RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ASD-R03

WestJet's Security Architecture Made Simple We Finally Got It Right!

Richard Sillito

Solution Architect, IT Security
WestJet
@dhoriyo

Fort Henry Ontario

Flight Plan

Applying Principals

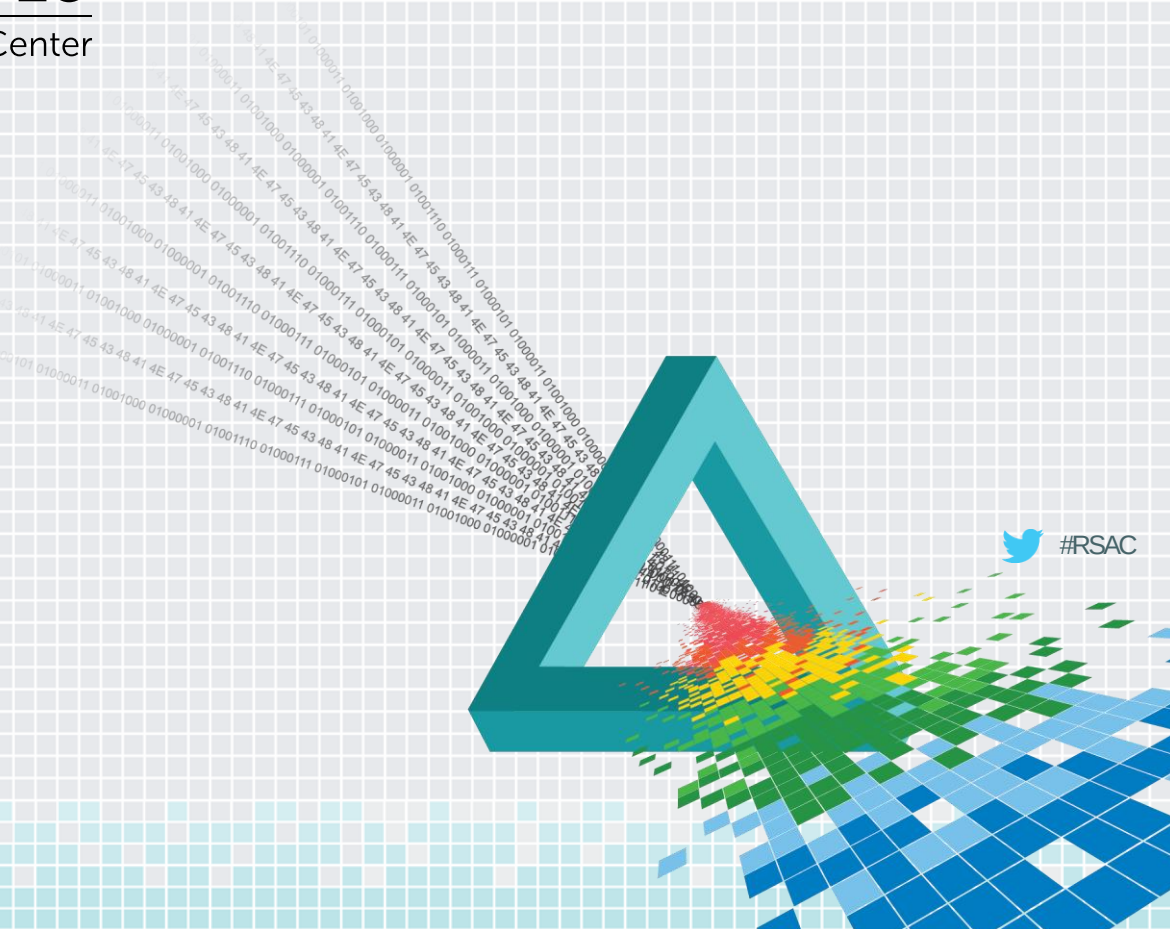
The Solution

Summary

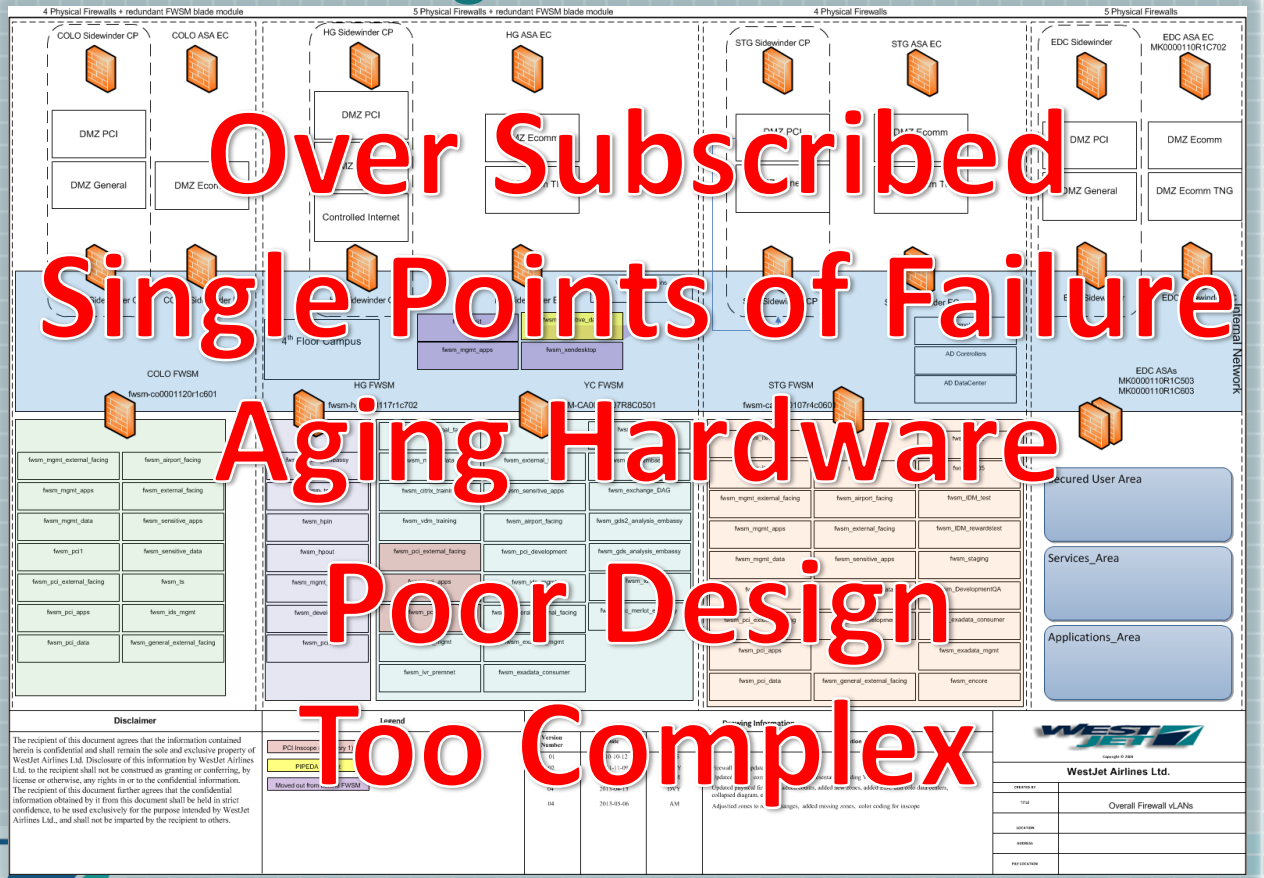
The Problem

Questions

The Problem



What wrong with the network?



Over Subscribed

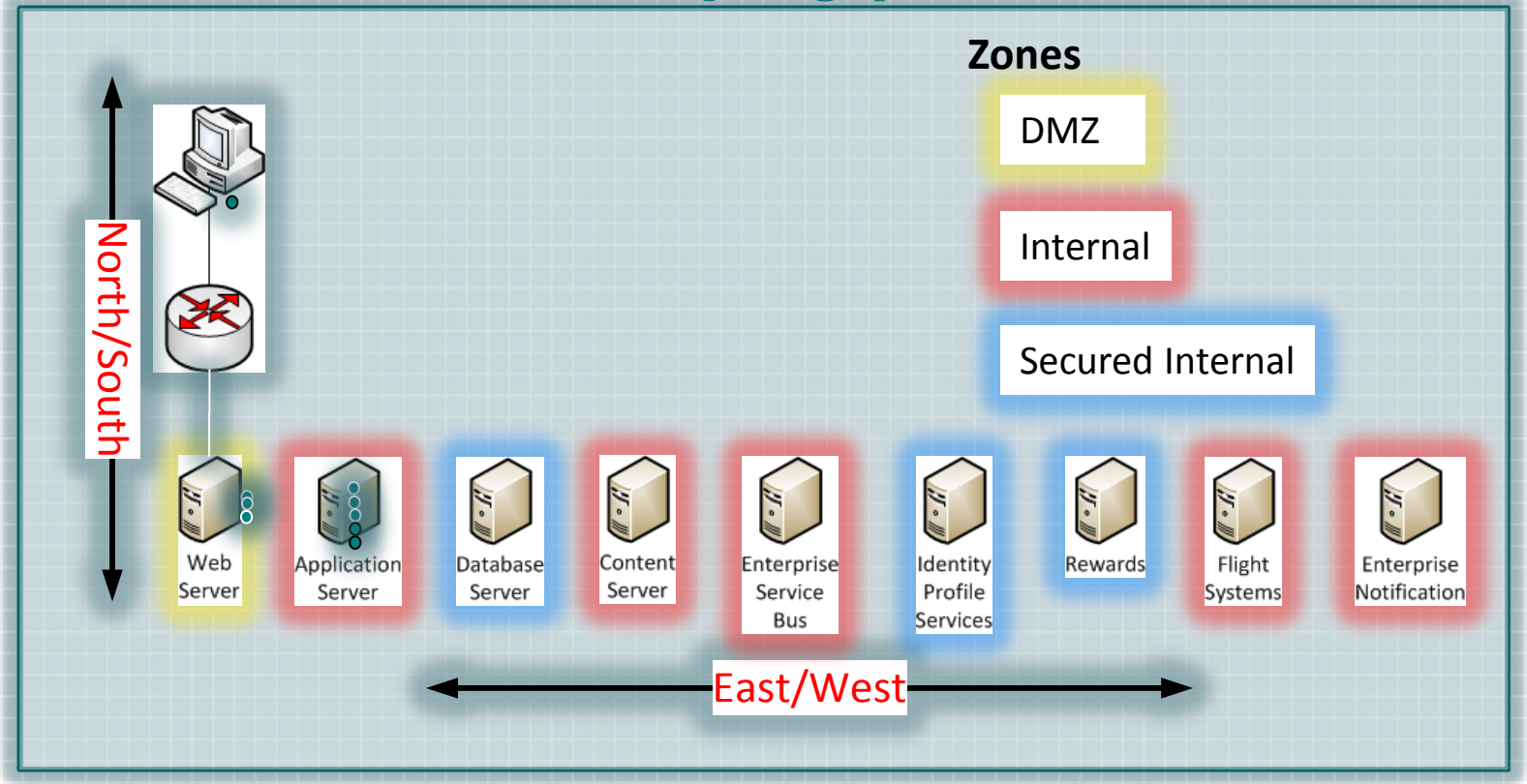
Single Points of Failure

Aging Hardware

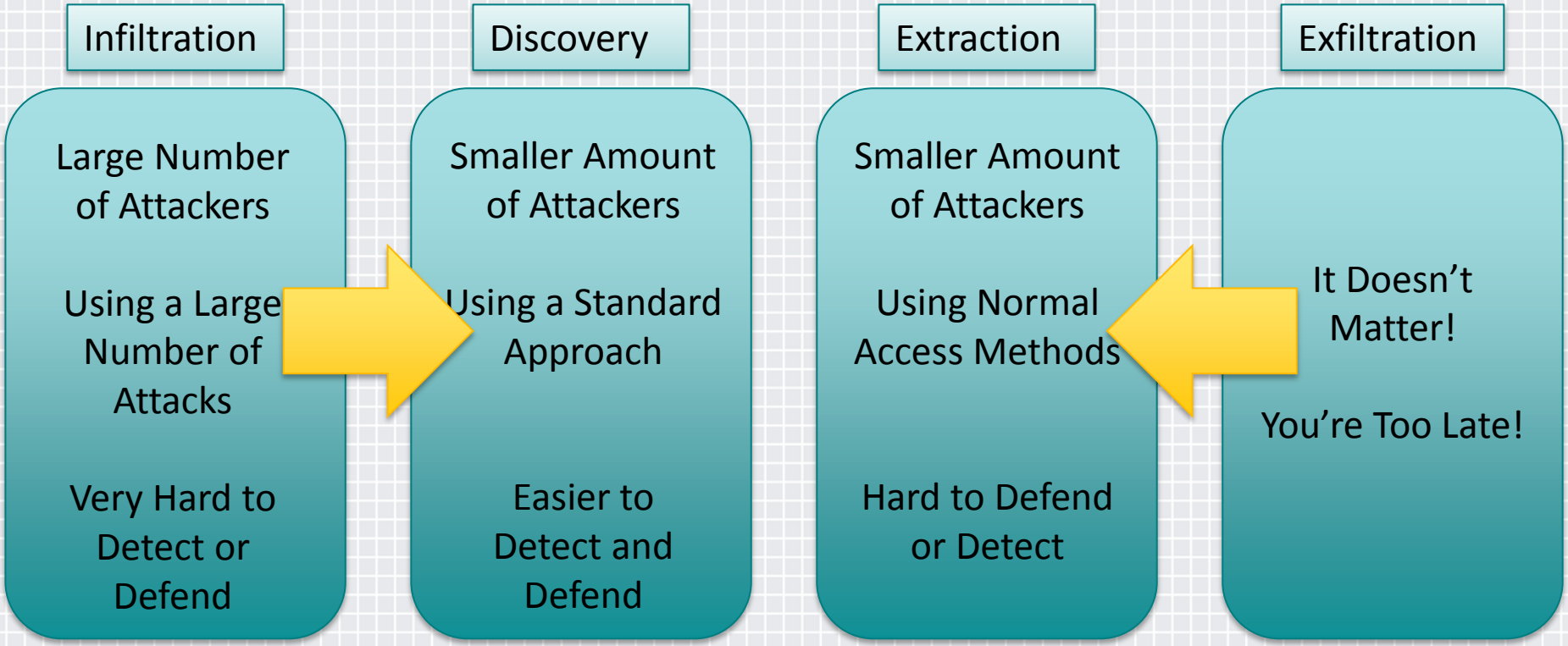
Poor Design

Too Complex

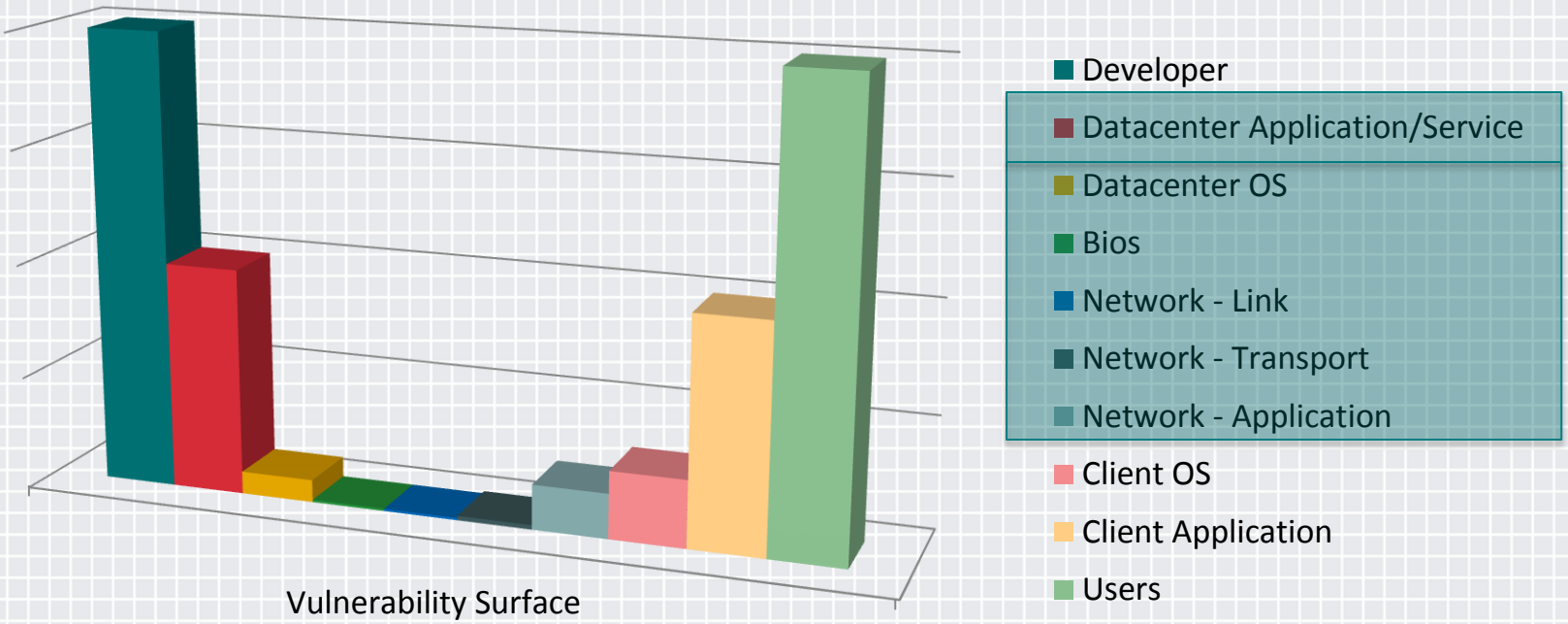
The underlying problem



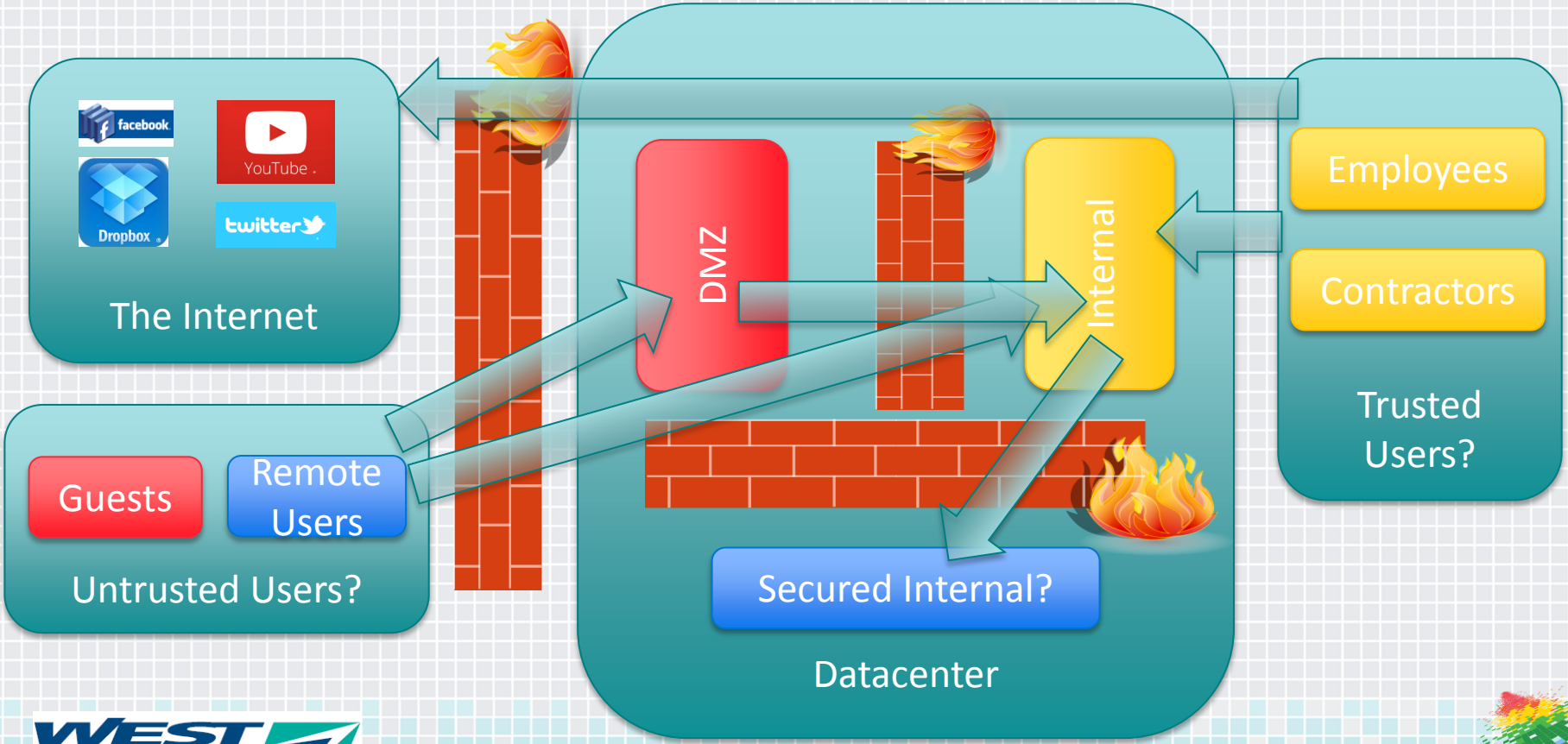
The Threat


Infiltration
Large Number of Attackers
Using a Large Number of Attacks
Very Hard to Detect or Defend
Discovery
Smaller Amount of Attackers
Using a Standard Approach
Easier to Detect and Defend
Extraction
Smaller Amount of Attackers
Using Normal Access Methods
Hard to Defend or Detect
Exfiltration
It Doesn't Matter!
You're Too Late!

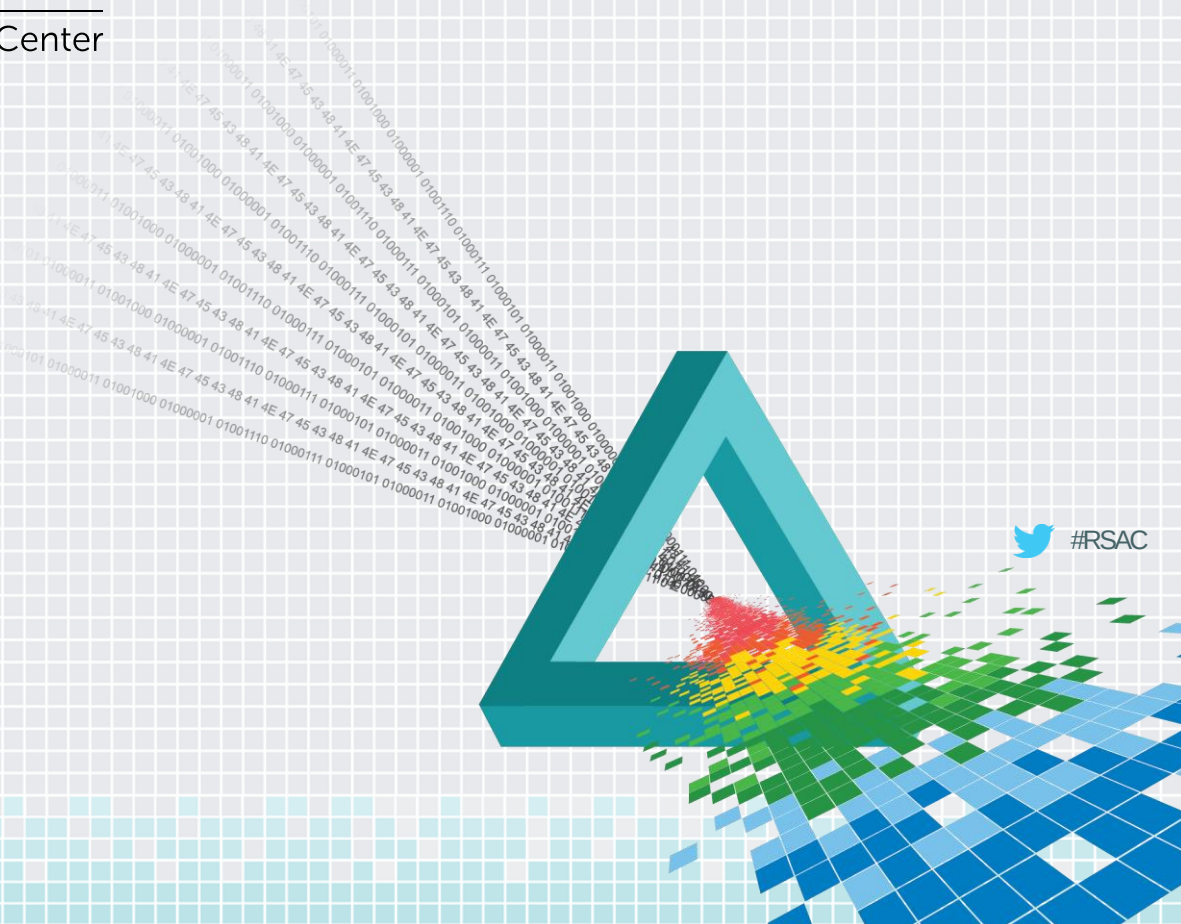
Vulnerability Surface



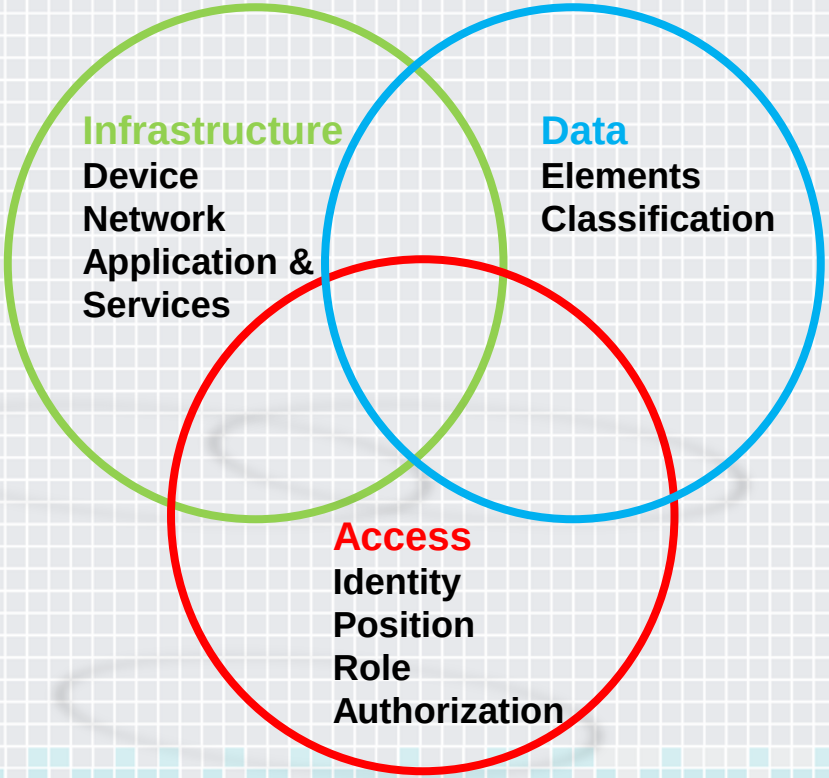
Existing Datacenter – Never Worked



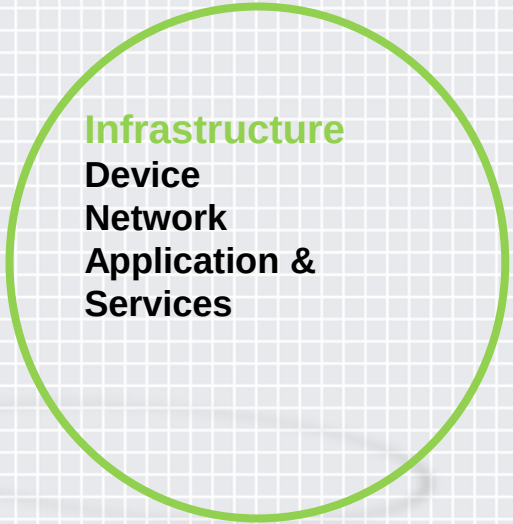
The Solution



Security Architecture Made Simple (SAMS)

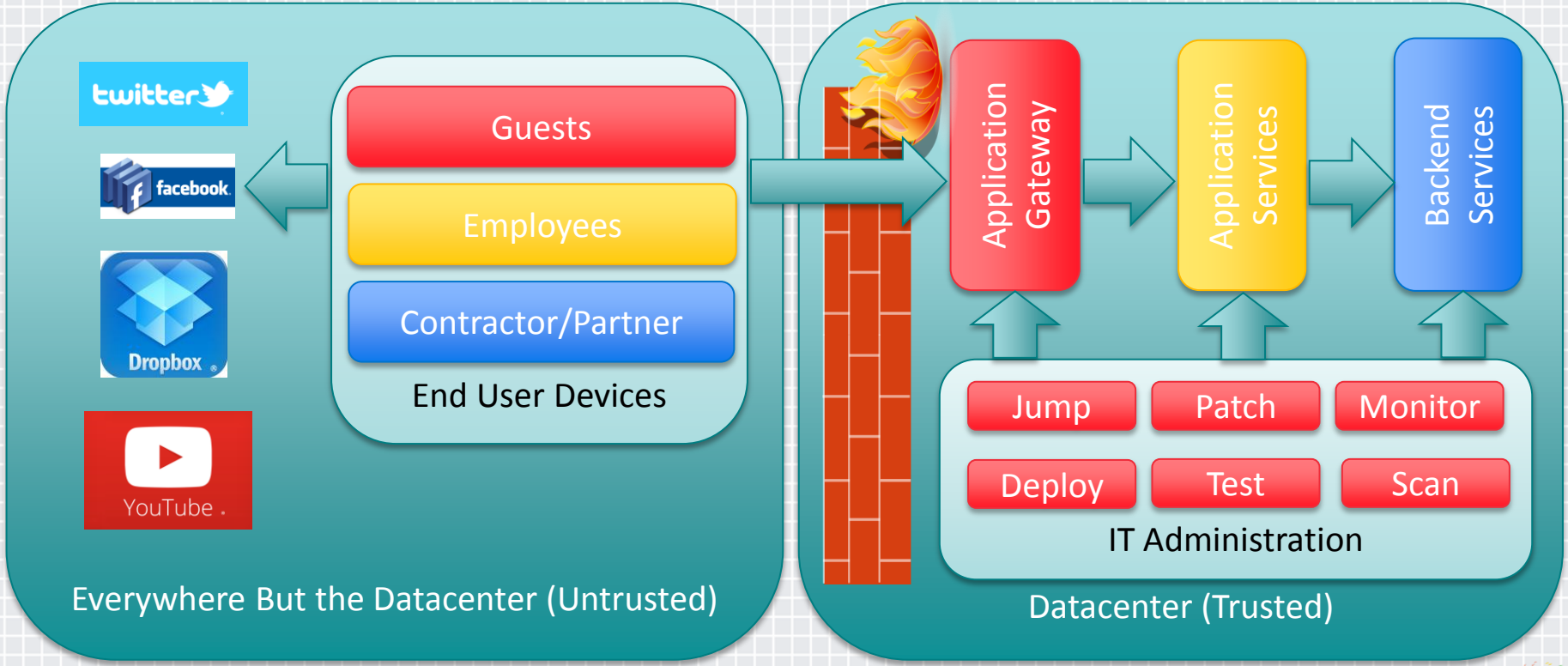


Security Architecture Made Simple (SAMS)

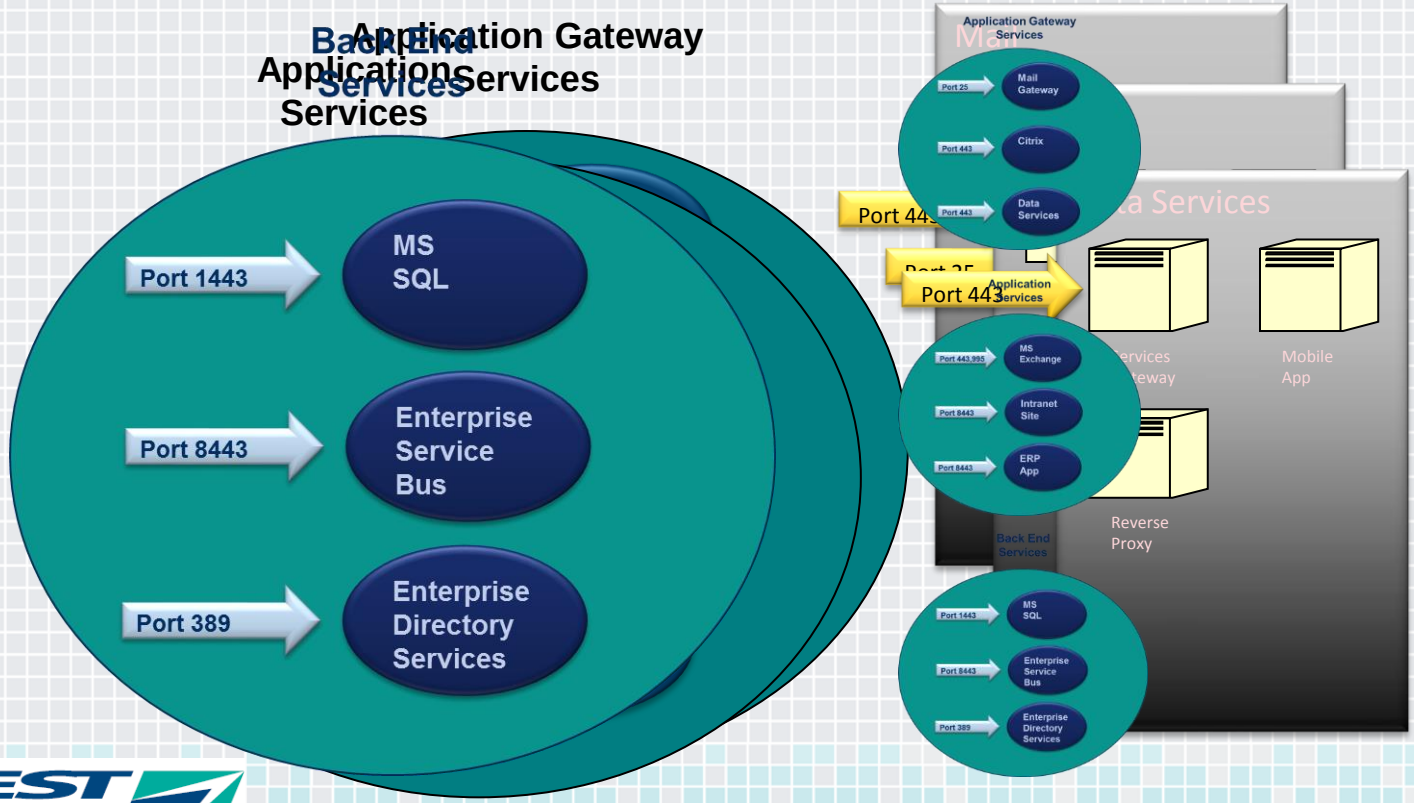


Security Architecture Made Simple (SAMS)

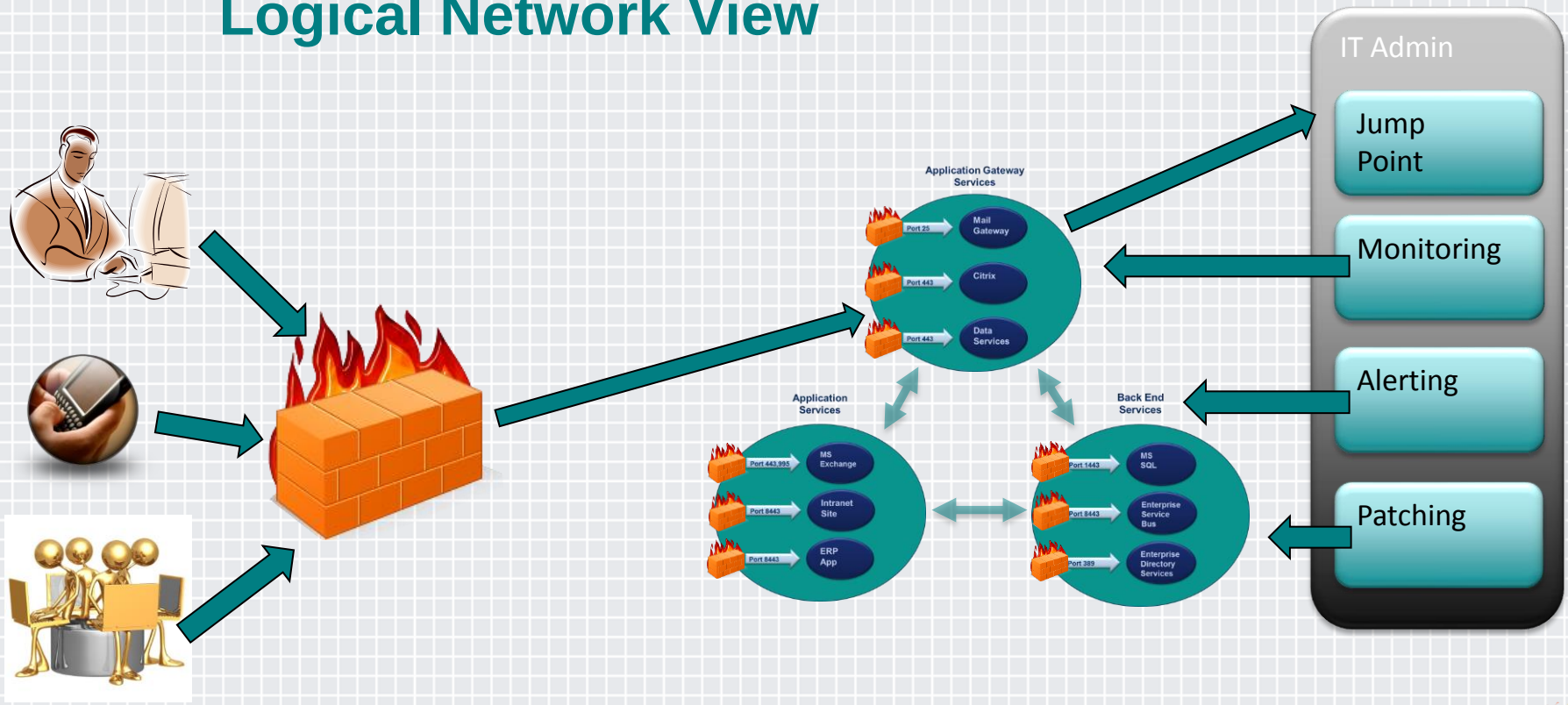
SAMS - Infrastructure



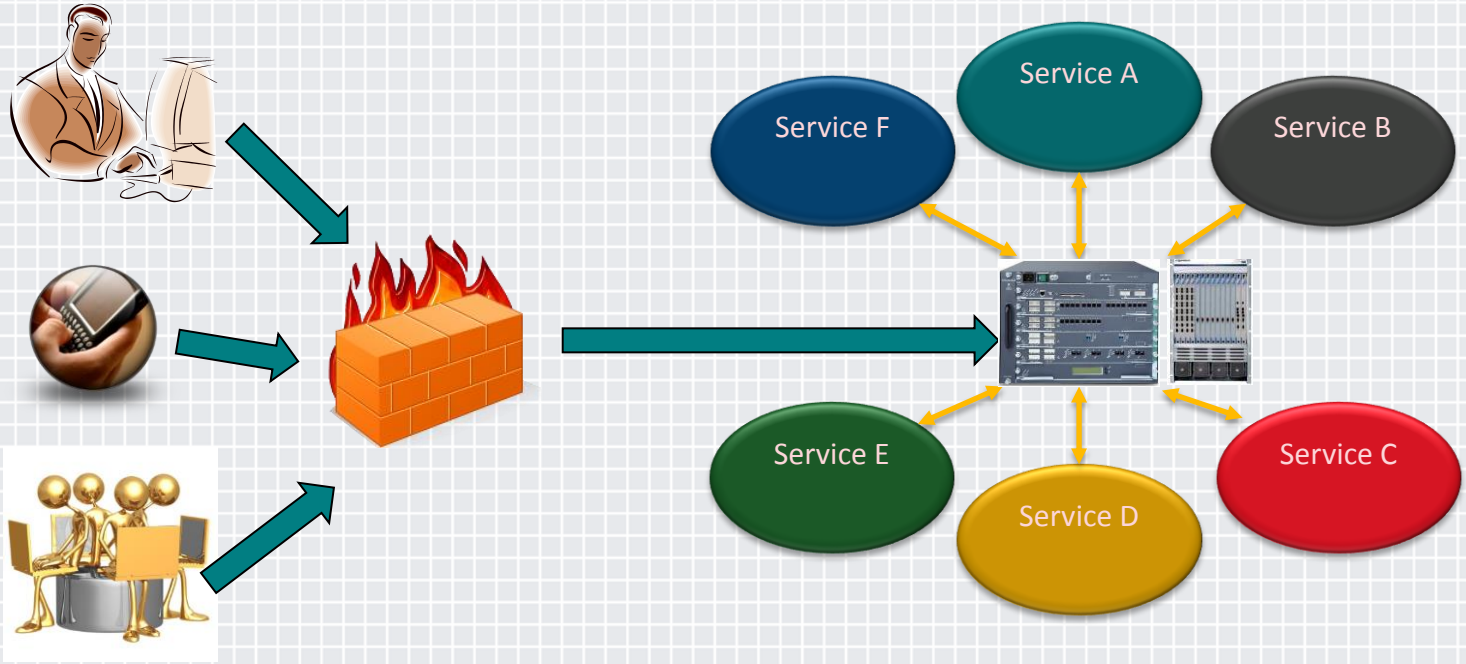
SAMS – Infrastructure Logical Network View



SAMS – Infrastructure
Logical Network View



Using Core Router and Core Firewall



Traditional Approach

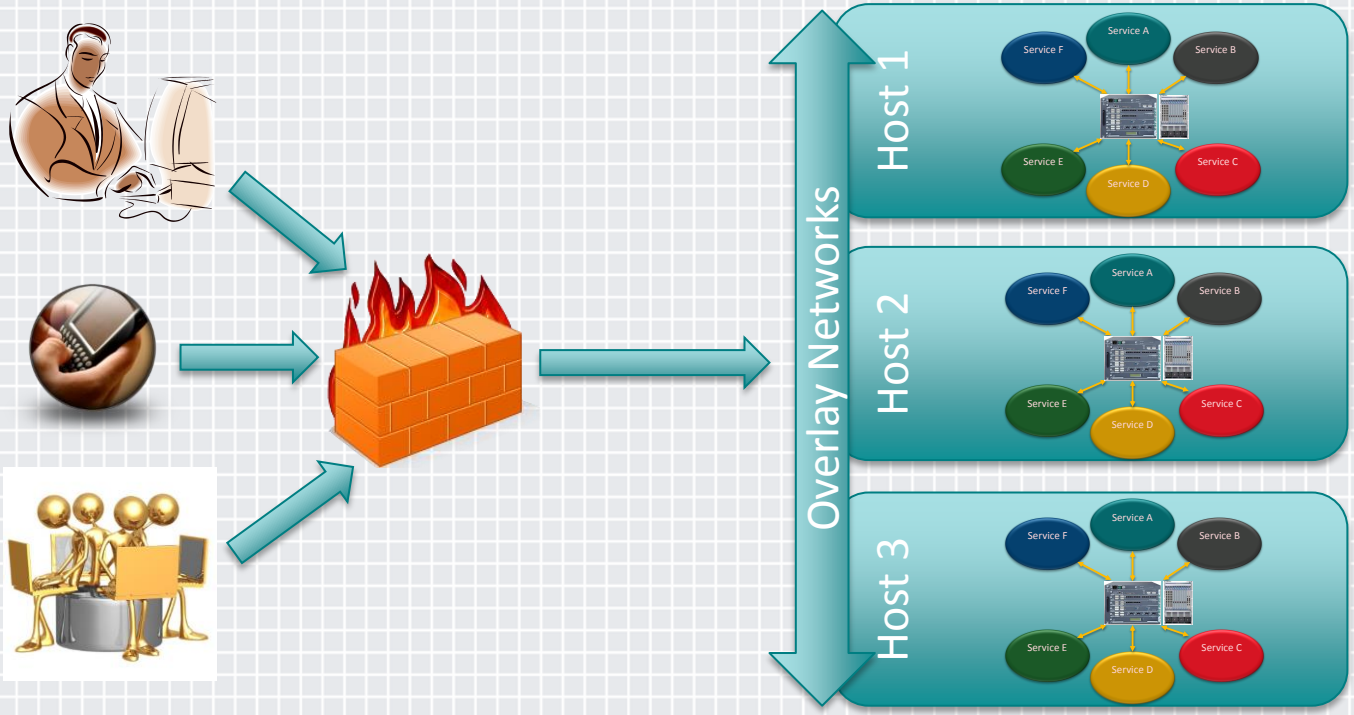
Pros

- Known Technology
- Somewhat Flexible
- Minimal Training

Cons

- Difficult to Scale the Solution
- Hub Model Requires all Traffic Traverse the Core
- Difficult to Insert Additional Security Services

The Software Defined Approach



SDN/S Approach

Pros

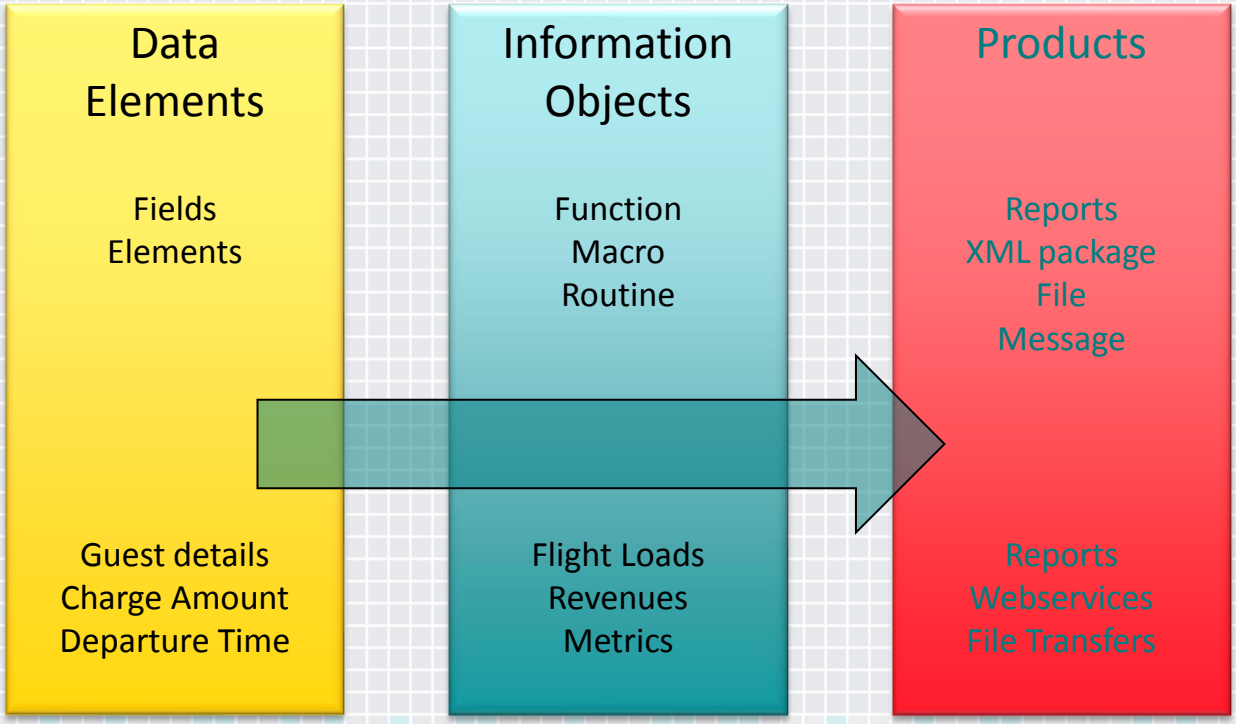
- Easily Scaled
- Very Flexible
- Optimized Routing
- Allows Insertion of Security Services
- Automation/Orchestration

Cons

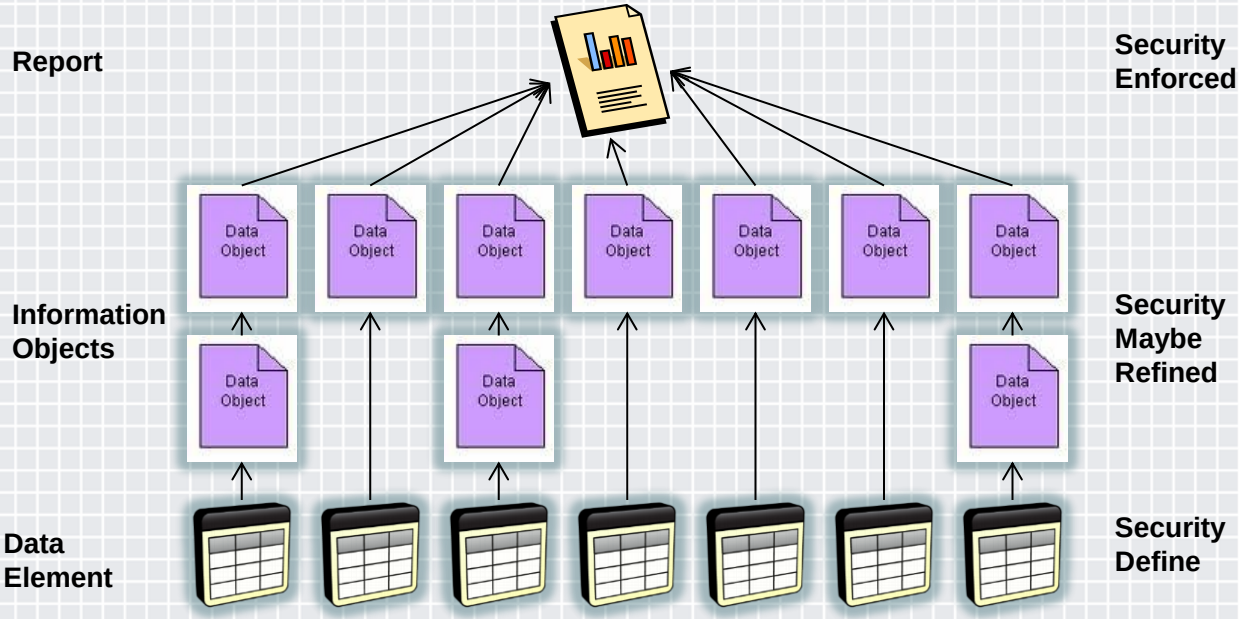
- Emerging Technology
- Standards are Not Well Defined
- Vendor Eco Systems are Developing
- Monitoring Solutions are Not Well Developed

Security Architecture Made Simple (SAMS)

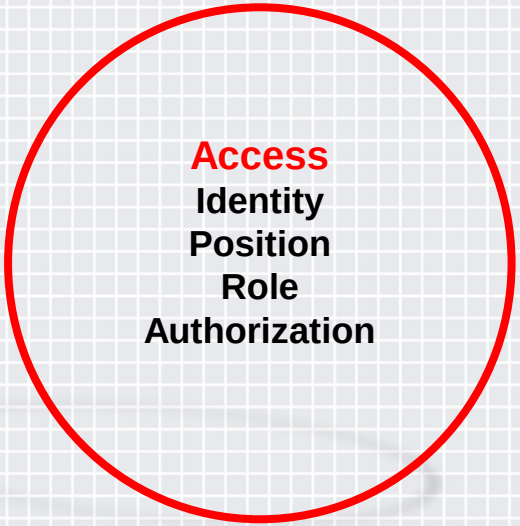
Security Architecture Made Simple
SAMS Data



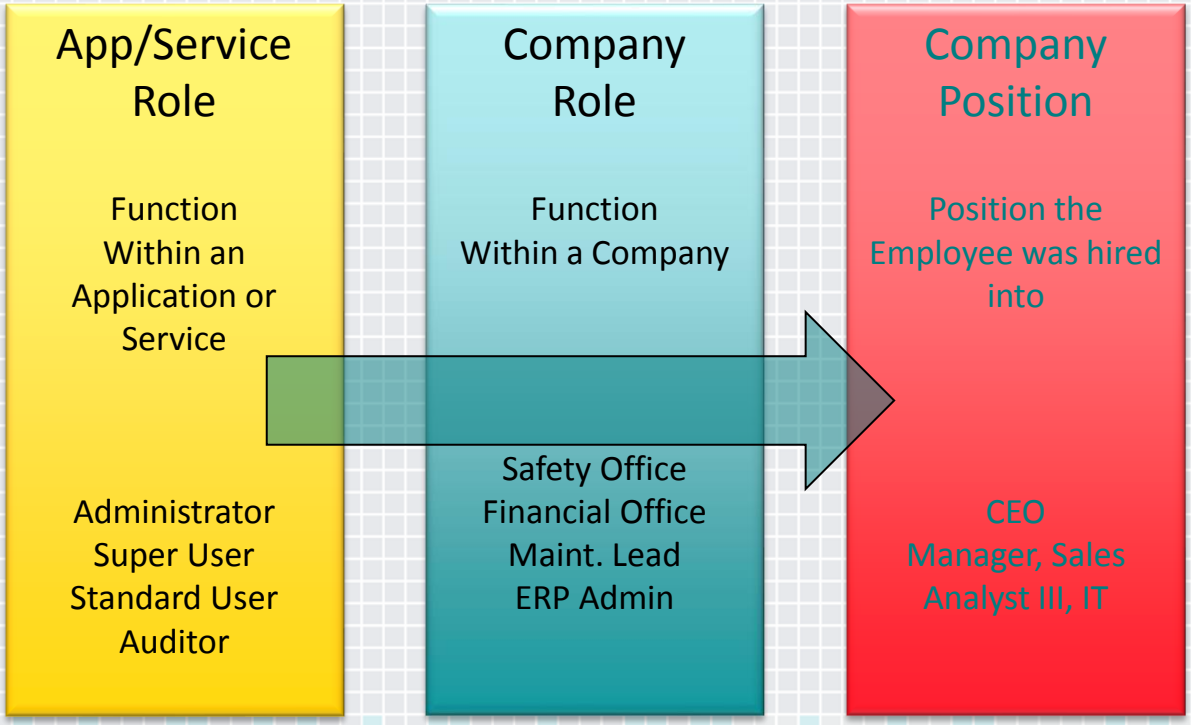
SAMS Data Example



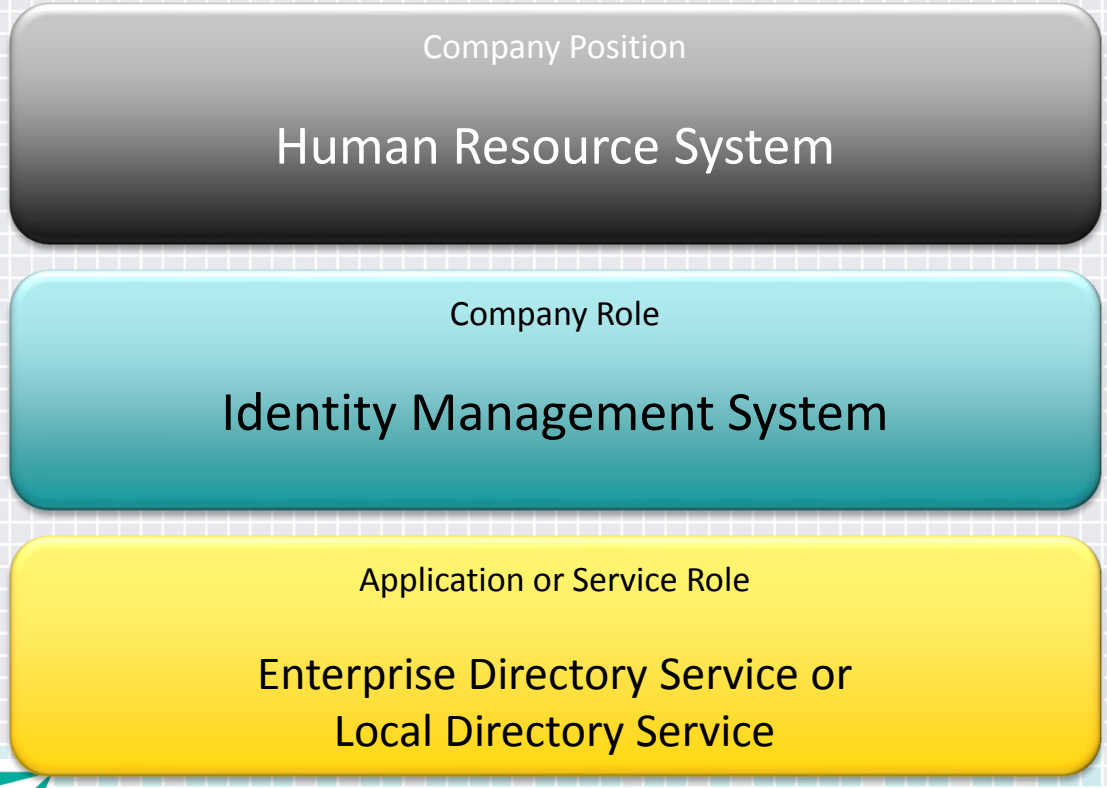
Security Architecture Made Simple (SAMS)



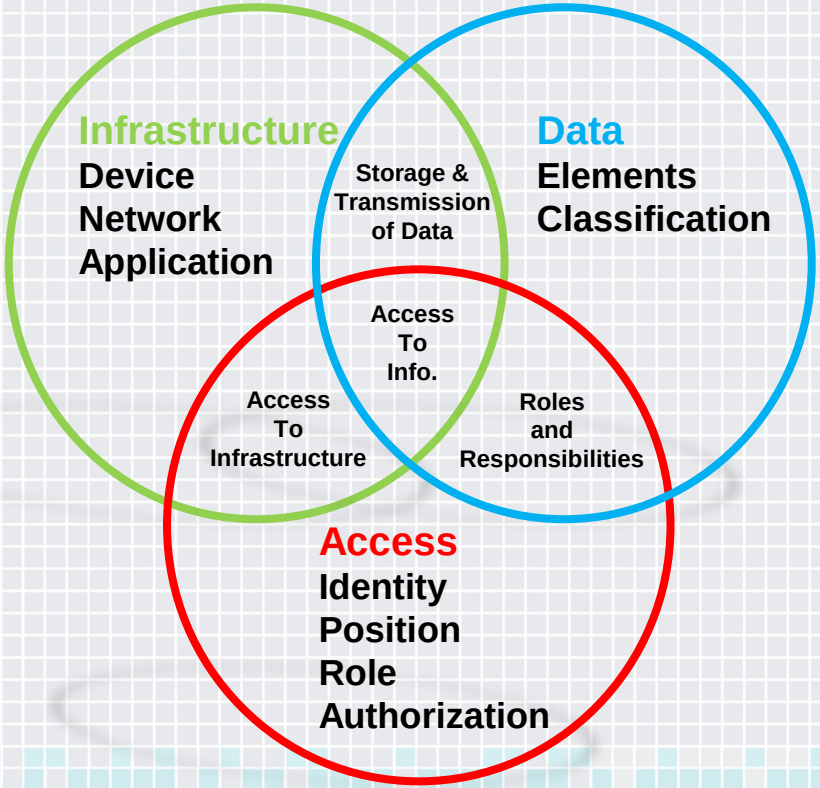
Security Architecture Made Simple
SAMS Access



Security Architecture Made Simple
SAMS Access



Security Architecture Made Simple (SAMS)



Products to look for (HyperLinked)

- Vmware NSX
- Palo alto, Check Point
- McAfee NSM
- Tivoli Identity Management
- Arkin Net Analytics Platform (www.arkin.net)

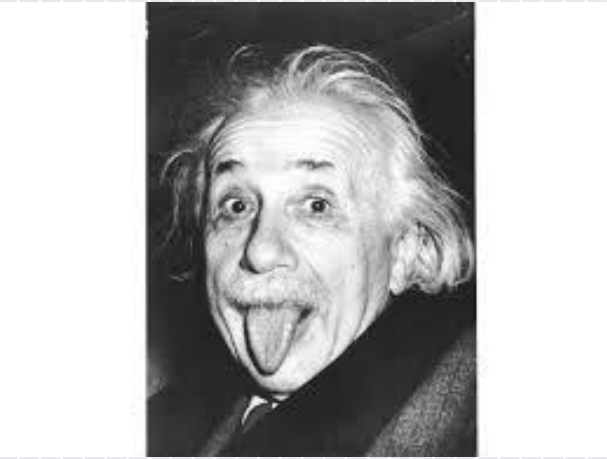
Apply Slide

- Consider network challenges
- Decide on a security strategy that will work for your organization
- Familiarize yourself with Software Defined Network & Security
- Accept that Bring Your Own Device is really your friend
- Figure out a plan to migrate your network
- Start making changes (evolution not revolution)

Summary

“If you can't explain it to a six year old, you don't understand it yourself.”

Albert Einstein



Thanks and Recognition

Inspiration

- Dump your DMZ by Joern Wettern
- BYOD and the Death of the DMZ by Lori MacVittie
- Zero Trust Model John Kindervag

Thanks

VTeam

- Dominador DeLeon – Sr. TSA - Infrastructure Ops
- Justin Domshy – Manager of Environments
- Mike Gromek - Technical Architect III
- Darrell Lizotte – Technical Architect III
- Randy Seabrook – Manager Architecture
- Derek Sharman - Sr. Analyst-Config Management
- Walter Wenzl - Sr Analyst-Config Management
- Michael Slavens - Security Support Analyst III
- Peter Graw - Technical Architect III, IT – Infrastructure
- Quentin Hall - Technical Architect III
- Tao Yu - Sr. TSA Telecomm

VMWare

- Vern Bolinius
- Ray Budavari
- Bruno Germain
- Darren Humphries

Bosses

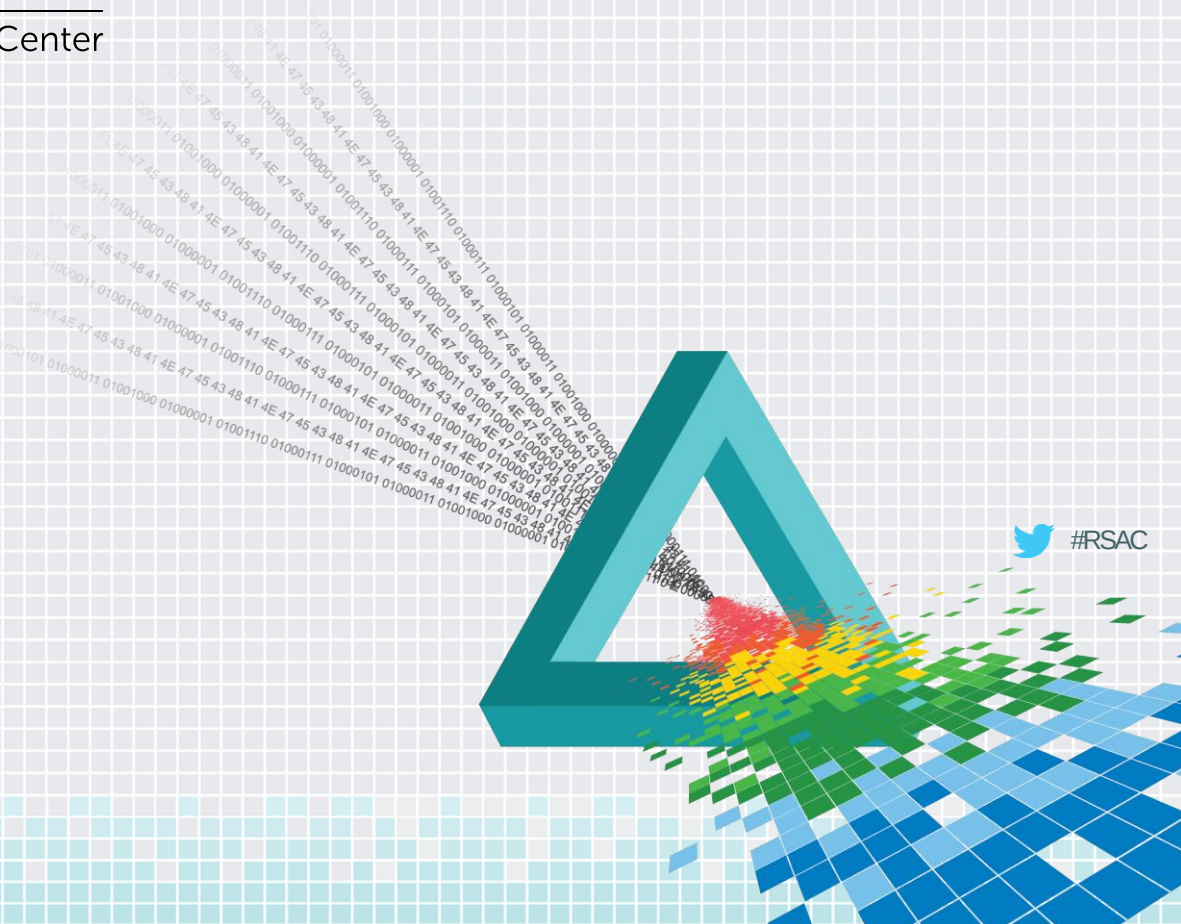
- Cheryl Smith (Former CIO)
- Dan Neal (My Boss)

My Family

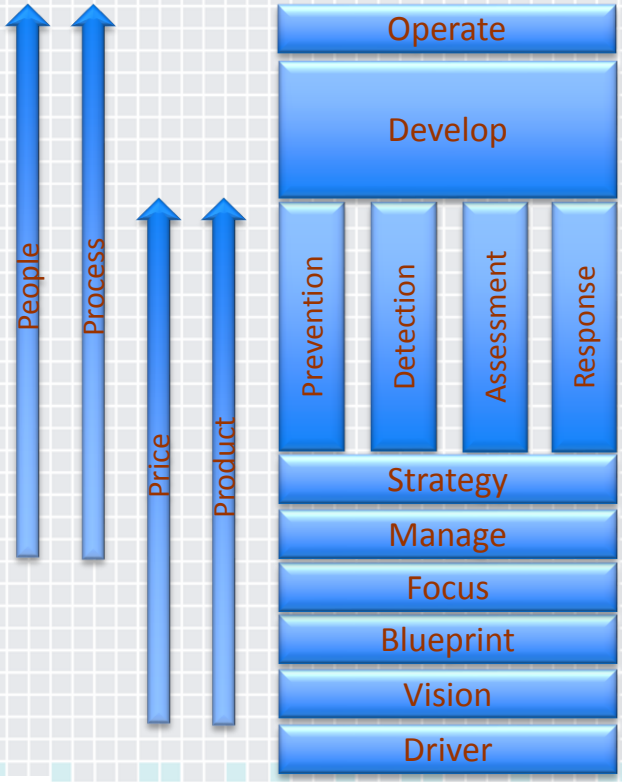
- Patrick, Brittney, Taz

Q & A

Bonus Slides



Service Development



Support (ITOC, Security Admin)

Technicians (Senior Analyst I, II)

Tech Leaders (Security Analyst III)

Manager

Director

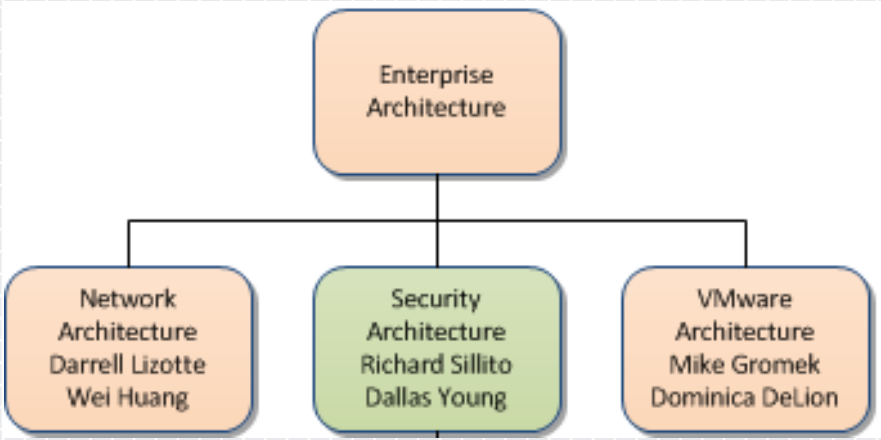
Architecture

Technology Council

Business

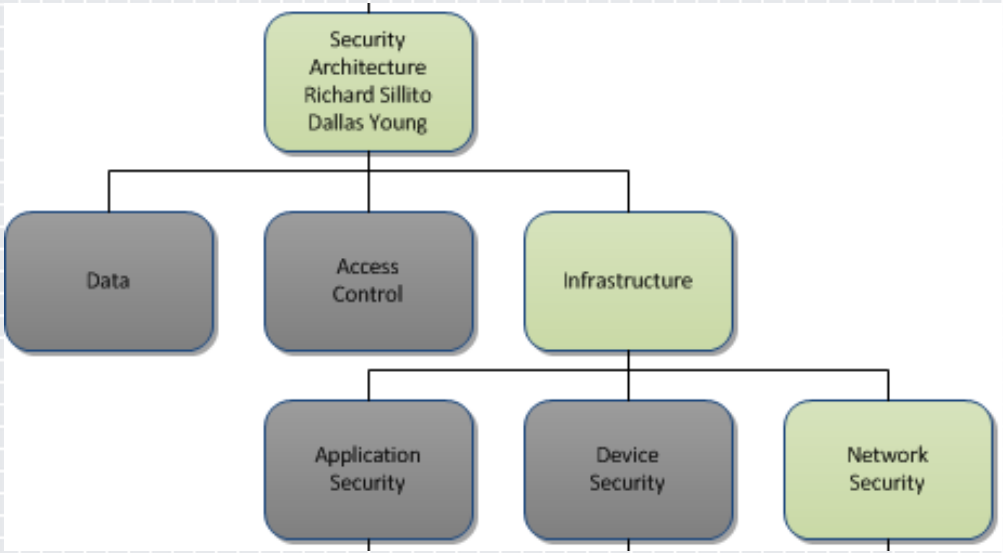
Define Future State

- Start at the top and get aligned!



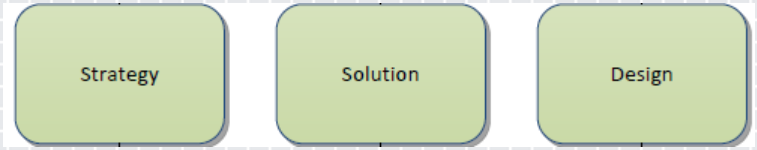
Define Future State

Break your world down into smaller pieces



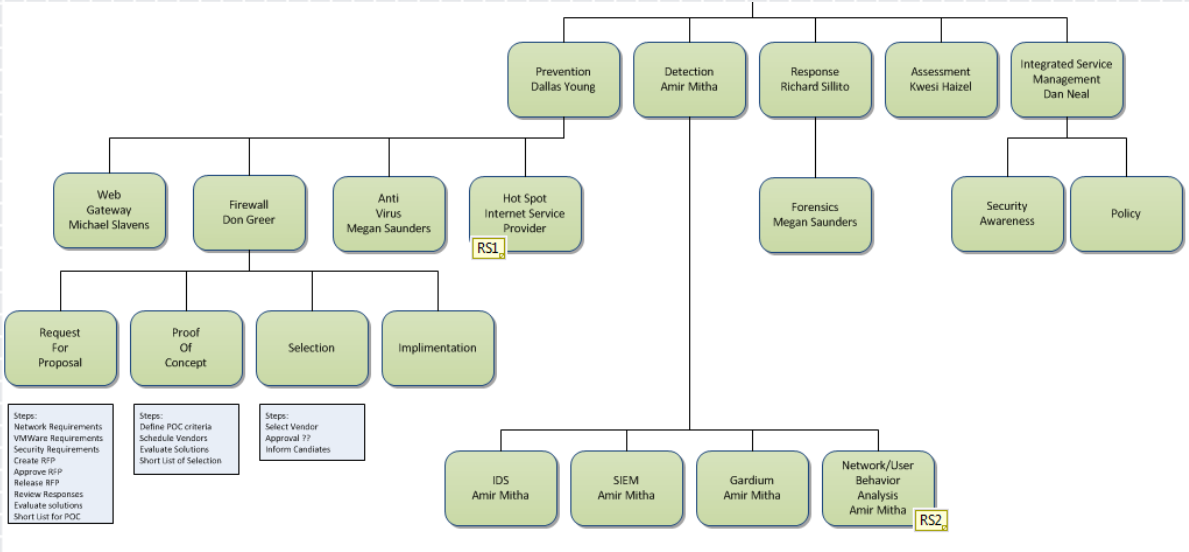
Define Future State

Have an approach!



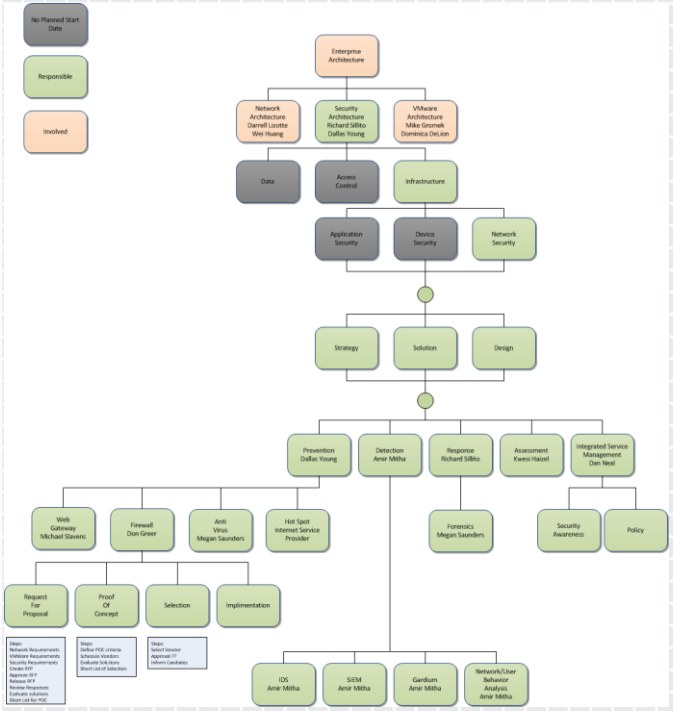
Define Future State

Figure out how you're going to get the work done

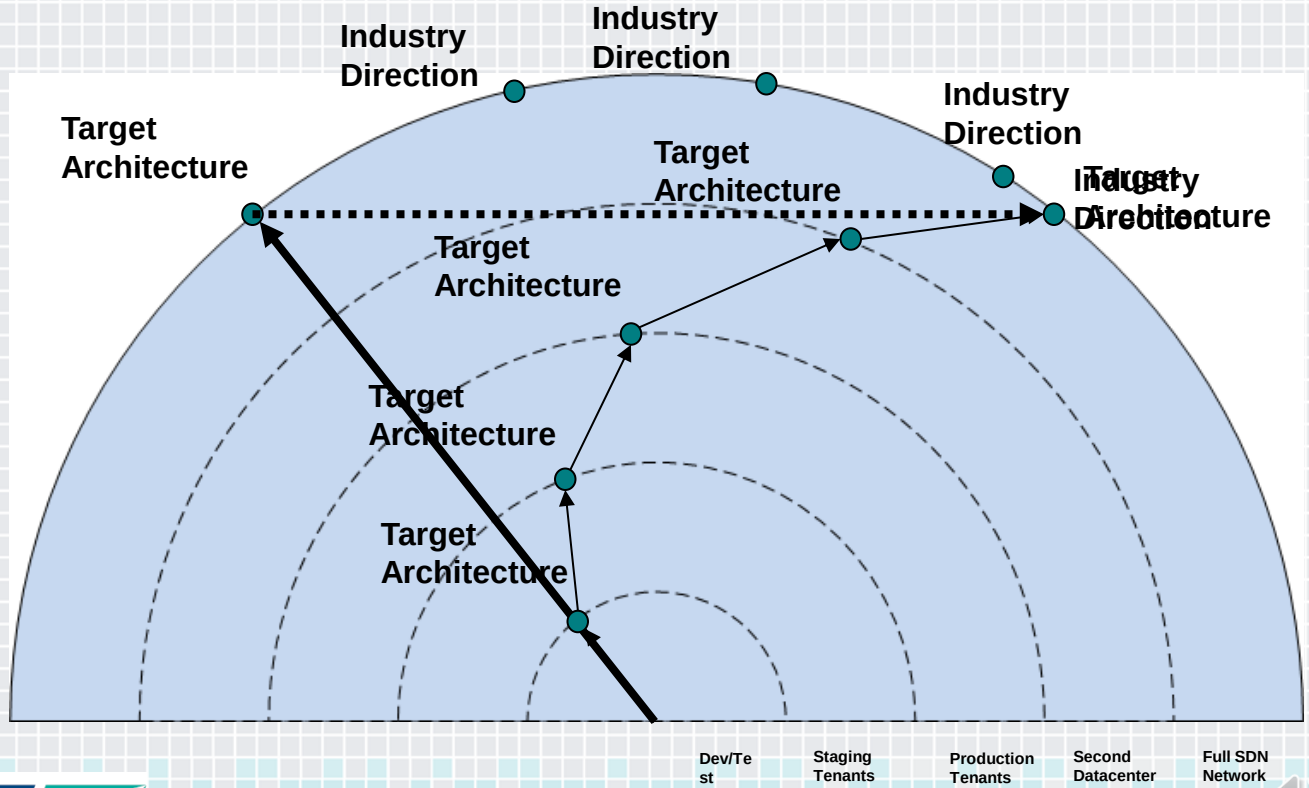


Define Future State

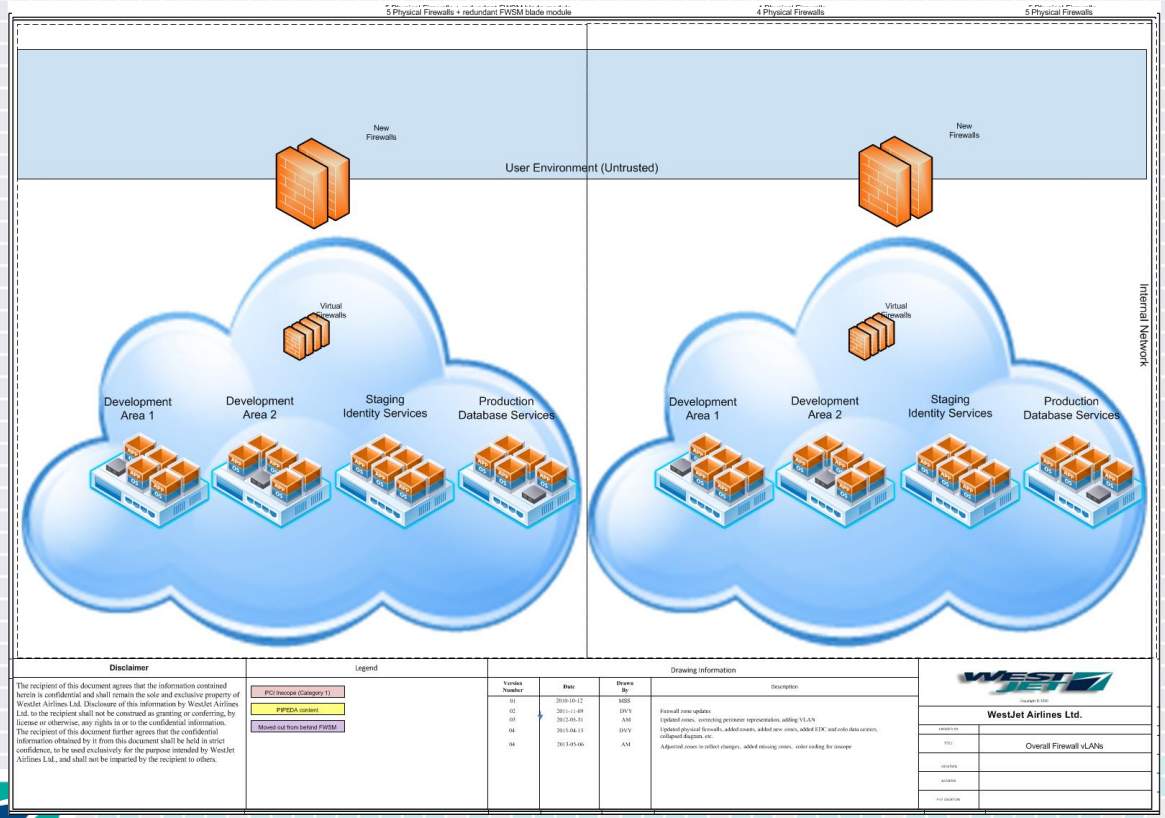
Now put it all together



Dealing with an evolving technology
Software Defined Datacenter



The Evolution



Software Defined Datacenter (De-mystifying the cloud)