FORESCOUT®

FORESCOUT - ZERO TRUST PLATFORM

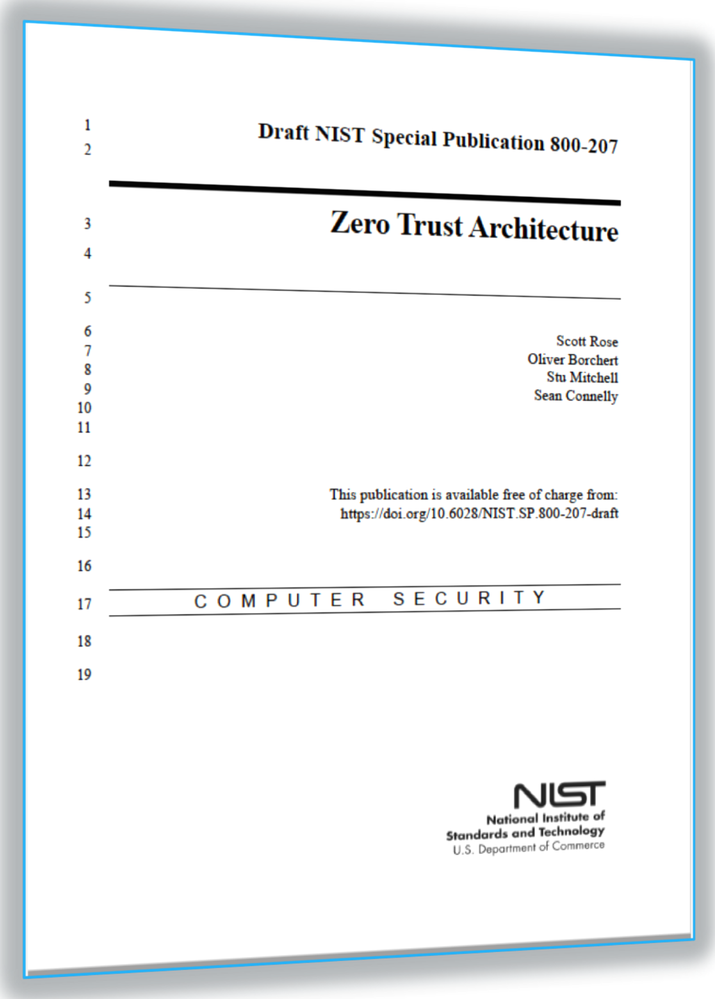
Tim Jones

Senior Director of Systems Engineering – Public Sector

Forescout Technologies, Inc.

November 14th 2019

Quick Forescout View of NIST Zero Trust Tenets…



Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

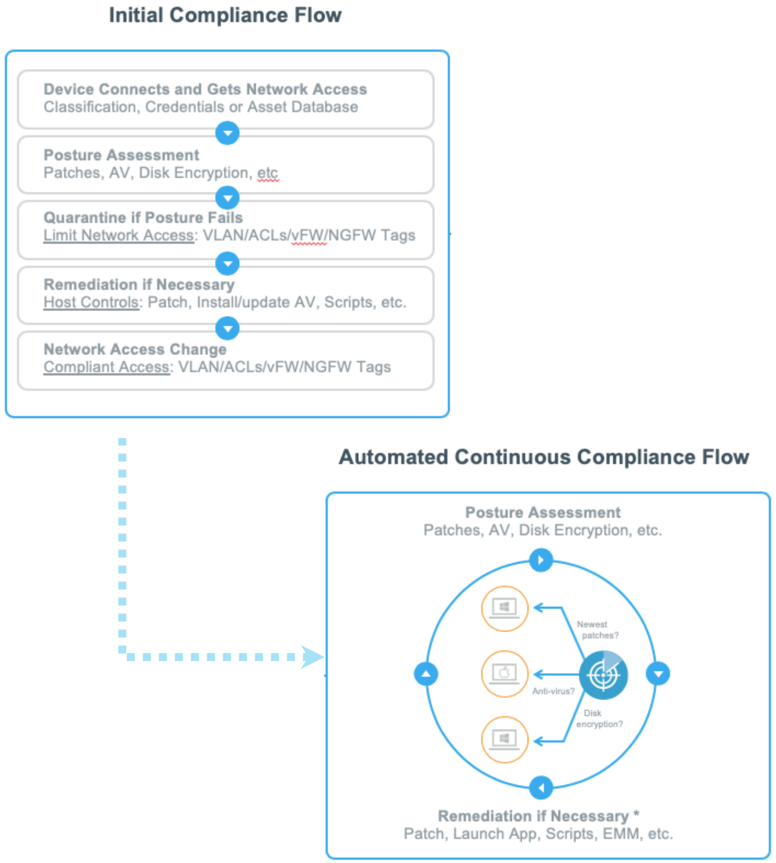
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Within SP 800-207 a *Zero Trust Architecture* is designed and deployed adhering to the following basic tenets:

1. All data sources and computing services are considered resources – *"composed of several different classes of devices."*
2. All communication is secure regardless of network location –*"there should not be any trust automatically granted based on the device being on enterprise network infrastructure."*
3. Access to individual enterprise resources is granted on a per-connection basis – *"Trust in the requester is evaluated before the access is granted."*
4. Access to resources is determined by policy, including the observable state of user identity and the requesting system, and may include other behavioral attributes. – *"Requesting system state includes device characteristics such as software versions installed, network location, previously observed behavior, installed credentials, etc."*

Continued … Forescout Maps to NIST Zero Trust Tenets

** Moving from point-in-time compliance to continuous compliance assessment, as shown here is critical to the success of CDM to move from improving cyber hygiene to automated risk mitigation and ongoing monitoring of the system.*



Initial Compliance Flow

Device Connects and Gets Network Access
Classification, Credentials or Asset Database

Posture Assessment
Patches, AV, Disk Encryption, etc

Quarantine if Posture Fails
Limit Network Access: VLAN/ACLs/vFW/NGFW Tags

Remediation if Necessary
Host Controls: Patch, Install/update AV, Scripts, etc.

Network Access Change
Compliant Access: VLAN/ACLs/vFW/NGFW Tags

Automated Continuous Compliance Flow

Posture Assessment
Patches, AV, Disk Encryption, etc.

Remediation if Necessary *
Patch, Launch App, Scripts, EMM, etc.

Within **SP 800-207** a ***Zero Trust Architecture*** is designed and deployed adhering to the following basic tenets:

5. The enterprise ensures all owned and associated systems are in the **most secure state possible and monitors systems to ensure that they remain in the most secure state possible** –*"An enterprise implementing a ZTA strategy should establish a* ***Continuing Diagnostics and Mitigation (CDM)*** *program to monitor the state of systems and apply patches/fixes as needed. Systems that are discovered to be subverted, vulnerable, and/or non-enterprise-owned may be treated differently (including denial of all connections to enterprise resources) than systems owned by or associated with the enterprise that are deemed to be in their most secure state."*
6. User authentication is dynamic and strictly enforced before access is allowed – *"This is a constant cycle of access, scanning and assessing threats, adapting, and continuously authenticating."* Think **DoD C2C**

DoD's Zero Trust Initiative

DoD C2C Framework is the First Step to ZTN

Background and Overview:

- **USCYBERCOM Initiative**: Commander's top priority, created cross-functional analysis team led by 1-Star
- "**DreamPort**" facility was hub for capability analysis … transitioned directly into operations in Pentagon enclave
- **Forescout** is foundational capability for all six categories of **USCYBERCOM defined endpoint devices**

Phases of C2C Operations

- Phase 1: Discover and **Classify**
- Phase 2: **Authenticate** and **Authorize**
- Phase 3: Pre-Connect **Compliance**
- Phase 4: Post-Connect **Compliance**

DoD Zero Trust Decision Points

- D0: Is Device **Known**?
- D1: **Authentication** … a **Managed** Device?
- D2: **Authorization** … is device **Healthy**?
- D3: User **Authentication**?
- D4: User **Authorization**?
- D5: Take Control of **Authorized Users/Devices** in various Zero Trust Enterprise Use Cases

- D6: ….
- D7: ….
- D8: ….
- D9: ….

User/Device Controlled through **Orchestration** of cybersecurity tools

Comply-to-Connect Operations
and
Zero Trust Decision Points
based on
Identical Core Principles

DO NOT DISTRIBUTE

Forescout Network Segmentation Solution Mapping…

eyeSight

What’s on my network?

Discover/classify/asses

—

Grouping device/app/user by business context

—

Hierarchy of device groups by business logic

eyeSegment

How does it communicate?

Mapping port/protocol/destination to the device groups

How do controls impact my environment?

Ability to test/monitor/simulate controls

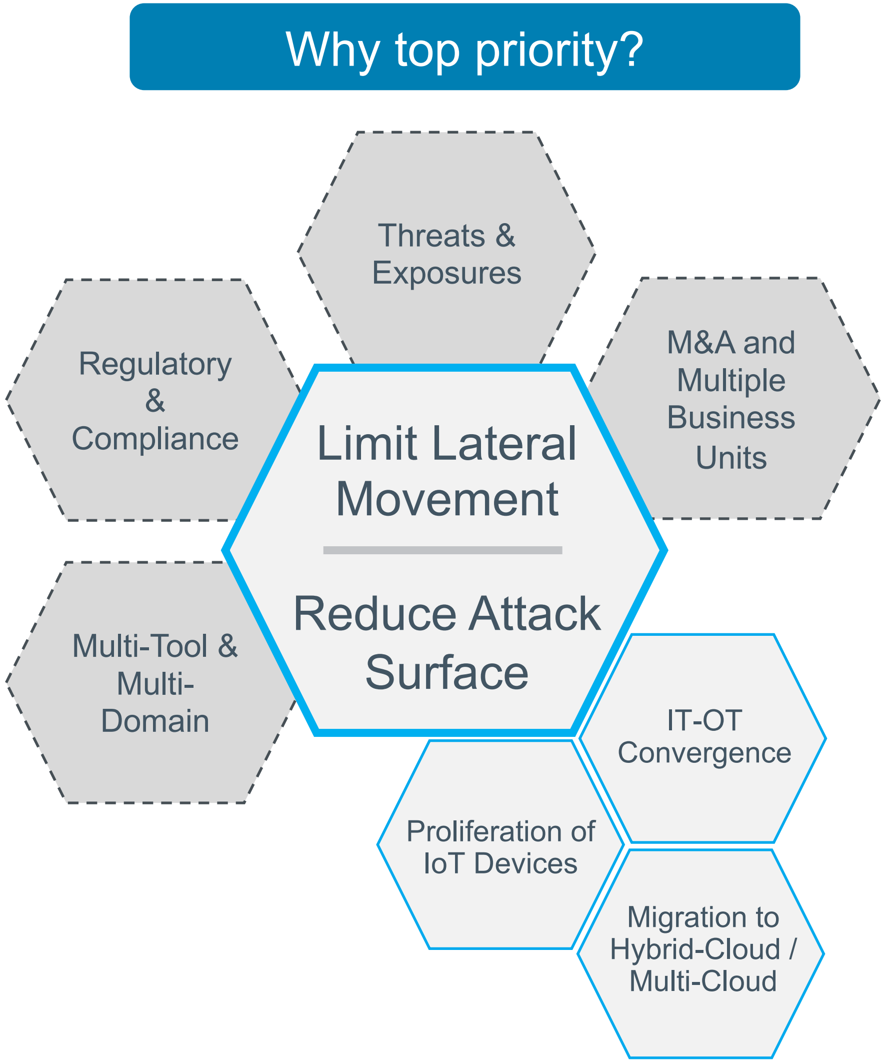
eyeControl eyeExtend

How do I orchestrate controls across different control technologies?

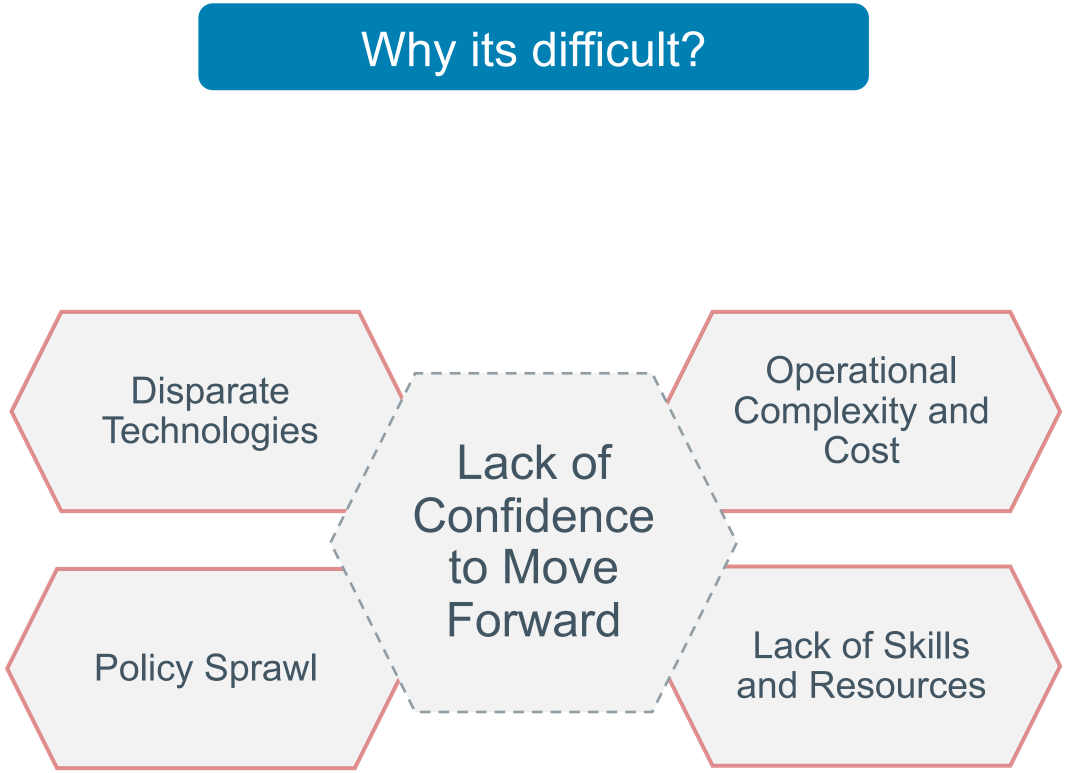
eyeControl/eyeExtend

Network Segmentation Is Becoming Harder!

Digital Transformation and Rising Challenges

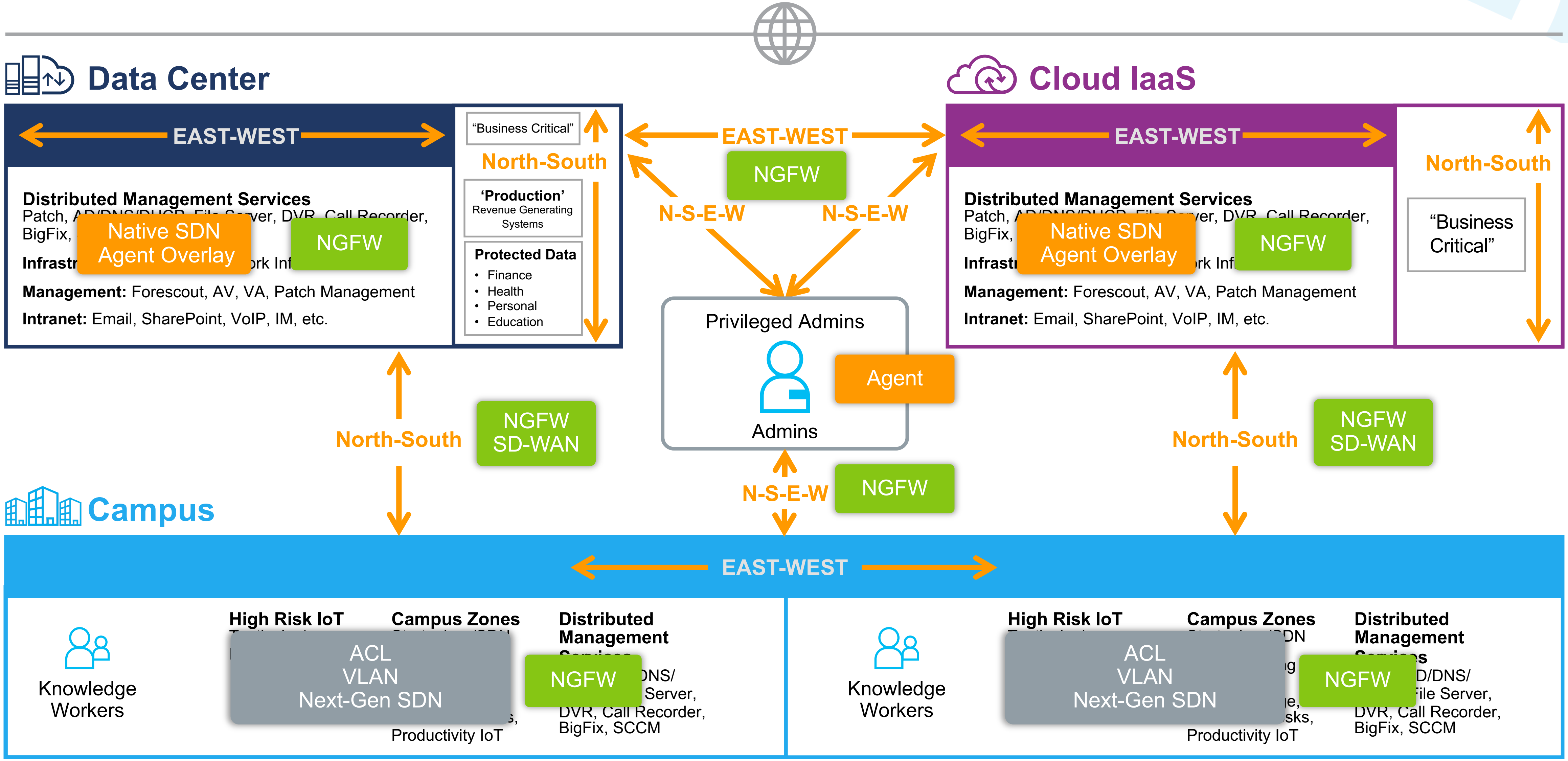

Why top priority?
Threats & Exposures
Regulatory & Compliance
M&A and Multiple Business Units
Limit Lateral Movement
Reduce Attack Surface
Multi-Tool & Multi-Domain
IT-OT Convergence
Proliferation of IoT Devices
Migration to Hybrid-Cloud / Multi-Cloud

&


Why its difficult?
Disparate Technologies
Operational Complexity and Cost
Lack of Confidence to Move Forward
Policy Sprawl
Lack of Skills and Resources

DO NOT DISTRIBUTE

Siloed Controls Across Multiple Domains



Data Center

EAST-WEST

Distributed Management Services
Patch, AD/DNS/DHCP, File Server, DVR, Call Recorder,
BigFix,

Infrastr ork Inf

Native SDN Agent Overlay

NGFW

Management: Forescout, AV, VA, Patch Management

Intranet: Email, SharePoint, VoIP, IM, etc.

"Business Critical"

North-South

'Production'
Revenue Generating Systems

Protected Data
- Finance
- Health
- Personal
- Education

EAST-WEST

NGFW

N-S-E-W

N-S-E-W

Privileged Admins

Admins

Agent

N-S-E-W

NGFW

Cloud IaaS

EAST-WEST

Distributed Management Services
Patch, AD/DNS/DHCP, File Server, DVR, Call Recorder,
BigFix,

Infrastr ork Inf

Native SDN Agent Overlay

NGFW

Management: Forescout, AV, VA, Patch Management

Intranet: Email, SharePoint, VoIP, IM, etc.

North-South

"Business Critical"

North-South

NGFW SD-WAN

North-South

NGFW SD-WAN

Campus

EAST-WEST

Knowledge Workers

High Risk IoT

Campus Zones

ACL
VLAN
Next-Gen SDN

Productivity IoT

Distributed Management Services
DNS/
Server,
DVR, Call Recorder,
BigFix, SCCM

NGFW

Knowledge Workers

High Risk IoT

Campus Zones
SDN

ACL
VLAN
Next-Gen SDN

Productivity IoT

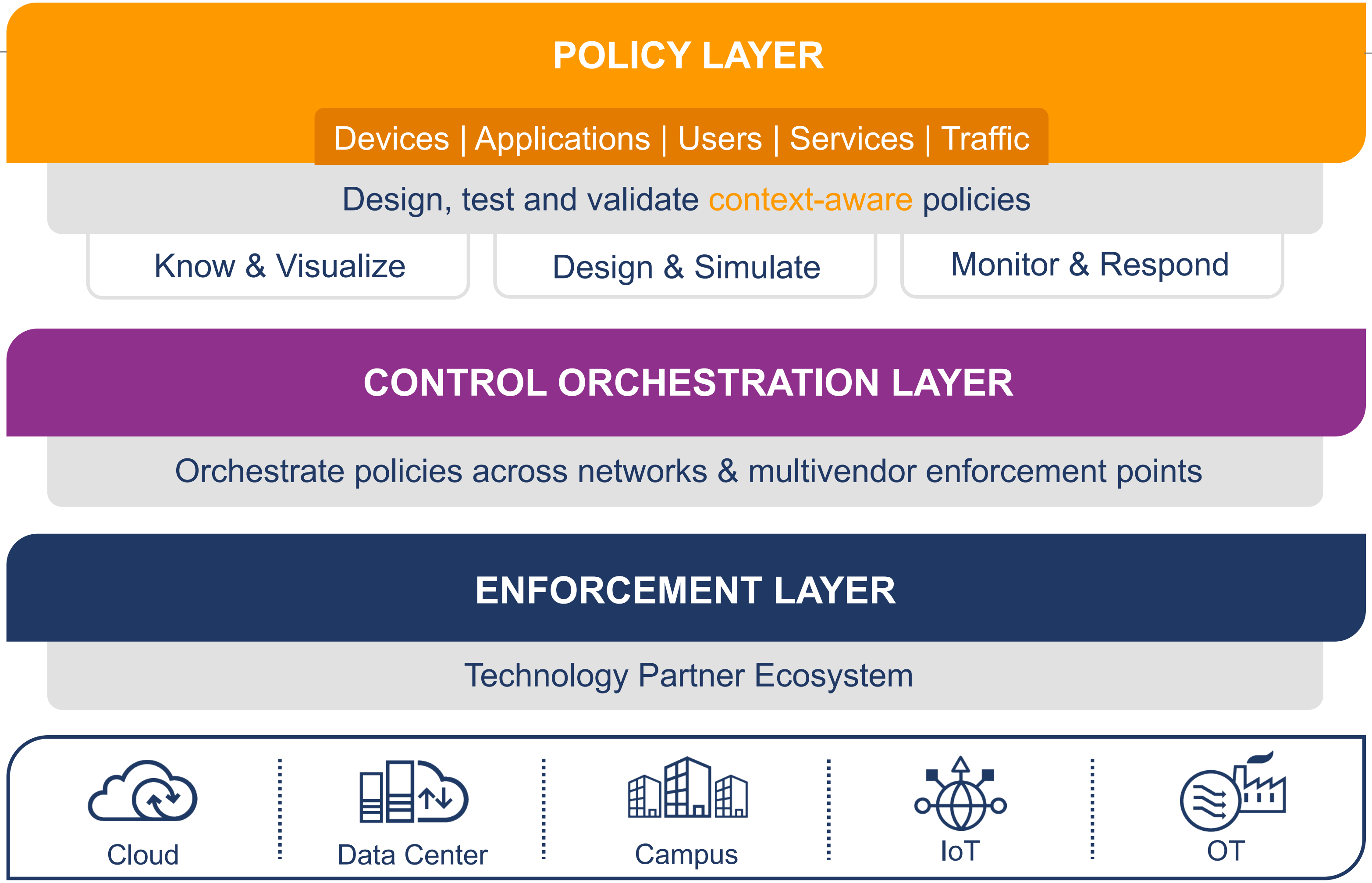
Distributed Management Services
D/DNS/
File Server,
DVR, Call Recorder,
BigFix, SCCM

NGFW

DO NOT DISTRIBUTE

Forescout Approach

- Unparalleled context into the entire connected network from campus to data center to cloud
- Leverage external tools and information to add context to connected devices
- Transforming connected inventory into a logical taxonomy of devices, applications, users and services.



POLICY LAYER

Devices | Applications | Users | Services | Traffic

Design, test and validate context-aware policies

Know & Visualize

Design & Simulate

Monitor & Respond

CONTROL ORCHESTRATION LAYER

Orchestrate policies across networks & multivendor enforcement points

ENFORCEMENT LAYER

Technology Partner Ecosystem

- Automatically map traffic flows to a logical taxonomy of users, applications, services and devices.

Understand and Visualize

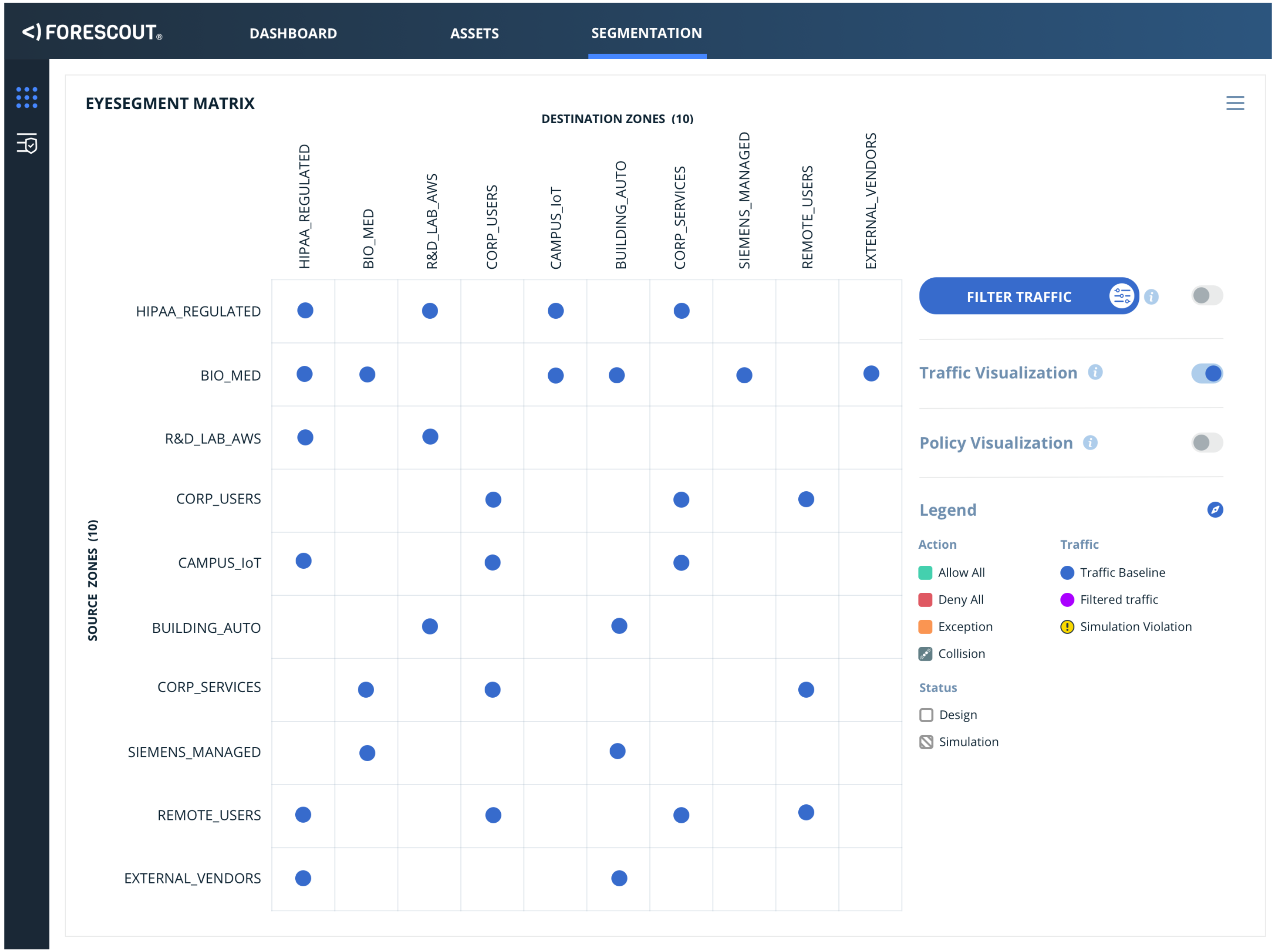
Logical Taxonomy of Users, Devices & Applications

IP	Clarification	Business Hierarchy
10.2.2.12	Badge Scanner	Building Automation Users & Devices
10.2.2.25	Ip Camera	
10.2.2.46	Badge Application Web Server	
10.2.2.5	Physical Security User	
10.0.5.46	R&D User	R&D Users & Workloads
10.0.5.5	R&D Application	

Translate IP Address into Context and Groups

- Non-managed device classified and grouped automatically
  - Building Automation
  - OT Systems
  - Business IoT
- Add context to managed devices
  - AD Group (Finance users)
  - CMDB Context (Payment application, criticality)
  - Compliance status
  - eyeExtend Partner Information
- All Devices
  - Location
  - Port/Protocol

Know and Visualize



EYESEGMENT MATRIX

DESTINATION ZONES (10)

SOURCE ZONES (10)

	HIPAA_REGULATED	BIO_MED	R&D_LAB_AWS	CORP_USERS	CAMPUS_IoT	BUILDING_AUTO	CORP_SERVICES	SIEMENS_MANAGED	REMOTE_USERS	EXTERNAL_VENDORS
HIPAA_REGULATED	●		●		●		●			
BIO_MED	●	●			●	●		●		●
R&D_LAB_AWS	●		●							
CORP_USERS				●			●		●	
CAMPUS_IoT	●			●			●			
BUILDING_AUTO			●			●				
CORP_SERVICES		●		●					●	
SIEMENS_MANAGED		●				●				
REMOTE_USERS	●			●			●		●	
EXTERNAL_VENDORS	●					●				

FILTER TRAFFIC

Traffic Visualization ● on

Policy Visualization ○ off

Legend

Action	Traffic
🟩 Allow All	● Traffic Baseline
🟥 Deny All	● Filtered traffic
🟧 Exception	⚠ Simulation Violation
▨ Collision	

Status

□ Design

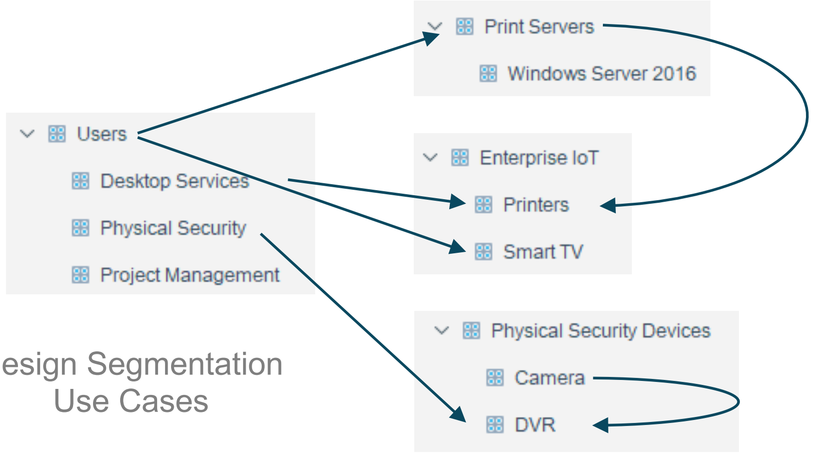
▨ Simulation

Visualize Baseline Traffic Flows

Automatically map traffic flows to a logical taxonomy of users, applications, services and devices across the entire enterprise network without deploying agents.

Design and Simulate

Simulate Policies to Test Impact



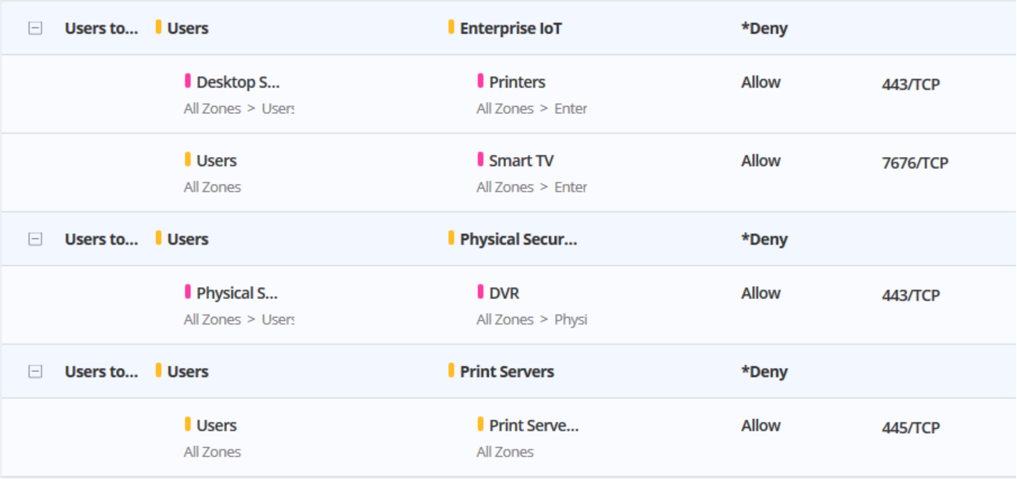
Users
- Desktop Services
- Physical Security
- Project Management

Print Servers
- Windows Server 2016

Enterprise IoT
- Printers
- Smart TV

Physical Security Devices
- Camera
- DVR

Design Segmentation Use Cases



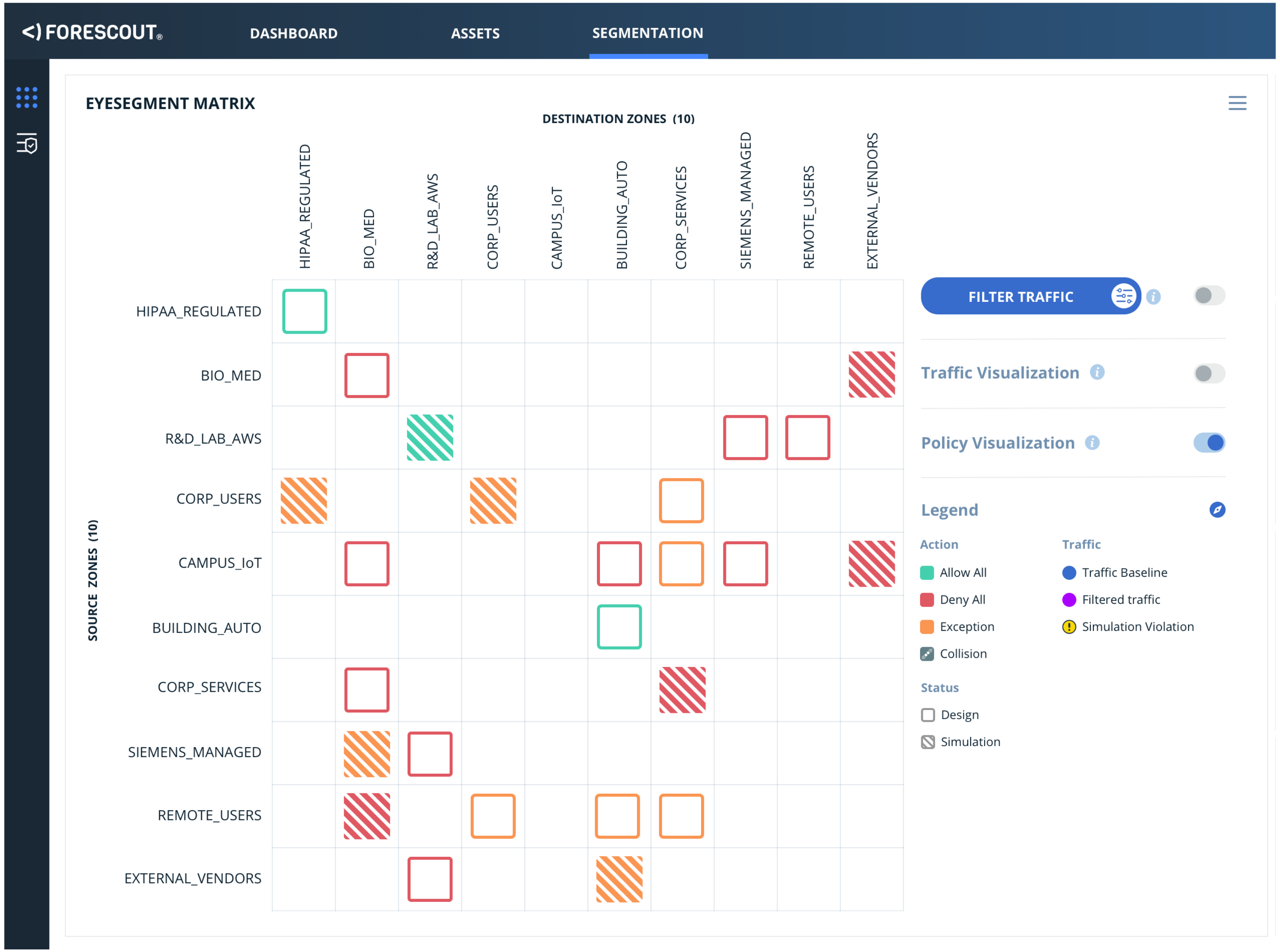
⊟	Users to...	Users	Enterprise IoT	*Deny	
		Desktop S... All Zones > User:	Printers All Zones > Enter	Allow	443/TCP
		Users All Zones	Smart TV All Zones > Enter	Allow	7676/TCP
⊟	Users to...	Users	Physical Secur...	*Deny	
		Physical S... All Zones > User:	DVR All Zones > Physi	Allow	443/TCP
⊟	Users to...	Users	Print Servers	*Deny	
		Users All Zones	Print Serve... All Zones	Allow	445/TCP

Simulate Segmentation Controls

Test Segmentation Impact Before Implementation

- Design, create and fine-tune effective segmentation policies based on a logical business taxonomy
- Proactively simulate policies before putting them into effect across your environment
- Determine how specific policies would impact the rest of the network from a single policy layer in order to minimize business disruption.

Monitor and Respond



EYESEGMENT MATRIX

DESTINATION ZONES (10)

SOURCE ZONES (10)	HIPAA_REGULATED	BIO_MED	R&D_LAB_AWS	CORP_USERS	CAMPUS_IoT	BUILDING_AUTO	CORP_SERVICES	SIEMENS_MANAGED	REMOTE_USERS	EXTERNAL_VENDORS
HIPAA_REGULATED	🟩									
BIO_MED		🟥								▨🟥
R&D_LAB_AWS			▨🟩					🟥	🟥	
CORP_USERS	▨🟧			▨🟧			🟧			
CAMPUS_IoT		🟥				🟥	🟧	🟥		▨🟥
BUILDING_AUTO						🟩				
CORP_SERVICES		🟥					▨🟥			
SIEMENS_MANAGED		▨🟧	🟥							
REMOTE_USERS		▨🟥		🟧		🟧	🟧			
EXTERNAL_VENDORS			🟥			▨🟧				

FILTER TRAFFIC

Traffic Visualization

Policy Visualization

Legend

Action
- 🟩 Allow All
- 🟥 Deny All
- 🟧 Exception
- ▨ Collision

Traffic
- ● Traffic Baseline
- ● Filtered traffic
- ⚠ Simulation Violation

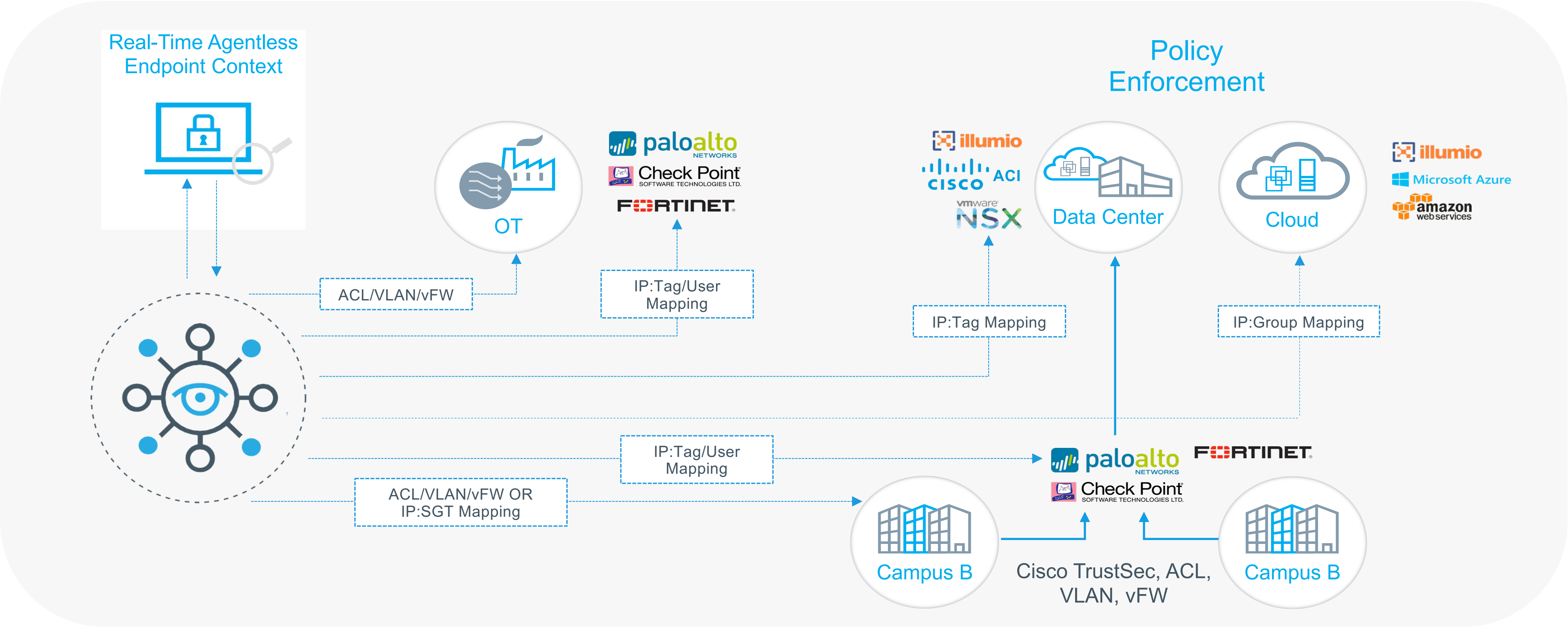
Status
- □ Design
- ▨ Simulation

Real-Time Policy Visualizations

- Monitor and respond to segmentation policies abstracted from the underlying controls
- Continuously monitor enterprise infrastructure controls and assure that segmentation controls are implemented across extended enterprise
- Ability to filter down to specific source/destination, port, protocol

Segmentation Orchestration and Automation from a Single Policy

Dynamically Extend Segmentation to Any Device on Any Network



Thank You…

Tim Jones | tim.jones@forescout.com | (703) 338-2028