CISCO The bridge to possible

SD-Access Success Stories

Concept to Reality by Stanford Health and Yale University

Kanu Gupta, Product Manager
Tim Sheets, Director, Network Services, YALE University
Maitrik Gandhi, Network Engineer. STANFORD Healthcare

BRKENS-1801

Cisco Webex App

Questions?

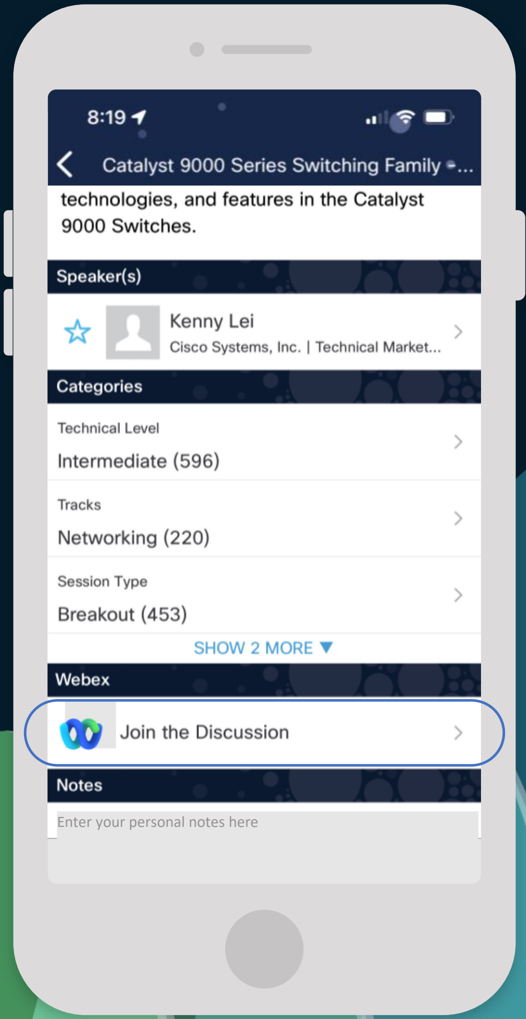
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click "Join the Discussion"
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKENS-1801



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

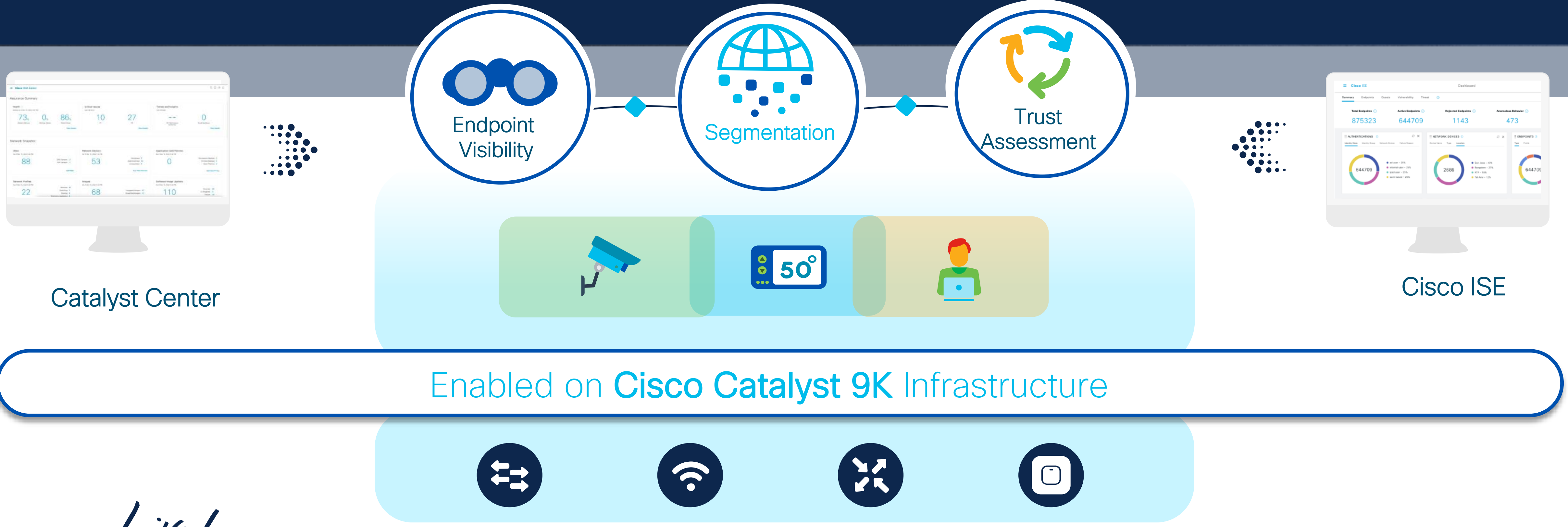
Notes

Enter your personal notes here

Agenda

- Software-Defined Access: Driving Adoption and Delivering Business Outcomes
- SD-Access in Action: YALE University Success Story
- Impact of Software Defined Access: STANFORD Healthcare

Zero-Trust Security for Network and Cloud



Endpoint Visibility

Segmentation

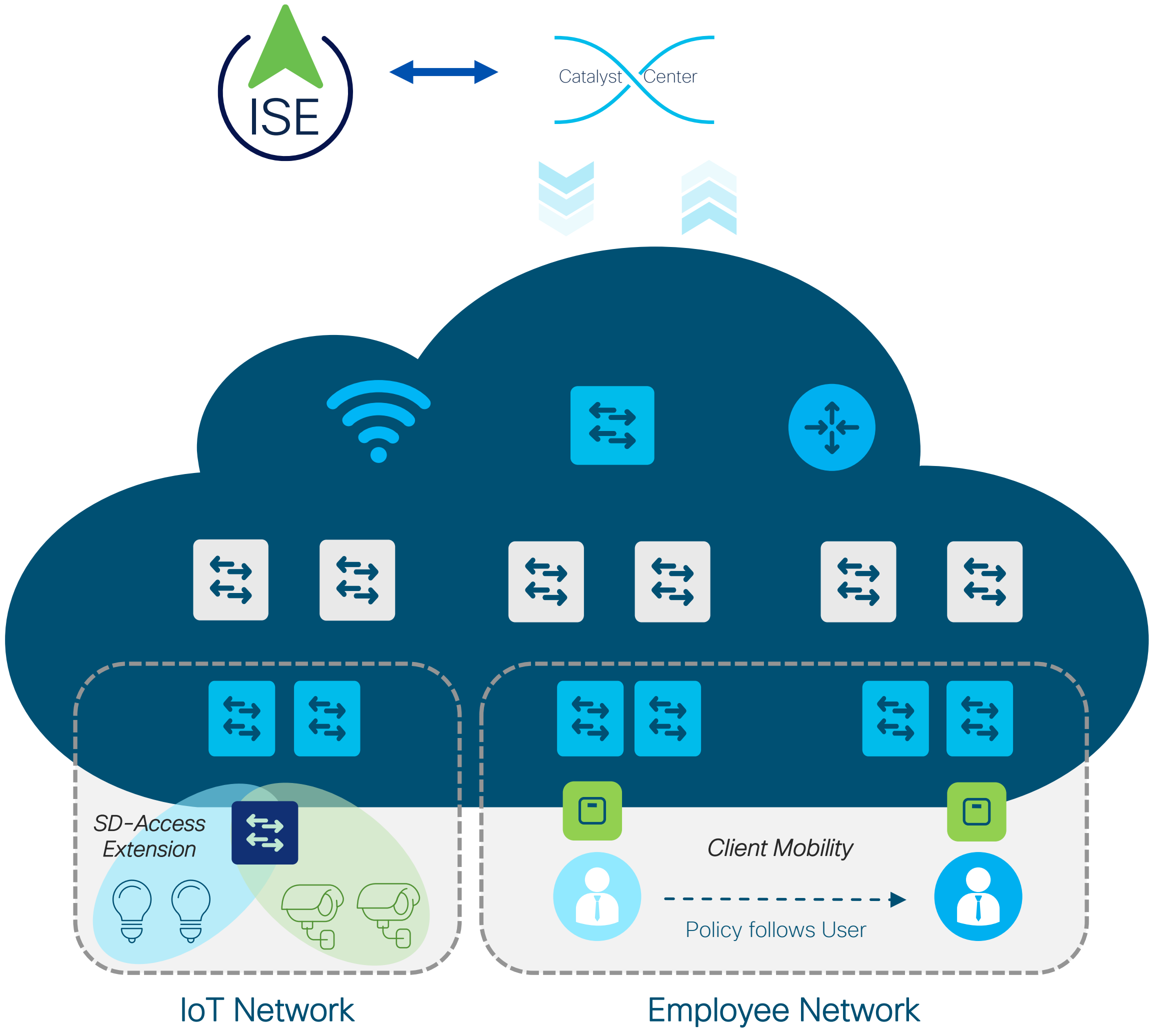
Trust Assessment

Catalyst Center

Cisco ISE

Enabled on **Cisco Catalyst 9K** Infrastructure

Secure The Access with **Software-Defined Access**



Fabric Architecture enabling
Powerful Outcomes

Identity-based **Segmentation**

Wired/Wireless **Convergence**

IT & OT **Integration**

Enterprise Grade for Every Sector

SD-Access LISP **Industry Leading Campus Architecture**

Deployments

4050+

Momentum

40%

YoY growth in customers

Key use case

70%

Wireless

+ 66%

API (YoY)

Usage

24K+

Sites

1.8M+

Devices

Miercom PERFORMANCE VERIFIED

Top verticals: Government, Finance, Professional services, and Manufacturing

Adopted by 31% of U.S. **Fortune 100** Companies

EMEA: 52%

Americas 29%

APJC 19%

SD-Access LISP Customer Success

	Healthcare		Education + Energy		Manufacturing	
	UCLA Health	Stanford HEALTH CARE	Yale	BR PETROBRAS	Ford	TOYOTA
SCALE	5300 devices 15K+endpoints	6200 devices 10K+endpoints	6500 devices 66K+endpoints	5300 devices 57K+endpoints	4500 devices 10K+endpoints	16k devices 98K+endpoints
REQUIREMENTS	Zer-Trust Access HIPAA Compliance		API Tooling Resilient Network & Security Visibility		EV Manufacturing Reliable Wall to Wall WIFI Connectivity	

Segmentation at Scale | Unified Wired/Wireless Policy | IT/OT Integration Experience

Speaking at this Cisco Live BRKENS 1801, BRKENS 1802, CIUG-1003

Fasten Your Seatbelts: Take-Off Observations from Yale University’s Next Generation Network Program

SHAWN CLARK, NGN PROGRAM DIRECTOR

DAN MASSAMENO, IT ARCHITECT

TIM SHEETS, DIRECTOR, NETWORK SERVICES

Yale Information Technology

June 2024

Agenda

- Overview
- Case for Change
- Stakeholders
- Deliverables
- Vision
- Transition
- Takeaways

Yale University’s

Next Generation Network

The Next Generation Network project will help **advance** Yale’s teaching, health, and research service missions, and **safeguard** campus community information. NGN will provide a more **modern**, **resilient**, and **secure** Yale Network environment.

Next Generation Network: The Case for Change

Yale

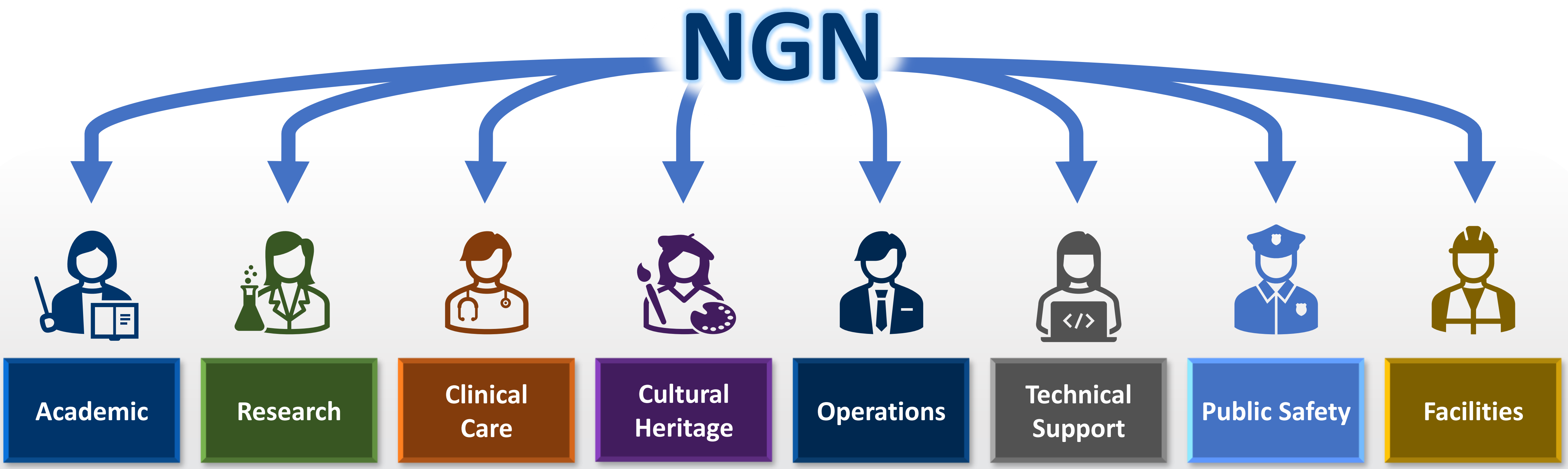
Increasing forces (both internal and external) necessitated the need for change:

- Global University Presence
- Device Diversity (IOT, BYO), Security Complexities & Converged Networking
- High-Speed Research Networks (100G+) & Institutional Collaboration
- Rising Technical Debt at Institutions That Deprioritized Network Upkeep
- Data Moving to Cloud
- Desire for Seamless WiFi

Decreasing instances of network issues across the University became critical:

- Frequent Network Disruptions
- Slow Data Transfer Speeds
- Increased Security Breach Risks
- SSO Limitations & Sign-In Challenges

Next Generation Network: Solving for Stakeholder Needs



NGN

Academic

Learning management systems, library resources online, and more are dependent on the network to execute our education mission

Research

The network is foundational to accessing research clusters and instrumentation as well as working across peer institutions

Clinical Care

The information doctors use in patient interaction is almost entirely system-based, accessed through the network

Cultural Heritage

Making Yale's collections accessible to patrons and scholars worldwide is dependent on a robust network

Operations

Connecting staff and supporting data across the network is vital to our University business operations

Technical Support

Keeping Yale's network and data secure while allowing for research and academic flexibility on campus and remotely

Public Safety

Monitoring people and buildings for a large, city university requires a reliable and robust network

Facilities

Allowing network connections for buildings and grounds operations across our campuses

Next Generation Network: Key Deliverables

REMEDIATING
1,136 Data Closets

CONSOLIDATING
5 Networks into 1

REPLACING
12,000 Network Devices

DEVELOPING
Role-based Access

AUTOMATING
Cybersecurity Response

1

FOUNDATIONAL

- Comprehensive **update of network equipment** to modern standards
- **Converge separate networks** and increase capacity
- Establish appropriate **redundar network pathways**
- **Remediation** in building network closets
- Increased **security visibility** and network authentication
- Privileged **Account Management**

2

MEDICAL STABILIZATION

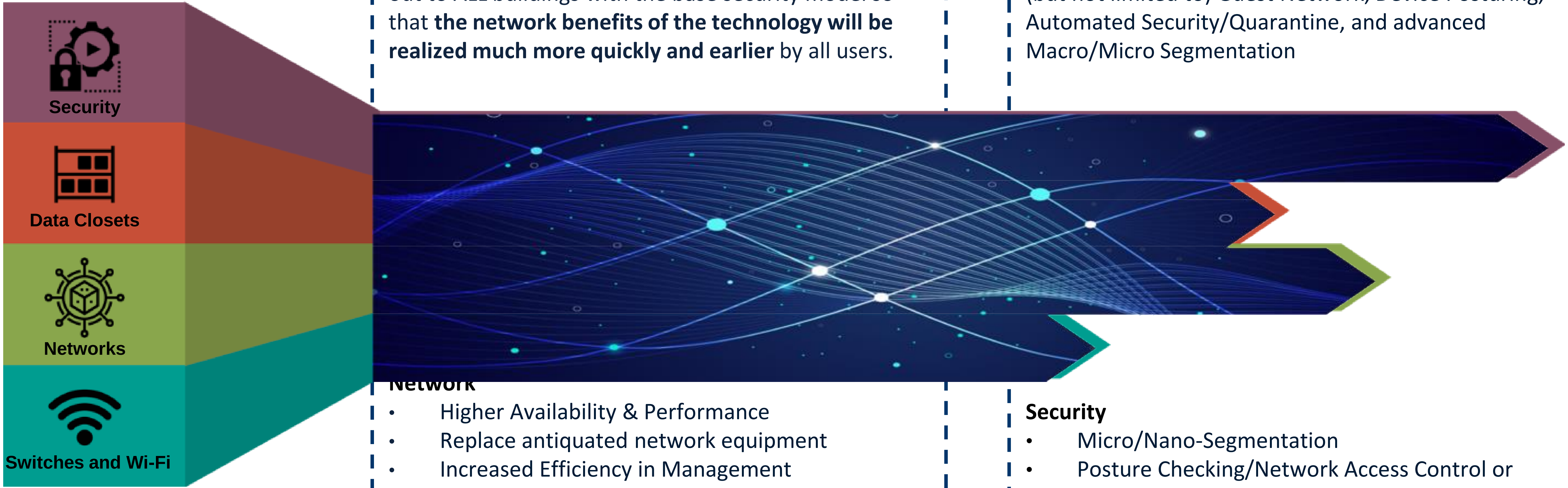
- **Stabilize** Health Campus Network
- Partner with **Clinical Phone Refresh** project

3

ADVANCED SECURITY

- **Enhanced protection** for high-risk assets with balanced security for university opennes
- Establish **cybersecurity detection** and response capabilities

Next Generation Network: Release Approach in Support of Key Deliverables



Foundational Release

Software Defined Access (SDA) hardware will be rolled-out to ALL buildings with the base security model so that **the network benefits of the technology will be realized much more quickly and earlier** by all users.

Network

- Higher Availability & Performance
- Replace antiquated network equipment
- Increased Efficiency in Management

Security

- Increased Network Security Visibility
- Auto-alerting on malicious network attacks
- Authentication

Advanced Security Release(s)

Implement **more advanced security features** including (but not limited to) Guest Network, Device Posturing, Automated Security/Quarantine, and advanced Macro/Micro Segmentation

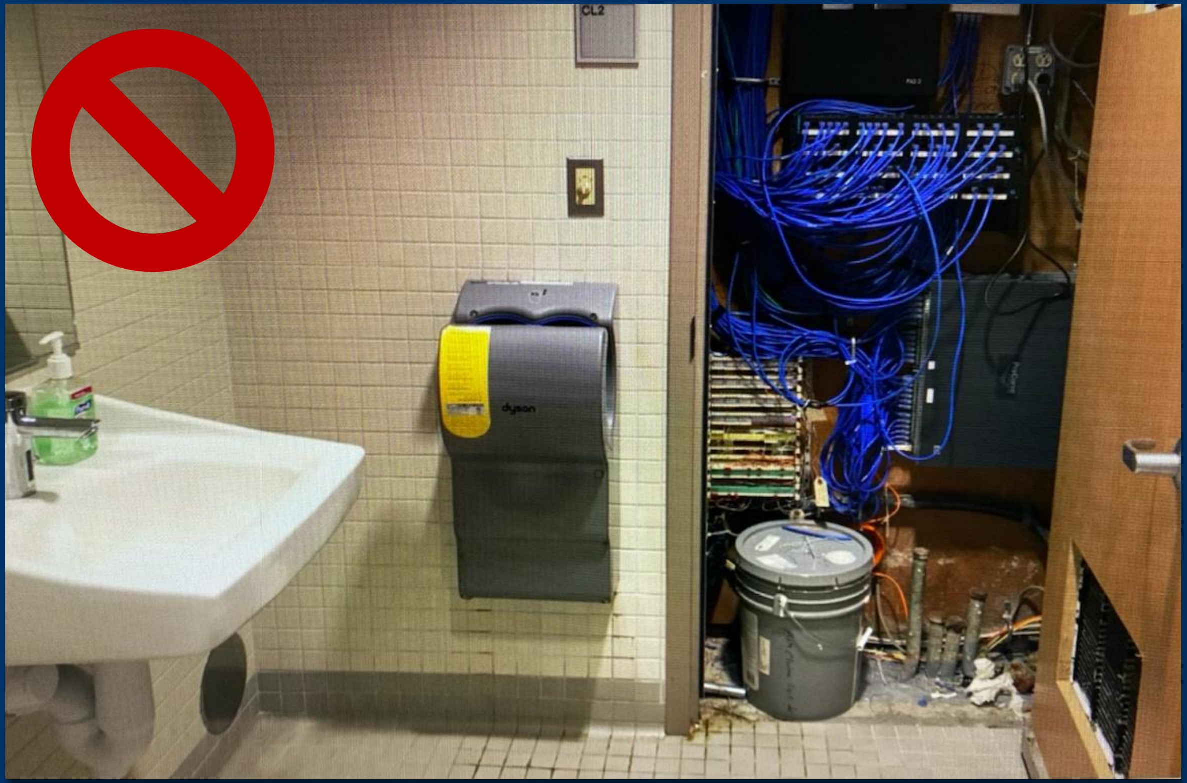
Security

- Micro/Nano-Segmentation
- Posture Checking/Network Access Control or Change of Authorization
- Role Based Access Control
- Location Based Access Control
- Yale-YNHHS Network Integration

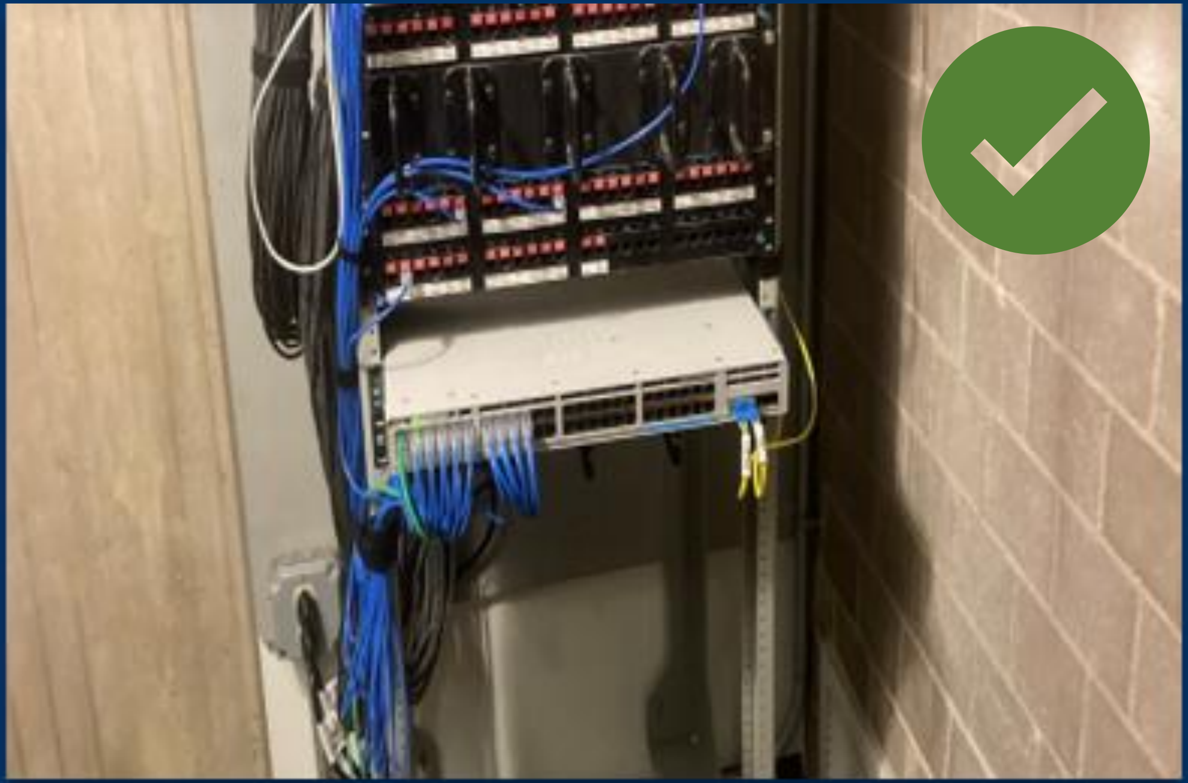
Next Generation Network: The Value of Closet Remediation

Yale

BEFORE NGN

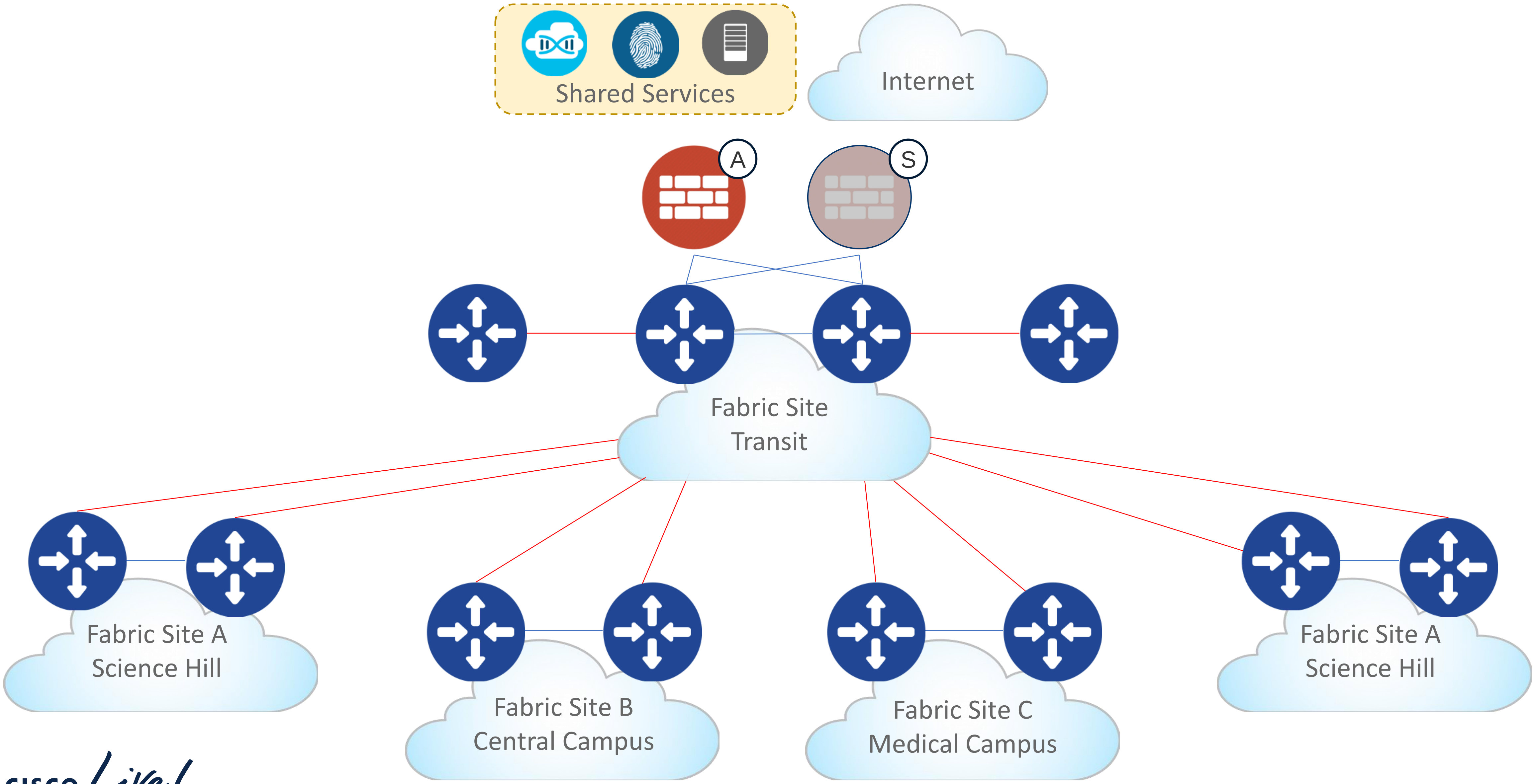


AFTER NGN



Next Generation Network: Yale Architecture Expansion (Bird's Eye View)

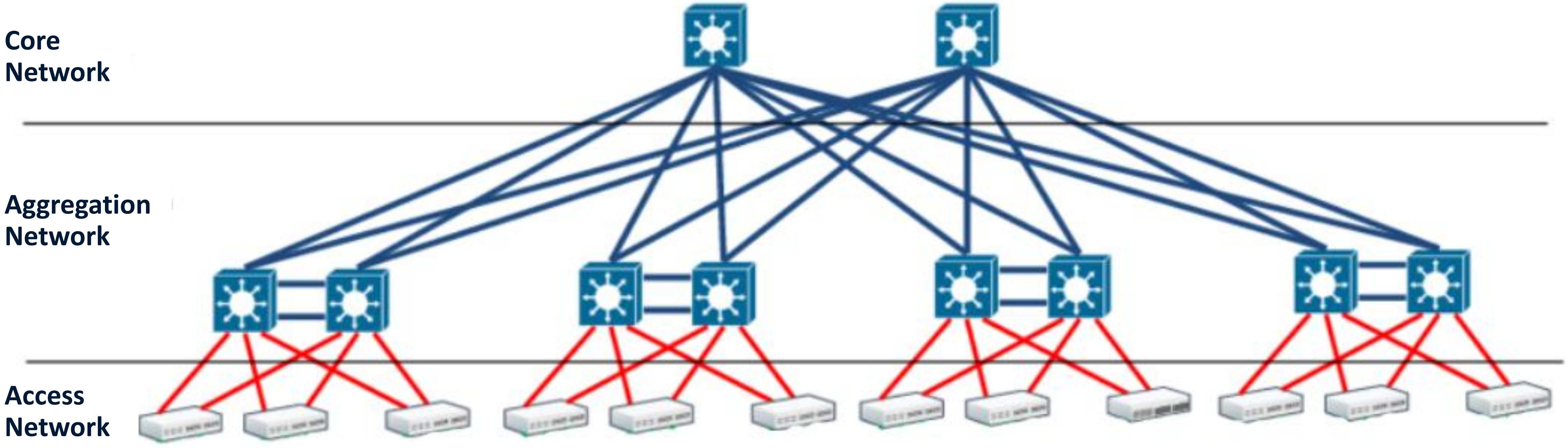
Yale



Next Generation Network: Layer 1 Vision

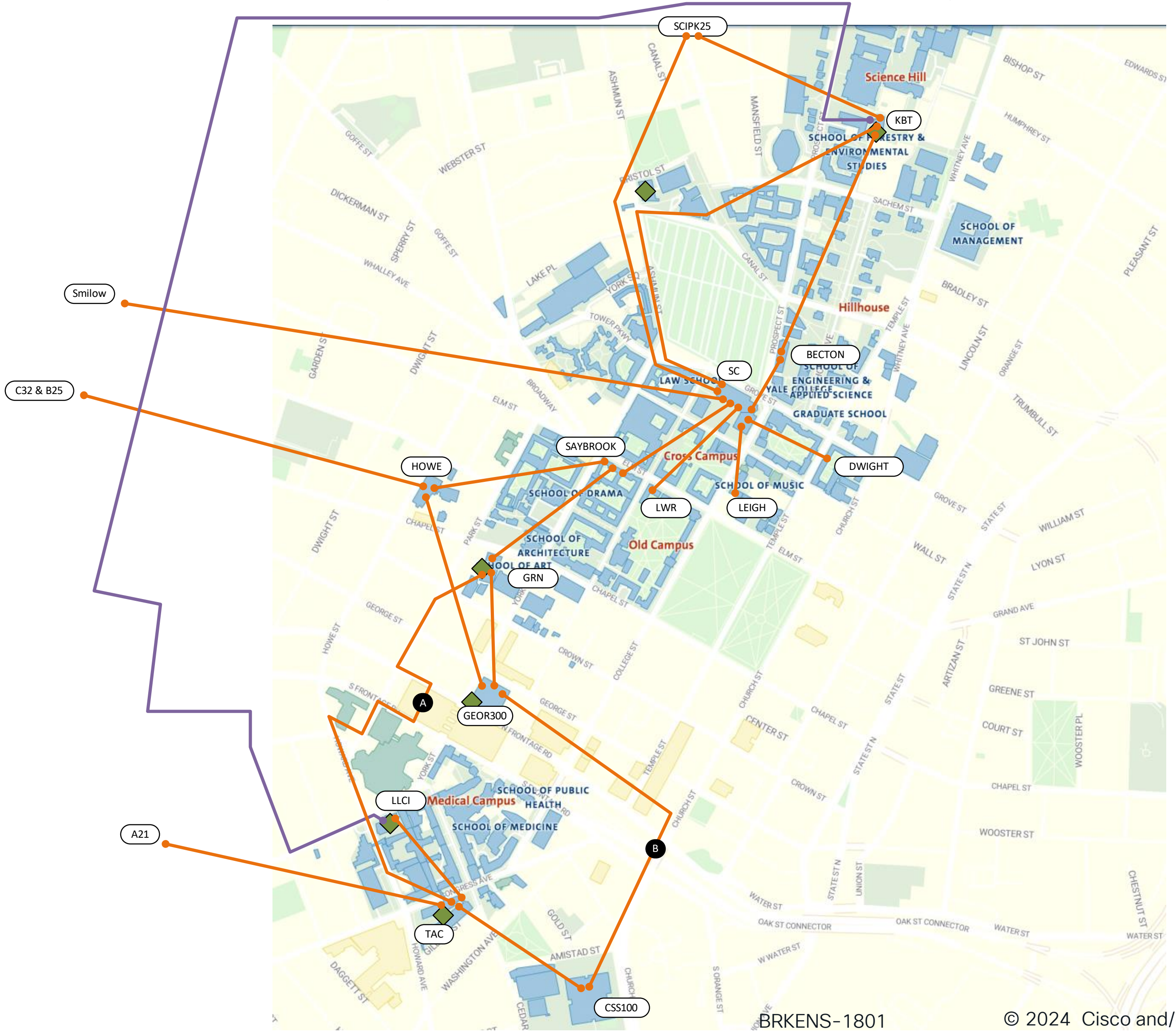
Yale

Layer-1 – The Vision



Next Generation Network: Layer 1 Reality

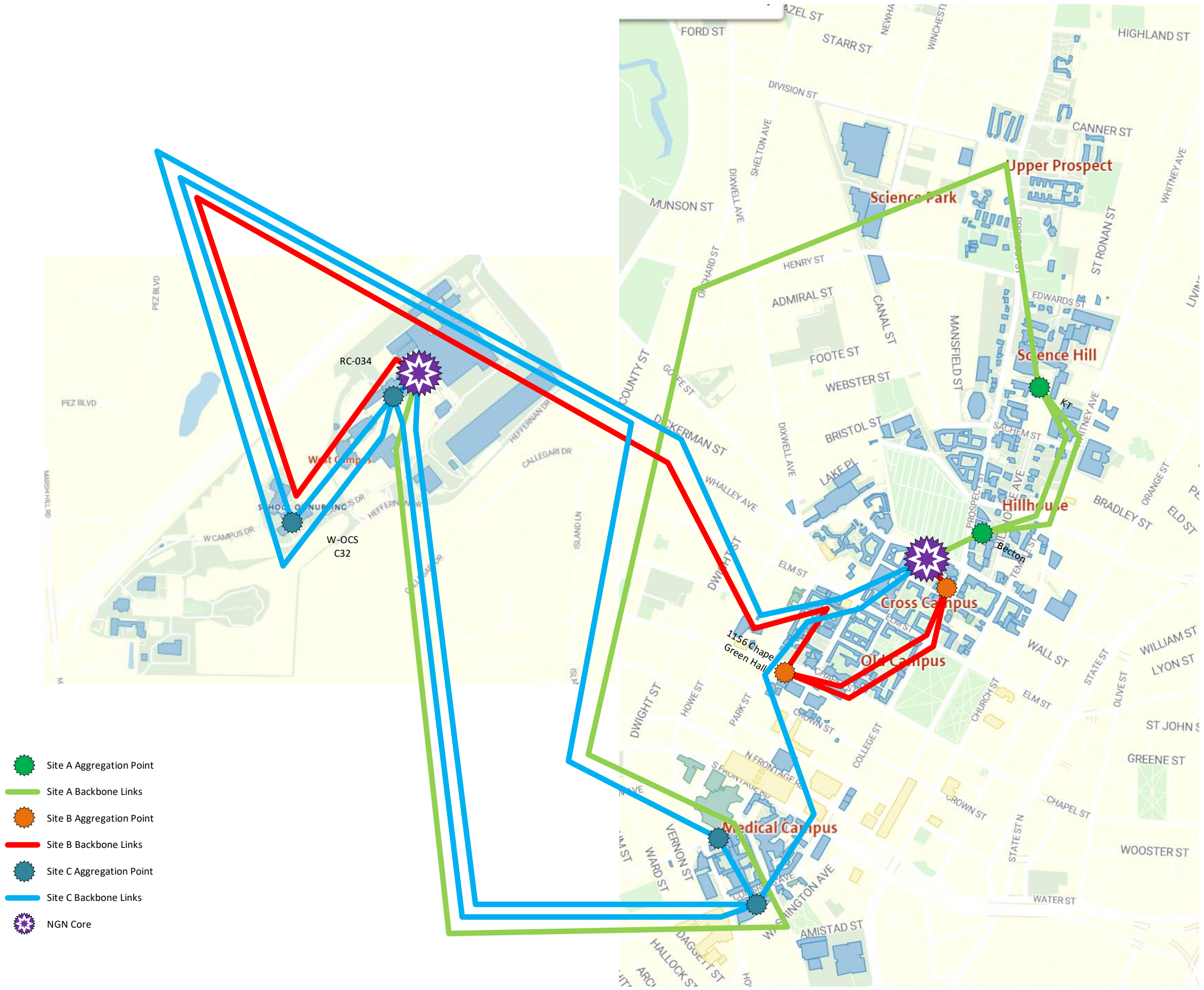
Layer-1 – The Reality



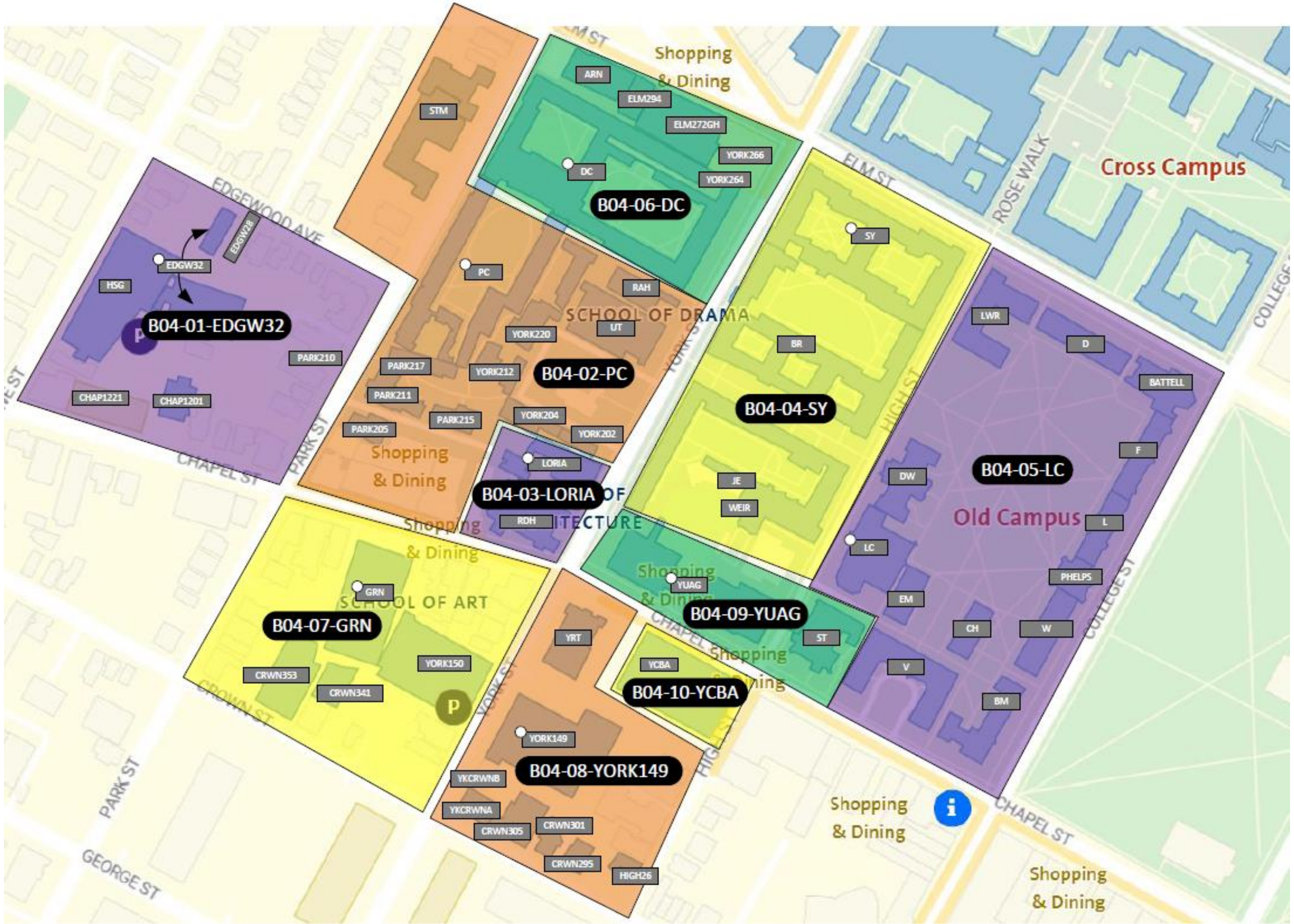
Next Generation Network: Layer 1 Fiber Placement

Layer-1 Aggregation Points

Yale worked to find the right locations for major fiber aggregation points:

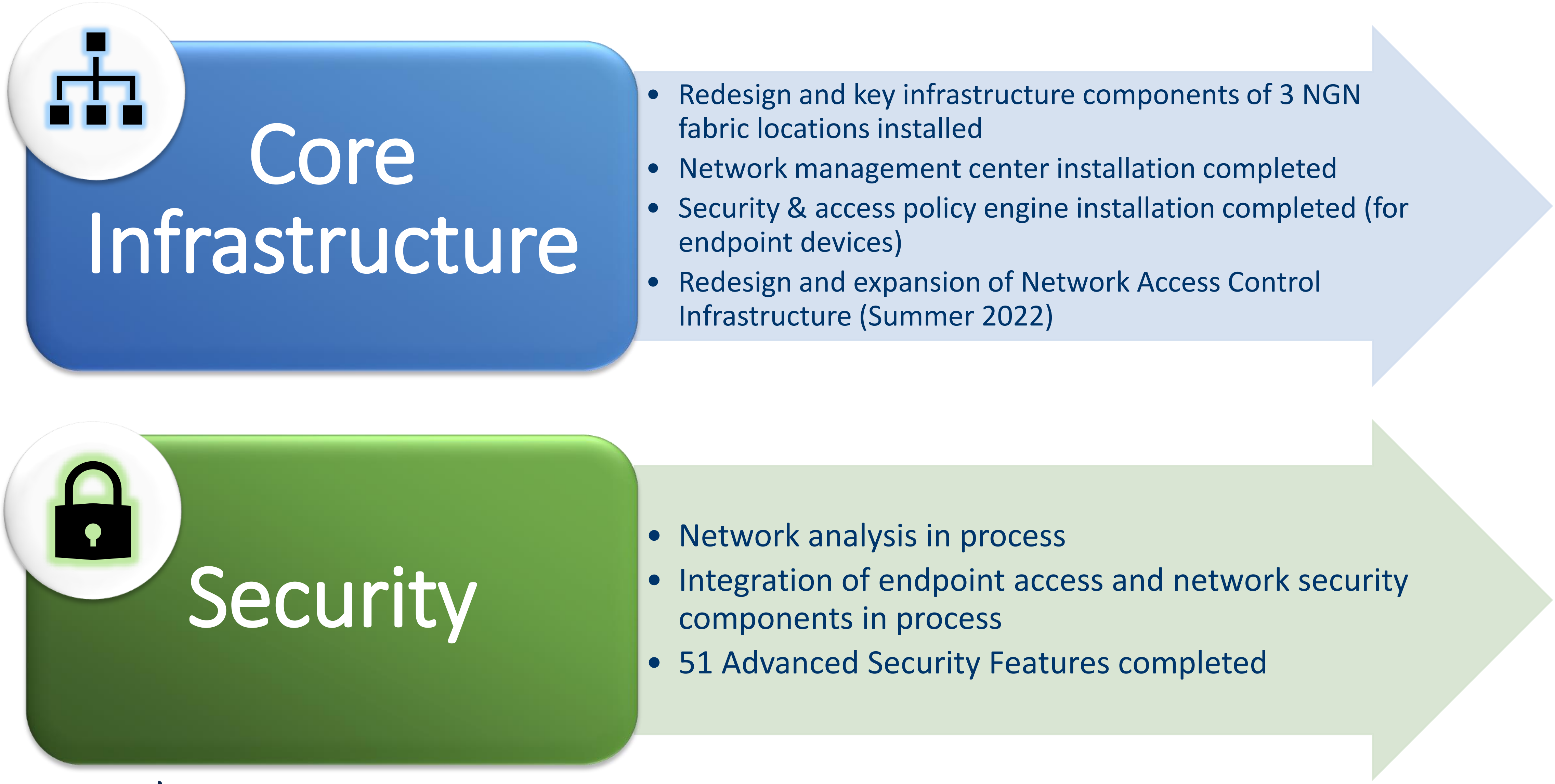


Next Generation Network: Layer -1 Hub Placement



Next Generation Network: Current Status (as of 5/1/24)

Yale



Core Infrastructure

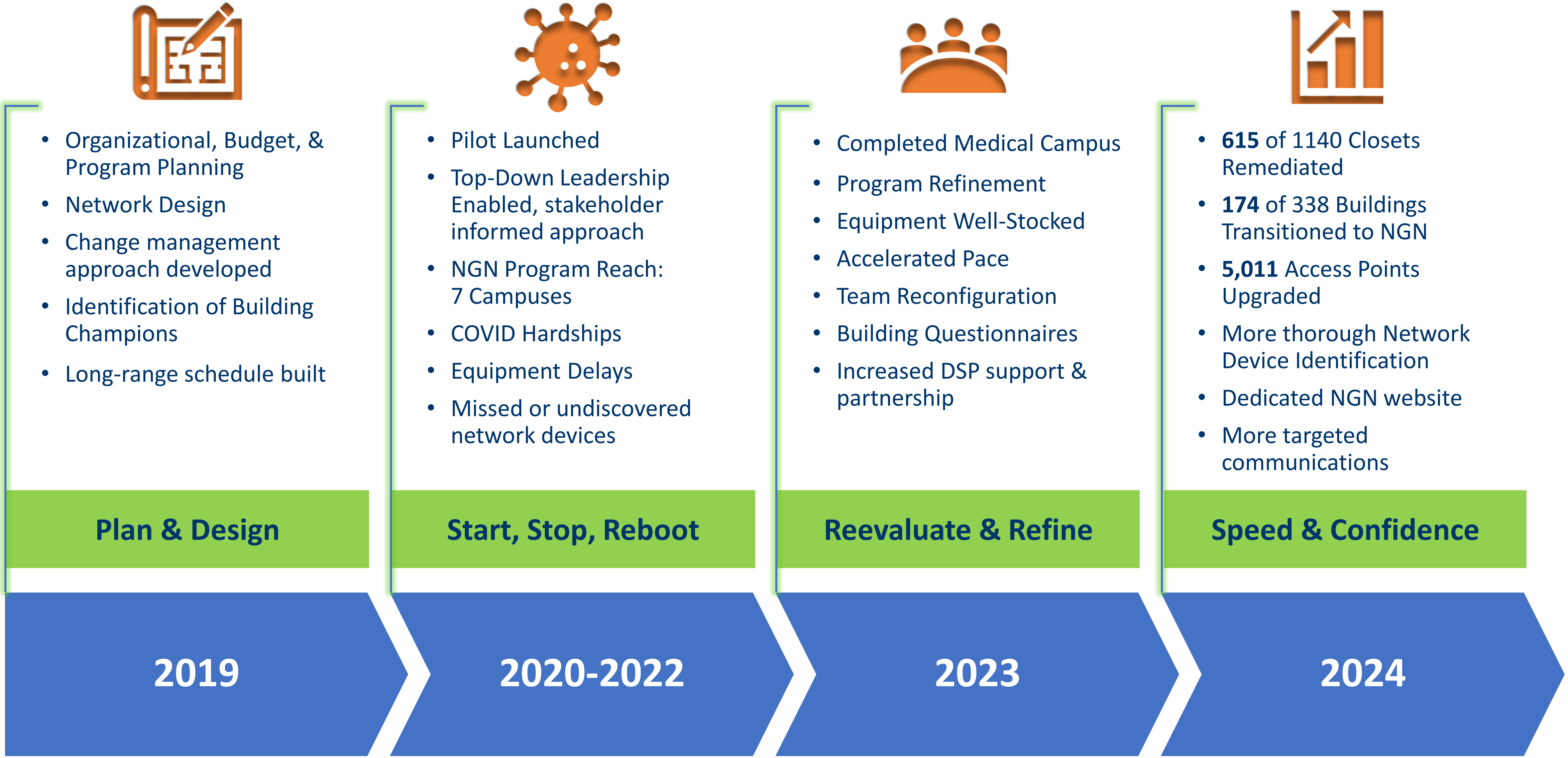
- Redesign and key infrastructure components of 3 NGN fabric locations installed
- Network management center installation completed
- Security & access policy engine installation completed (for endpoint devices)
- Redesign and expansion of Network Access Control Infrastructure (Summer 2022)

Security

- Network analysis in process
- Integration of endpoint access and network security components in process
- 51 Advanced Security Features completed

Next Generation Network: A Journey of Transition

Yale



2019

Plan & Design

- Organizational, Budget, & Program Planning
- Network Design
- Change management approach developed
- Identification of Building Champions
- Long-range schedule built

2020-2022

Start, Stop, Reboot

- Pilot Launched
- Top-Down Leadership Enabled, stakeholder informed approach
- NGN Program Reach: 7 Campuses
- COVID Hardships
- Equipment Delays
- Missed or undiscovered network devices

2023

Reevaluate & Refine

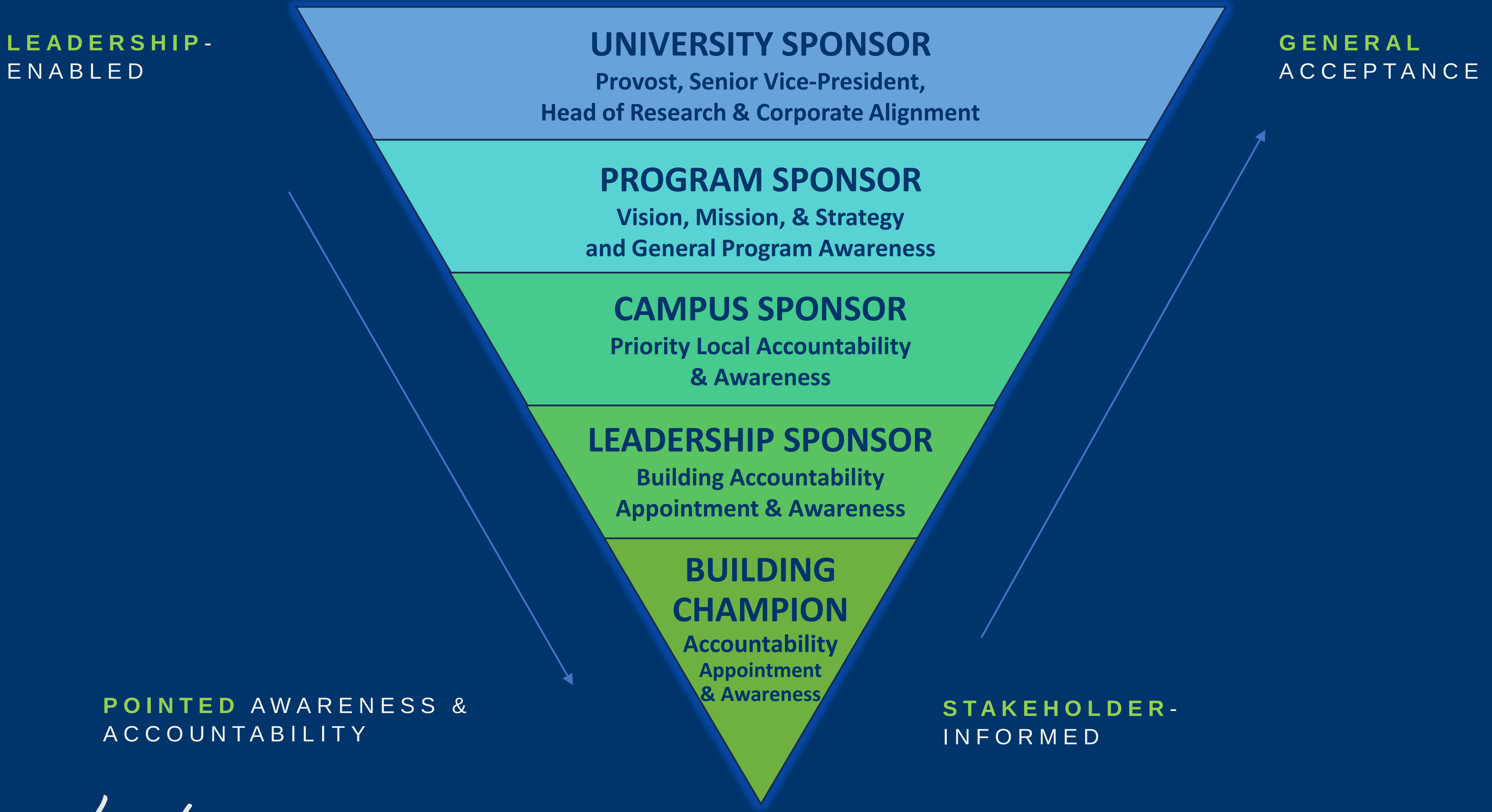
- Completed Medical Campus
- Program Refinement
- Equipment Well-Stocked
- Accelerated Pace
- Team Reconfiguration
- Building Questionnaires
- Increased DSP support & partnership

2024

Speed & Confidence

- **615** of 1140 Closets Remediated
- **174** of 338 Buildings Transitioned to NGN
- **5,011** Access Points Upgraded
- More thorough Network Device Identification
- Dedicated NGN website
- More targeted communications

Next Generation Network: Built Upon Sponsor-Enabled Change



LEADERSHIP-ENABLED

GENERAL ACCEPTANCE

UNIVERSITY SPONSOR
Provost, Senior Vice-President,
Head of Research & Corporate Alignment

PROGRAM SPONSOR
Vision, Mission, & Strategy
and General Program Awareness

CAMPUS SPONSOR
Priority Local Accountability
& Awareness

LEADERSHIP SPONSOR
Building Accountability
Appointment & Awareness

BUILDING CHAMPION
Accountability
Appointment
& Awareness

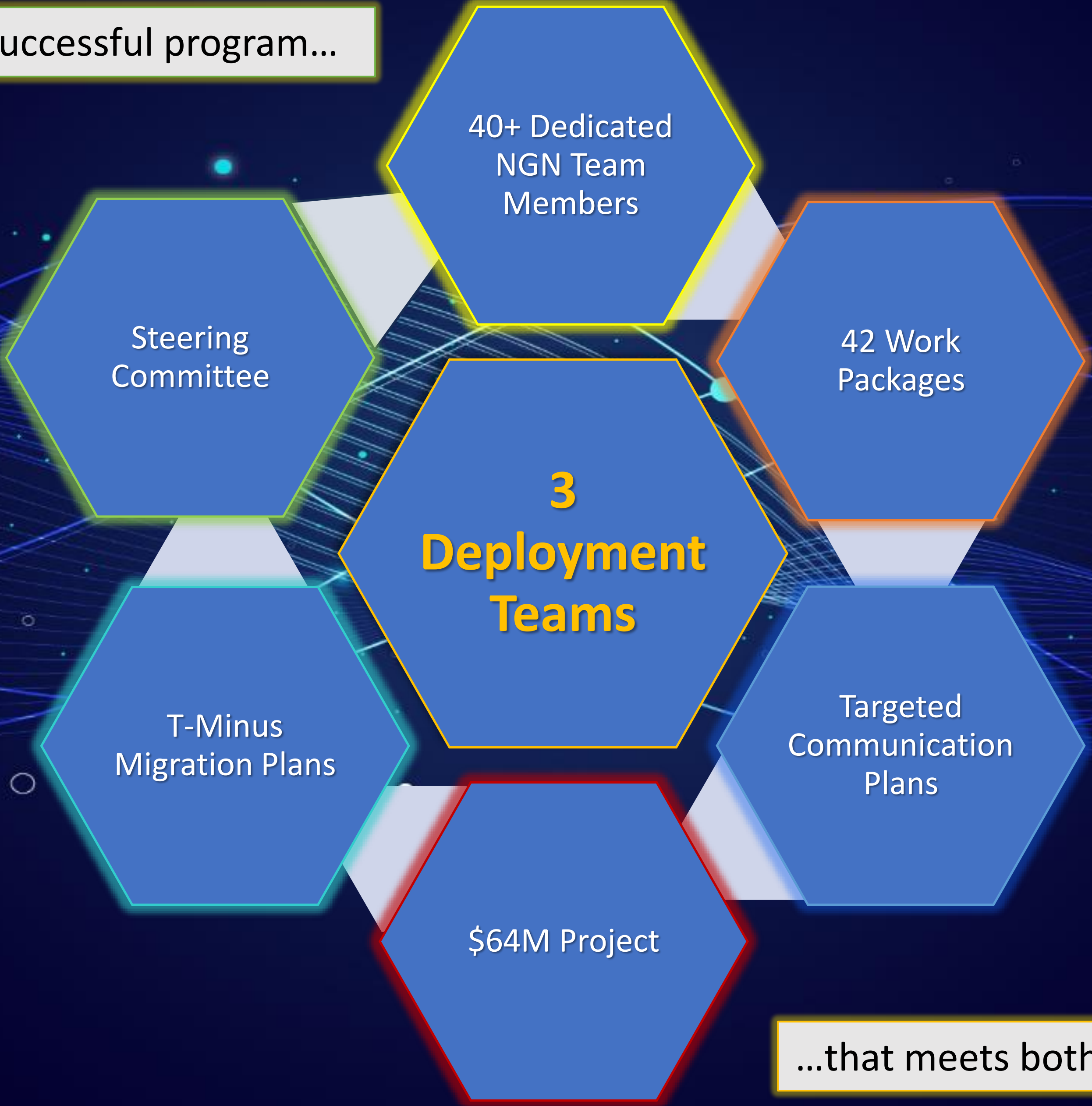
POINTED AWARENESS & ACCOUNTABILITY

STAKEHOLDER-INFORMED

Next Generation Network: Bones of the Project

Yale

Firing on all fronts to ensure a successful program…



40+ Dedicated NGN Team Members

Steering Committee

42 Work Packages

3 Deployment Teams

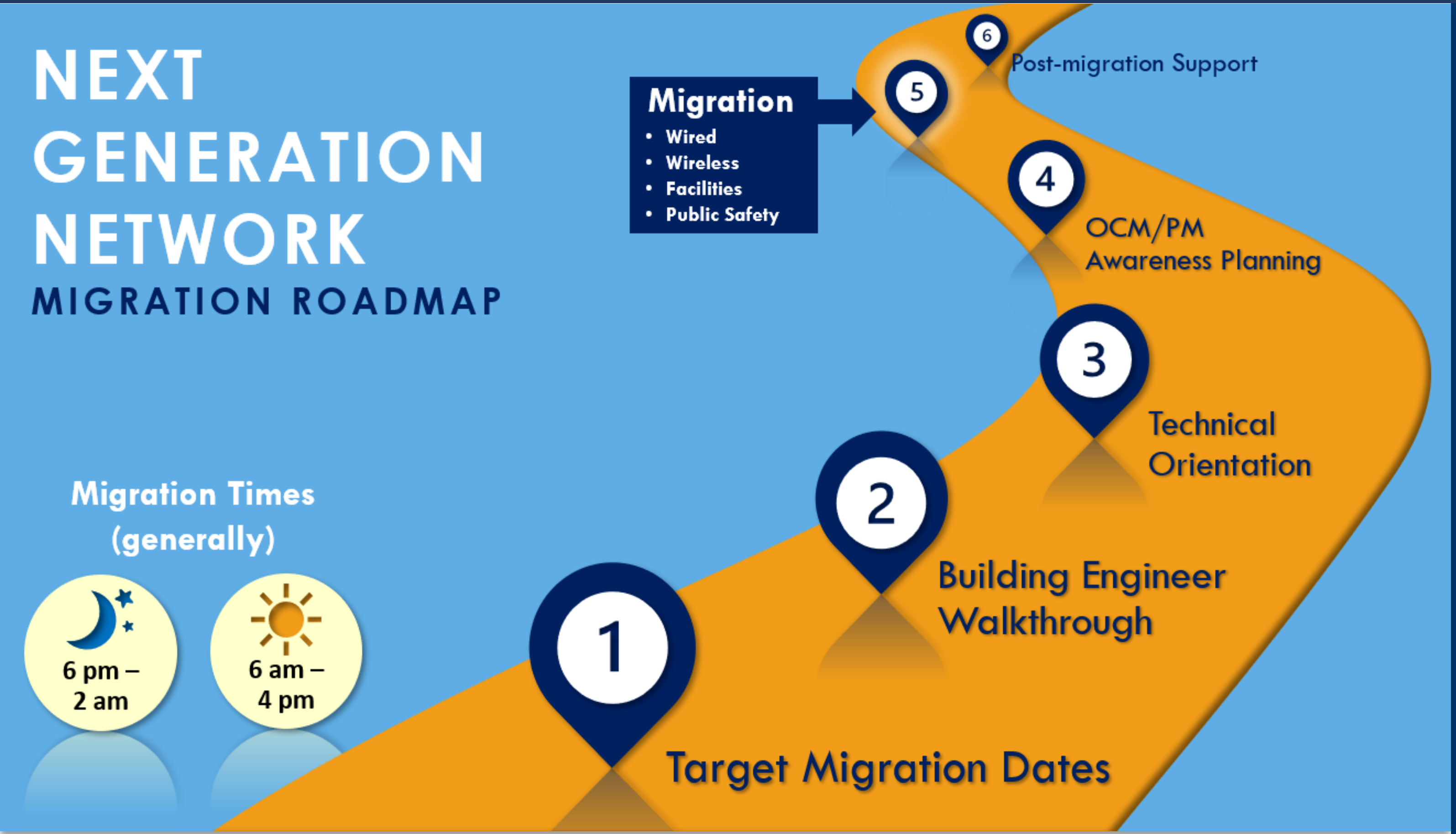
T-Minus Migration Plans

Targeted Communication Plans

$64M Project

…that meets both budget and time constraints

Next Generation Network: Broadening Discovery, Minimizing Risk



NEXT GENERATION NETWORK

MIGRATION ROADMAP

Migration
- Wired
- Wireless
- Facilities
- Public Safety

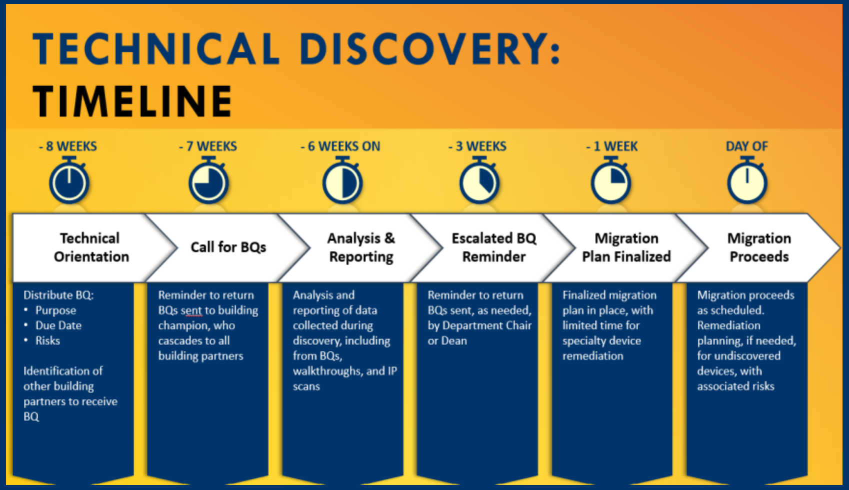
Migration Times (generally)

6 pm – 2 am

6 am – 4 pm

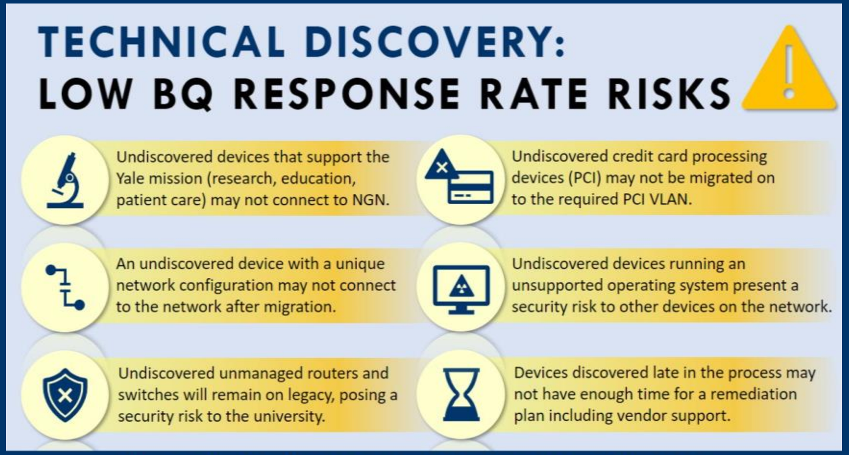
PROGRAM ORIENTATION

TECHNICAL ORIENTATION



TECHNICAL DISCOVERY: TIMELINE

- 8 WEEKS	- 7 WEEKS	- 6 WEEKS ON	- 3 WEEKS	- 1 WEEK	DAY OF
Technical Orientation	**Call for BQs**	**Analysis & Reporting**	**Escalated BQ Reminder**	**Migration Plan Finalized**	**Migration Proceeds**
Distribute BQ: • Purpose • Due Date • Risks Identification of other building partners to receive BQ	Reminder to return BQs sent to building champion, who cascades to all building partners	Analysis and reporting of data collected during discovery, including from BQs, walkthroughs, and IP scans	Reminder to return BQs sent, as needed, by Department Chair or Dean	Finalized migration plan in place, with limited time for specialty device remediation	Migration proceeds as scheduled. Remediation planning, if needed, for undiscovered devices, with associated risks



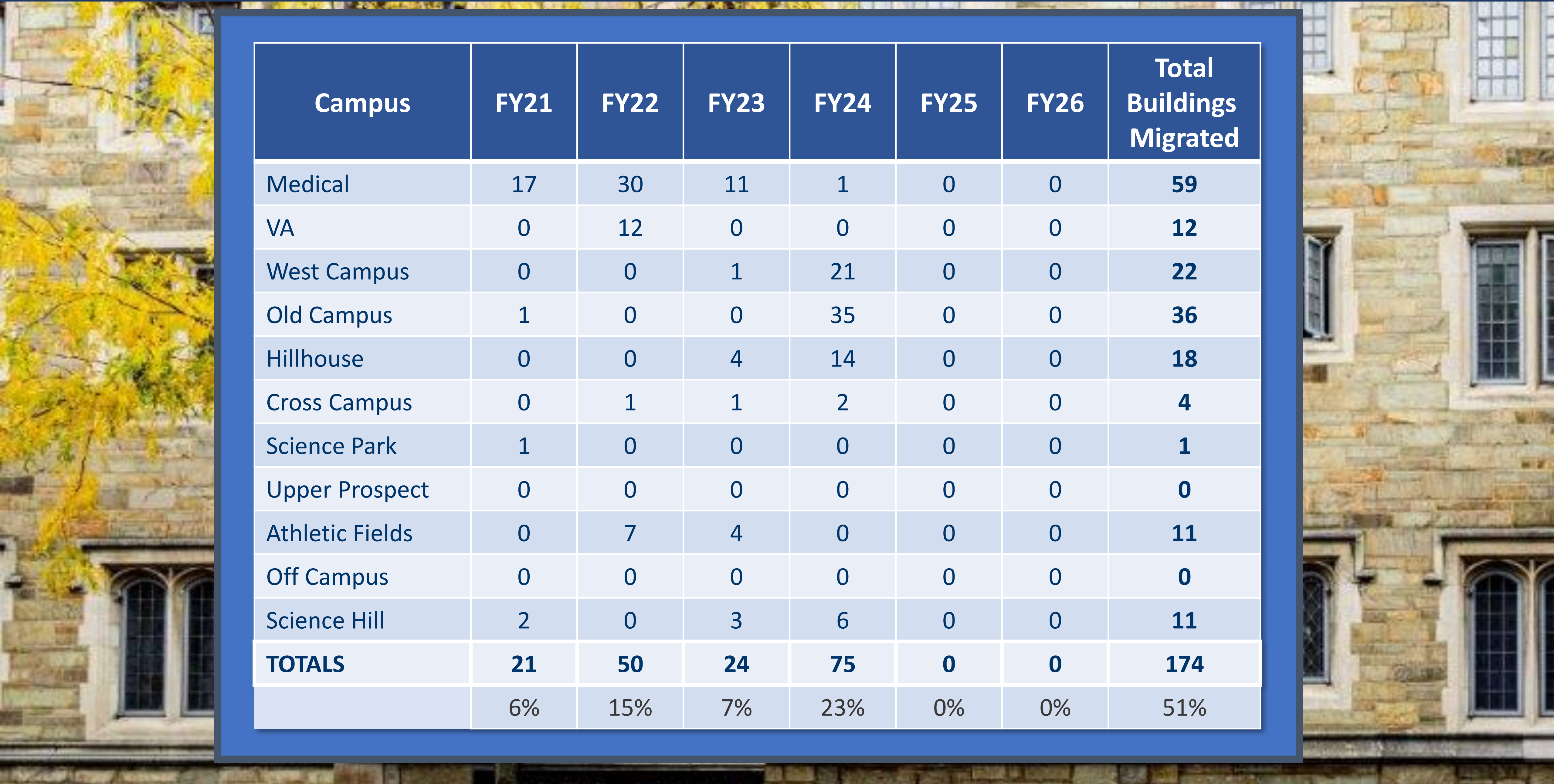
TECHNICAL DISCOVERY: LOW BQ RESPONSE RATE RISKS

- Undiscovered devices that support the Yale mission (research, education, patient care) may not connect to NGN.
- Undiscovered credit card processing devices (PCI) may not be migrated on to the required PCI VLAN.
- An undiscovered device with a unique network configuration may not connect to the network after migration.
- Undiscovered devices running an unsupported operating system present a security risk to other devices on the network.
- Undiscovered unmanaged routers and switches will remain on legacy, posing a security risk to the university.
- Devices discovered late in the process may not have enough time for a remediation plan including vendor support.

ANY OF THE ABOVE MAY DELAY POST-MIGRATION REMEDIATION.

Next Generation Network: Program Completed To Date by Campus (as of 5/1/23)

Yale



Campus	FY21	FY22	FY23	FY24	FY25	FY26	Total Buildings Migrated
Medical	17	30	11	1	0	0	**59**
VA	0	12	0	0	0	0	**12**
West Campus	0	0	1	21	0	0	**22**
Old Campus	1	0	0	35	0	0	**36**
Hillhouse	0	0	4	14	0	0	**18**
Cross Campus	0	1	1	2	0	0	**4**
Science Park	1	0	0	0	0	0	**1**
Upper Prospect	0	0	0	0	0	0	**0**
Athletic Fields	0	7	4	0	0	0	**11**
Off Campus	0	0	0	0	0	0	**0**
Science Hill	2	0	3	6	0	0	**11**
TOTALS	**21**	**50**	**24**	**75**	**0**	**0**	**174**
	6%	15%	7%	23%	0%	0%	51%

Key Takeaways

- Security needs to be at the heart of any core network upgrades
- Expect the unexpected and be ready to pivot
- For large-scale institutional change, create a user acceptance model supported by change management methodologies
- A project team must be supported by people and processes that help to move the project forward

Thank you

The bridge to possible

SD-Access and Micro Segmentation at Stanford Health Care

The Success Story

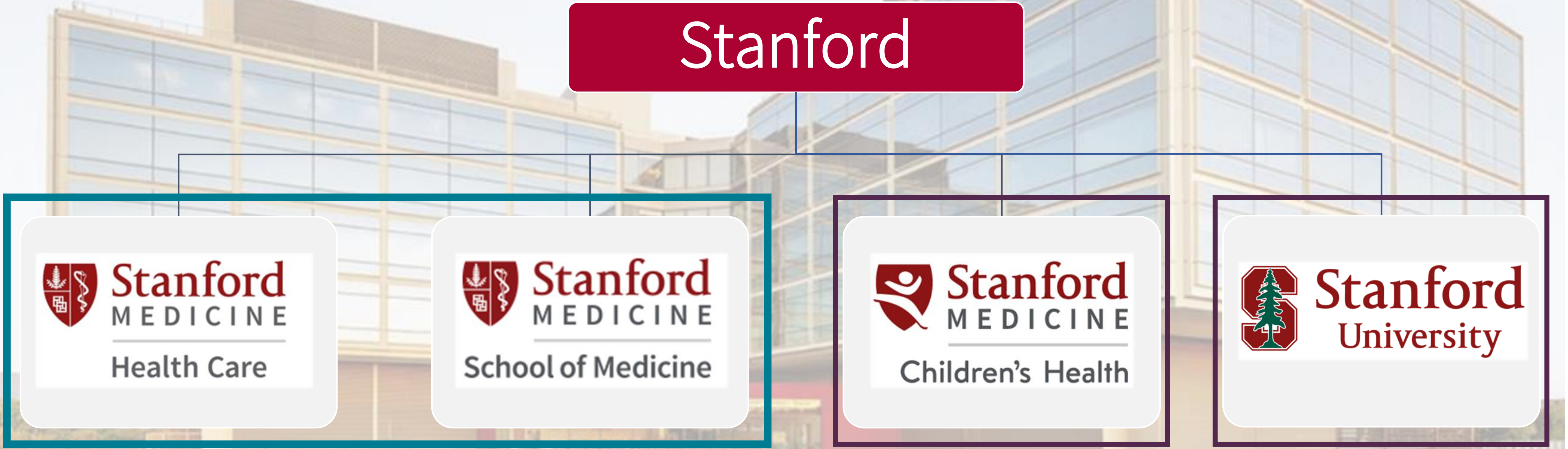
MAITRIK GANDHI, Lead Network Engineer
@NetAutomations

BRKENS-1801

Agenda

- About Stanford Health Care
- Key Driving Factors
- Our Deployment Strategy
- Challenges we conquered
- Benefits realized
- Our Journey

Organizational Ecosystem



Stanford

Stanford MEDICINE Health Care

Stanford MEDICINE School of Medicine

Stanford MEDICINE Children's Health

Stanford University

Stanford Health Care

INCLUDES Stanford Health Care, Tri-Valley, and Stanford Medicine Partners

Hospitals, MOBs (Medical Office Buildings), & Clinics

3,758
Physicians on
Active Medical Staff

1,492
Residents & Fellows

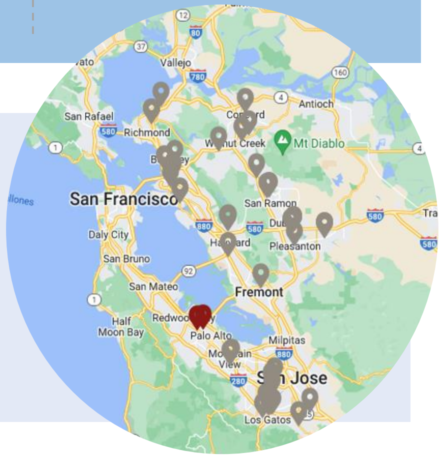
19,921
Employees

861
Licensed Beds

43,204
Admissions

2,396,454
Outpatient Visits

Clinic Service
Locations



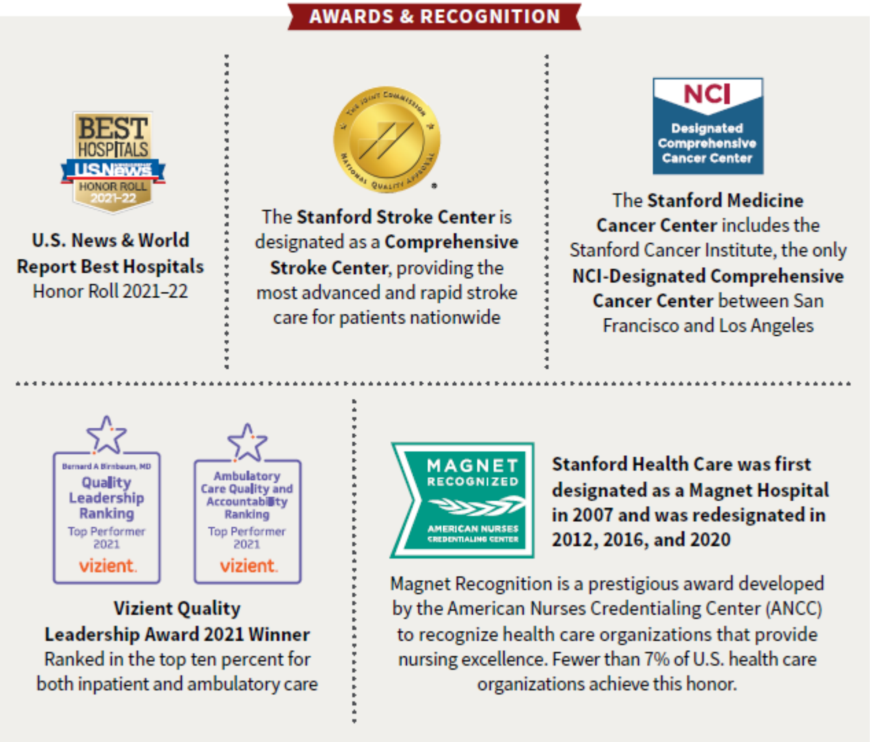
185,610
ED & Urgent Care
Visits/year

606,643
Video Visits

$642.5M
Community Benefit Investment

Awards & Recognitions

Stanford Health Care


AWARDS & RECOGNITION
BEST HOSPITALS
USNews
HONOR ROLL 2021-22
THE JOINT COMMISSION
NATIONAL QUALITY APPROVAL
NCI
Designated Comprehensive Cancer Center
Bernard A Birnbaum, MD
Quality Leadership Ranking
Top Performer 2021
vizient.
Ambulatory Care Quality and Accountability Ranking
Top Performer 2021
vizient.
MAGNET RECOGNIZED
AMERICAN NURSES CREDENTIALING CENTER

U.S. News & World Report Best Hospitals Honor Roll 2021–22

The **Stanford Stroke Center** is designated as a **Comprehensive Stroke Center**, providing the most advanced and rapid stroke care for patients nationwide

The **Stanford Medicine Cancer Center** includes the Stanford Cancer Institute, the only **NCI-Designated Comprehensive Cancer Center** between San Francisco and Los Angeles

Vizient Quality Leadership Award 2021 Winner
Ranked in the top ten percent for both inpatient and ambulatory care

Stanford Health Care was first designated as a Magnet Hospital in 2007 and was redesignated in 2012, 2016, and 2020

Magnet Recognition is a prestigious award developed by the American Nurses Credentialing Center (ANCC) to recognize health care organizations that provide nursing excellence. Fewer than 7% of U.S. health care organizations achieve this honor.

In the 2021–2022 U.S. News & World Report survey of America’s Best Hospitals, Stanford Health Care (SHC) received national recognition in 11 specialties, including:

- Cancer care
- Cardiology & heart surgery
- Diabetes & endocrinology
- Ear, nose, & throat
- Gastroenterology & GI surgery
- Geriatrics
- Gynecology
- Neurology & neurosurgery
- Orthopedics
- Pulmonology & lung surgery
- Urology

It’s always the network…

90+ Major Locations

3.5 Million Sq.ft. floor space

1200+ Network Devices

180,000+ Switchports

49K	11K	5K	7K	6.5 K	3K	2K
Laptop and PC	VOIP Phones	Access Points	Virtual Machines	Printers	IP Cameras	Patient Monitors
33K	1K	229	1.1K	184	141	6
Mobile Phones	TVs	Nurse Call	Infusion Pumps	Product Scanners	POC Diagnostics	Angiography
115	110	92	82	66	57	10
Ultrasound	Central Stations	IOT Gateways	ECGs	Sensors	Imaging Workstations	Fluoroscopy
24	23	19	13	31	721	27
Endoscopy	Lab Equipment	X-Ray	MRIs	*Game Consoles*	*Media Players*	*Cars*

Legacy Network - Limitations

1. Manageability

- Devices management and visibility
- Number of VRFs & Firewall rules
- DHCP scopes

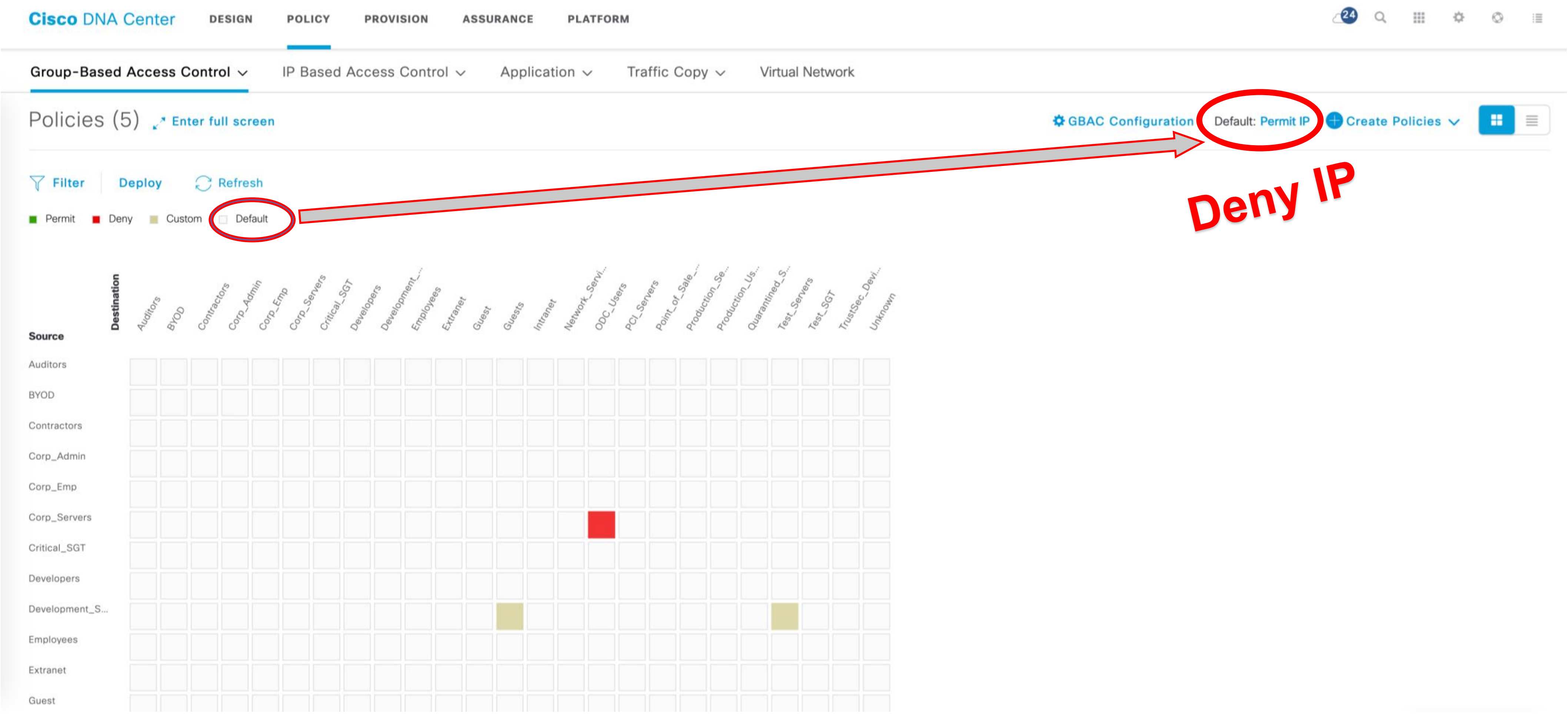
2. IP Mobility

- Spanning Tree
- Fixed address for Modalities
- Device roaming between ORs

3. Security

- Macro-Segmentation
- Non-standard vendor devices with legacy images
- Not a good security posture
- Increased cyber-security and ransomware risk

SD-Access for Micro-segmentation using Catalyst Center & ISE



Policies (5)

Default: Permit IP

Deny IP

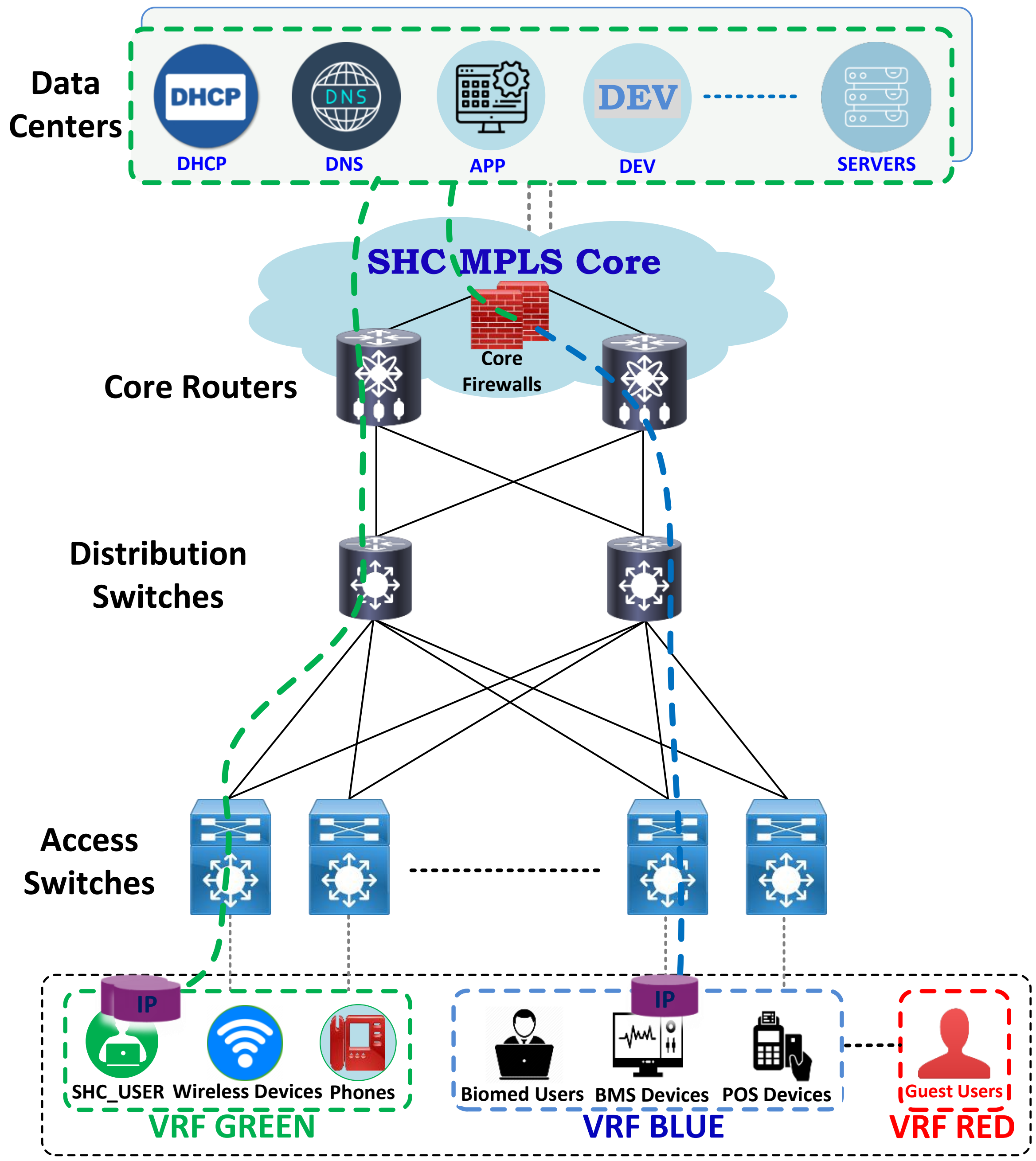
🟩 Permit 🟥 Deny ▨ Custom □ Default

Source \ Destination	Auditors	BYOD	Contractors	Corp_Admin	Corp_Emp	Corp_Servers	Critical_SGT	Developers	Development_...	Employees	Extranet	Guest	Guests	Intranet	Network_Servi...	ODC_Users	PCI_Servers	Point_of_Sale_...	Production_Se...	Production_Us...	Quarantined_S...	Test_Servers	Test_SGT	TrustSec_Devi...	Unknown
Auditors																									
BYOD																									
Contractors																									
Corp_Admin																									
Corp_Emp																									
Corp_Servers																🟥									
Critical_SGT																									
Developers																									
Development_S...													▨									▨			
Employees																									
Extranet																									
Guest																									

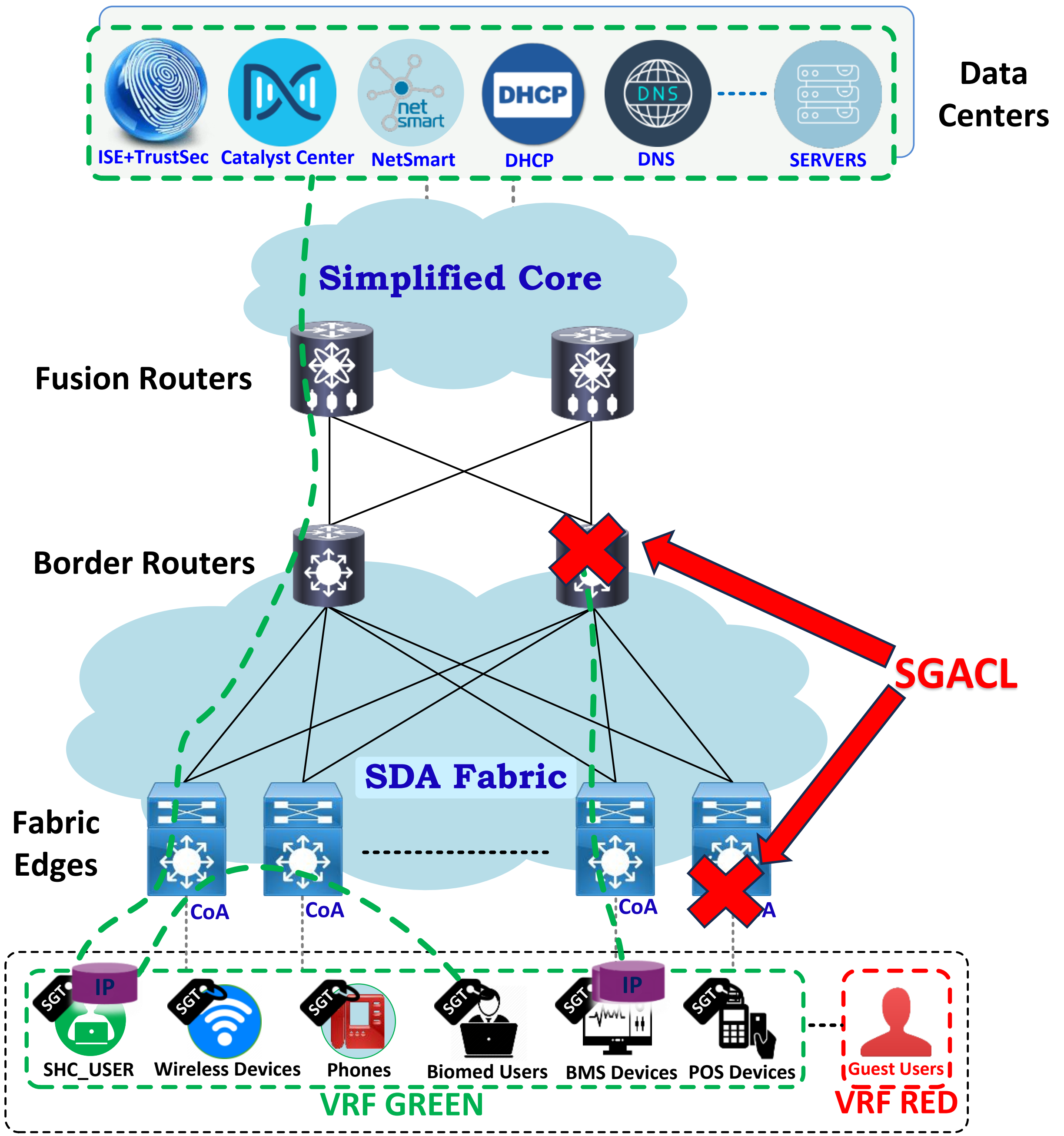
Zero Trust Access with implicit Default DENY

- Legacy devices with outdated Software
- Weak Security posture
- Attack surface & East-west propagation
- Scalability

Before(Traditional Network)

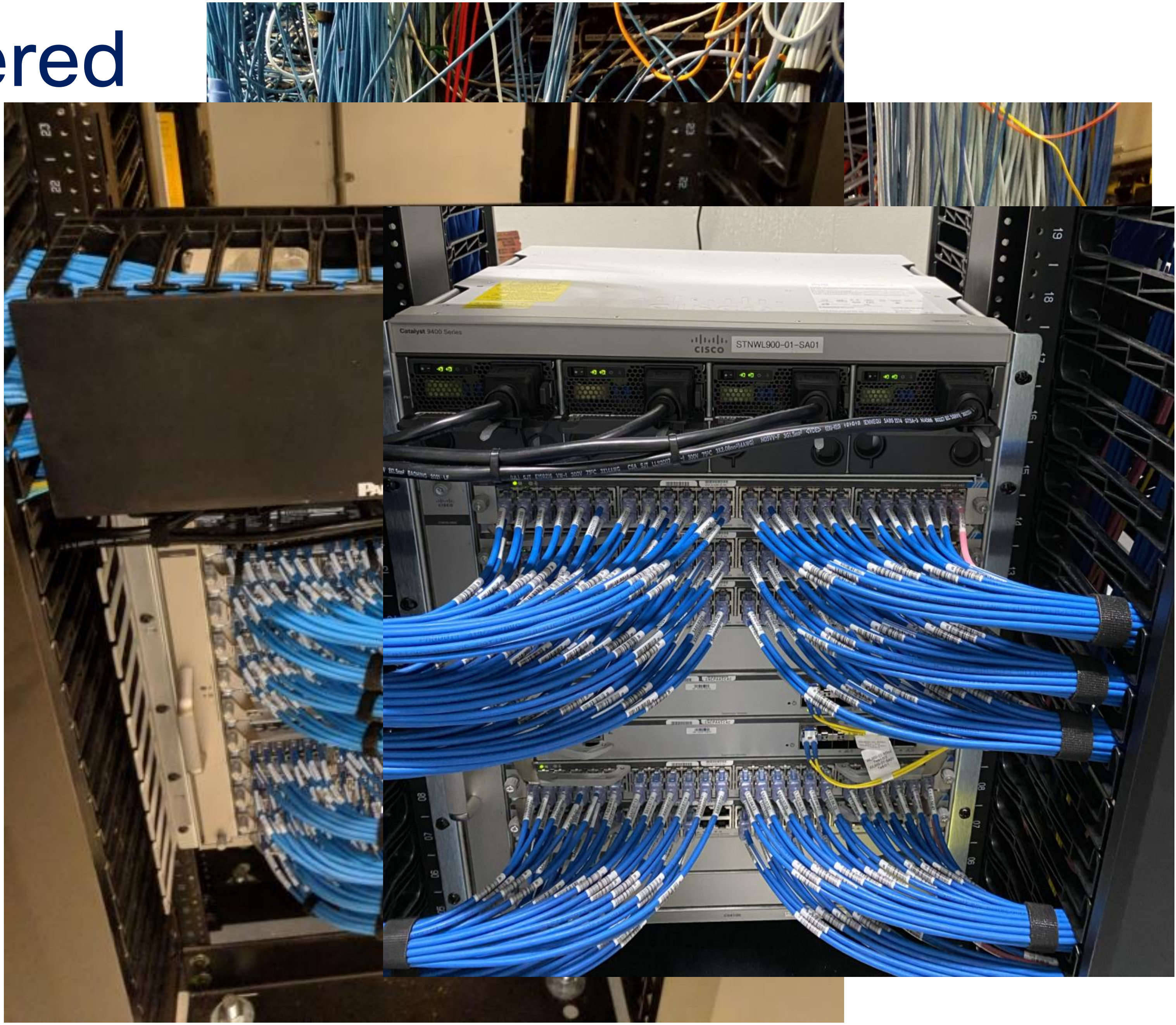


After(SDA & TrustSec)



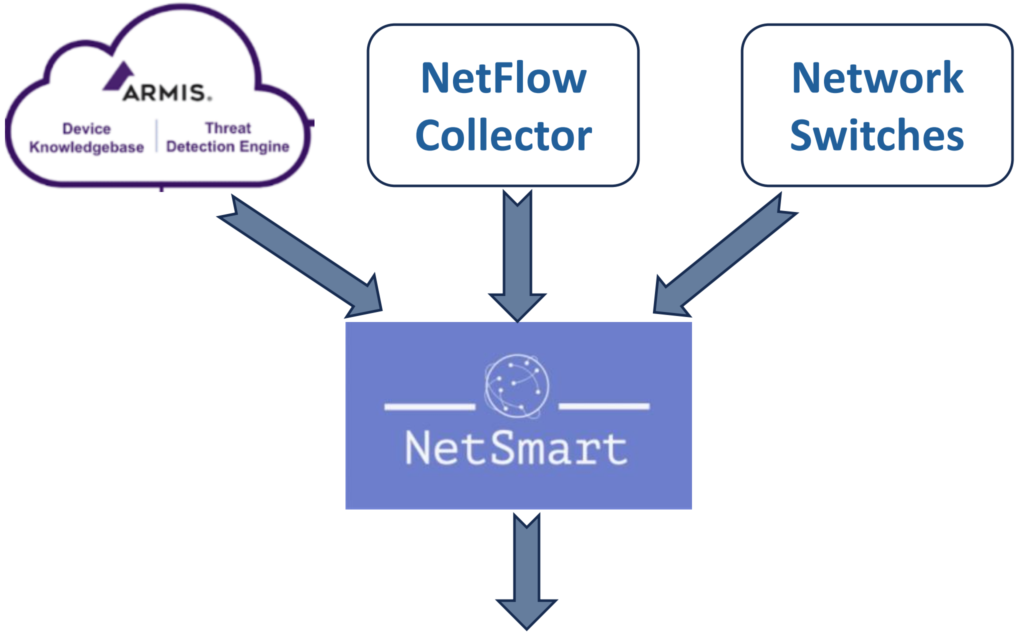
Challenges encountered

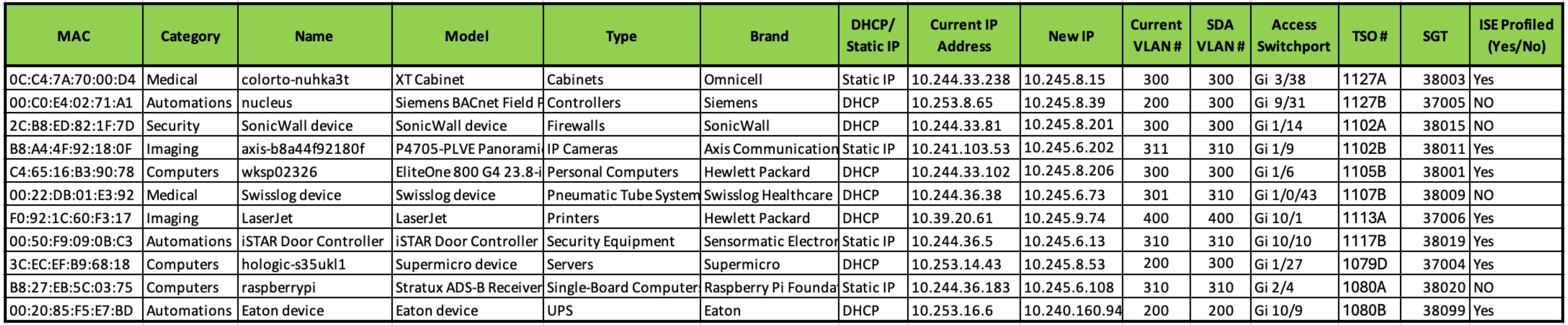
- Getting Downtime for migration
- IP Address change
- Phones migration (Meeting E911 requirements)
- ISE Profiling for every device type
- Identifying all North-South & East-West legitimate traffic
- Supporting Non-standard features with custom config



Stanford’s deployment strategy: Planning

- Create custom Config Templates
- Accurate Asset Inventory
- Netflow Analysis (Stealthwatch & NetSmart)
- Custom Automation Tools (NetSmart)
- 500+ SGT & 5000+ SGACLs





MAC	Category	Name	Model	Type	Brand	DHCP/ Static IP	Current IP Address	New IP	Current VLAN #	SDA VLAN #	Access Switchport	TSO #	SGT	ISE Profiled (Yes/No)
0C:C4:7A:70:00:D4	Medical	colorto-nuhka3t	XT Cabinet	Cabinets	Omnicell	Static IP	10.244.33.238	10.245.8.15	300	300	Gi 3/38	1127A	38003	Yes
00:C0:E4:02:71:A1	Automations	nucleus	Siemens BACnet Field F	Controllers	Siemens	DHCP	10.253.8.65	10.245.8.39	200	300	Gi 9/31	1127B	37005	NO
2C:B8:ED:82:1F:7D	Security	SonicWall device	SonicWall device	Firewalls	SonicWall	DHCP	10.244.33.81	10.245.8.201	300	300	Gi 1/14	1102A	38015	NO
B8:A4:4F:92:18:0F	Imaging	axis-b8a44f92180f	P4705-PLVE Panorami	IP Cameras	Axis Communication	Static IP	10.241.103.53	10.245.6.202	311	310	Gi 1/9	1102B	38011	Yes
C4:65:16:B3:90:78	Computers	wksp02326	EliteOne 800 G4 23.8-i	Personal Computers	Hewlett Packard	DHCP	10.244.33.102	10.245.8.206	300	300	Gi 1/6	1105B	38001	Yes
00:22:DB:01:E3:92	Medical	Swisslog device	Swisslog device	Pneumatic Tube System	Swisslog Healthcare	DHCP	10.244.36.38	10.245.6.73	301	310	Gi 1/0/43	1107B	38009	NO
F0:92:1C:60:F3:17	Imaging	LaserJet	LaserJet	Printers	Hewlett Packard	DHCP	10.39.20.61	10.245.9.74	400	400	Gi 10/1	1113A	37006	Yes
00:50:F9:09:0B:C3	Automations	iSTAR Door Controller	iSTAR Door Controller	Security Equipment	Sensormatic Electror	Static IP	10.244.36.5	10.245.6.13	310	310	Gi 10/10	1117B	38019	Yes
3C:EC:EF:B9:68:18	Computers	hologic-s35ukl1	Supermicro device	Servers	Supermicro	DHCP	10.253.14.43	10.245.8.53	200	300	Gi 1/27	1079D	37004	Yes
B8:27:EB:5C:03:75	Computers	raspberrypi	Stratux ADS-B Receiver	Single-Board Computer	Raspberry Pi Founda	Static IP	10.244.36.183	10.245.6.108	310	310	Gi 2/4	1080A	38020	NO
00:20:85:F5:E7:BD	Automations	Eaton device	Eaton device	UPS	Eaton	DHCP	10.253.16.6	10.240.160.94	200	200	Gi 10/9	1080B	38099	Yes

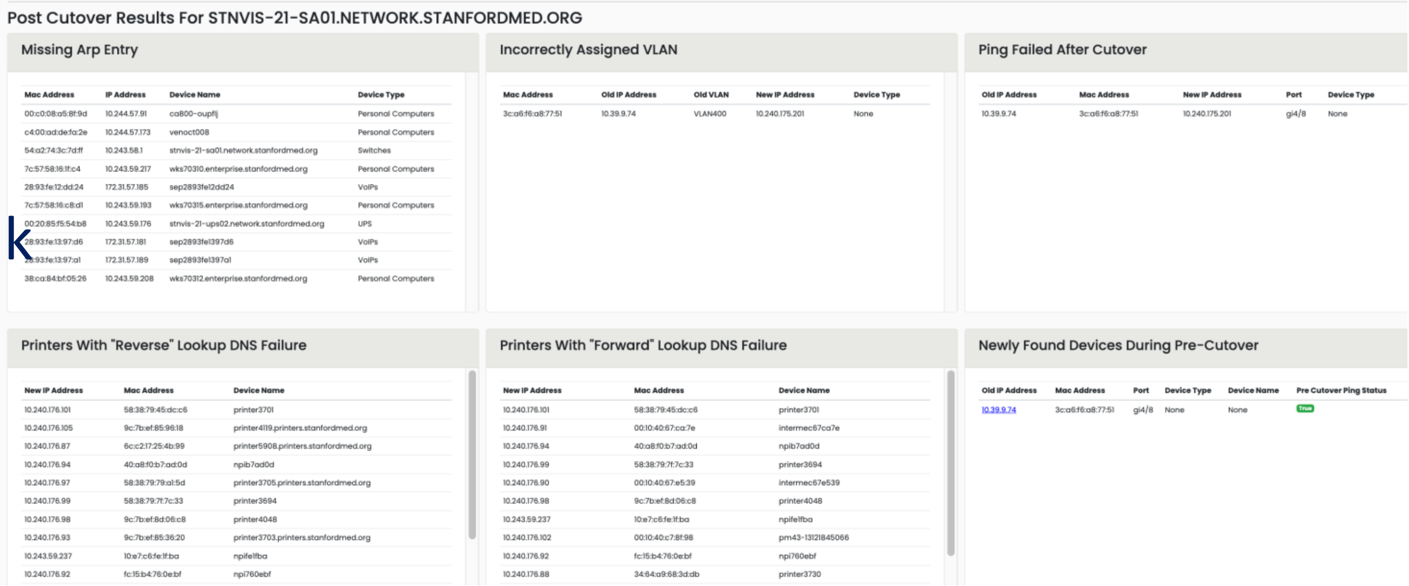
Stanford’s deployment strategy: Execution

- Build SDA Fabric with Catalyst Center
  - Design
  - Provision
  - Build the Fabric
  - SXP between Border node & ISE
- Host onboarding
  - Based on ISE Profiles, correct Vlan & SGT applied to Switchports
  - Automatic SGACL Policies applied to Fabric Edge & Border nodes

Stanford’s deployment strategy: Validation

- Post cutover validation by NetSmart

- Monitor Default DENY logs on Splunk



Post Cutover Results For STNVIS-21-SA01.NETWORK.STANFORDMED.ORG

Missing Arp Entry

Mac Address	IP Address	Device Name	Device Type
00:c0:08:a5:8f:9d	10.244.57.91	ca800-oupfij	Personal Computers
c4:00:ad:de:fa:2e	10.244.57.173	venoct008	Personal Computers
54:a2:74:3c:7d:ff	10.243.58.1	stnvis-21-sa01.network.stanfordmed.org	Switches
7c:57:58:16:1f:c4	10.243.59.217	wks70310.enterprise.stanfordmed.org	Personal Computers
28:93:fe:12:dd:24	172.31.57.185	sep2893fe12dd24	VoIPs
7c:57:58:16:c8:d1	10.243.59.193	wks70315.enterprise.stanfordmed.org	Personal Computers
00:20:85:f5:54:b8	10.243.59.176	stnvis-21-ups02.network.stanfordmed.org	UPS
28:93:fe:13:97:d6	172.31.57.181	sep2893fe1397d6	VoIPs
28:93:fe:13:97:a1	172.31.57.189	sep2893fe1397a1	VoIPs
38:ca:84:bf:05:26	10.243.59.208	wks70312.enterprise.stanfordmed.org	Personal Computers

Incorrectly Assigned VLAN

Mac Address	Old IP Address	Old VLAN	New IP Address	Device Type
3c:a6:f6:a8:77:51	10.39.9.74	VLAN400	10.240.175.201	None

Ping Failed After Cutover

Old IP Address	Mac Address	New IP Address	Port	Device Type
10.39.9.74	3c:a6:f6:a8:77:51	10.240.175.201	gi4/8	None

Printers With "Reverse" Lookup DNS Failure

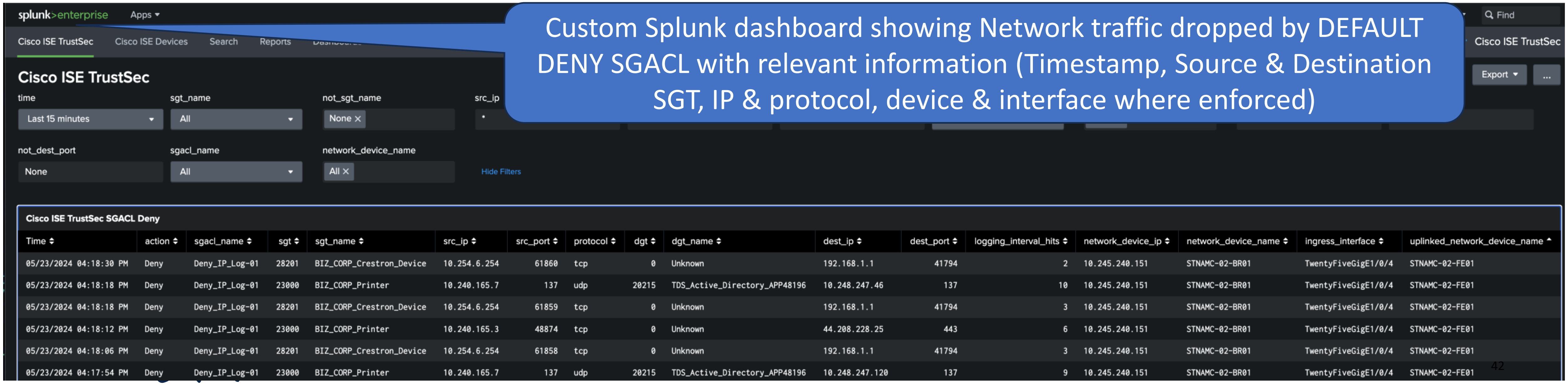
New IP Address	Mac Address	Device Name
10.240.176.101	58:38:79:45:dc:c6	printer3701
10.240.176.105	9c:7b:ef:85:96:18	printer4119.printers.stanfordmed.org
10.240.176.87	6c:c2:17:25:4b:99	printer5908.printers.stanfordmed.org
10.240.176.94	40:a8:f0:b7:ad:0d	npib7ad0d
10.240.176.97	58:38:79:79:a1:5d	printer3705.printers.stanfordmed.org
10.240.176.99	58:38:79:7f:7c:33	printer3694
10.240.176.98	9c:7b:ef:8d:06:c8	printer4048
10.240.176.93	9c:7b:ef:85:36:20	printer3703.printers.stanfordmed.org
10.243.59.237	10:e7:c6:fe:1f:ba	npife1fba
10.240.176.92	fc:15:b4:76:0e:bf	npi760ebf

Printers With "Forward" Lookup DNS Failure

New IP Address	Mac Address	Device Name
10.240.176.101	58:38:79:45:dc:c6	printer3701
10.240.176.91	00:10:40:67:ca:7e	intermec67ca7e
10.240.176.94	40:a8:f0:b7:ad:0d	npib7ad0d
10.240.176.99	58:38:79:7f:7c:33	printer3694
10.240.176.90	00:10:40:67:e5:39	intermec67e539
10.240.176.98	9c:7b:ef:8d:06:c8	printer4048
10.243.59.237	10:e7:c6:fe:1f:ba	npife1fba
10.240.176.102	00:10:40:c7:8f:98	pm43-13121845066
10.240.176.92	fc:15:b4:76:0e:bf	npi760ebf
10.240.176.88	34:64:a9:68:3d:db	printer3730

Newly Found Devices During Pre-Cutover

Old IP Address	Mac Address	Port	Device Type	Device Name	Pre Cutover Ping Status
10.39.9.74	3c:a6:f6:a8:77:51	gi4/8	None	None	True



Custom Splunk dashboard showing Network traffic dropped by DEFAULT DENY SGACL with relevant information (Timestamp, Source & Destination SGT, IP & protocol, device & interface where enforced)

Cisco ISE TrustSec

time: Last 15 minutes

sgt_name: All

not_sgt_name: None ×

src_ip: *

not_dest_port: None

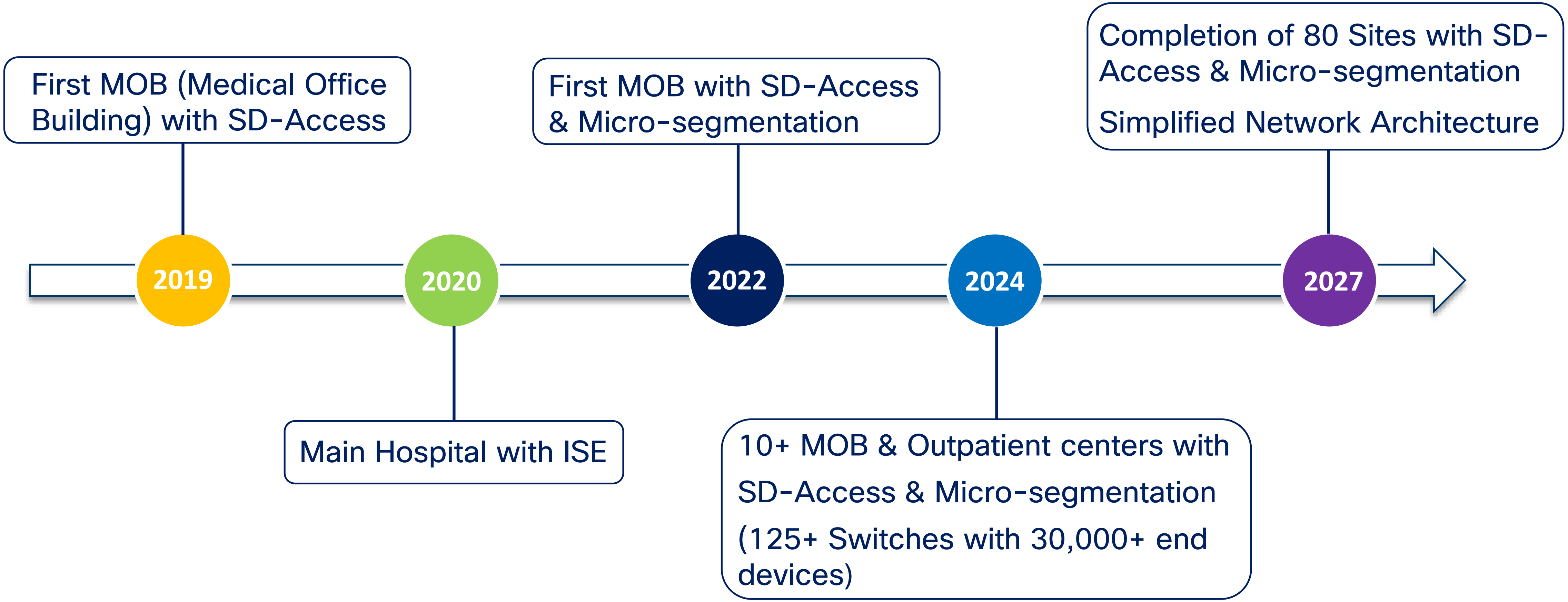
sgacl_name: All

network_device_name: All ×

Cisco ISE TrustSec SGACL Deny

Time	action	sgacl_name	sgt	sgt_name	src_ip	src_port	protocol	dgt	dgt_name	dest_ip	dest_port	logging_interval_hits	network_device_ip	network_device_name	ingress_interface	uplinked_network_device_name
05/23/2024 04:18:30 PM	Deny	Deny_IP_Log-01	28201	BIZ_CORP_Crestron_Device	10.254.6.254	61860	tcp	0	Unknown	192.168.1.1	41794	2	10.245.240.151	STNAMC-02-BR01	TwentyFiveGigE1/0/4	STNAMC-02-FE01
05/23/2024 04:18:18 PM	Deny	Deny_IP_Log-01	23000	BIZ_CORP_Printer	10.240.165.7	137	udp	20215	TDS_Active_Directory_APP48196	10.248.247.46	137	10	10.245.240.151	STNAMC-02-BR01	TwentyFiveGigE1/0/4	STNAMC-02-FE01
05/23/2024 04:18:18 PM	Deny	Deny_IP_Log-01	28201	BIZ_CORP_Crestron_Device	10.254.6.254	61859	tcp	0	Unknown	192.168.1.1	41794	3	10.245.240.151	STNAMC-02-BR01	TwentyFiveGigE1/0/4	STNAMC-02-FE01
05/23/2024 04:18:12 PM	Deny	Deny_IP_Log-01	23000	BIZ_CORP_Printer	10.240.165.3	48874	tcp	0	Unknown	44.208.228.25	443	6	10.245.240.151	STNAMC-02-BR01	TwentyFiveGigE1/0/4	STNAMC-02-FE01
05/23/2024 04:18:06 PM	Deny	Deny_IP_Log-01	28201	BIZ_CORP_Crestron_Device	10.254.6.254	61858	tcp	0	Unknown	192.168.1.1	41794	3	10.245.240.151	STNAMC-02-BR01	TwentyFiveGigE1/0/4	STNAMC-02-FE01
05/23/2024 04:17:54 PM	Deny	Deny_IP_Log-01	23000	BIZ_CORP_Printer	10.240.165.7	137	udp	20215	TDS_Active_Directory_APP48196	10.248.247.120	137	9	10.245.240.151	STNAMC-02-BR01	TwentyFiveGigE1/0/4	STNAMC-02-FE01

Our Journey



2019

First MOB (Medical Office Building) with SD-Access

2020

Main Hospital with ISE

2022

First MOB with SD-Access & Micro-segmentation

2024

10+ MOB & Outpatient centers with SD-Access & Micro-segmentation (125+ Switches with 30,000+ end devices)

2027

Completion of 80 Sites with SD-Access & Micro-segmentation

Simplified Network Architecture

A Tale of two MOBs…

MOB1 - Y2013

MOB2 - Y2023

MOB1 - Y2013		MOB2 - Y2023
8	Switches	8
~3000	End Devices	~3000
8	VRFs	3
64	Subnets	3
No	Roaming	Yes
No	Micro-segment	Yes

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: kangupta@cisco.com

cisco The bridge to possible

Thank you

cisco Live!