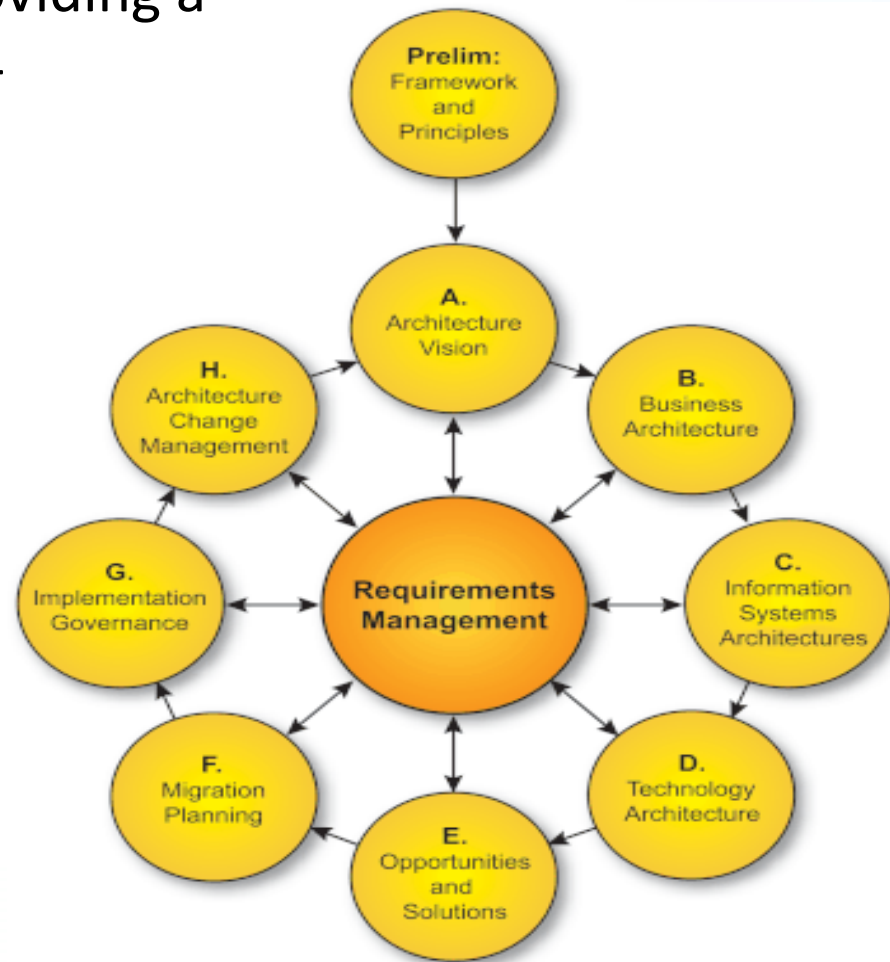


“Why Does Visibility Matter?”

**Presented by: Shawn Butler
Enterprise Architect**

The Open Group Architecture Framework (TOGAF)

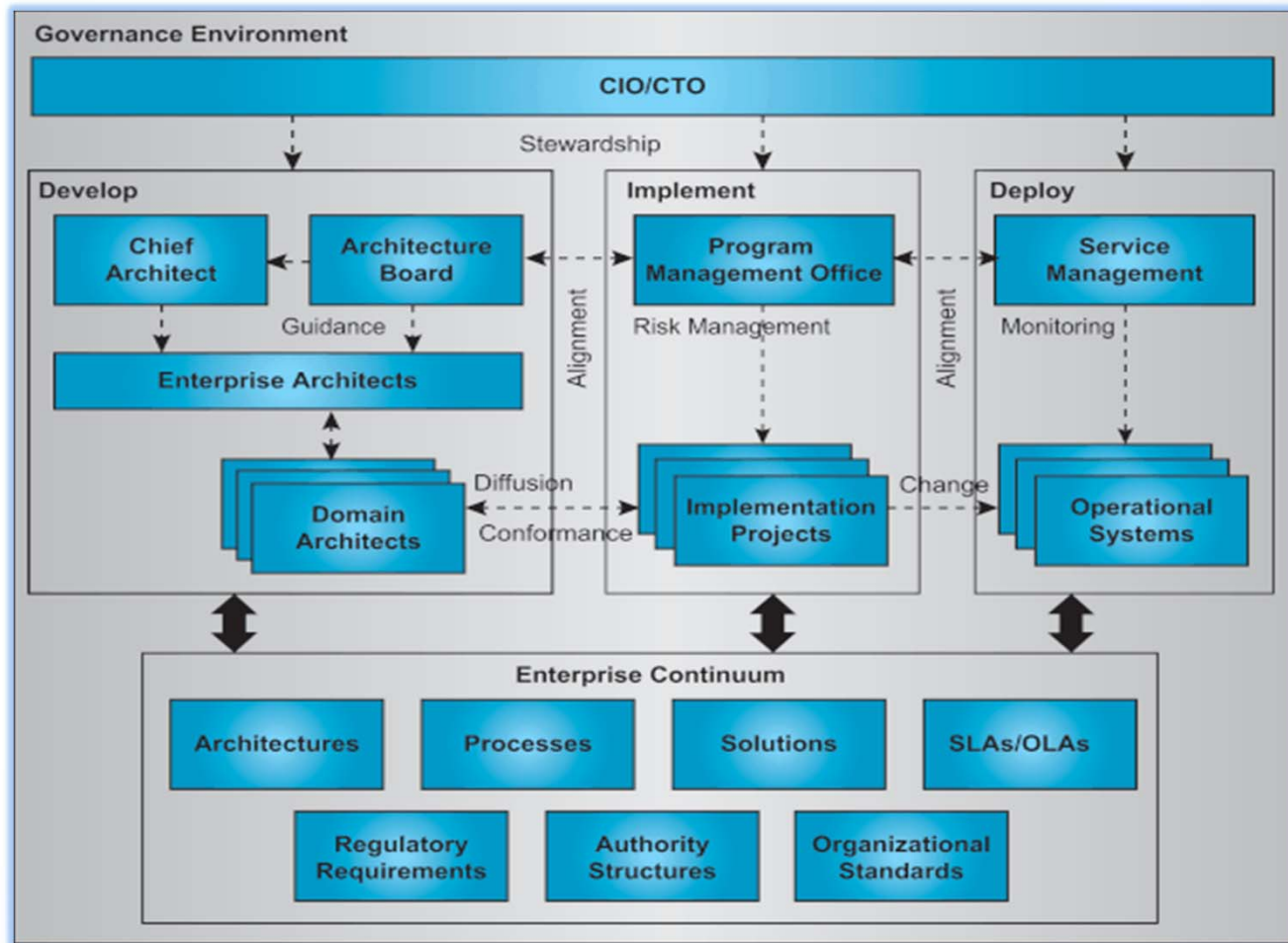
- Architectural framework providing a comprehensive approach for -
 - Planning
 - Design
 - Implementation
 - Governance
- Modeled at four levels
 - Business
 - Application
 - Data
 - Technology



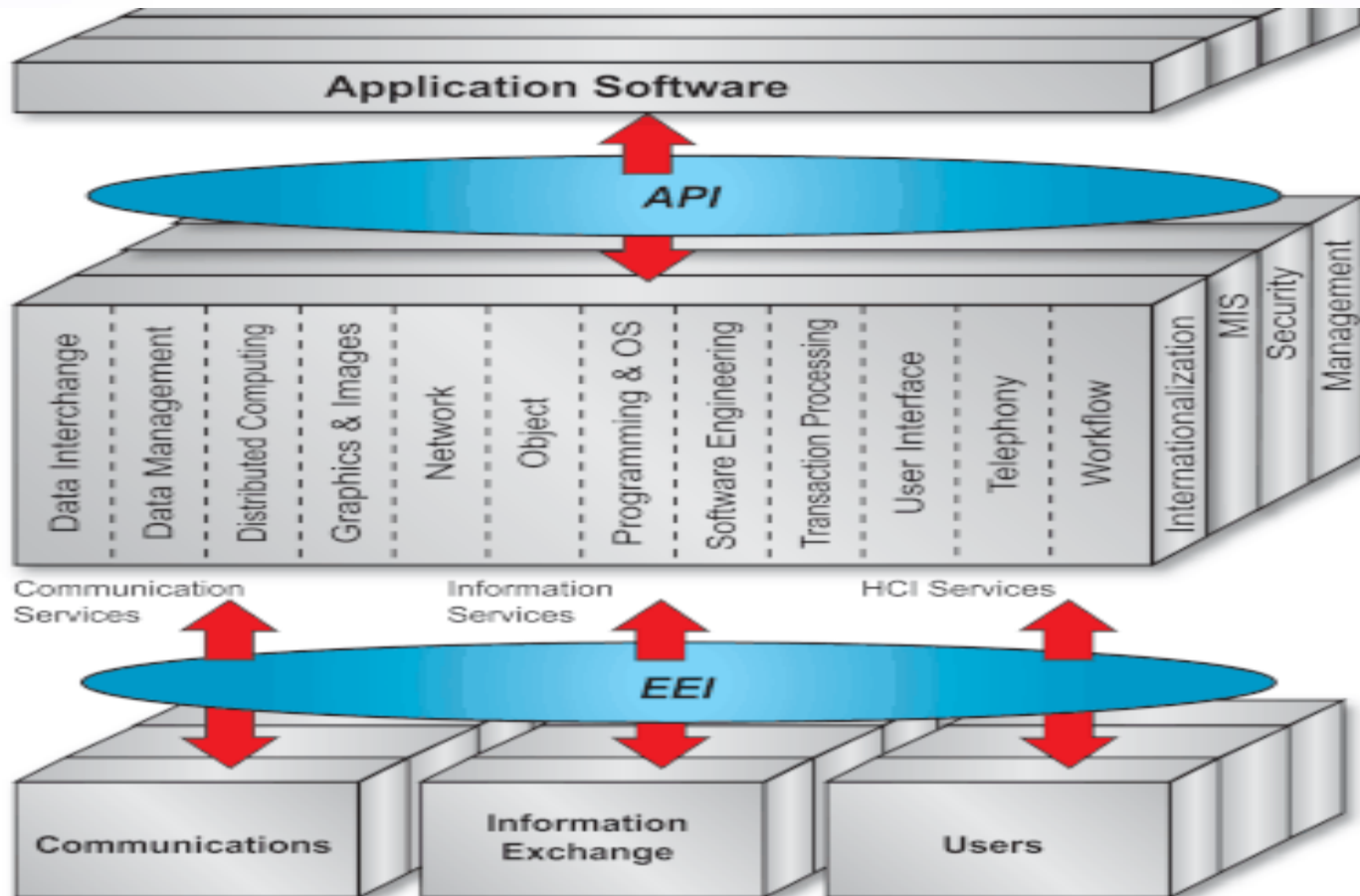
TOGAF Framework



Identify Gaps



Interoperability



Tool Sets – Auditing and Discovery

Management Applications

Project

Add wireless Internet access on Floor 3.

Determine modem locations

Restock modems

Wall repair

IT GRC

Compliance Manager defines Risk Control.

Compliance Manager creates Control Test Definition.



Custom App

Facilities Management

Incident

Number: INC0000017

Caller: Joe Employee

Location:

Category: Hardware

Subcategory: None

Problem

Problem Summary Counts

Critical Problems: 1

Overdue Problems: 0

Problems Opened > 1 Week: 0

Change

Change Request Summary

Change Request Details

Custom App

HR Management

Operational Applications

Service Catalog & Request

Order Things

Browse the Service Catalog

Computers and Hardware

SDLC

SPNT0000005

Stories [1 of 2 Lists]

Sprint = Sprint 5

- STRY0000005 Add module for managi
- STRY0000013 Amend database modu
- STRY0000014 Amend system to allow

Release

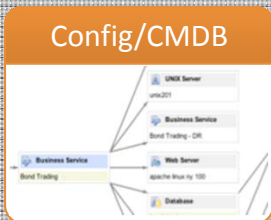
Release Request Summary

Release Request Details

Custom App

Vendor/Contract Management

Infrastructure Applications



Discovery

Related Items:

- Backup done by - Groups
- DR provided by - Business Services
- Depends on - Linux Servers

Asset

Display name: APC 42U 3100 SP2 NetShelter Rack

Manufacturer: APC

Short description: APC AR3100SP2 42U NetShelter 5X 600P

Model categories: Rack

Asset tracking strategy: Leave its category

Acquisition method: None

Orchestration

Workflow

Stage: Fulfillment

VMWare - Provision

Notification

Stage: Delivery

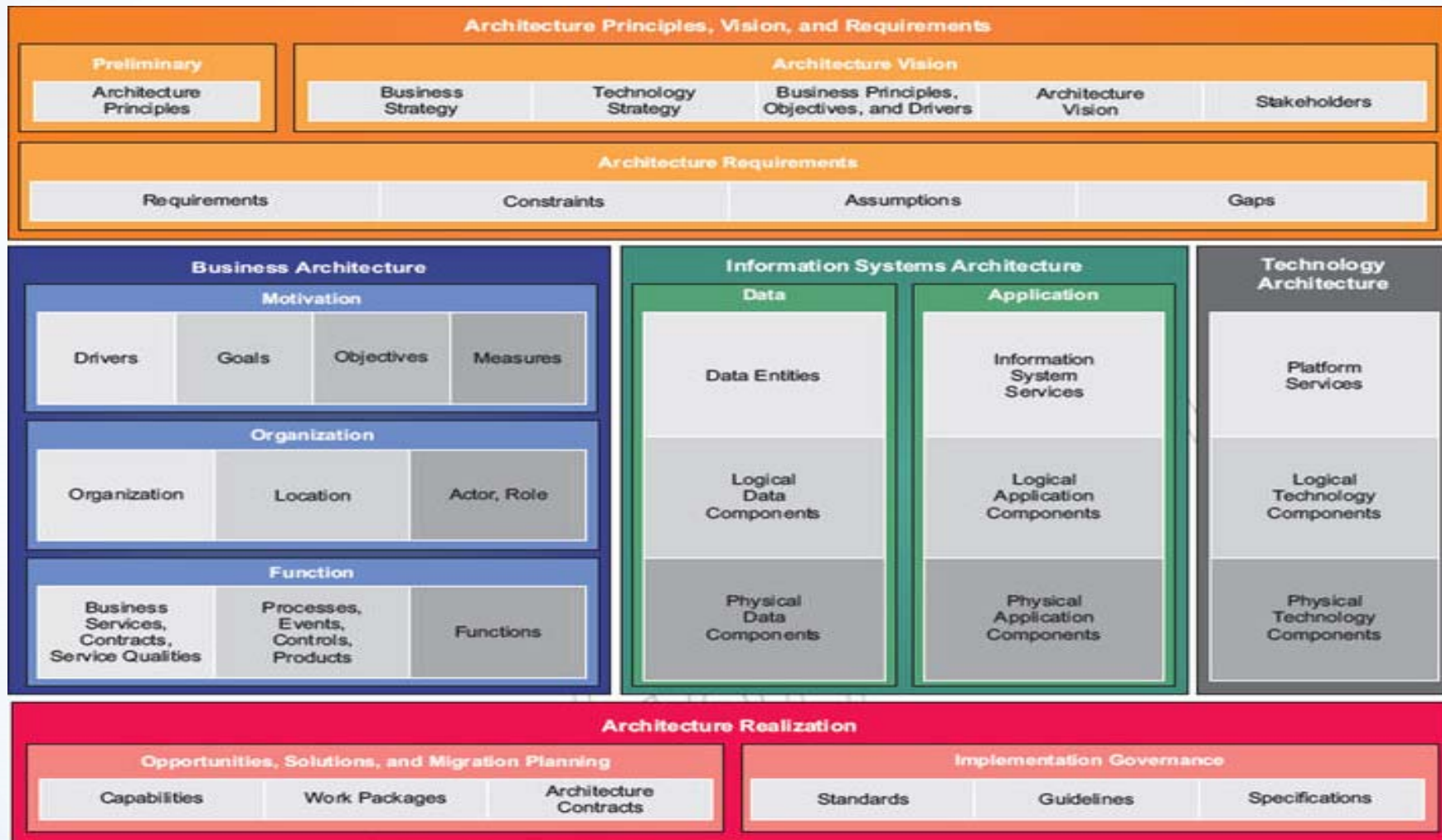
Email Successful VM Creation to Requester

Custom App

Shipping/Logistics Management

Service Management

Define the Foundation



Process and Framework

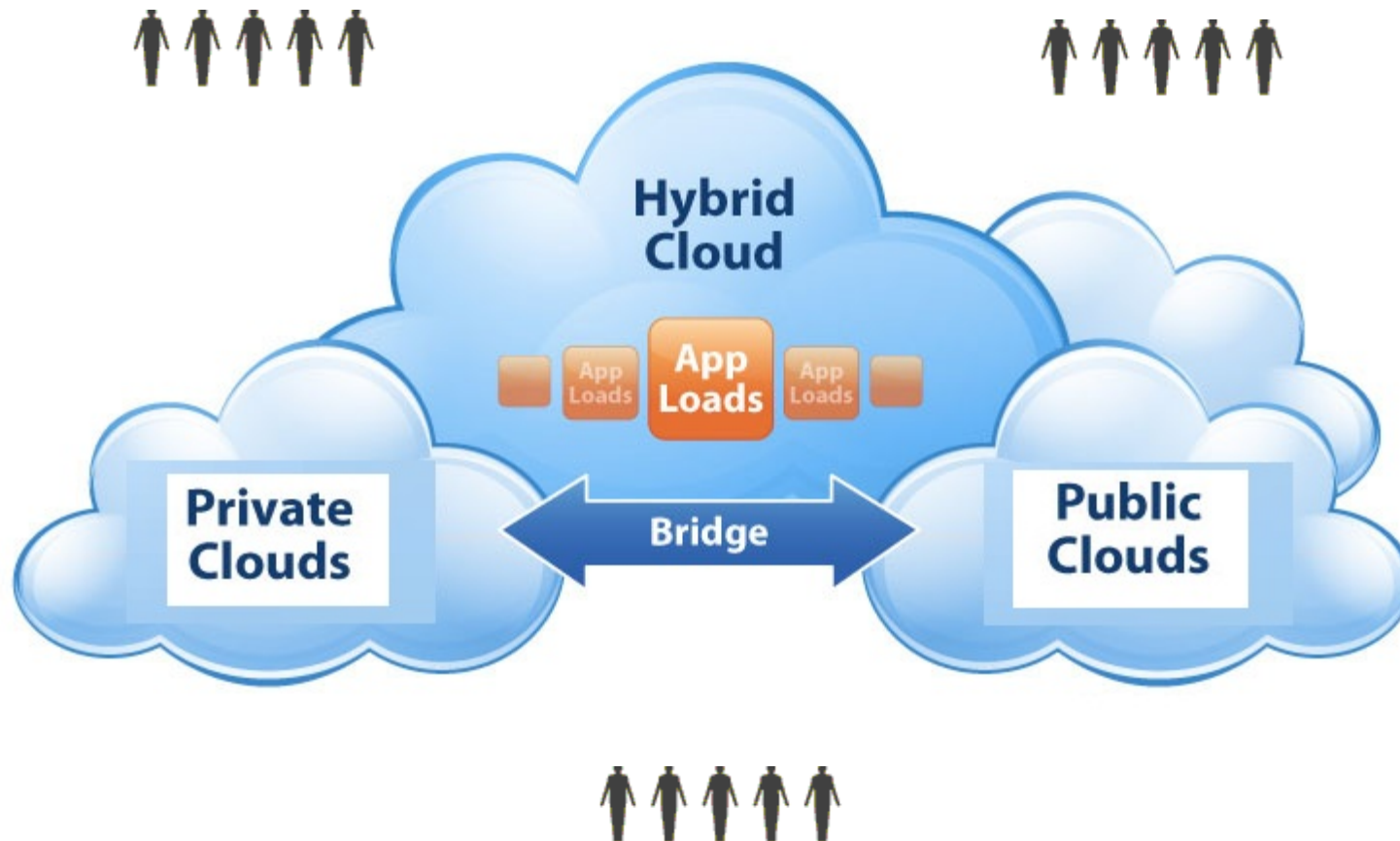


© 2008 The Open Group

TOGAF Phase		Architecture Context		Architecture Definition			Transition Planning		Architecture Governance	
		Initial Iteration	Iteration 1	Iteration 2	Iteration <i>n</i>	Iteration 1	Iteration <i>n</i>	Iteration 1	Iteration <i>n</i>	
Preliminary		Core	Informal	Informal	Informal					Light
Architecture Vision		Core	Informal	Informal	Informal	Informal	Informal			Light
Business Architecture	Baseline	Informal	Core	Light	Core	Informal	Informal			Light
	Target	Informal	Informal	Core	Core	Informal	Informal			Light
Application Architecture	Baseline	Informal	Core	Light	Core	Informal	Informal			Light
	Target	Informal	Informal	Core	Core	Informal	Informal			Light
Data Architecture	Baseline	Informal	Core	Light	Core	Informal	Informal			Light
	Target	Informal	Informal	Core	Core	Informal	Informal			Light
Technology Architecture	Baseline	Informal	Core	Light	Core	Informal	Informal			Light
	Target	Informal	Informal	Core	Core	Informal	Informal			Light
Opportunities and Solutions		Informal	Light	Light	Light	Core	Core	Informal	Informal	
Migration Planning		Informal	Light	Light	Light	Core	Core	Informal	Informal	
Implementation Governance						Informal	Informal	Core	Core	
Change Management			Informal	Informal	Informal	Informal	Informal	Core	Core	

- Core: primary focus activity for the iteration
- Light: secondary focus activity for the iteration
- Informal: potential activity for the iteration, not formally mentioned in the method

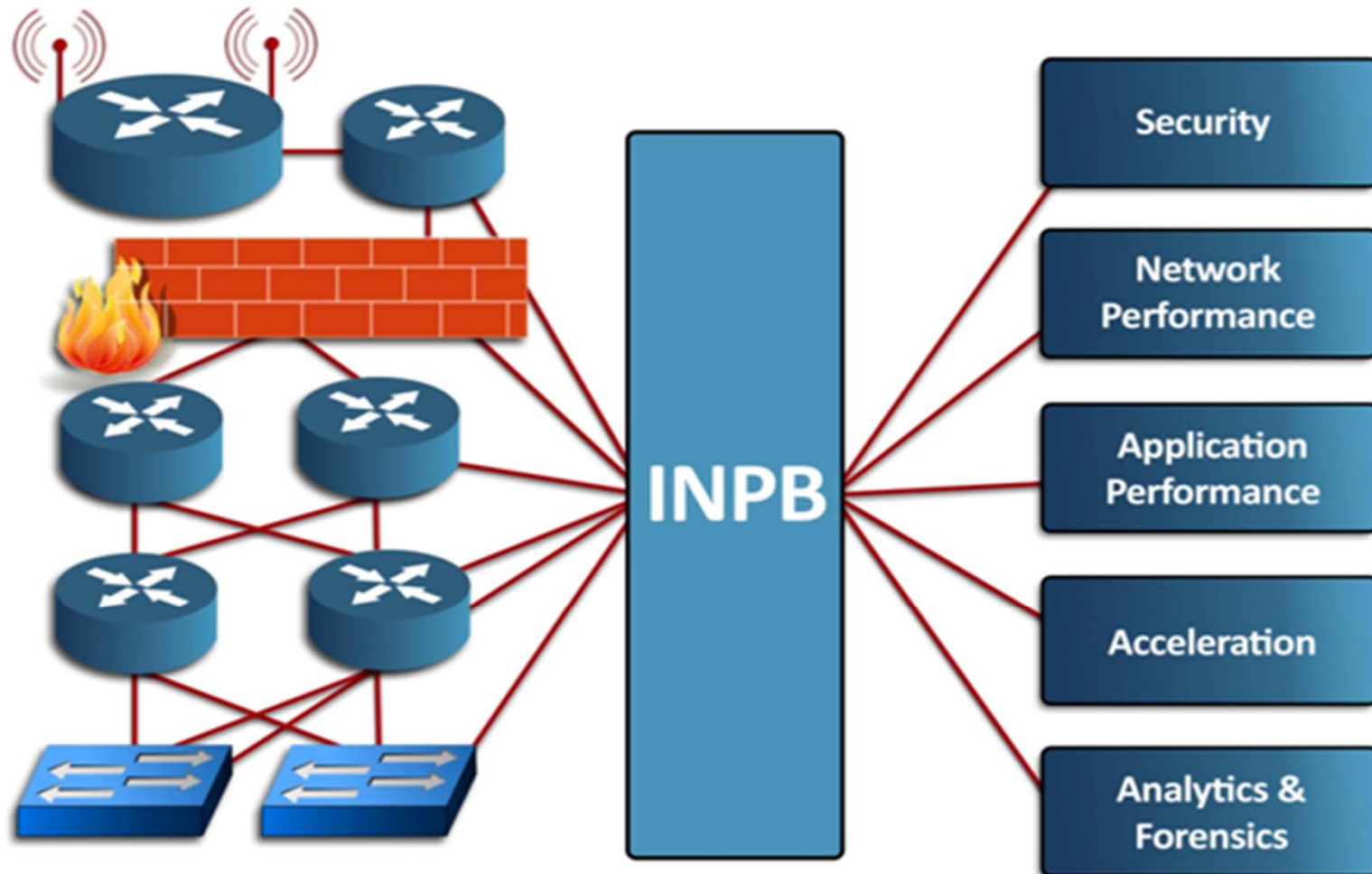
Traffic Flows and User Communities



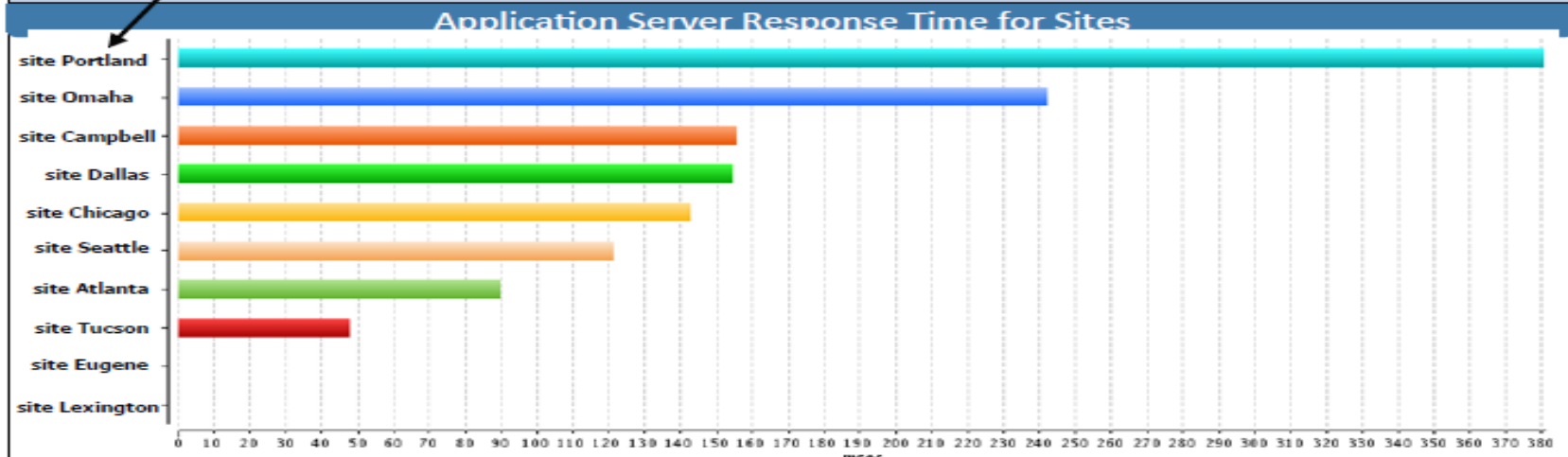
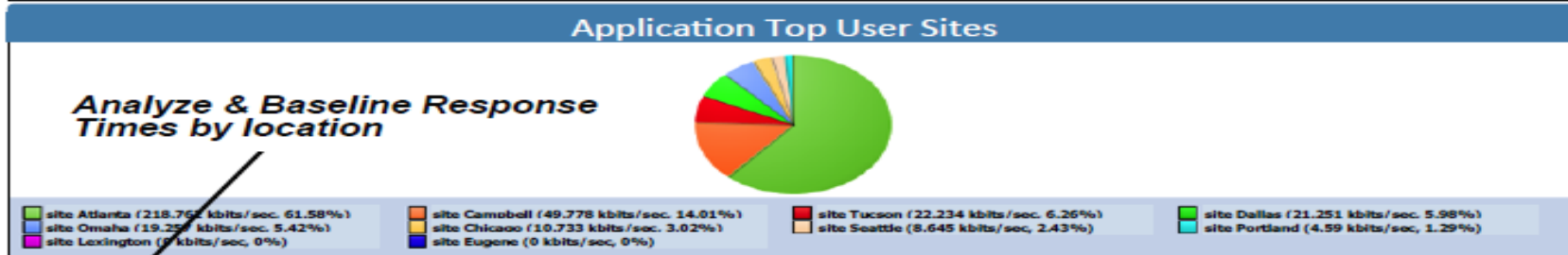
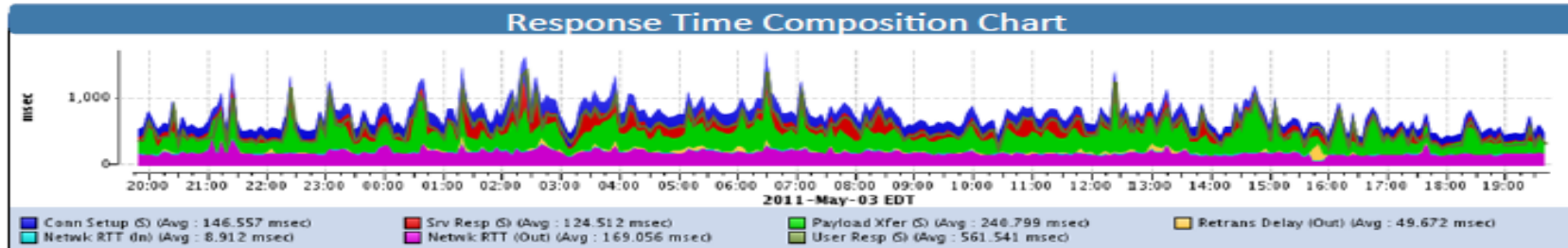
Where Do I Go, Which way does it go?



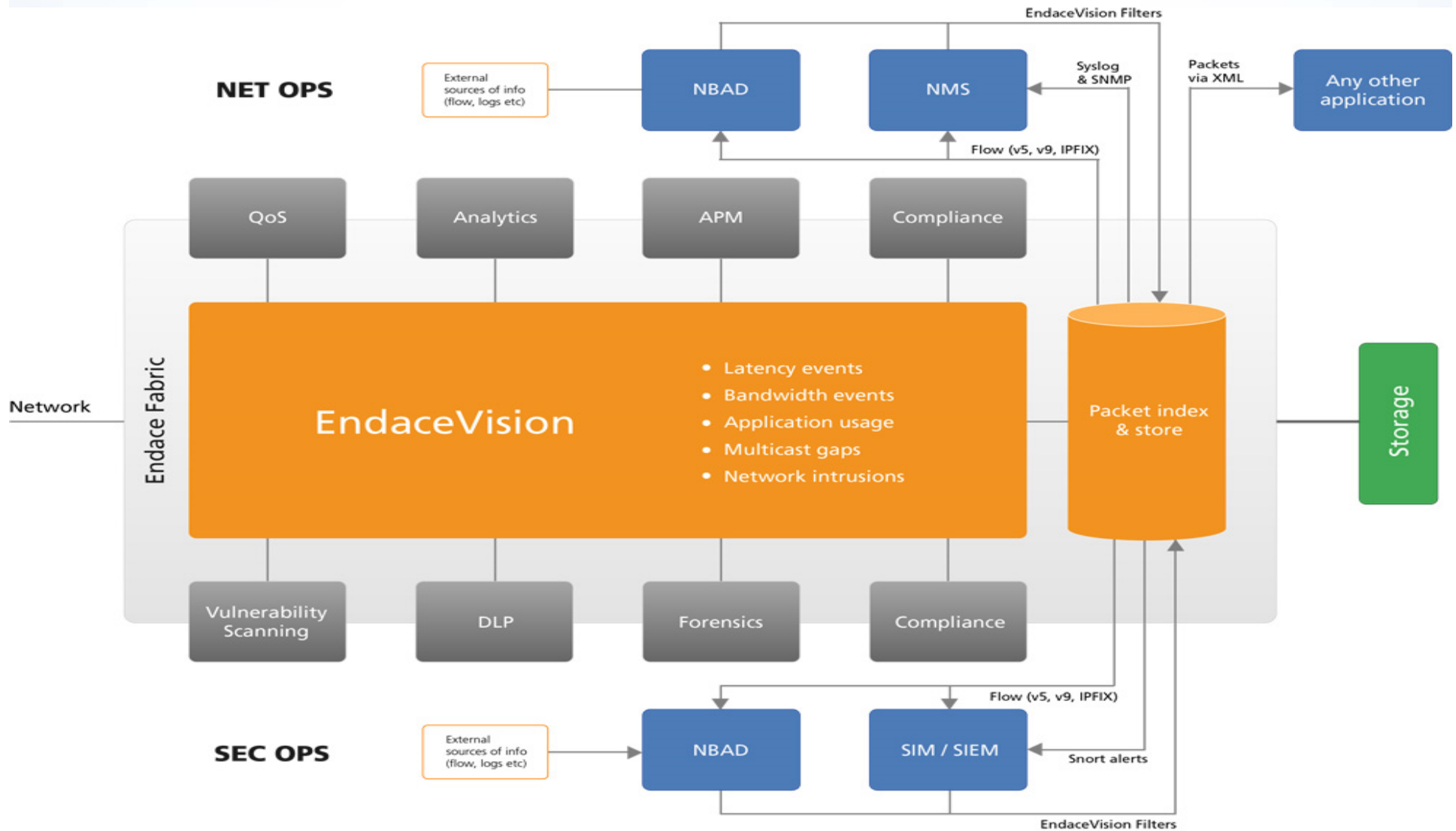
Flow Mapping and Traffic Direction



Dependency Mapping, Base lining



Correlations and Deep Packet Inspection



Testing and Load Simulation



Client Can Leverage Across the Following:



Note – the User can leverage across MANY devices:

- IDS/IPS and Firewalls
- Load Balancers & Proxy Devices
- Additional Perimeter/LAN network devices
- Including Servers & Applications, as appropriate

Realistic Blended Application Traffic

- +150 Applications
- Mail/Messaging
- Voice/Video/Media
- Microsoft File Service
- Database
- Social Media/Gaming

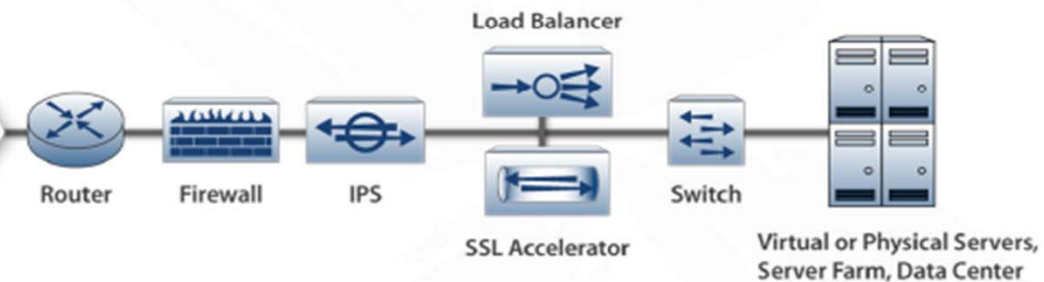
Live Security Attacks

- 4,500+ live security attacks
- 80+ evasion techniques
- Complete Microsoft Tuesday coverage

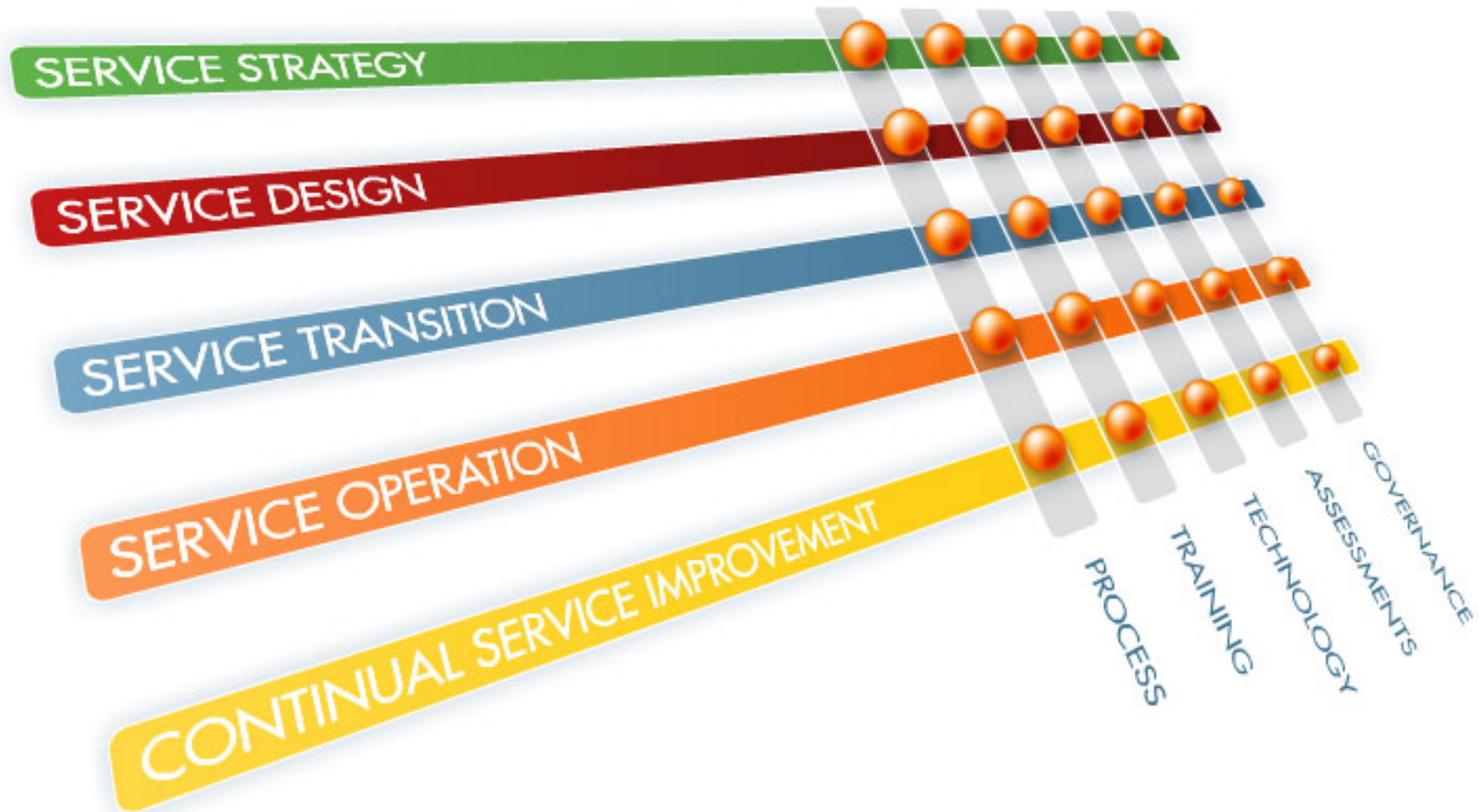
Performance

- 30 Million simultaneous TCP sessions
- 1.5 Million TCP sessions per second
- 20 Gbps blended application traffic
- 80,000+ SSL sessions/second

Converged Traffic



Service Delivery: A Continual Process

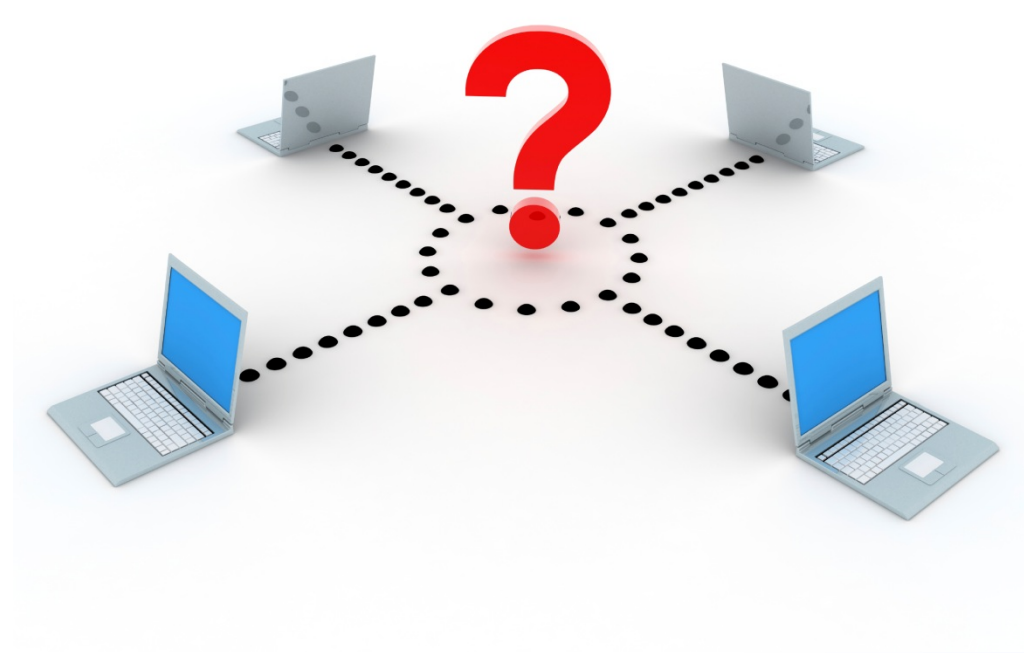


Recap and Considerations

- Network Optimization
- Current Tool Sets
- Applications - Simultaneous Sessions
- Configurations and Policies
- Inbound and Outbound Flows - User Communities
- Resource and Bandwidth Availability
- Storage/Content
- Traffic Direction and Mapping
- Deep Packet Inspection
- Integration, Correlations, and Analytics
- Fault Isolation
- Visibility and Predictability
- Accountability - SLA's
- Synchronization and Interoperability
- Enhancing Operational Efficiencies
- Improving Service Delivery

Thank You

Shawn Butler
Enterprise Architect
FishNet Security
Shawn.butler@fishnetsecurity.com



Join the FishNet Security Online Community

www.FishNetSecurity.com/6Labs

Our Experts. Your Solutions.



/company/fishnet-security



/fishnetsecurity



/fishnetsecurity