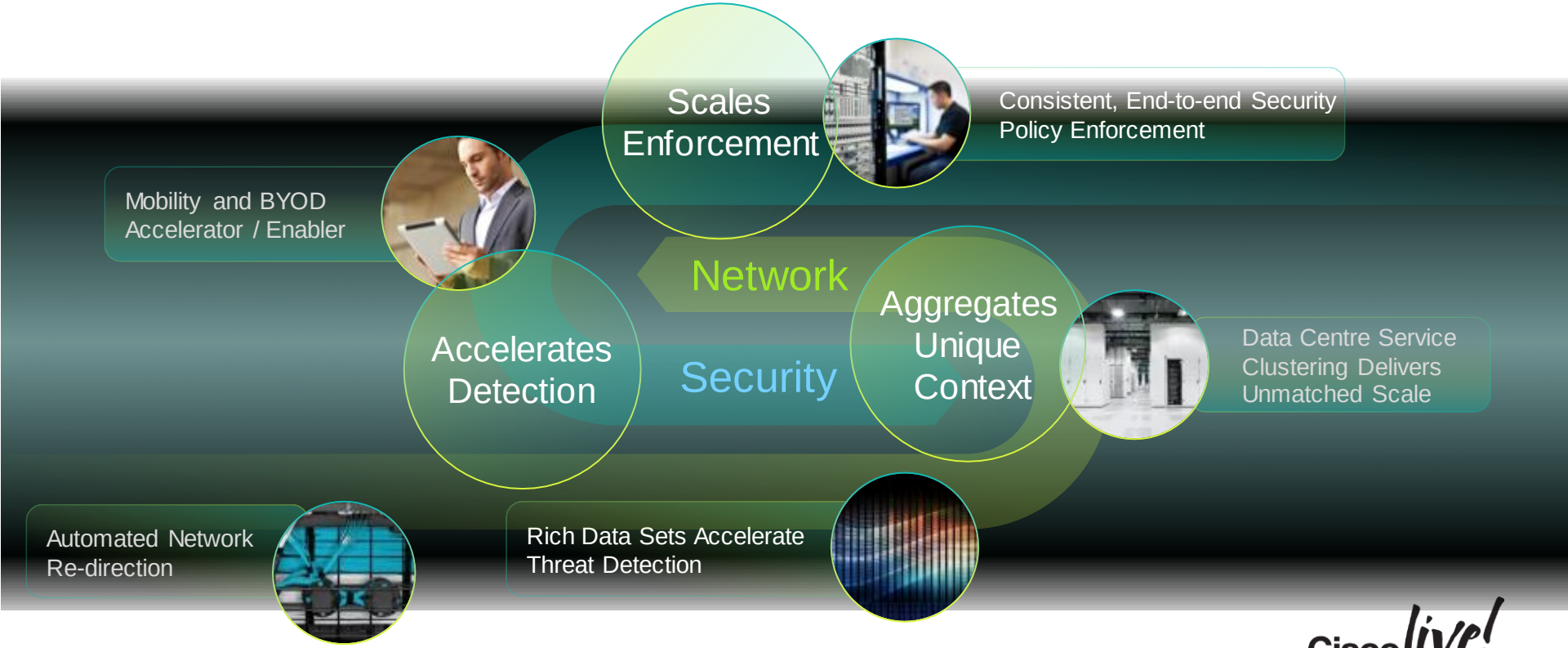
Visibility and Context

Agenda

- Introduction
- **Security in the Data Centre**
  - **Key Requirements**
- Data Centre Design
- Data Centre Security with Application Centric Infrastructure
- Conclusion

Security in the Data Centre

Synergy between Security and the Network



Security in the Data Centre

Key Requirements

Scale	Need for elastic scaling through network integration
Resiliency	High availability is imperative for applications in the data centre
Flexibility	Need for reducing complexity in inserting services
Actionable Security	Desire to extend a chain of trust from the user to the application

Security in the Data Centre

Key Requirements

Scale	Need for elastic scaling through network integration
Resiliency	High availability is imperative for applications in the data centre
Flexibility	Need for reducing complexity in inserting services
Actionable Security	Desire to extend a chain of trust from the user to the application

Scalability Requirements

★ Best Practice

- Policies ★
- Performance and Latency ★
- Application Tiers
- Security Operations (SecOps)
- Modular Enclaves ★
- Enclave Management and Lifecycle Management

Scalability Requirements

Scalable Policies with TrustSec

- Simplified Access Management
- Accelerated Security Operations
- Consistent Policies - Anywhere

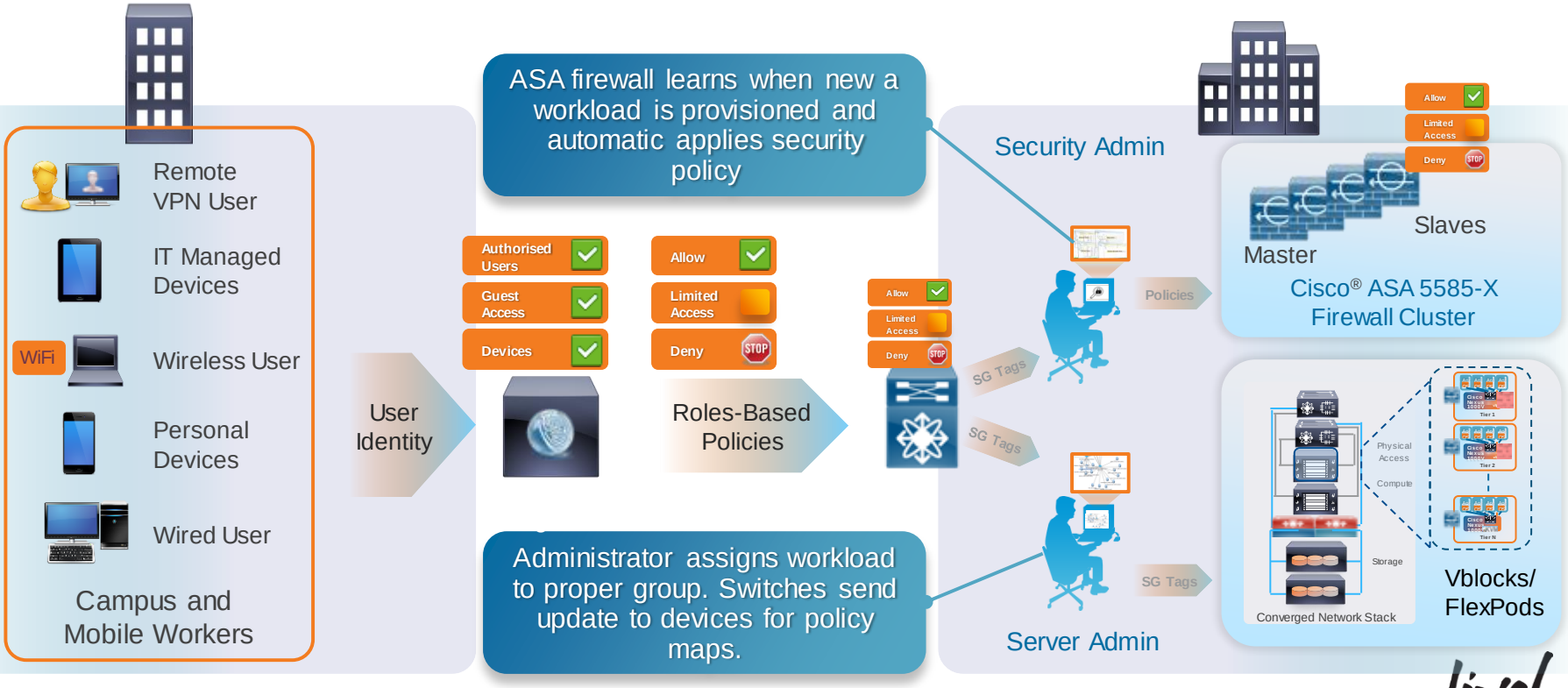
```
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243
255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255
eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq
4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
access-list 102 deny ip 124.236.172.134 255.255.255.255 gt 859 56.81.14.184 255.55.255.255 gt
2754
access-list 102 deny icmp 227.161.68.159 0.0.31.255 lt 3228 78.113.205.236 255.55.255.255 lt
486
```

Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

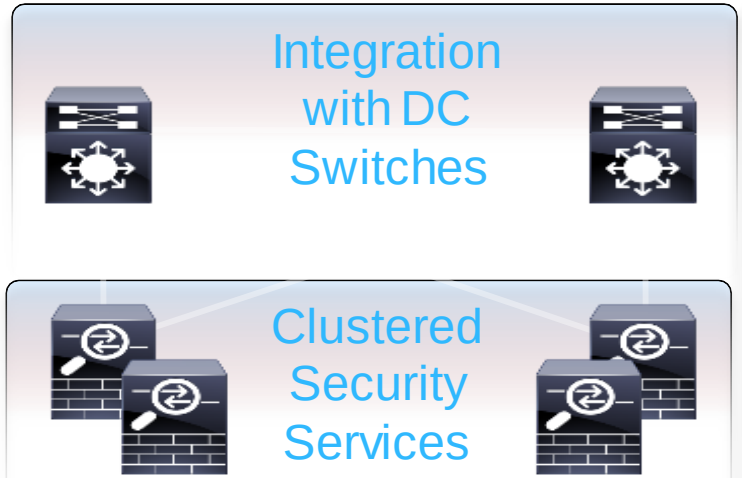
Scalability Requirements

Scalable Policy Enforcement and Management



Scalability Requirements

Scalable Performance



Technology	Benefit
Integration with VSS, vPC and Fabric Path	Ease of Deployment Solves Asymmetric Traffic
Consistent Scaling Factor	Linear, Predictable Performance Increase
Pay as You Grow	Only Buy What You Need
FW, VPN, IPS Services	Compliance and Security

Security in the Data Centre

Key Requirements

Scale	Need for elastic scaling through network integration
Resiliency	High availability is imperative for applications in the data centre
Flexibility	Need for reducing complexity in inserting services
Actionable Security	Desire to extend a chain of trust from the user to the application

Resiliency Requirements

★ Best Practice

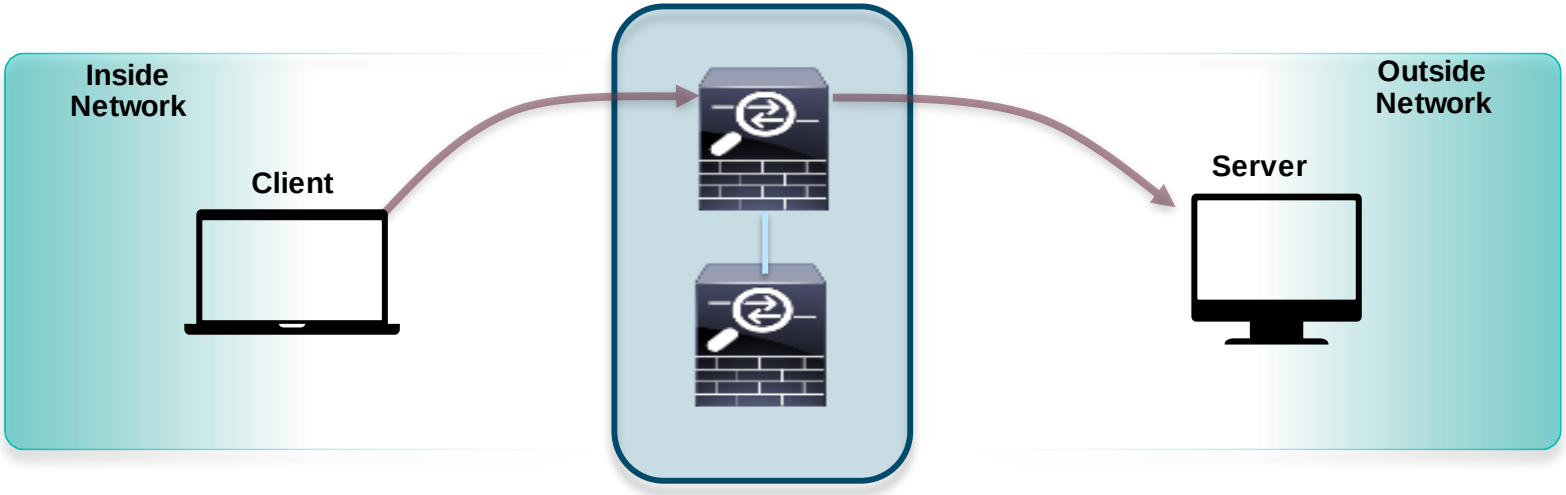
- Asymmetric traffic handling ★
- Flow redundancy ★
- No traffic black-holing and packet loss

Resiliency Requirements

Resilient Traffic Handling – Symmetric Traffic

Resiliency Requirements

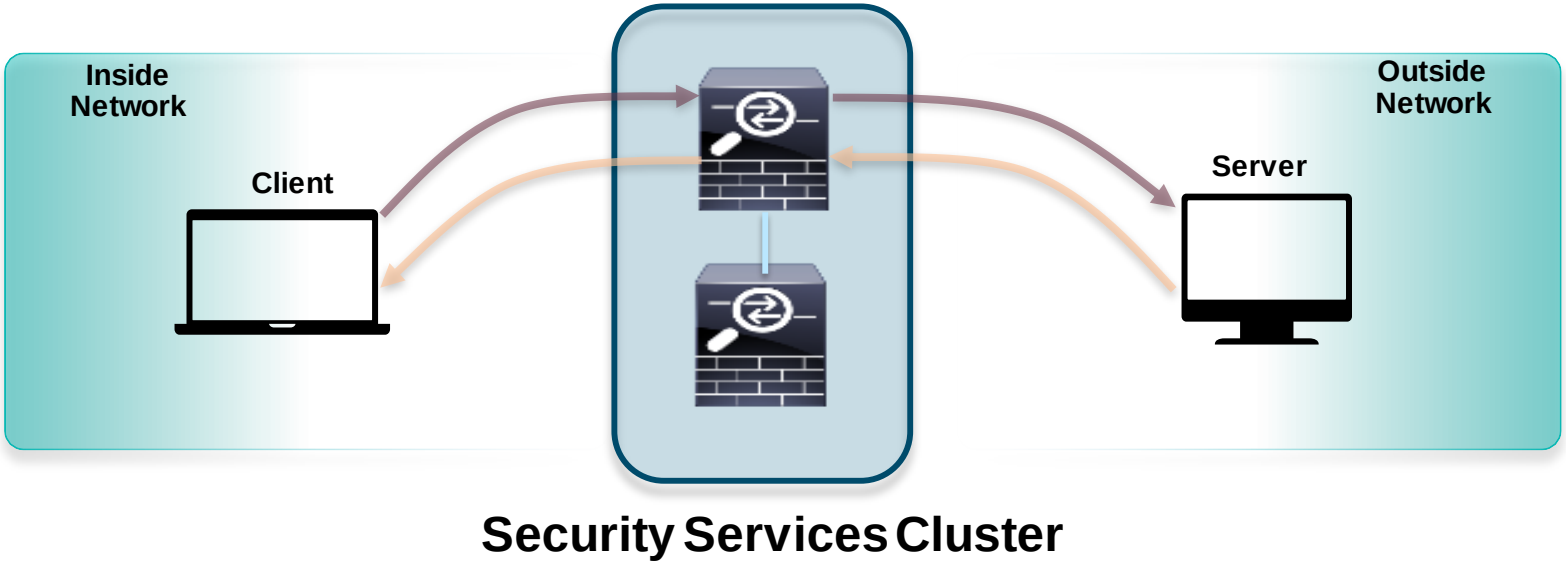
Resilient Traffic Handling – Symmetric Traffic



Security Services Cluster

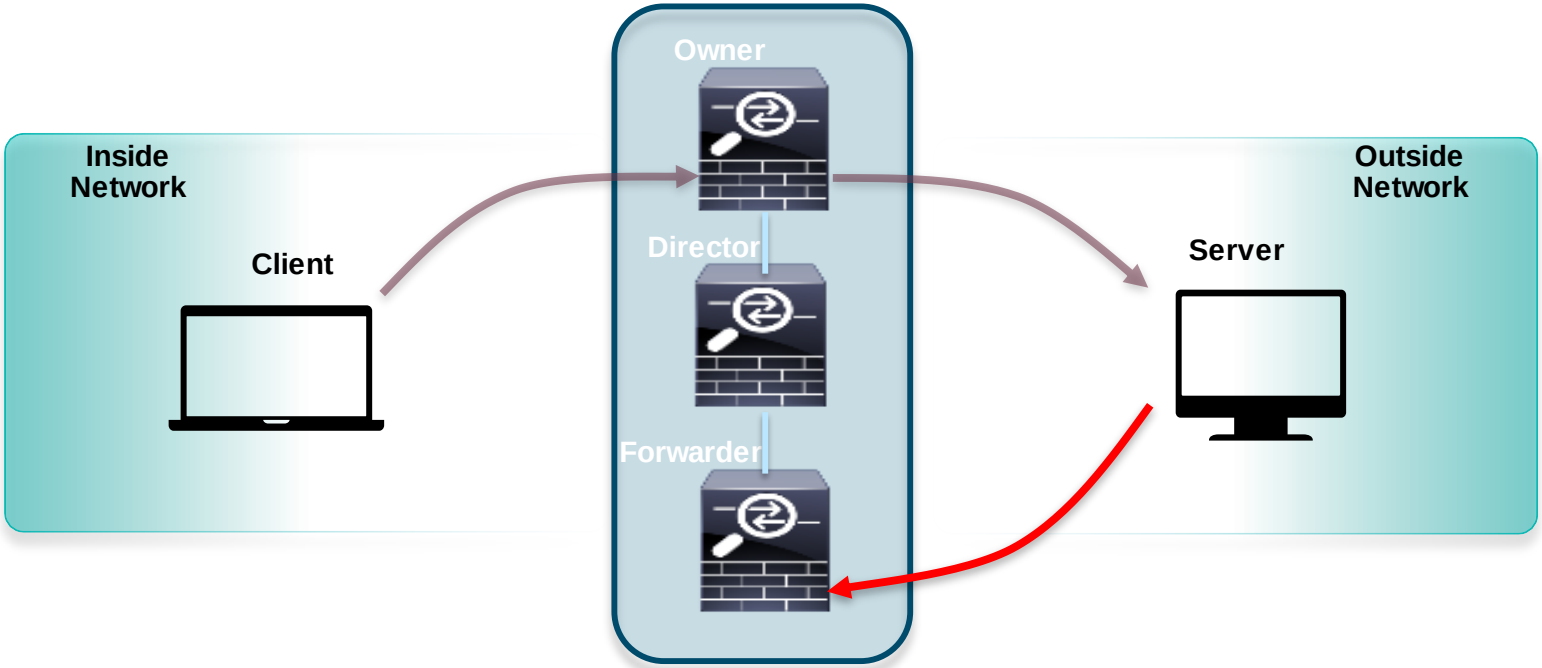
Resiliency Requirements

Resilient Traffic Handling – Symmetric Traffic



Resiliency Requirements

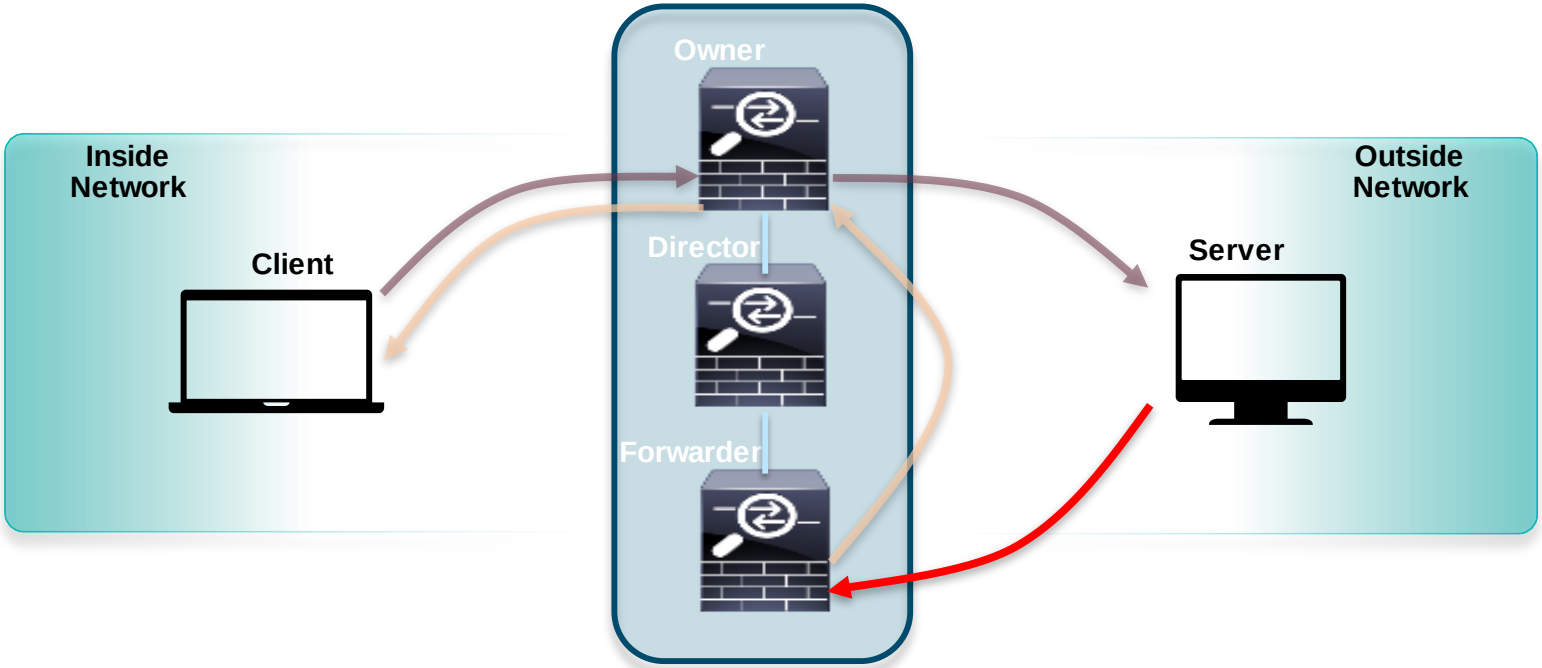
Resilient Traffic Handling – Asymmetric Traffic



Security Services Cluster

Resiliency Requirements

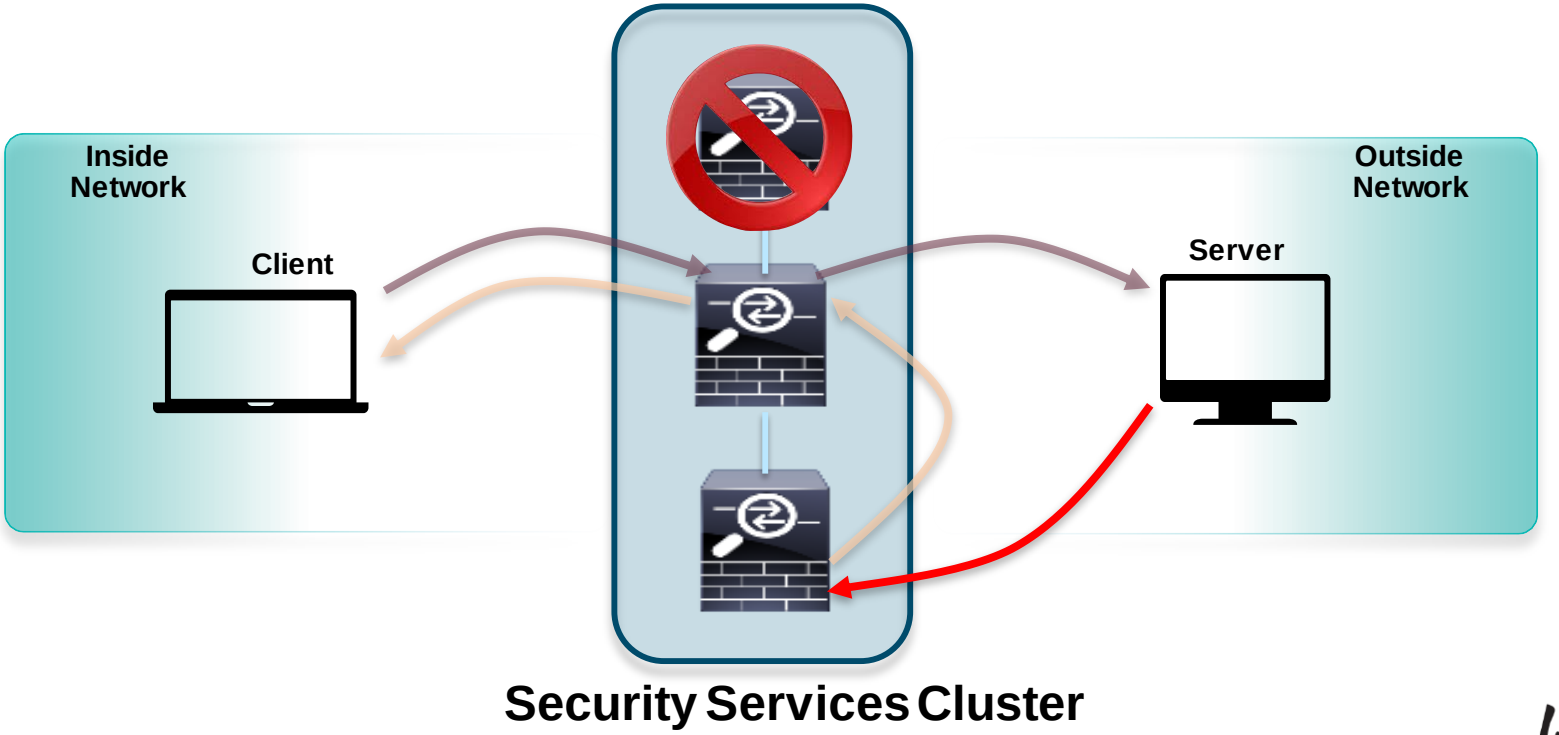
Resilient Traffic Handling – Asymmetric Traffic



Security Services Cluster

Resiliency Requirements

Resilient Traffic Handling - Failure



Myth Buster – Data Centre Edition

Myth # 2

Security is a performance bottleneck

FACT: Scalability is a problem for many Internet-edge security solutions. **BUT** with the right technologies like clustering and load aggregation can help to resolve that problem.

BUSTED

Security in the Data Centre

Key Requirements

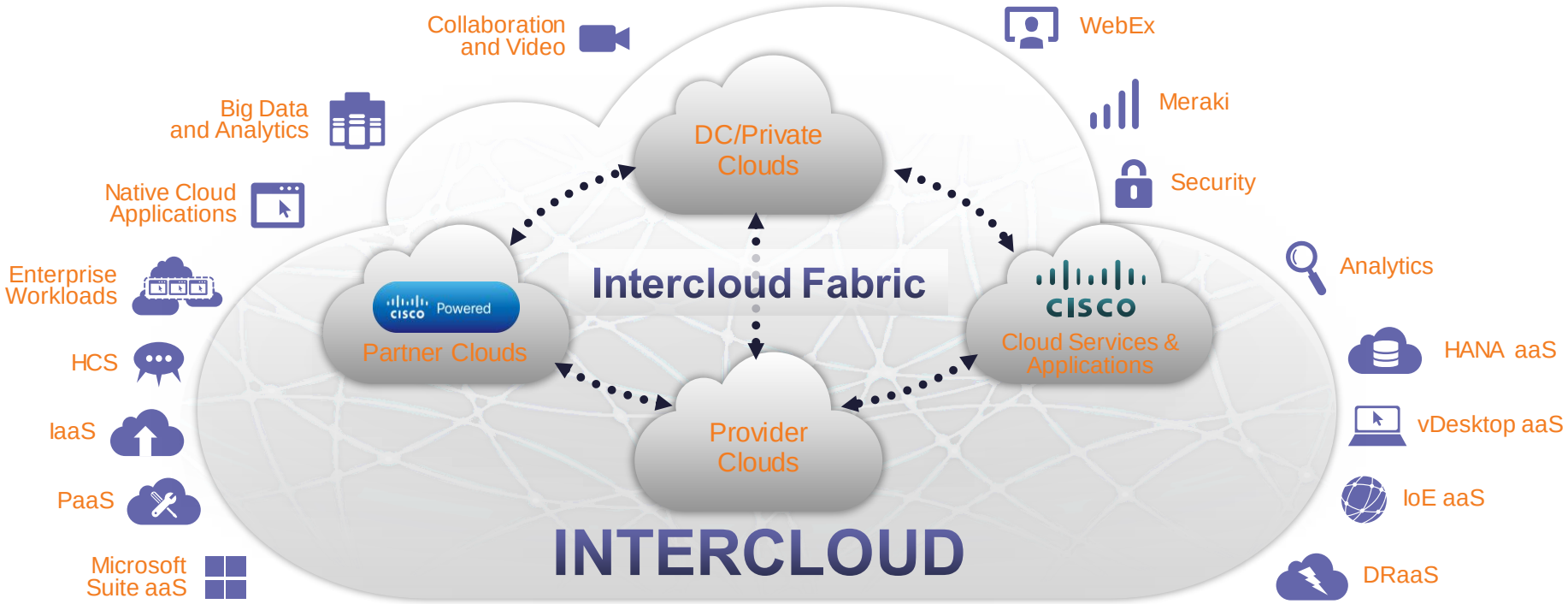
Scale	Need for elastic scaling through network integration
Resiliency	High availability is imperative for applications in the data centre
Flexibility	Need for reducing complexity in inserting services
Actionable Security	Desire to extend a chain of trust from the user to the application

Flexibility Requirements

★ Best Practice

- Workload mobility
  - Inter host and inter DC mobility
- Horizontal Scalability of virtual and physical workloads
  - ASA cluster scale
- Dynamic Link Aggregation in Layer 2 ★
- Minimal Change in data centre design ★
- On-demand provisioning
- Orchestration and onboarding

Cisco Intercloud and Intercloud Fabric



Myth Buster – Data Centre Edition

Myth # 4

Security requires a change in my Data Centre design

FACT: Inserting Security in the Data Centre if done incorrectly will require changes in the routing design of the data centre potentially making Security a potential bottleneck

BUSTED

Security in the Data Centre

Key Requirements

Scale	Need for elastic scaling through network integration
Resiliency	High availability is imperative for applications in the data centre
Flexibility	Need for reducing complexity in inserting services
Actionable Security	Desire to extend a chain of trust from the user to the application

Actionable Security Requirements

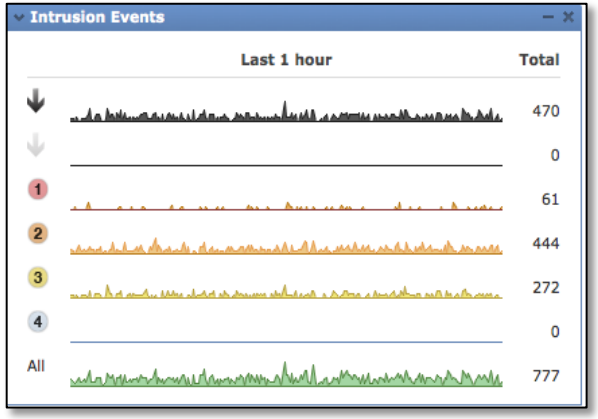
★ Best Practice

- Data loss prevention
- Consistent policies throughout the fabric ★
- Signature and reputation based protection
- Threat containment and remediation
- East-west protection ★
- Behavioural analysis
- Secure application tiering ★

Actionable Security

Impact Assessment

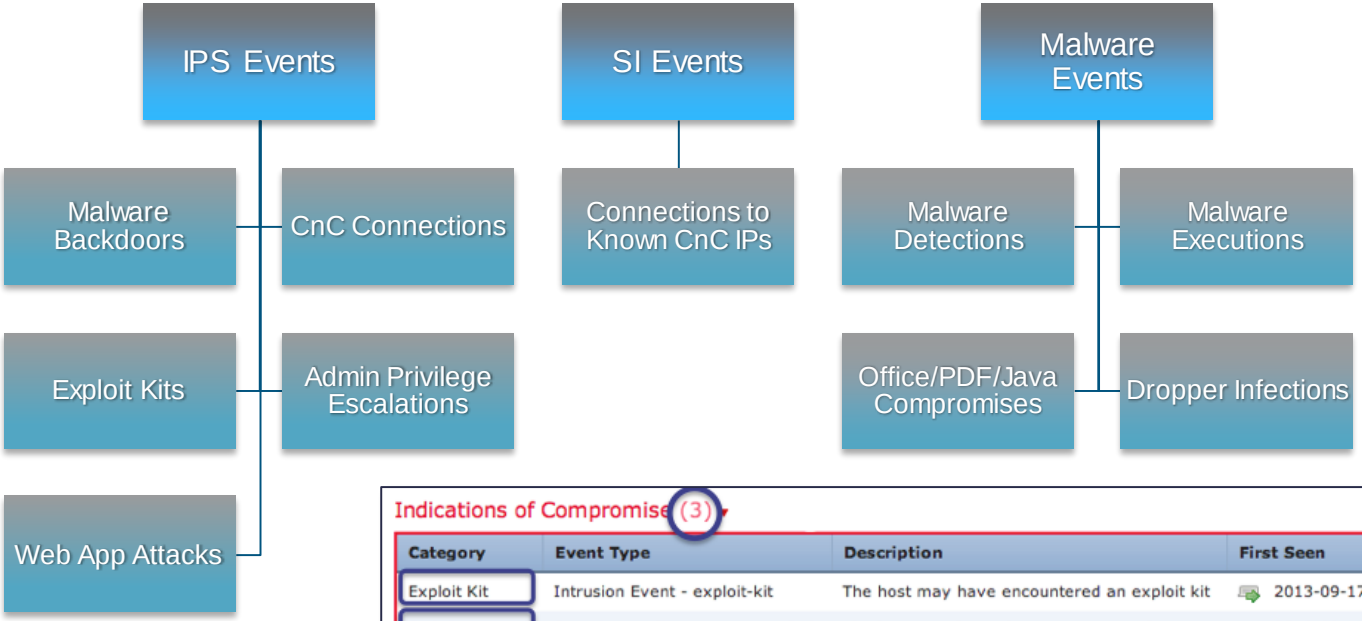
- Relies on information from passive discovery: OS, client and server application
- Correlates all Intrusion Events to an Impact of the attack against the target
- Allows analysts to focus on the smaller subset of events that they could be vulnerable to



IMPACT FLAG	ADMINISTRATOR ACTION	WHY
1	Act Immediately, Vulnerable	Event corresponds to vulnerability mapped to host
2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use, but no vuln mapped
3	Good to Know, Currently Not Vulnerable	Relevant port not open or protocol not in use
4	Good to Know, Unknown Target	Monitored network, but unknown host
0	Good to Know, Unknown Network	Unmonitored network

Actionable Security

Indications of Compromise (IOCs)



Indications of Compromise (3)

Edit Rule States | Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

Actionable Security

Detecting Suspecting Data Loss

Alarm Type

IP Address

Username

Flow Table

Policy violation details

Host Group Dashboard | Alarm Table

Filter | Domain : Alpha | Source or Target Host Group : Inside Hosts | First Active Time : Last 14 days

Alarm Table – 45 records

Policy	Start Active...	Alarm	Source	Source Host Gr...	Source User...	Target	Target...	Details
Inside Hosts	8-Feb-2012 5:05:00 PM (11 days 22 hours 48 minutes ago)	Suspect Data Loss	10.34.74.123	SJCM, Wired Data		Multiple Hosts		Observed 4.08G bytes. Policy maximum allows up to 81.92M bytes.
Inside Hosts	16-Feb-2012 11:40:00 AM (4 days 4 hours 13 minutes ago)	Suspect Data Loss				Multiple Hosts		Observed 16.8M bytes. Expected 4.86M bytes, tolerance of 50 allows up to 15.33M bytes.
Inside Hosts	8-Feb-2012 12:40:00 PM (12 days 3 hours 13 minutes ago)	Suspect Data Loss				Multiple Hosts		Observed 11.92M bytes. Expected 1.16M bytes, tolerance of 50 allows up to 10M bytes.
Inside Hosts	8-Feb-2012 12:10:00 PM (12 days 3 hours 43 minutes ago)	Suspect Data Loss						Observed 11.79M bytes. Expected 1.16M bytes, tolerance of 50 allows up to 10M bytes.
Inside Hosts	7-Feb-2012 8:50:00 PM (12 days 19 hours 3 minutes ago)	Suspect Data Loss						Observed 11.63M bytes. Expected 1.16M bytes, tolerance of 50 allows up to 10M bytes.
Inside Hosts	15-Feb-2012 3:10:00 PM (5 days 43	Suspect Data Loss				Multiple Hosts		Observed 44.59M bytes. Expected 3.17M bytes, tolerance of 50 allows up

Quick View This Row
Disable Alarm(s)...
Host Policy...
Workflow
Mitigation
Notes
Flows
Associated External Events
for Host [redacted]:
Host Snapshot
Top
Status
Security
Hosts

Flow Table
Network and Server Performance
Flow Traffic
Peer Vs. Peer
Peer Vs. Port
Time Vs. Peer
Time Vs. Port

Actionable Security

Detecting Spreading Malware

Filter | Domain : [redacted] | Time : February 1, 2012
Host : 10.40.10.254

Identification | Alarms | Security | CI Events | Top Active Flows | Identity, DHCP & Host Notes | Exporter Interfaces

Alarm Counts – 1 record

Appliance	Critical	Major
FlowCollector01 (10.192.0.192)		5(0)

Alarms – 21 records

Start Active Time	Alarm	Source	Details
Feb 1, 2012 8:39:30 PM (12 days 19 hours 27 minutes ago)	Worm Propagation	10.40.10.254	Worm propagated from Source Host using ms-rpc (135/tcp) (Double-click for details)
Feb 1, 2012 7:40:00 PM (12 days 20 hours 26 minutes ago)	New Flows Initiated	10.40.10.254	Observed 1.07k flows. Policy maximum allows up to 1k flows.
Feb 1, 2012 7:39:30 PM (12 days 20 hours 27 minutes ago)	Worm Propagation	10.40.10.254	Worm propagated from Source Host using ms-rpc (135/tcp) (Double-click for details)
Feb 1, 2012 6:40:00 PM (12 days 21 hours 26 minutes ago)	New Flows Initiated	10.40.10.254	Observed 1.12k flows. Policy maximum allows up to 1k flows.
Feb 1, 2012 6:39:30 PM (12 days 21 hours 27	Worm Propagation	10.40.10.254	Worm propagated from Source Host using ms-rpc (135/tcp)

Actionable Security

Threat Intelligence with Big Data

SECURITY SENSOR BASE

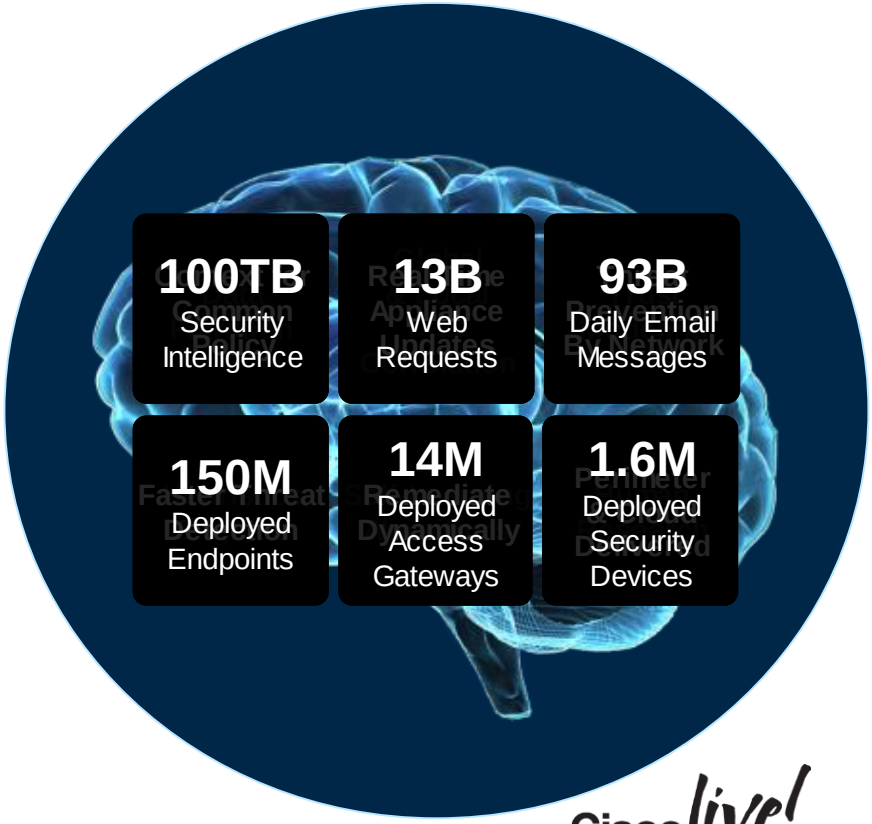
Broadest range of threat & vulnerability data sources

THREAT ANALYTICS

Global and local correlation through analytics and human intelligence

INTELLIGENCE DELIVERED

Contextual Policy with Distributed Enforcement



Agenda

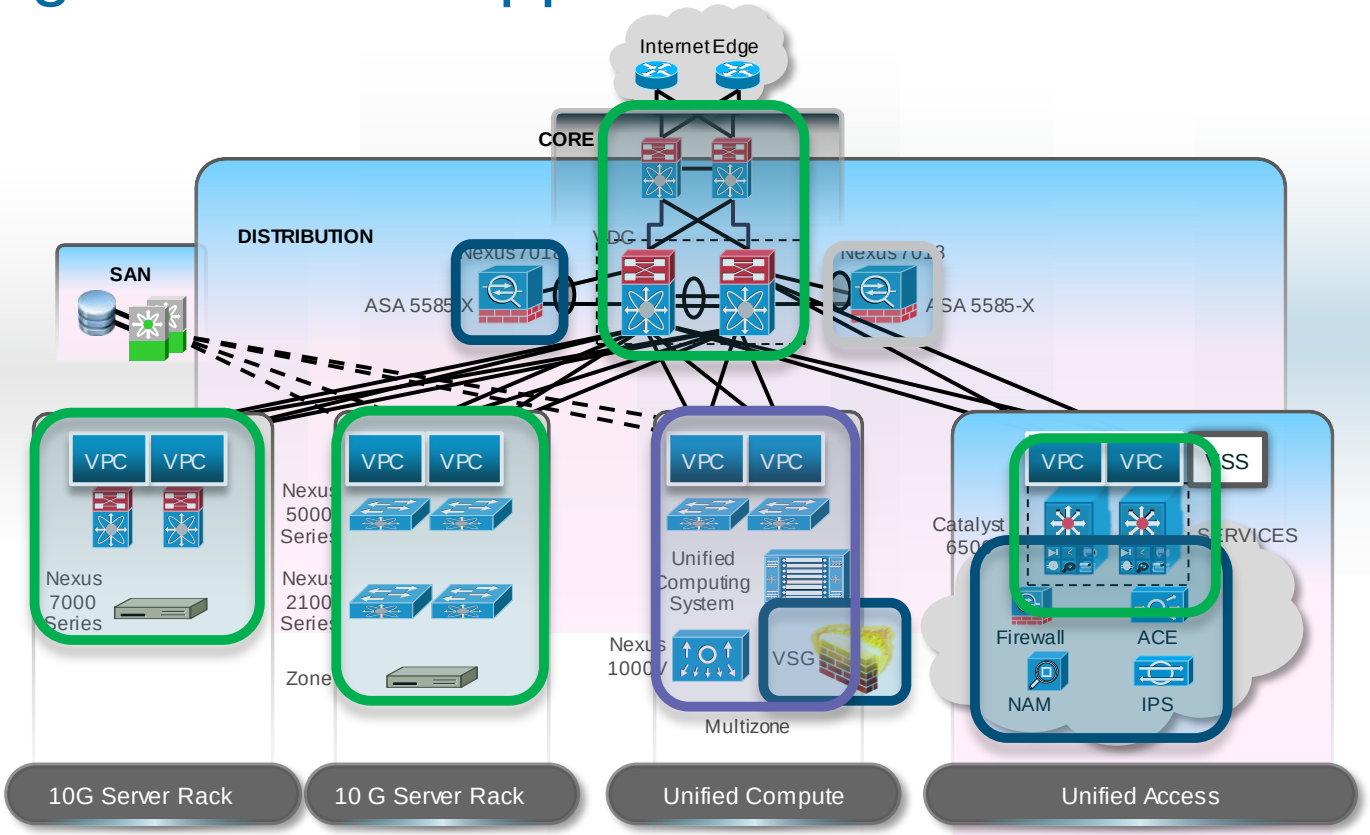
- Introduction
- Security in the Data Centre
- **Data Centre Design**
  - **Modular approach to Security**
  - **Secure Data Centre for the Enterprise**
- Data Centre Security with Application Centric Infrastructure
- Conclusion

Requiring a Modular Approach

= Compute

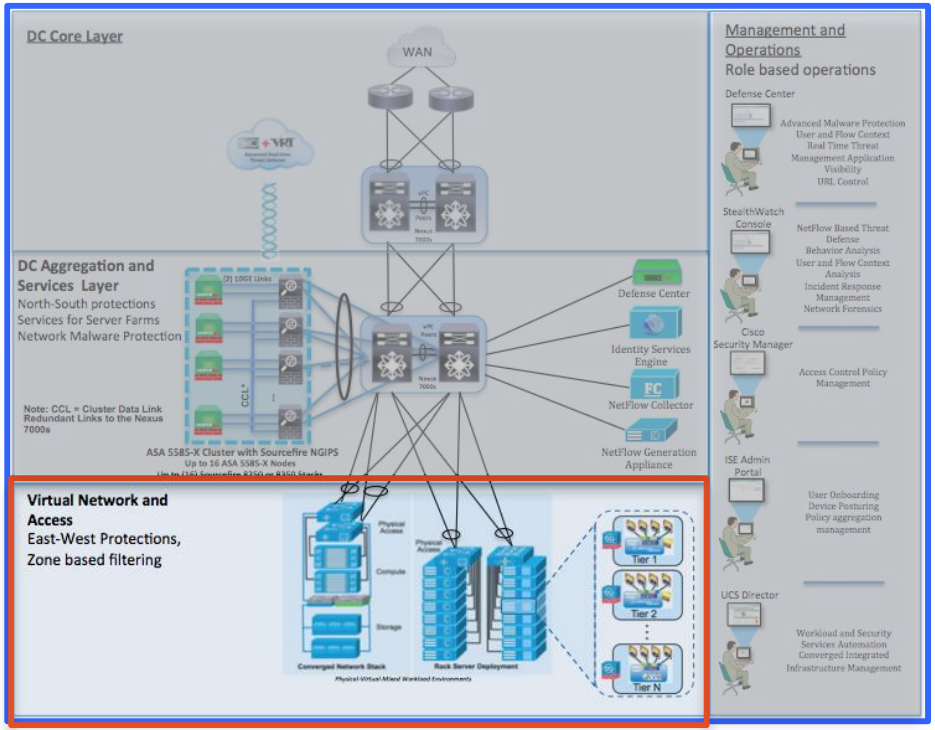
= Network

= Security



Requiring a Modular Approach

Securing the Virtual Network

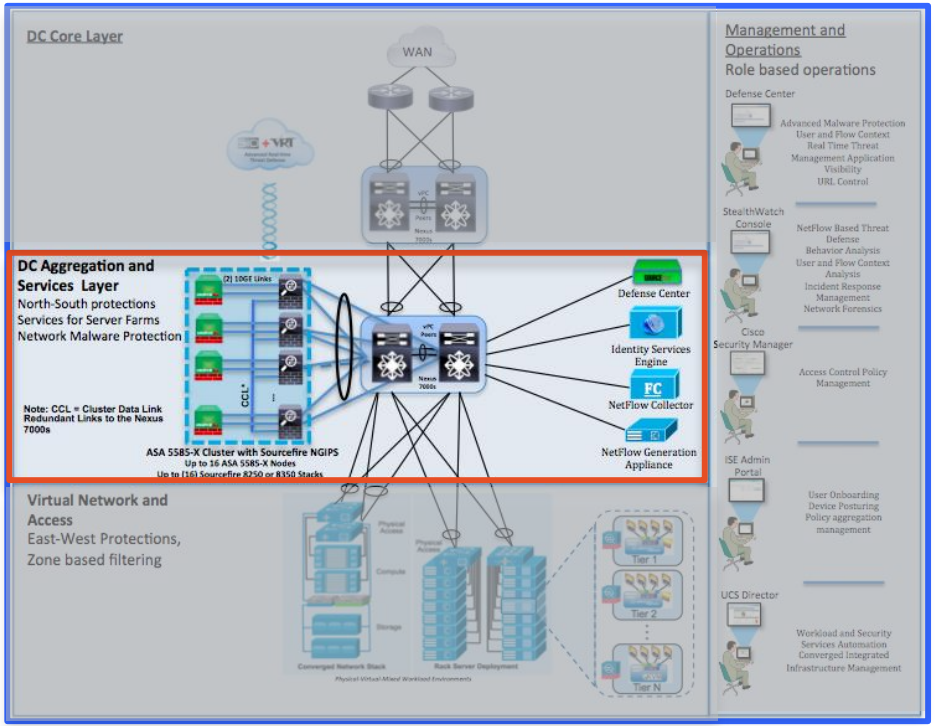


Virtual Network and Access

- Secure Enclaves Architecture Guide
- Content Created for the Server Administrators
- Secure Integrated Infrastructure
  - Flexpod, Vblock
    - Compute
    - Storage
    - Hypervisor Virtualisation
  - Infrastructure Mgmt.
  - Access Layer
  - Secure Enclaves
  - UCS Director for Automation

Requiring a Modular Approach

Scaling the Data Centre

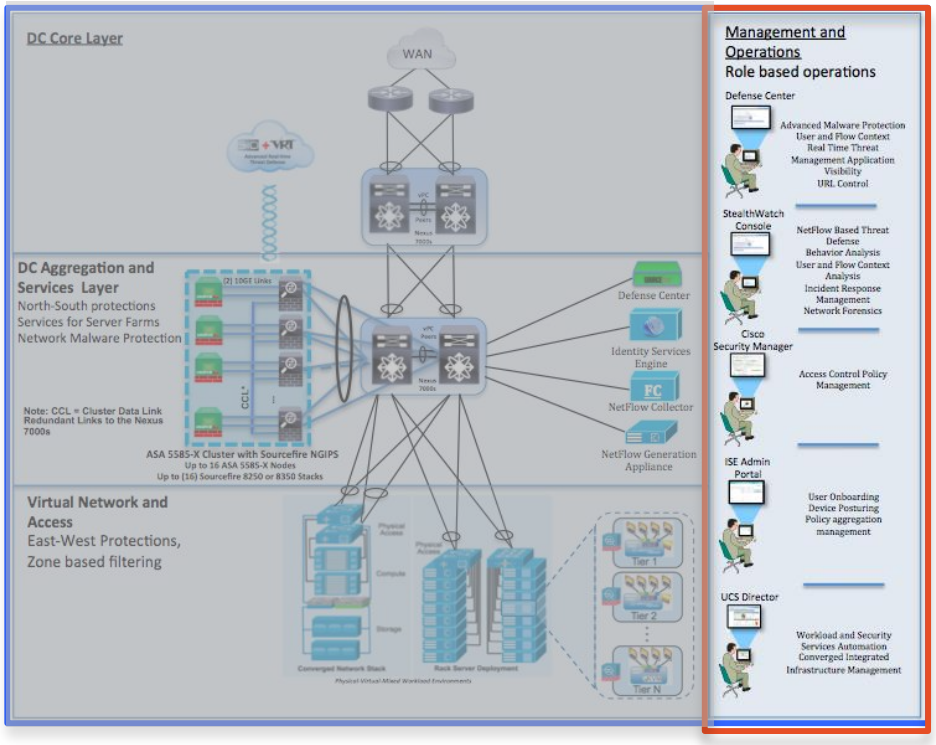


DC Aggregation and Services Layer

- NextGen IPS in ASA Cluster
  (Asymmetrical Flow Support is Maintained!!!)
- FireSIGHT Management Centre
  (aka Defence Centre)
- User Context
- Application Control
- URL Filtering
- Network-Based AMP
- End Point AMP
  (Client and Server)
- Retrospection
- IPS
- File Trajectory
- 320Gbps Firewall and NextGen IPS Throughput

Requiring a Modular Approach

Right tool for the right job with Telemetry and Analytics

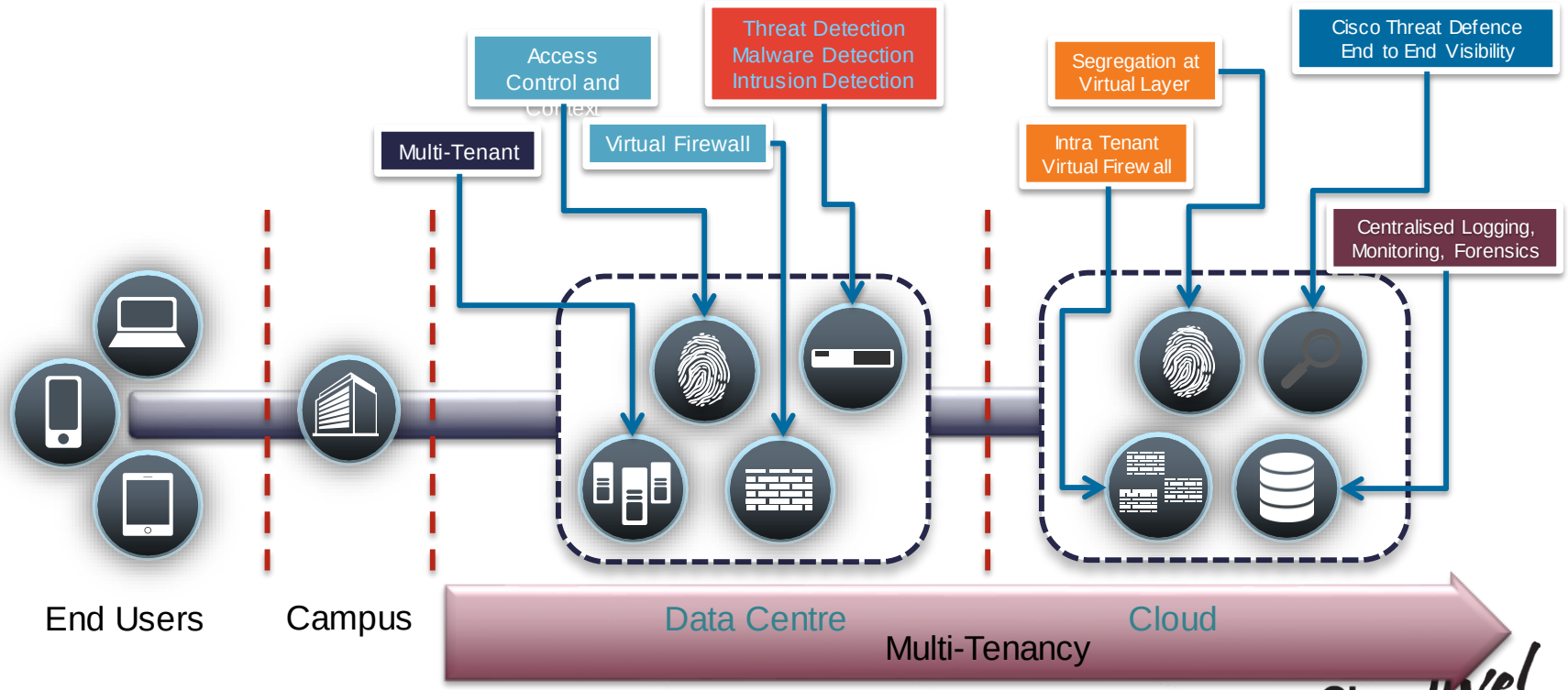


Management and Operations

- Security Incident Response Team
  - FireSIGHT Management Centre
- Security Policy Management Team
  - Cisco Security Manager
  - Identity Services Engine
- Server Administration Team
  - UCS Director
- Network Ops Teams
  - Lancope Stealthwatch

Requiring a Capabilities Approach

Security and Protections from Enterprise to Cloud Providers



Secure Data Centre for the Enterprise Portfolio

Comprehensive Set of Capabilities for the Cyber Defender

Cisco Secure Data Centre for the Enterprise Solution Portfolio

Secure Enclave Architecture

- Converged Infrastructure
  - Compute
  - Storage
  - Hypervisor (Flexpod, Vblock, VSPEX)
- Virtualisation
- Infrastructure Mgmt
- Access Layer
- Secure Enclaves

Single Site Clustering with TrustSec

- Firewall Clustering
- Intrusion Prevention
- Real Time Updates
- Management
- TrustSec
  - SXP
  - Secure Group Tags
  - Policy Enforcement
  - SGACLs
  - FWACLS

Threat Management with NextGen IPS

- NextGen IPS in ASA Cluster
- Defence Centre
- FireSIGHT
- User Context
- Application Control
- URL Filtering
- Network-Based AMP
- End Point AMP (Client and Server)

Cyber Threat Defence for Data Centre

- Lancope Stealthwatch
  - FlowCollector
  - FlowSensor
- NetFlow
- NSEL (Network Security Event Logging)

- Four solutions jointly validated to create a complete solution
- Modular approach
- Industry's most comprehensive security solution

Capabilities by Solution

Modular Approach to a Comprehensive Set of Capabilities

Legend
- Threat Containment and Remediation
- Access Control and Segmentation
- Application Visibility and Control
- Identity Management
- Logging and Traceability

Industry's Most Comprehensive Security Solution

Secure Enclave Architecture	Single Site Clustering with TrustSec	Threat Management with NextGen IPS		Cyber Threat Defence for Data Centre
Secure Application Tiering	Policy Consolidation	Device Access Control	System Audit Logs	User Identity Tracking
Layer 2 Workload Firewall	Roles-Based Policies	User Control	Audit Log Streaming	NetFlow Threat Analysis
Service Chaining	Secure Group Tags	Policy Enforcement User Notification	System Logs	NSEL Threat Analysis
Secure Automated Workload Deployment	Secure Group ACLs	Security Zones	NetFlow Integration	Historical Traffic Trending
Port Profile SGT Assignments	Scalable Performance	Host Identification	Automatic Updates	Botnet Detection
Service Level Tier Security	Cluster Health Status	Customisable Host Profiles	Global Correlation	Malware Detection
Intra Service Level Tier Security	Asymmetric Traffic	File Control	Threat Correlation	Data Loss Detection
Intra Workload Security	Data Black Hole Prevention	Application Detection	Intrusion Detection	Denial of Service Attack Detection
Intra Application Tier Security	Flow Redundancy	Application Control	Network-Based Malware	Root Cause Analysis
Out-of-Band Management	High Availability	SSL Application Detection	Endpoint-Based Malware	Automated Remediation
Roles-Based Automation	Real Time Updates	Network File Trajectory	Mobile Device Malware	Worm Propagation Visualisation
Roles-Based Management	Device Posturing	DLP—Sensitive Data Detection	Email Malware	Relational Flow Mapping
	Device Compliance Checks	DLP—Sensitive Data Control	Web Services Malware	
	End User Posturing	User Identification	Indications of Compromise	
	Active Directory LDAP Integration	User Access Posturing	Intelligent White Listing	
		Detailed User Activity Logging	Intelligent Black Listing	
		User to Email Mapping	Connection Intelligence	
		Active Directory LDAP Integration		

Myth Buster – Data Centre Edition

Myth # 3

Security disrupts data centre functionality

BUSTED

FACT: With the right security architecture which are purpose-built for DC environments, Security can be integrated seamlessly into any data centre – without interrupting applications, traffic, or services.

Agenda

- Introduction
- Security in the Data Centre
- Data Centre Design
- **Data Centre Security with Application Centric Infrastructure**
  - **Nomenclature**
  - **ACI Policy Model for Security**
  - **ACI Benefits**
- Conclusion

Classic Data Centre Challenges

Poor Scalability

Hard to insert resources, power/port constraints, “fat” flows, expansion

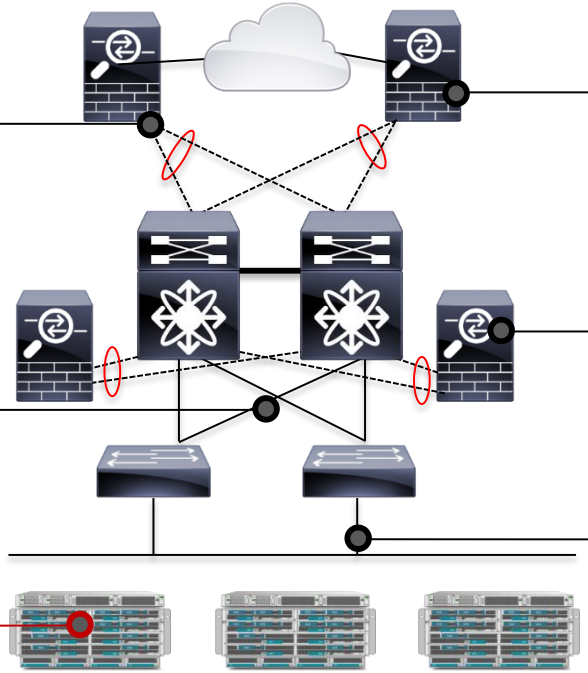
Low Versatility

Complex traffic engineering, VLAN/DRP, suboptimal paths

Physical Network Limits

Applications

Need intelligence to abstract application flows



Policy Set Complication

Overlapping rule sets, complex inheritance, oversubscription

Management Fragmentation

Separate interfaces, no common objects or templates

Cost of East-West Services

Multi-pass inspections, “slow” network traversal, “hairpinning”, waste of compute cycles

Right Security Architecture for the Data Centre?

PERIMETER CENTRIC

- Manual and Complex
- Static Topology
- Error-Prone
- Limited Places

VIRTUALISATION CENTRIC

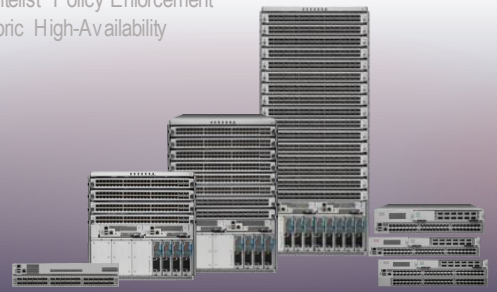
- No Physical Support
- Management Complexity
- Limited Visibility

APPLICATION CENTRIC

- Any workload and any place
- Automated
- Full Visibility

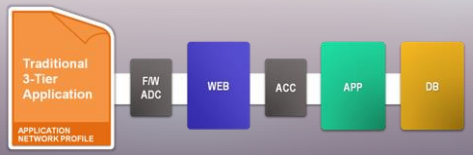
Application Centric Infrastructure (ACI)

Embedded Stateless L4 Firewall (zero trust)
Tenant Isolation
Group-based Security Policy* (3rd party included)
Whitelist Policy Enforcement
Fabric High-Availability



NEXUS 9500, 9300 and AVS

Declarative Policy Model
Fully Object-oriented and Open
Application Centric Desired State
Packaged deployment
Use, re-use and decommission with audit trails



APPLICATION CENTRIC POLICY

Centralised Management
Role-Based Access
Audit Logs
Health Monitoring
Open REST APIs

CONTROLLER

ACI

** Group-based security policy = includes physical and virtual, from Cisco and 3rd party, with embedded white-list security filtering. Superset of micro-segmentation*

Application Centric Infrastructure (ACI)

Flat Hardware Accelerated Network

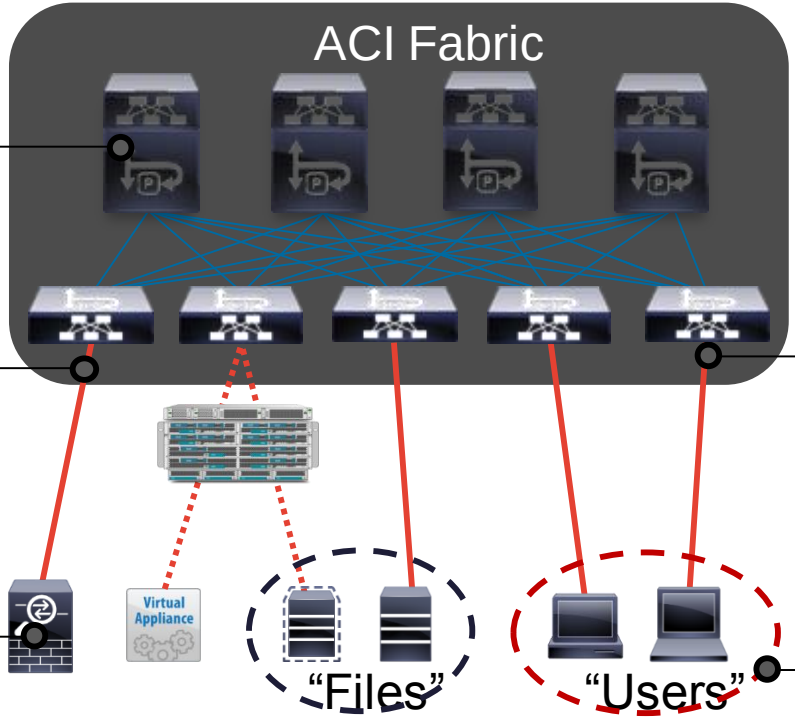
Full abstraction, de-coupled from VLANs and Dynamic Routing, low latency, built-in QoS

Flexible Insertion

Every device is one hop away, microsecond latency, no power or port availability constraints, ease of scaling

Unified Management and Visibility

ACI Controller manages all participating devices, change control and audit capabilities



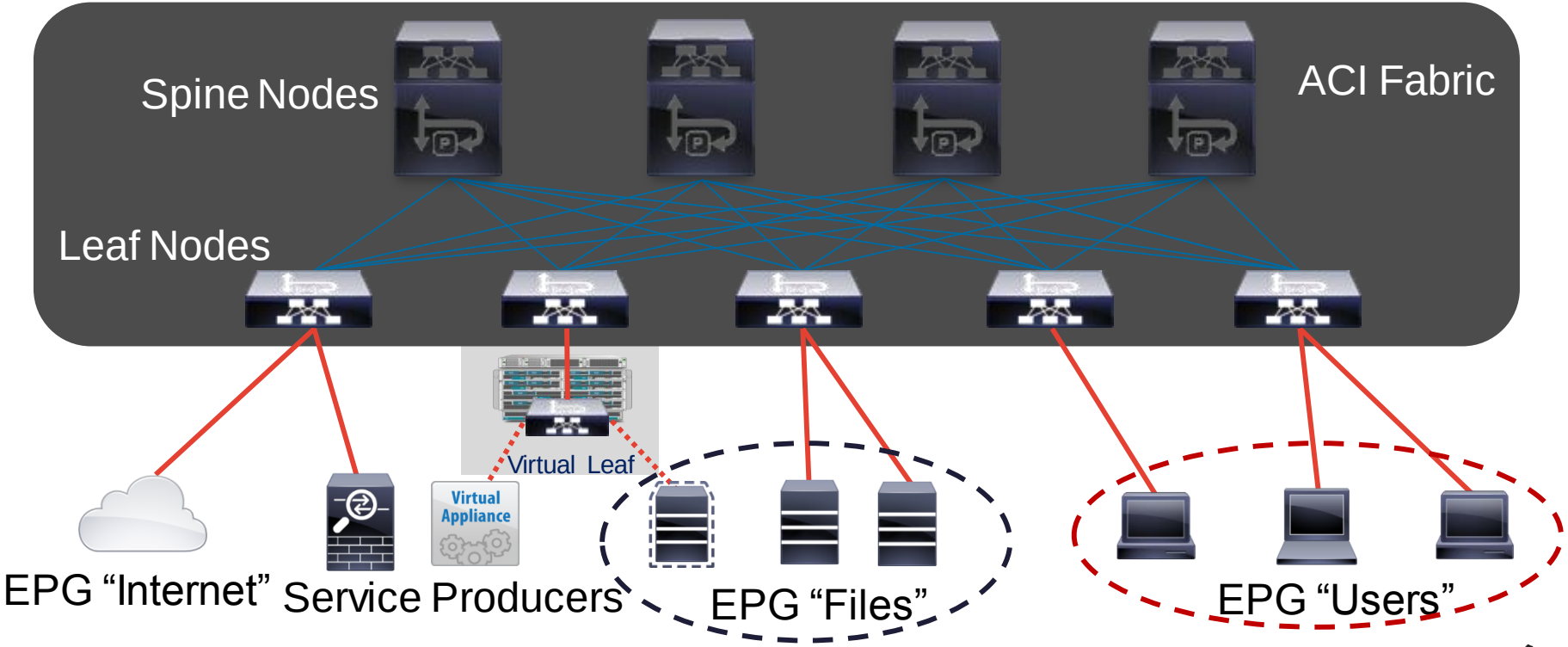
Fabric Port Services

Hardware filtering and bridging; default gateway; seamless service insertion, "service farm" aggregation

Logical Endpoint Groups by Role

Heterogeneous clients, servers, external clouds; fabric controls communication

ACI Nomenclature



ACI Nomenclature

ACI Device Roles

- ACI fabric nodes with negligible port-to-port latency
  - **Spine Nodes** create the backbone of the intelligent fabric and interconnect leaf nodes
  - **Leaf Nodes** provide connectivity for network endpoints, every device is one spine node away
  - **Virtual Leaf Nodes** extend ACI capabilities into VM environment and eliminate physical port traversal
- **Service Consumers** are the endpoint that rely on network services
  - Physical application servers or virtual machines, client machines
- **End Point Groups (EPGs)** provide logical abstraction for similar consumers
  - “Similar” in terms of application services and usage
- **Service Producers** or **Nodes** provide services to Consumers
  - ASA, IPS, Network Analysers, SSL accelerators – virtual and physical form factors
- Fabric enforces specific policies for any inter-EPG communication
  - Port-level basic filtering, QoS, redirection of application flows to service producers

ACI Nomenclature

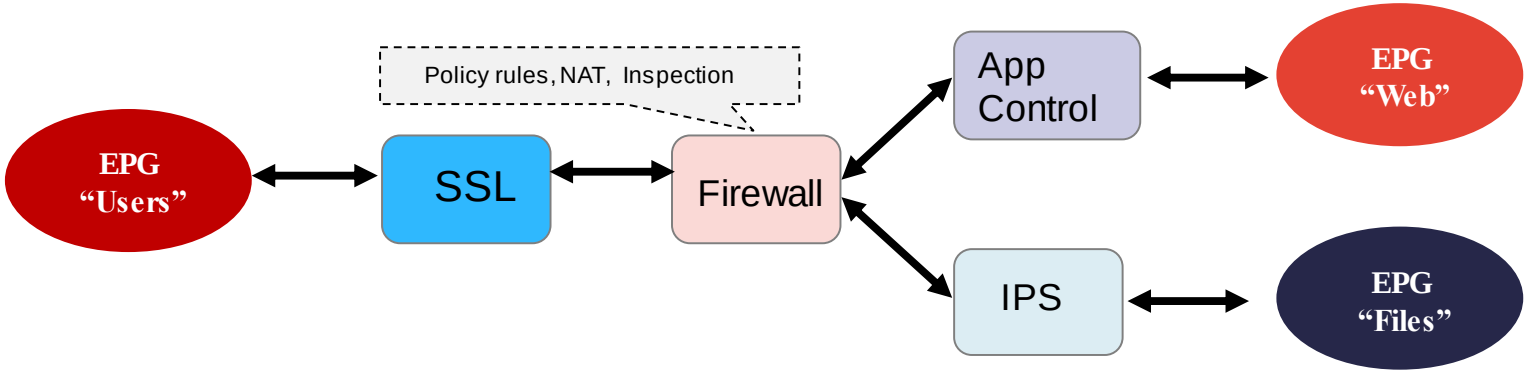
Application Flow Terminology

- **Application Policy Infrastructure Controller (APIC)** enables centralised management
- **Application Profiles** define EPGs and their network properties
  - Fabric bridges without flooding, acts as default gateway
  - Physically attach anywhere, build any logical topology within the fabric on demand
- **Contracts** describe rules for inter-EPG communication
  - Hardware port-based TCP/UDP filters offload more complex rules to dedicated security devices
  - Any available network services seamlessly insert into application flow path on demand
- **Service Graphs** or **Chains** insert service producers into application flow
  - Referenced from contracts; stateless load-balancing
  - Loop-free single-pass processing, different EPGs can load-share between multiple devices
  - Highly abstracted and universal; APIC configures service producers automatically

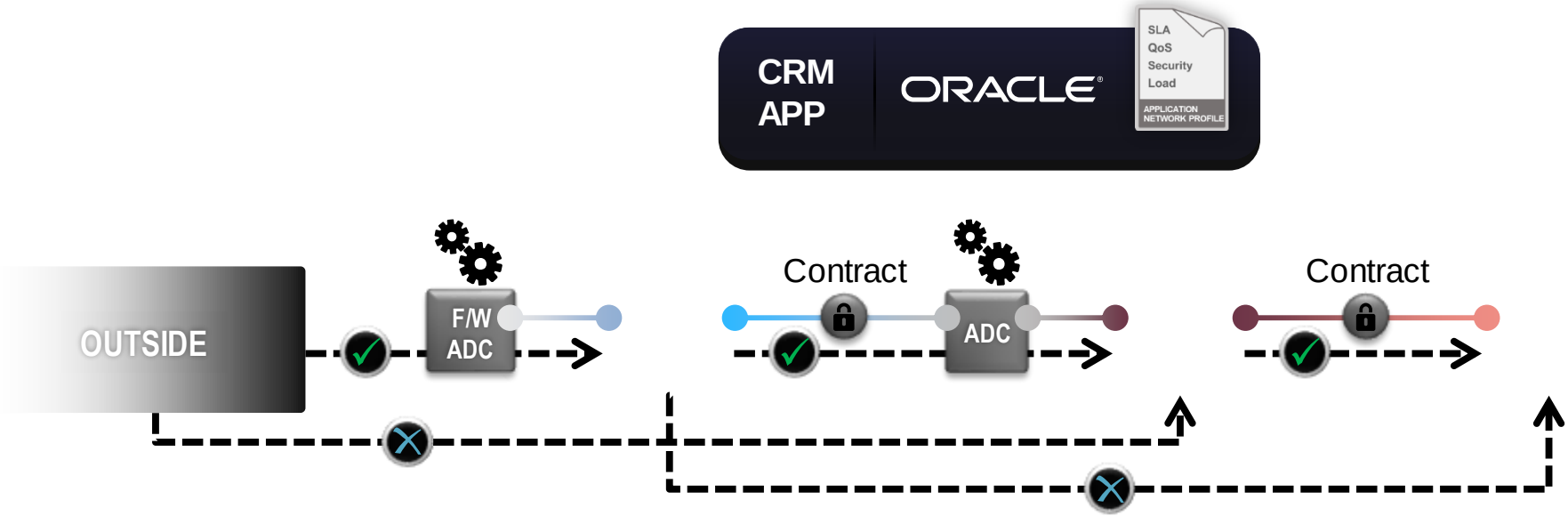
ACI Nomenclature

Typical Service Chain

- Full abstraction within the service chain
  - Every device only knows its function and exchanges packets with the fabric as instructed
  - High degree of modularity with low coupling, specific devices are interchangeable
- ACI maintains flow symmetry through the same device instance



Application Centric Policy Model for Security



WHAT COMPONENTS BRING SECURITY TO AN APPLICATION POLICY?

Endpoint Group:
A set of endpoints (VMs/servers) with the same policy

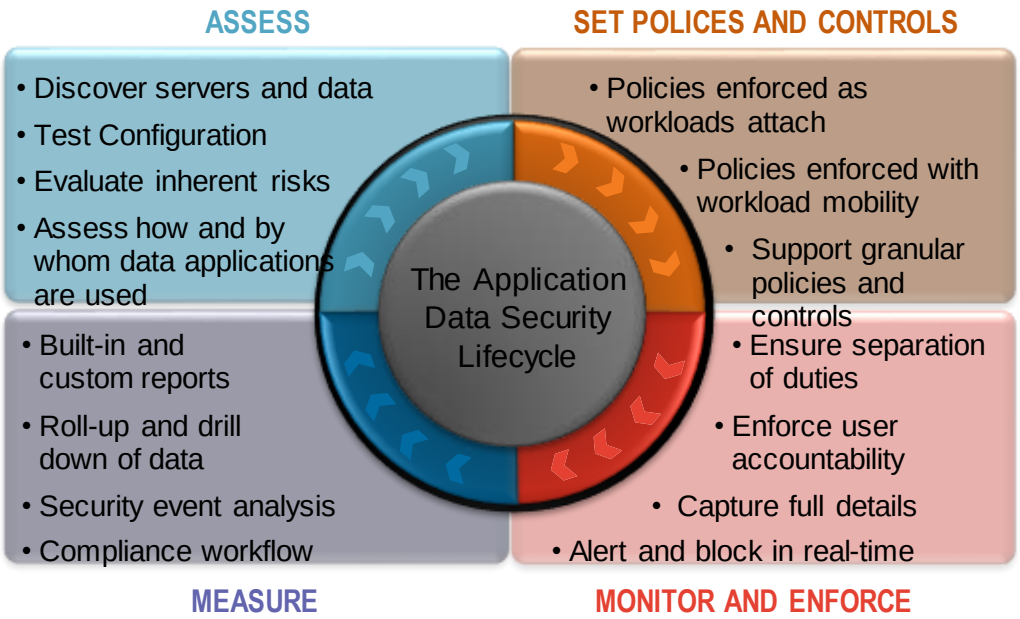
Contracts:
A set of rules governing communication between endpoint groups

Service Chains:
A set of network services between endpoint groups

ACI Benefits

Compliance Needs for Application Decommission

"Due to compliance regulations, when an application gets decommissioned, every IT resource associated with that must be removed and/or wiped out"



UCS allows one to dissociate service profile(s) associated with this application.
AUDIT OK !

Storage arrays can wipe-out the data or associated disks can be trashed.
AUDIT OK !

Current network approach and solutions don't have a way to map application workflow and "remove" it.
AUDIT FAIL ☹

ACI is the only one that can. Policies follow the application life-cycle*
AUDIT OK !

* associated ACI policy also gets removed when applications get decommissioned

ACI Benefits

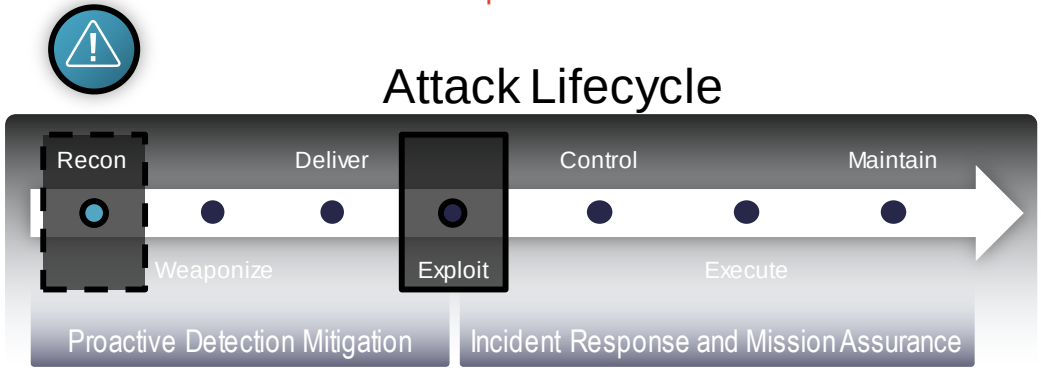
Attack Detection and Incident Response

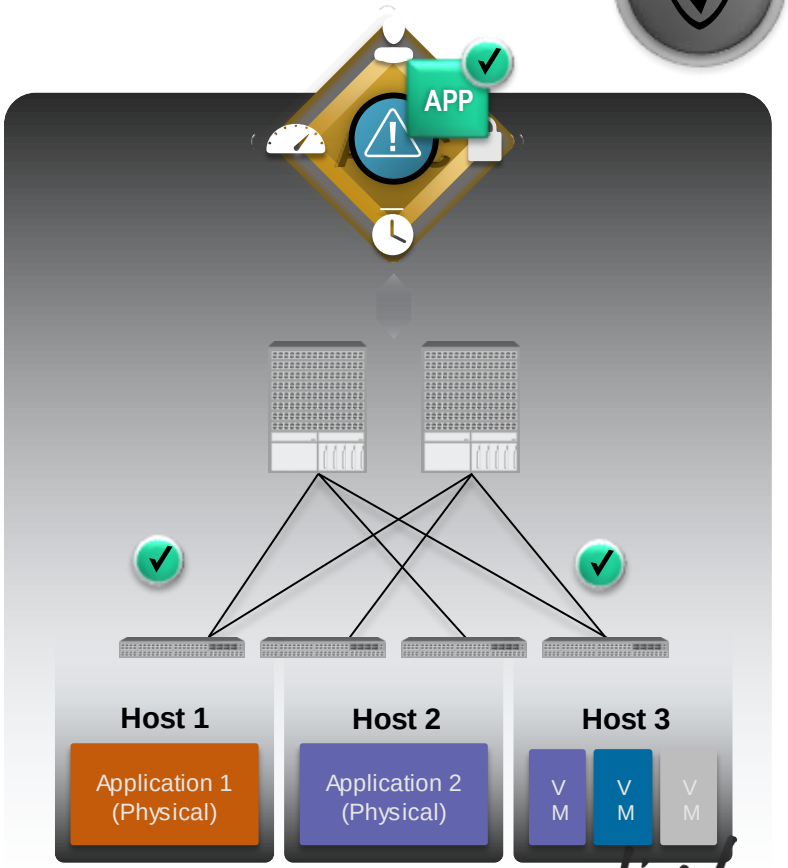
Deep visibility enables real-time changes to group policies to mitigate threats

Compliance app uses APIC north bound APIs to detect violation in real-time

APIC pushes security group policies to the devices as a part of incident response (quarantine, honeypot, etc.)

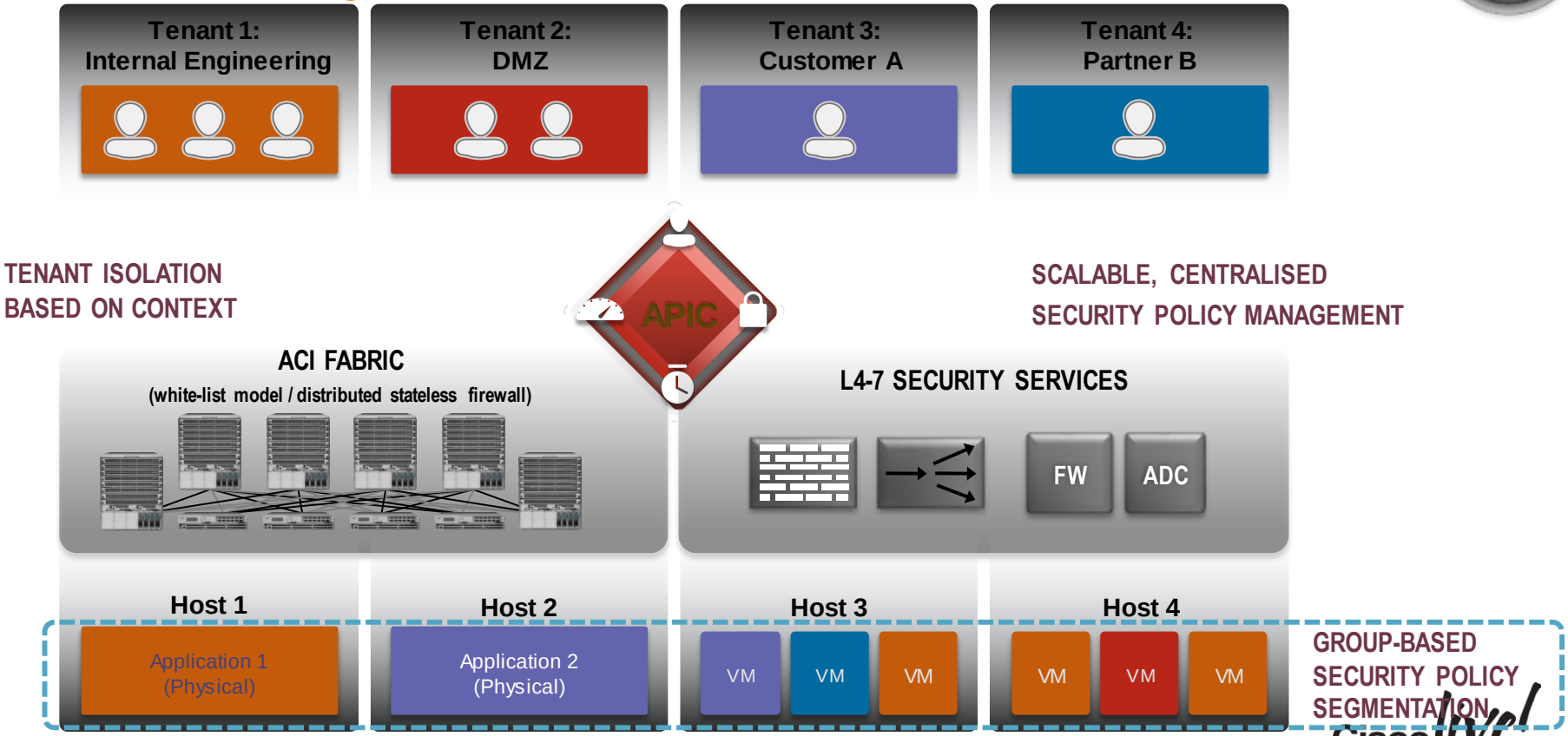
Compliance app uses APIC north bound APIs to provide assurance





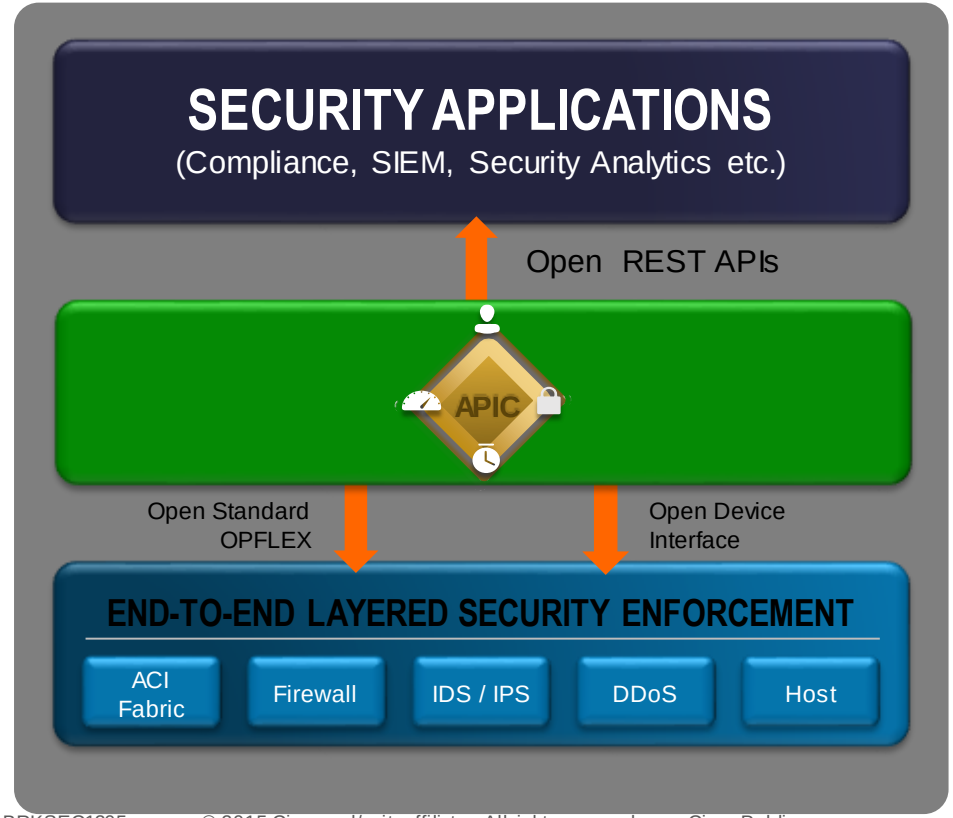
ACI Benefits

Isolation and Segmentation



ACI Benefits

Open Security Framework and Broad Ecosystem



Broad Ecosystem enables Choice, Investment Protection and supports Defence in Depth Security Strategy

Conclusion and Key Takeaways

- Security must be considered from the beginning for Data Centres
- Security must be available as a service to the Data Centre for consumption at no performance or scalability cost
- Visibility and context is key!
- Policies should be consistent across the data centre

Q & A

Complete Your Online Session Evaluation

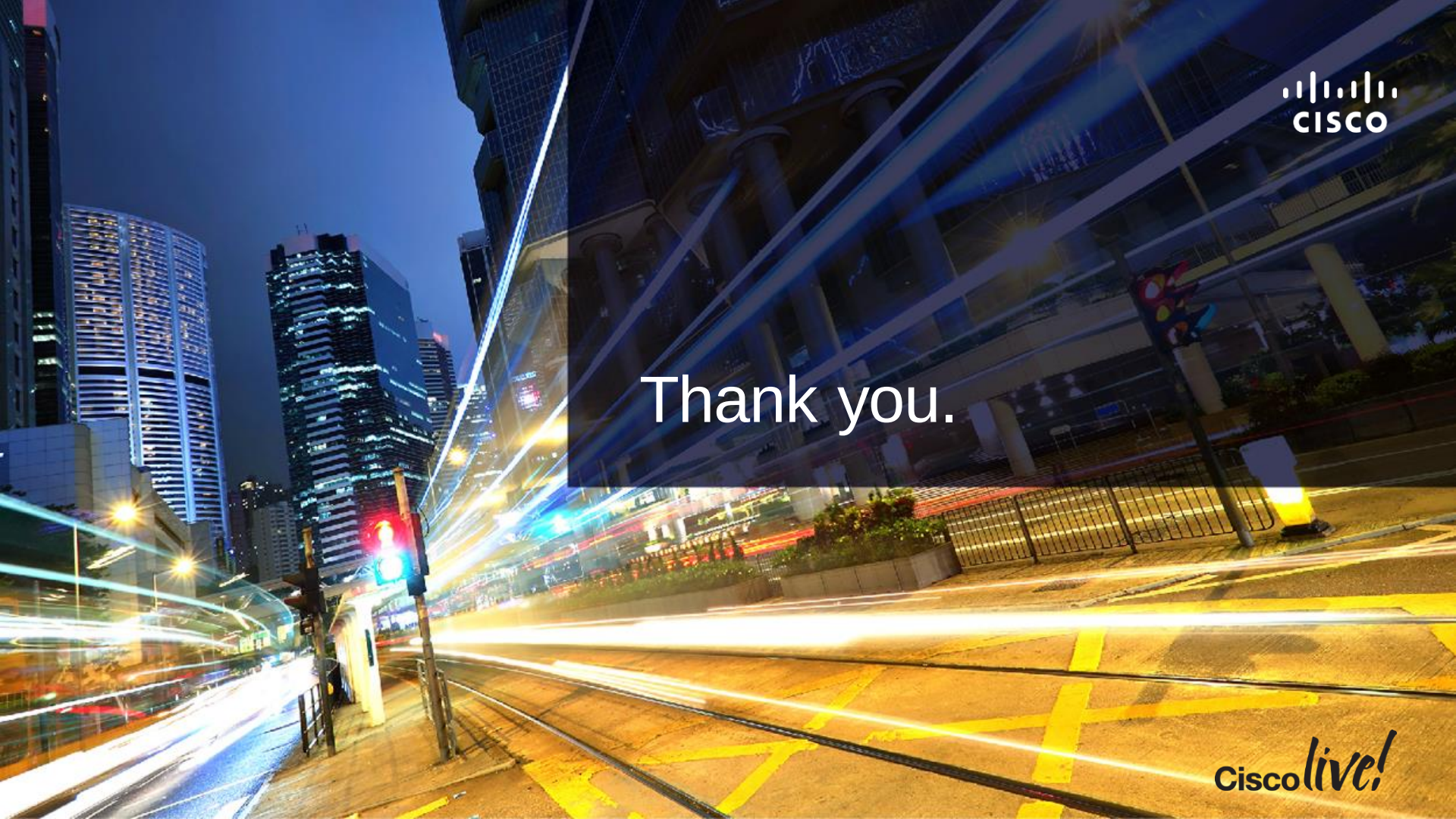
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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