

How It's Made: Cisco Secure Access

cisco Live !

John Rauser
Director of Software Engineering

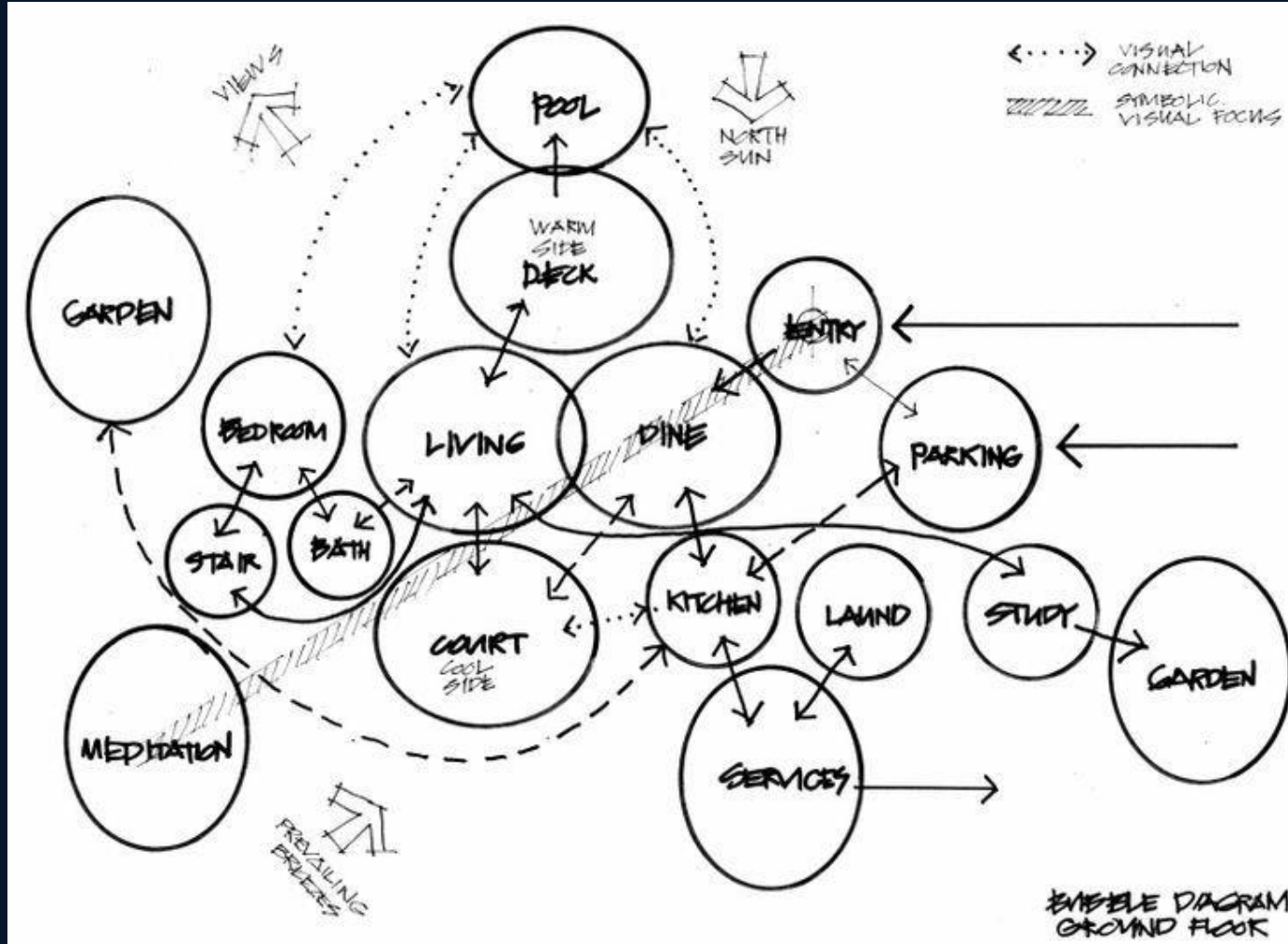


QUALITY
CHECKPOINT

METAL
DETECTOR

HEAT
SHRINK
TUNNEL

Patterns



A Pattern Language

Towns · Buildings · Construction



Christopher Alexander

Sara Ishikawa · Murray Silverstein

WITH

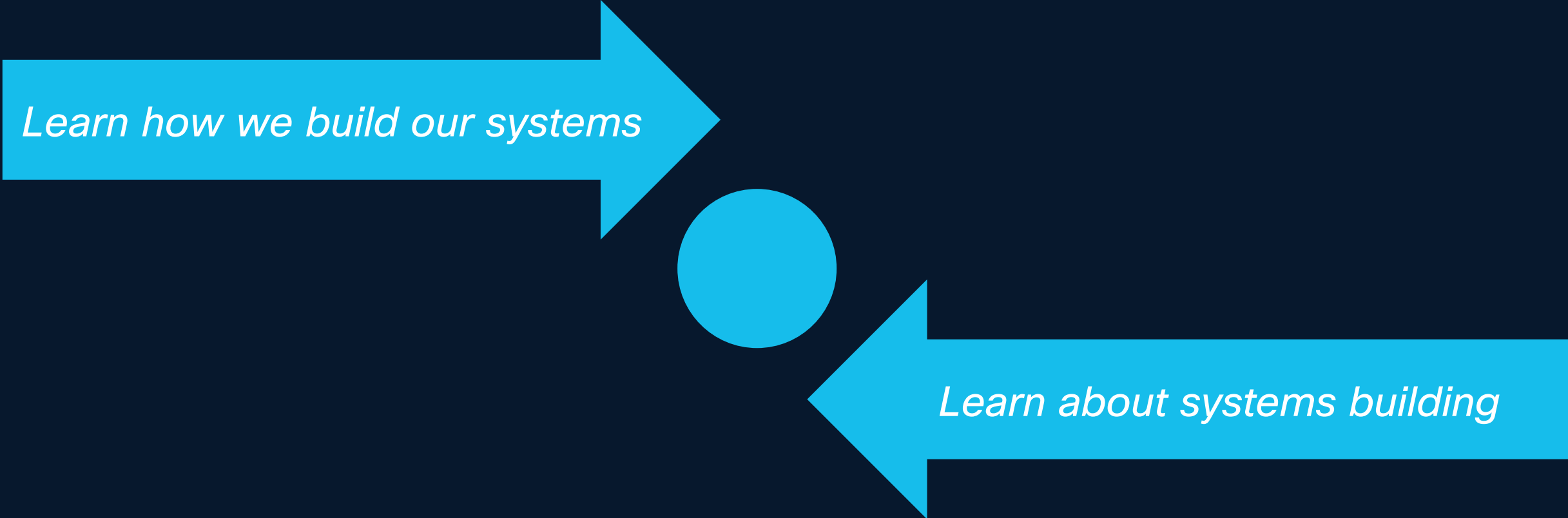
Max Jacobson · Ingrid Fiksdahl-King

Shlomo Angel

Agenda

- 1 Product
- 2 Quality
- 3 Design
- 4 Flow
- 5 Resiliency
- 6 Reliability
- 7 Systems Thinking
- 8 Continuous Learning

Two Goals



Learn how we build our systems

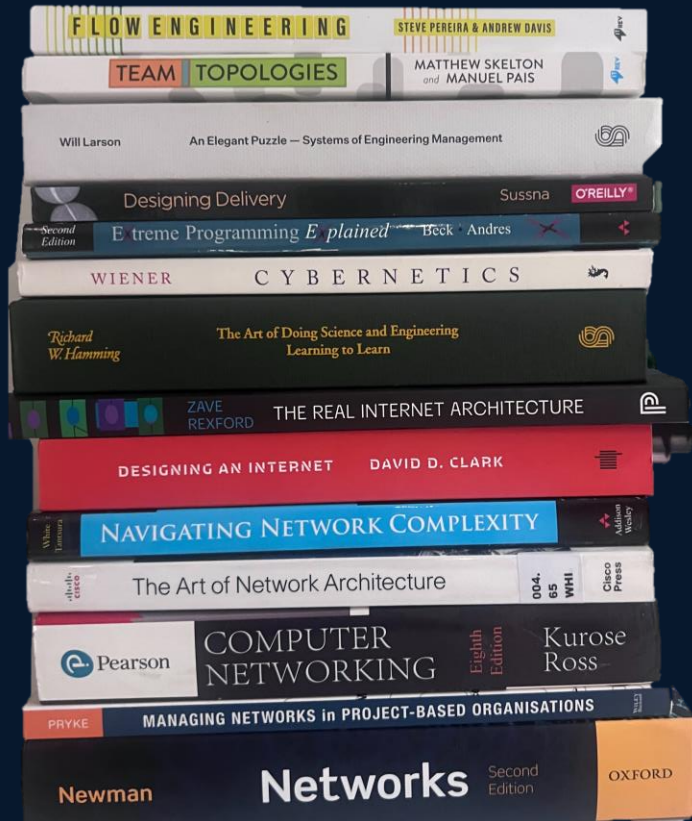
The diagram consists of two large blue arrows pointing towards each other, meeting at a central blue circle. The top arrow points right and contains the text 'Learn how we build our systems'. The bottom arrow points left and contains the text 'Learn about systems building'.

Learn about systems building

Who Am I?

John Rauser

- Director of Software Engineering, Cloud Security
- Working for Cisco for 6 years building high performance, cloud-delivered security solutions
- Developing Zero Trust Access in Secure Access
- Avid reader, speaker, blogger, writer
 - Website: webrauser.com
 - LinkedIn: @jrause



Cisco Webex App

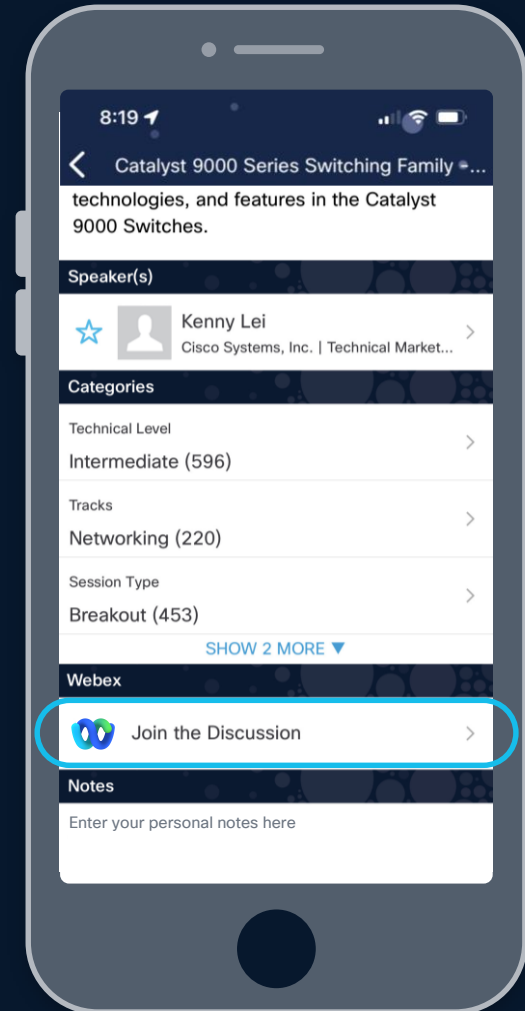
Questions?

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

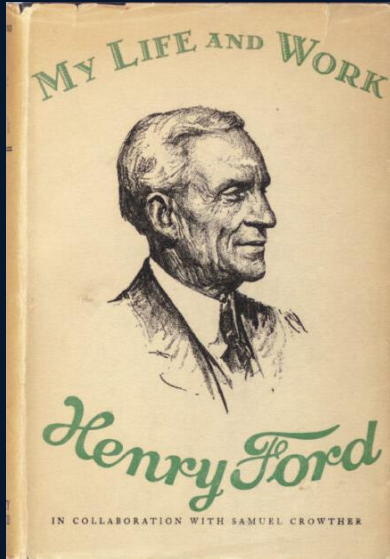
Webex spaces will be moderated by the speaker until June 13, 2025.



Secure Access Sessions!

- BRKCOC-2040: Cisco ITs Journey to SSE – Enabling Hybrid Work with Cisco Secure Access
- BRKSEC-2285: The Latest in Cisco Secure Access (SSE) Innovation
- BRKSEC-1015: Is VPN really dead and replaced by Zero Trust Network Access?
- BRKSEC-2882: Enterprise Browsers and Secure Client
- BRKSEC-2772: AI Driven Operations and Self-Healing Cisco Secure Access
- BRKSEC-2170: Universal Zero Trust with Cisco Secure Firewall
- BRKSEC-3027: Deep Dive into Cisco's Use of QUIC, MASQUE, and OS Native Capabilities to Deliver Frictionless Zero Trust Access

Pattern 1: Product



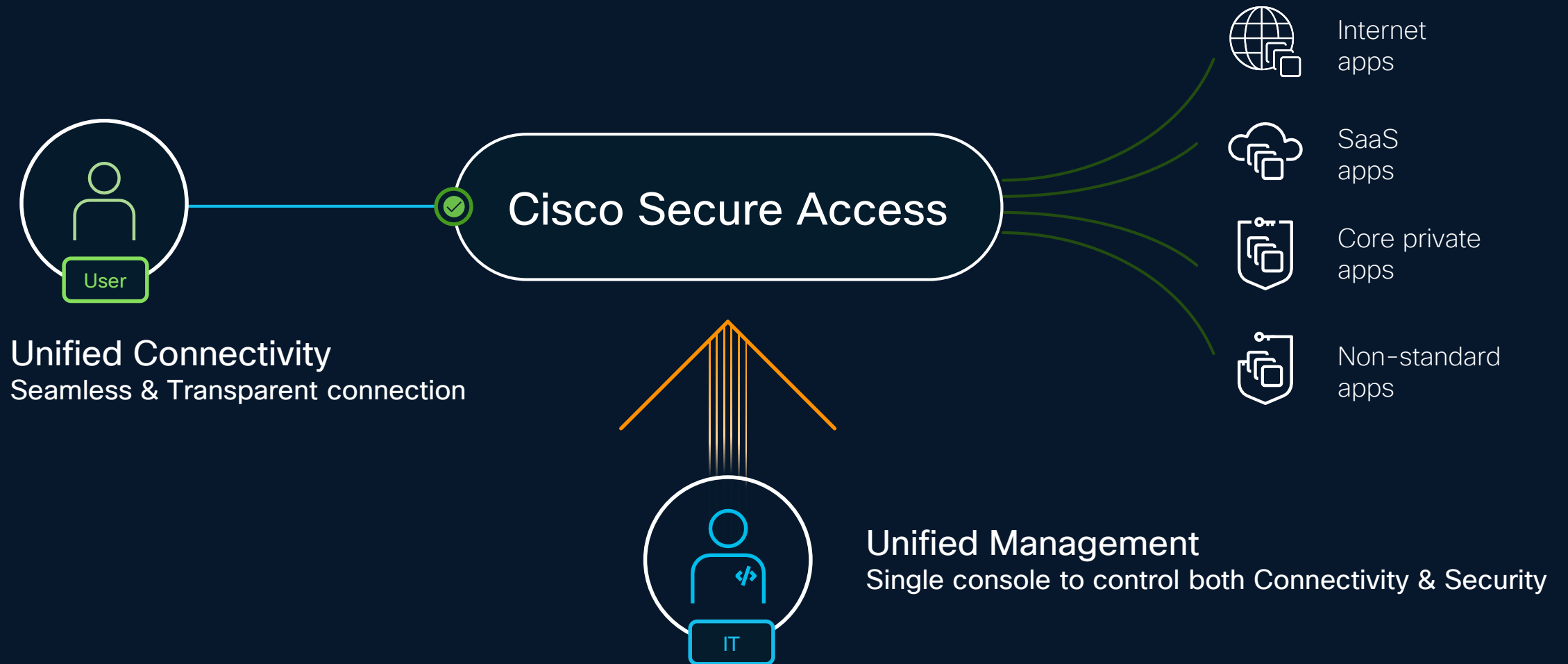
“If I had asked people what they wanted they would have said a faster horse”

Product

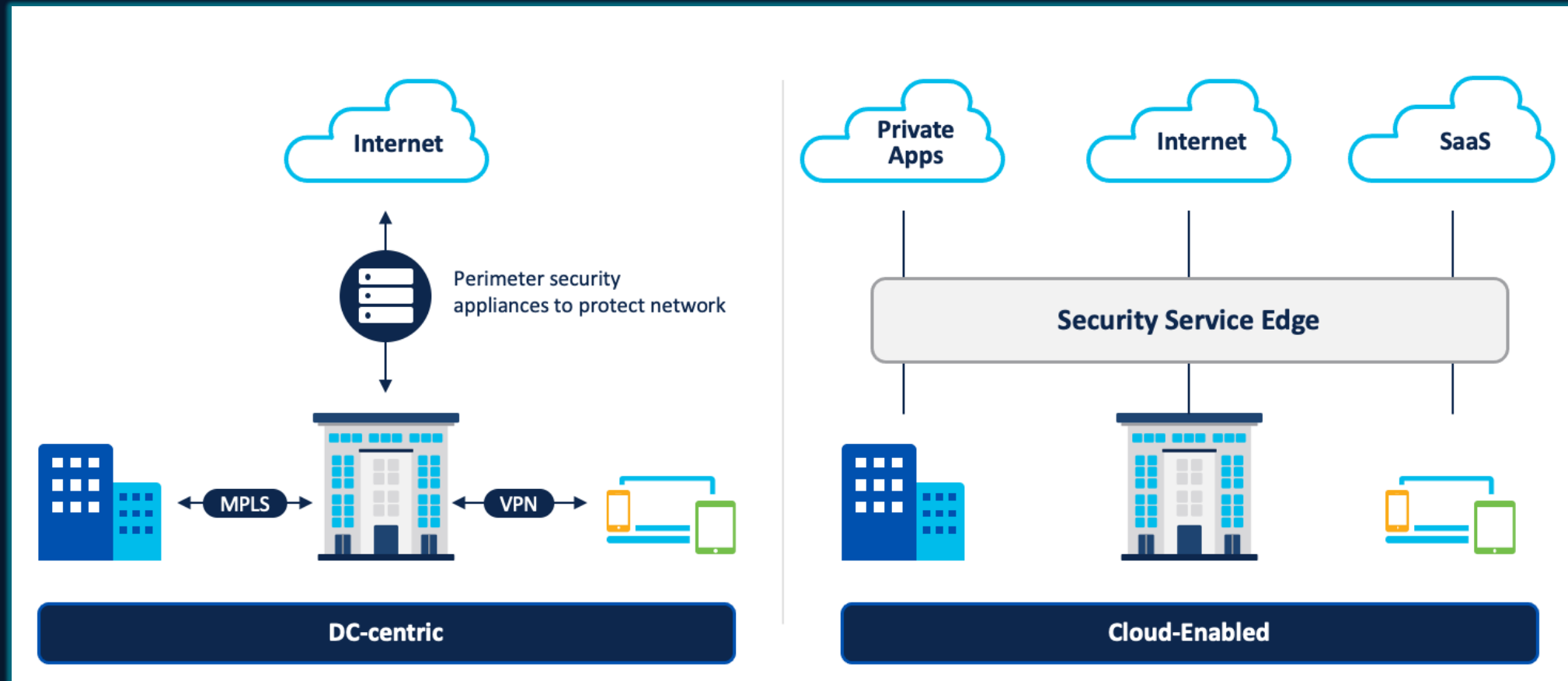
My Life and Work
1928

Cisco Secure Access

Unified Platform

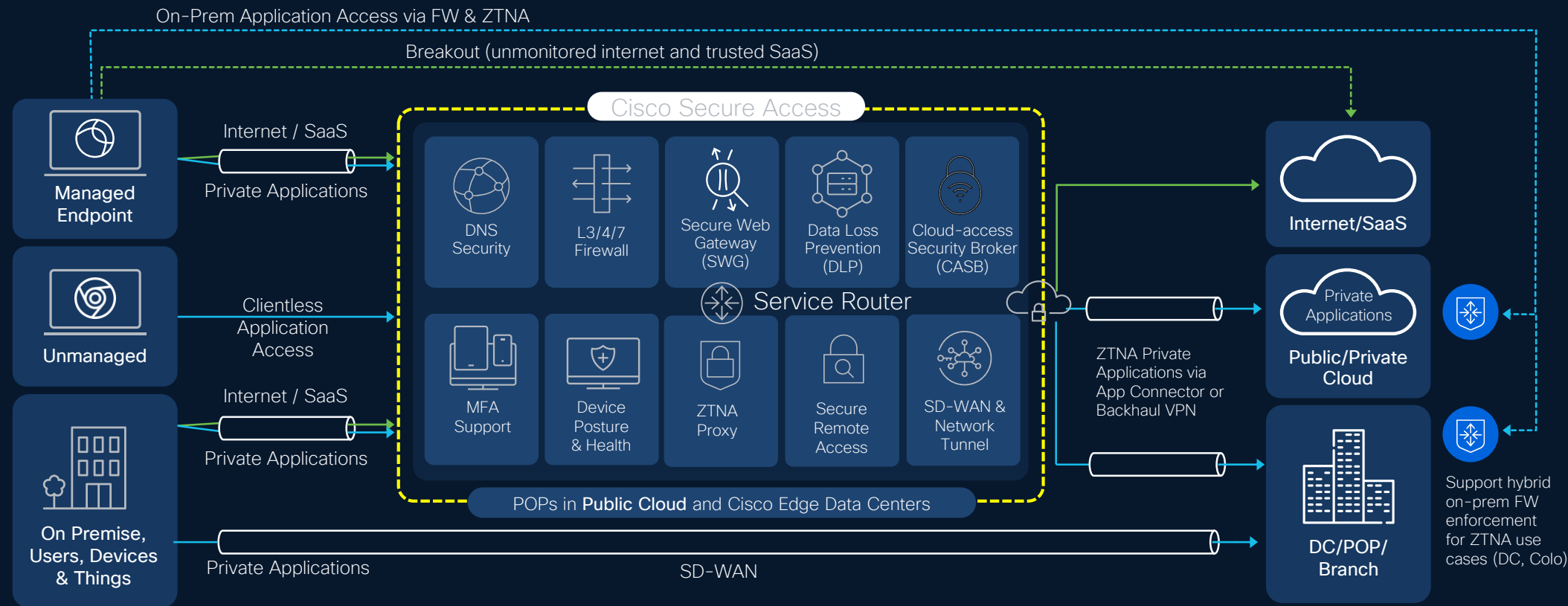


SSE: Network and Security Transformation



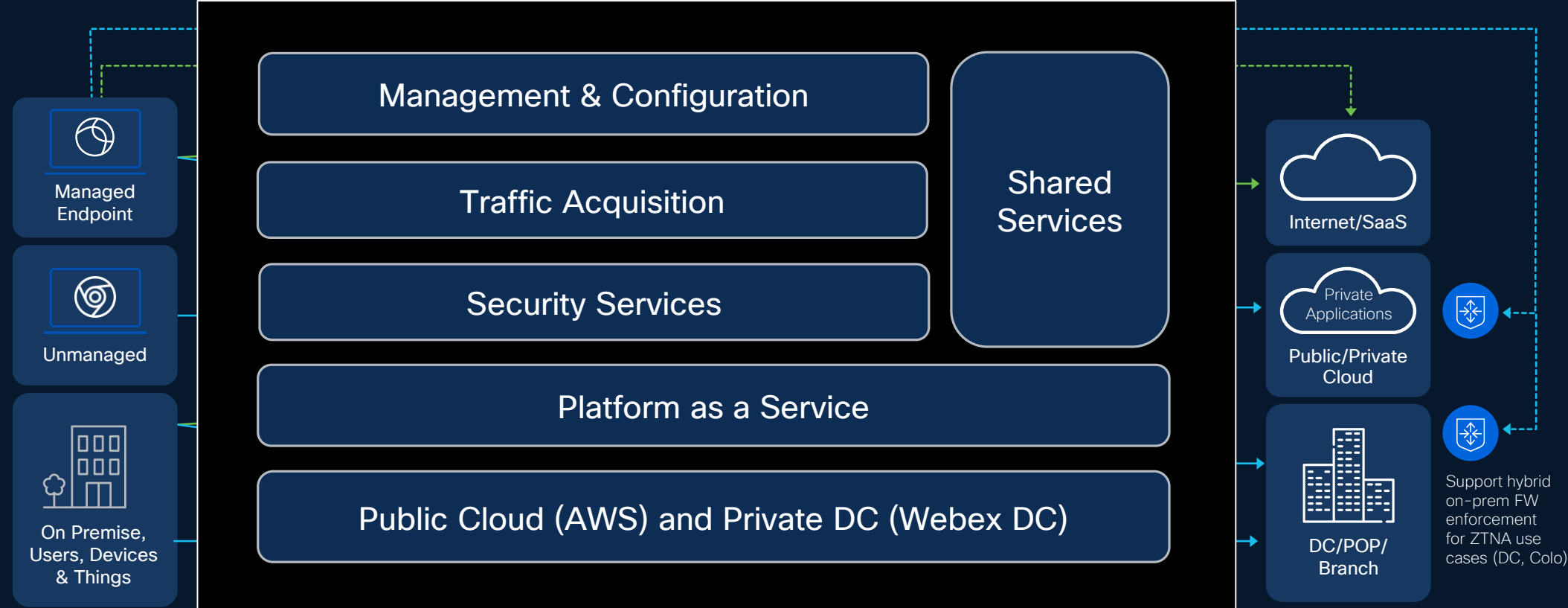
Cisco Secure Access

Overlay security service network with intelligent interconnect

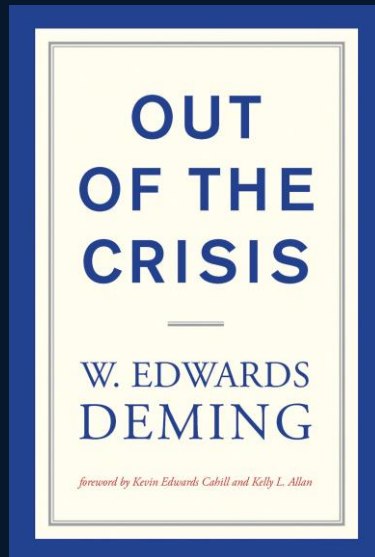
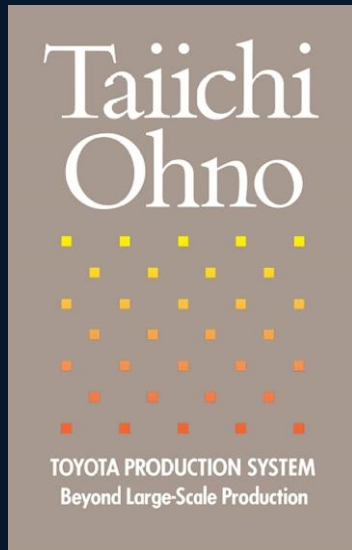


Cisco Secure Access

Overlay security service network with intelligent interconnect



Pattern 2: Quality



“Quality is everyone's responsibility” – Deming

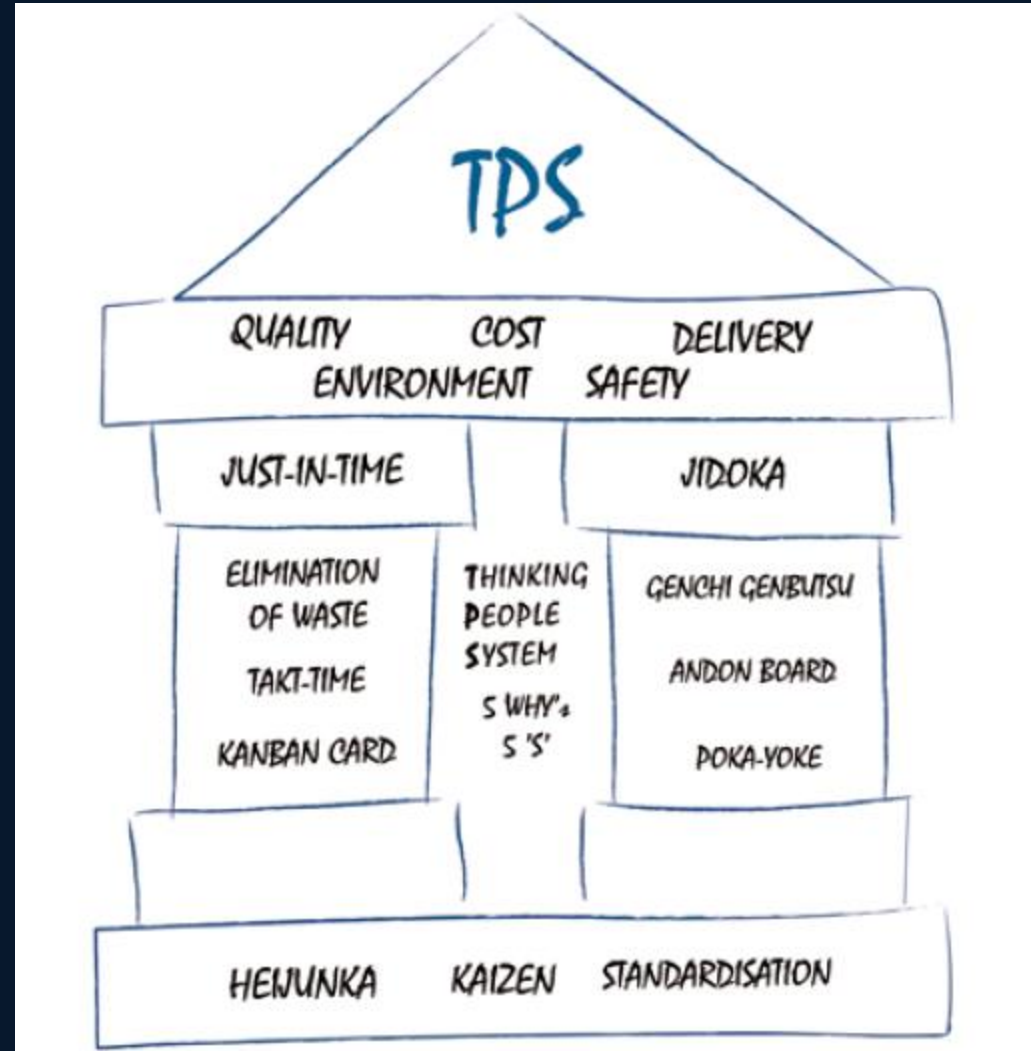
Product

My Life and Work
1928

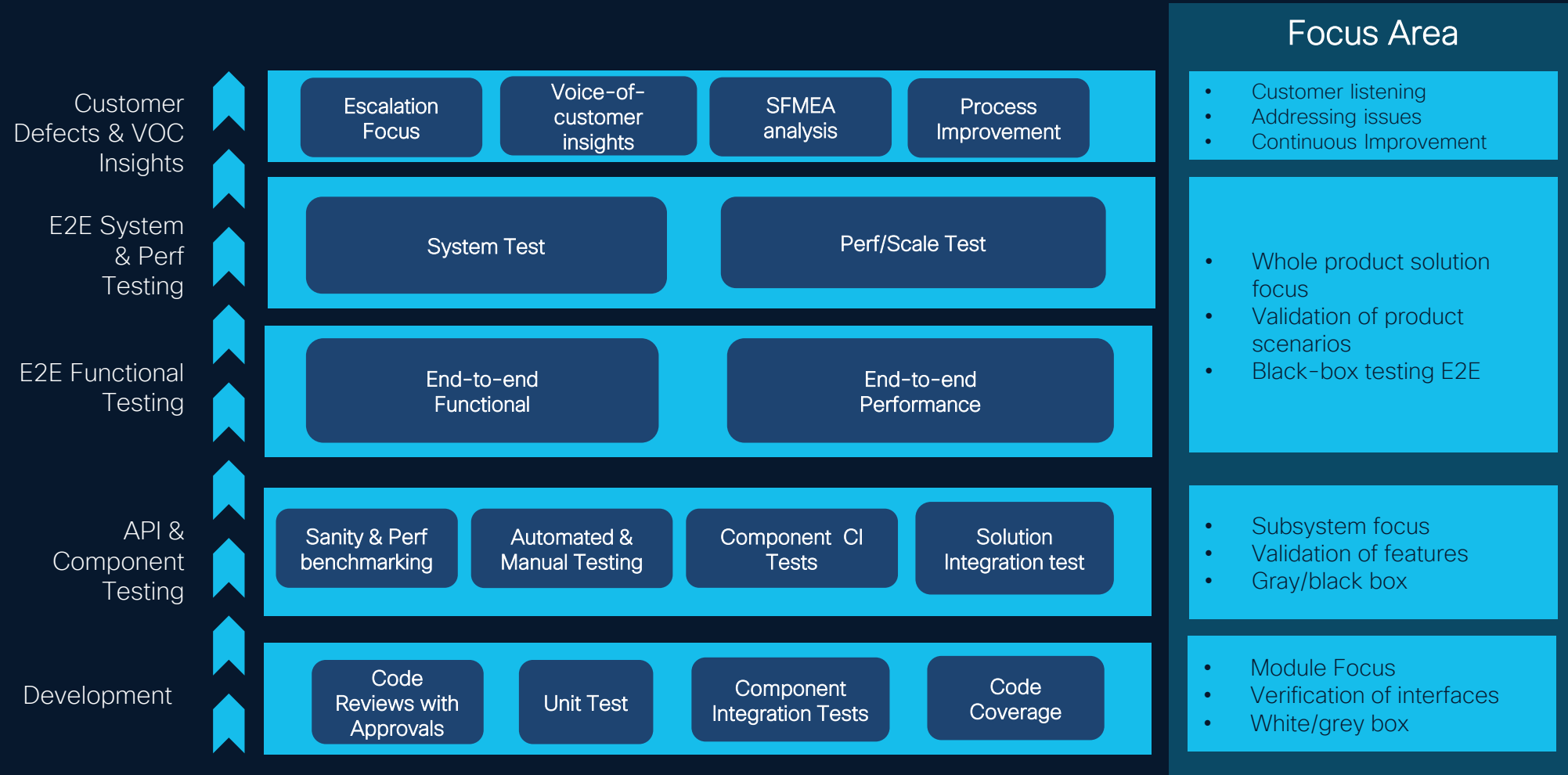
Quality

The Toyota Production System
1945–1980

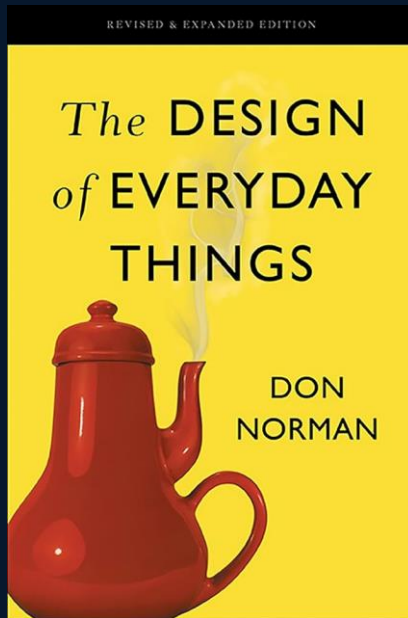
Toyota Production System



Cisco Secure Access – Layered Quality Framework



Pattern 3: Design



“Good design is actually a lot harder to notice than poor design”

Product	-----	<i>My Life and Work</i> 1928
Quality	-----	<i>Toyota Production System</i> 1945-1980
Design	-----	<i>The Design of Everyday Things</i> 1988

Secure Access

John Rauser

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name

Filters

Add Rule

2 Rules

Customize view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
	1	Allow Engineering to OpenAi	Internet	Allow	Any	Generative A...		-	
	2	Genreative AI Block	Internet	Block	Any	None		-	

Rows per page 100 1-2 of 2 1

Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination		-

User Experience

© 2025 Cisco and/or its affiliates. All rights reserved.

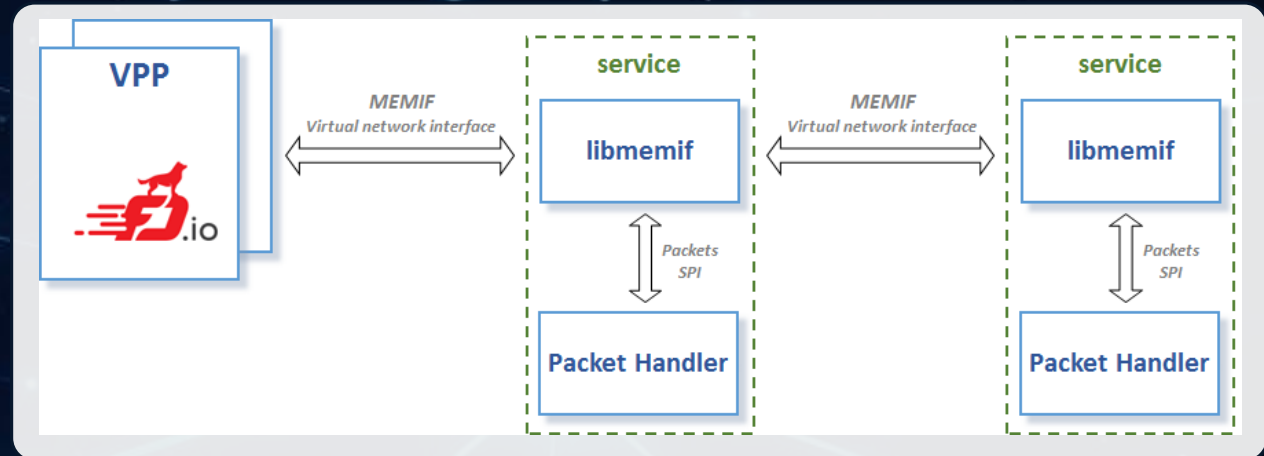
BRKSEC-2885

18

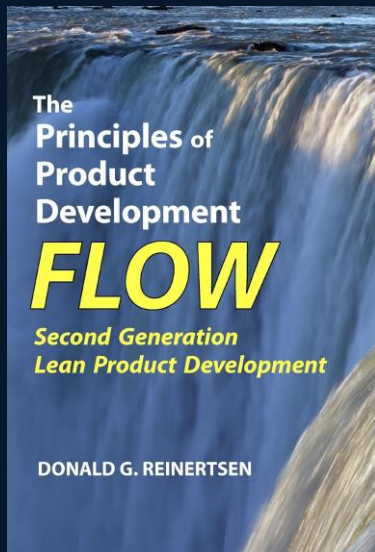
CISCO

Vector Packet Processing

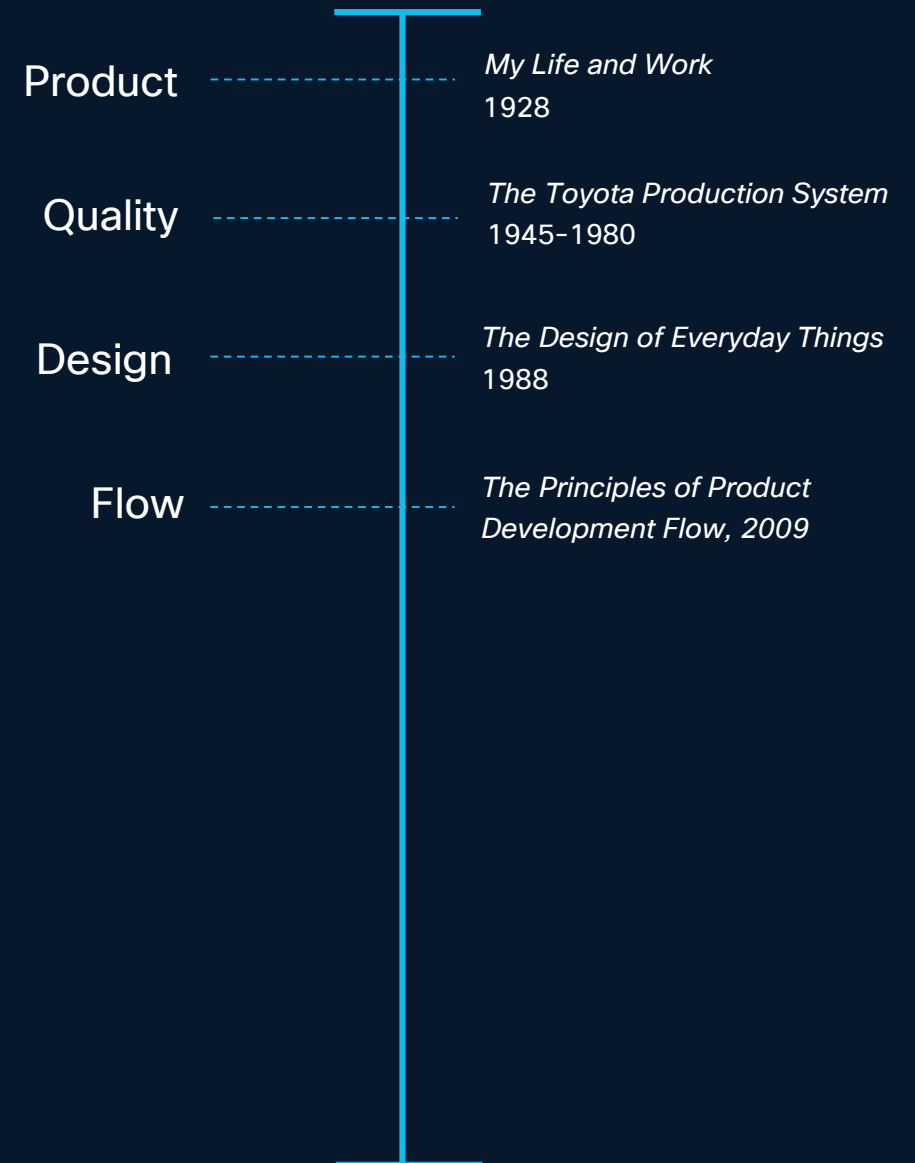
User Space Networking
Vector Processing
Memory Interfaces



Pattern 4: Flow



“Reducing batch size is the single most important change that an organization can make to improve flow”



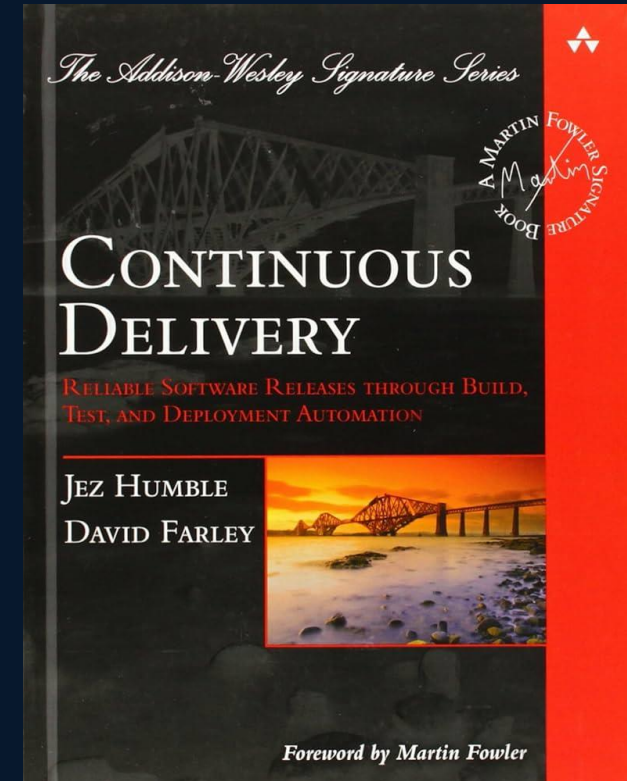
Continuous Delivery

Fundamental to High-Quality Delivery

- Minimizes errors from the interaction of changes
- Allows for fast feedback on changes
- Creates a bounded search for resolving issues

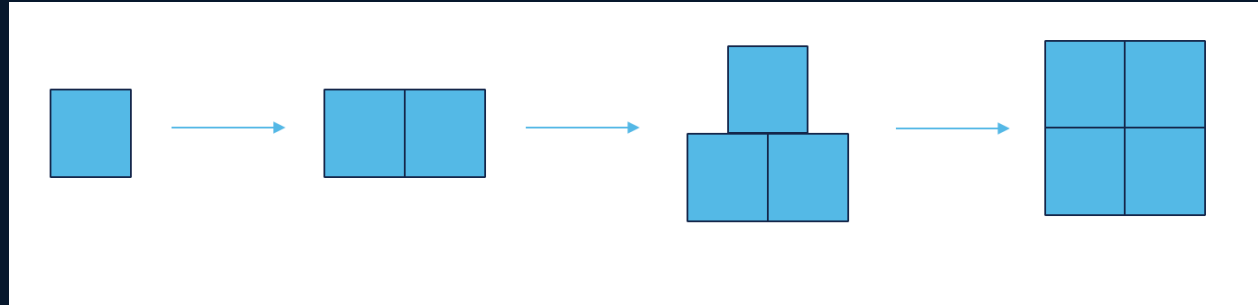
Single piece flow

- Changes are delivered individually
- Each "unit of value" is delivered independently
- Each change flows through the entire pipeline



Continuous Delivery

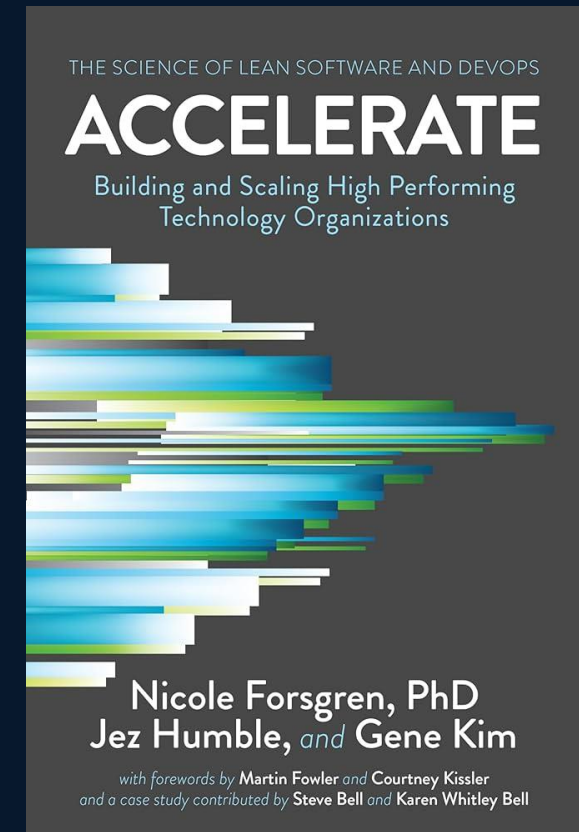
Development is always of moving from *working*, to *working*, to *working*
(no BIG BANGS)



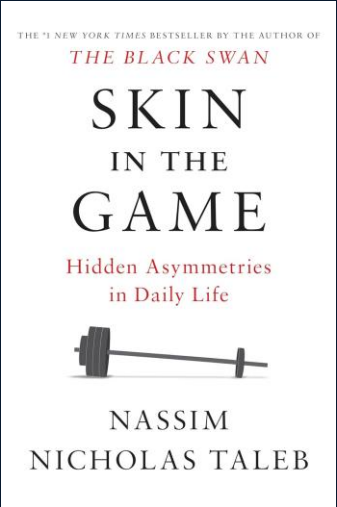
Gall's Law: “A complex system that works is invariably found to have evolved from a simple system that worked.”

Success Metrics (DORA)

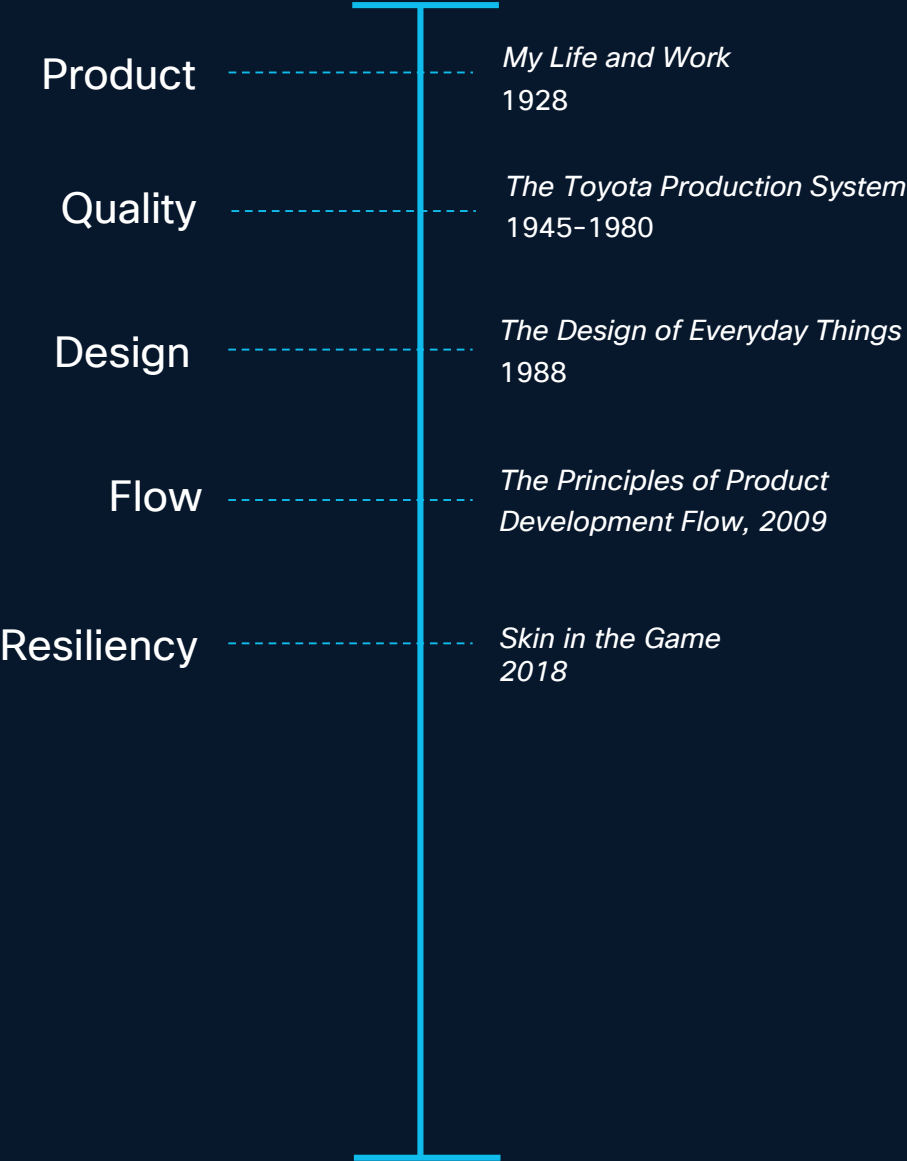
Software delivery performance metric	Elite	High	Medium	Low
Deployment frequency For the primary application or service you work on, how often does your organization deploy code to production or release it to end users?	On-demand (multiple deploys per day)	Between once per week and once per month	Between once per month and once every 6 months	Fewer than once per six months
Lead time for changes For the primary application or service you work on, what is your lead time for changes (i.e., how long does it take to go from code committed to code successfully running in production)?	Less than one hour	Between one day and one week	Between one month and six months	More than six months
Time to restore service For the primary application or service you work on, how long does it generally take to restore service when a service incident or a defect that impacts users occurs (e.g., unplanned outage or service impairment)?	Less than one hour	Less than one day	Between one day and one week	More than six months
Change failure rate For the primary application or service you work on, what percentage of changes to production or released to users result in degraded service (e.g., lead to service impairment or service outage) and subsequently require remediation (e.g., require a hotfix, rollback, fix forward, patch)?	0%-15%	16%-30%	16%-30%	16%-30%



Pattern 5: Resiliency



“Things designed by people without skin in the game tend to grow in complication”



On-call Engineering

- On-call is the cornerstone of everything we do ...
 - creates skin in the game
 - teaches us about our system
 - forces us to own our risk

“You Build it, you run it”

Werner Vogels, 2016

Priorities and Responsibilities

Individual



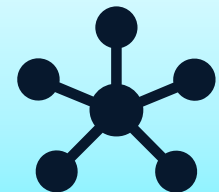
Architectural



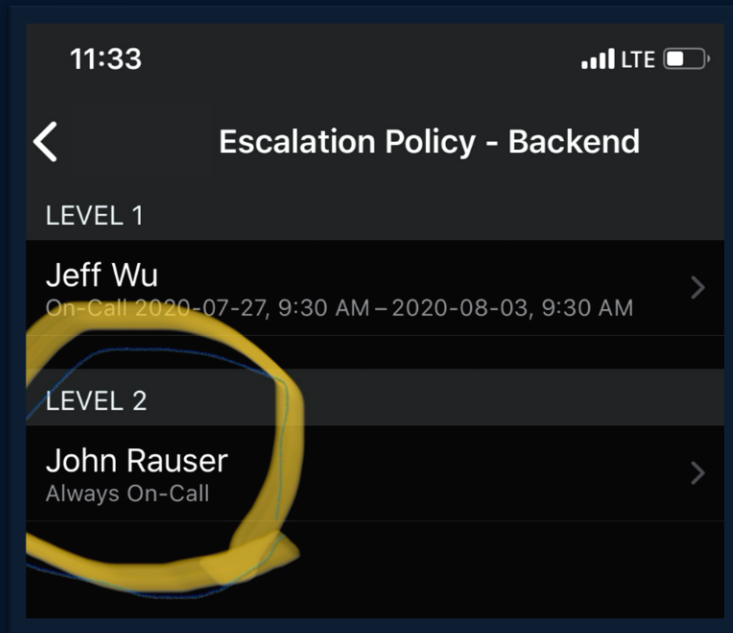
Team



Group



On-call Engineering



Always On-call!



Deployment

CI/CD, build, deploy, staging, rollback, waves, patching, autoscaling, forecasting



Observability

Monitoring, metrics, tracing, measurement, logging, dashboards, alerts, correlation, NOC



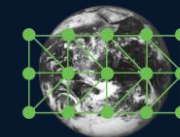
Reliability

End to end testing, performance, capacity, health & trend monitor, availability, toil mgmt



Data Plane

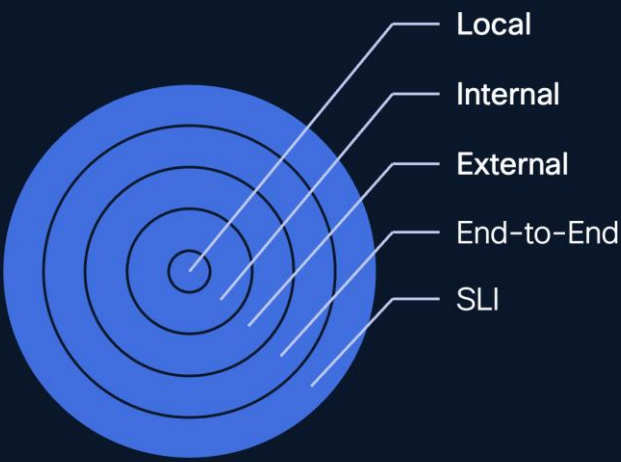
Service chaining, multi-tenancy, DAQ, fault recovery, steering, service discovery



Control Plane

Policy distribution, configuration management, logging & reporting, APIs

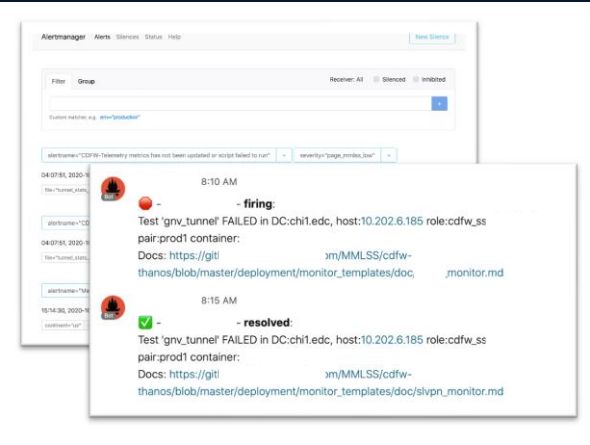
Monitors



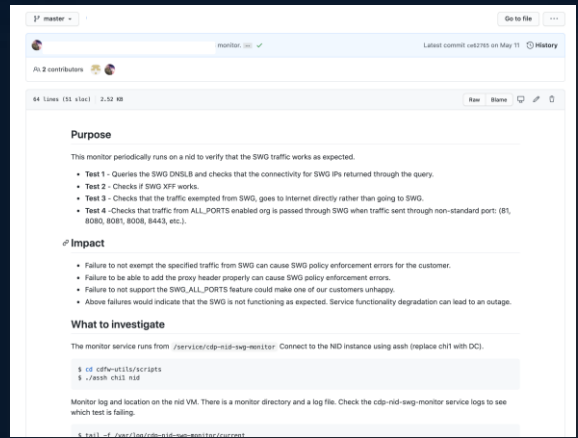
Logs & Metrics



Alerts



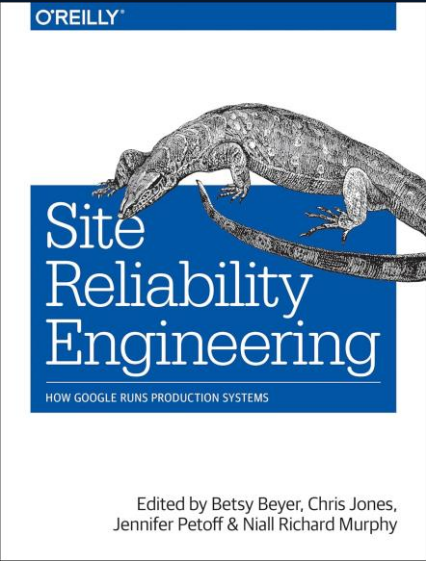
Runbooks



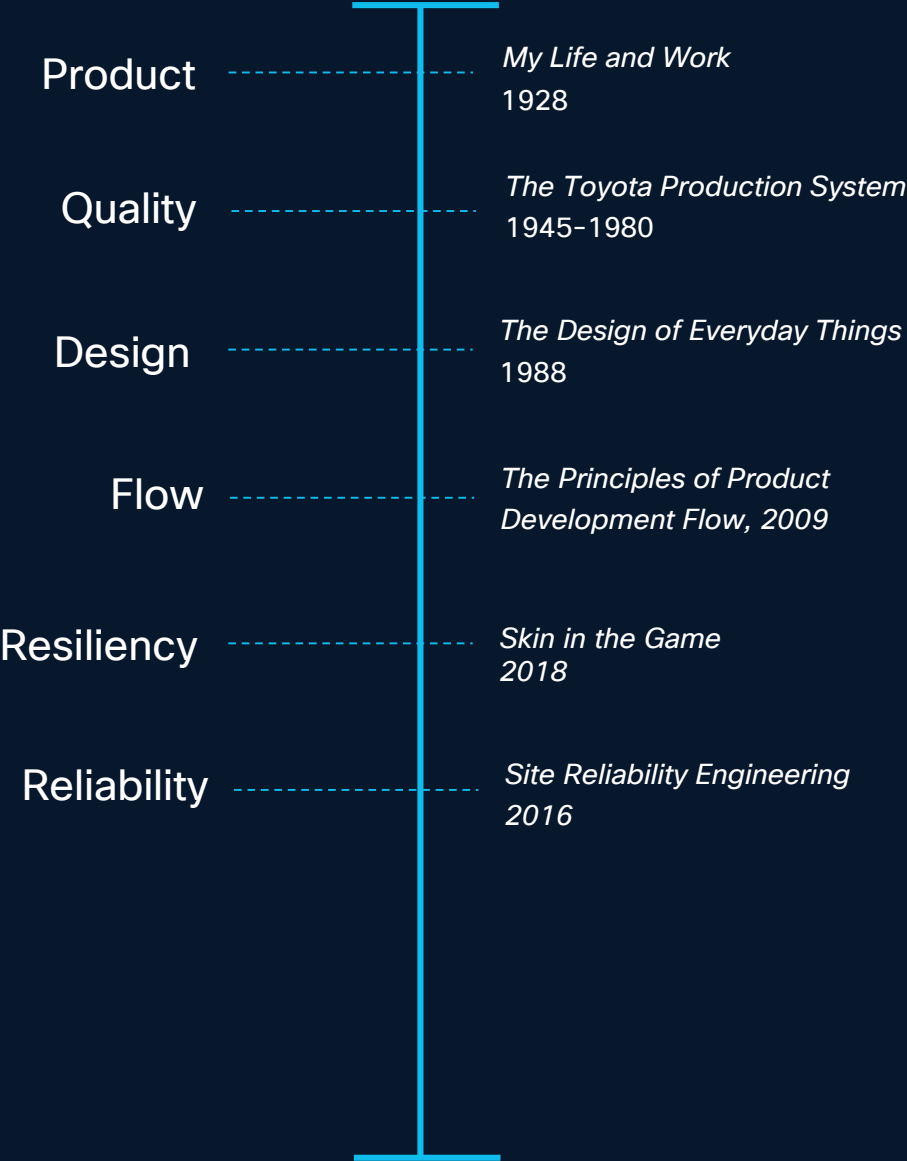
How AI is Changing This

- Tests & Monitors
 - Allows us to extend our coverage
- Logs & Metrics
 - Agents are helping to correlate and understand signals
 - Much quicker time to detect and time to resolve
- Alerts & Runbooks
 - Agents are taking over the initial step of gathering context
 - Recommending actions and remediations for us to take

Pattern 6: Reliability



"Hope is not a strategy."



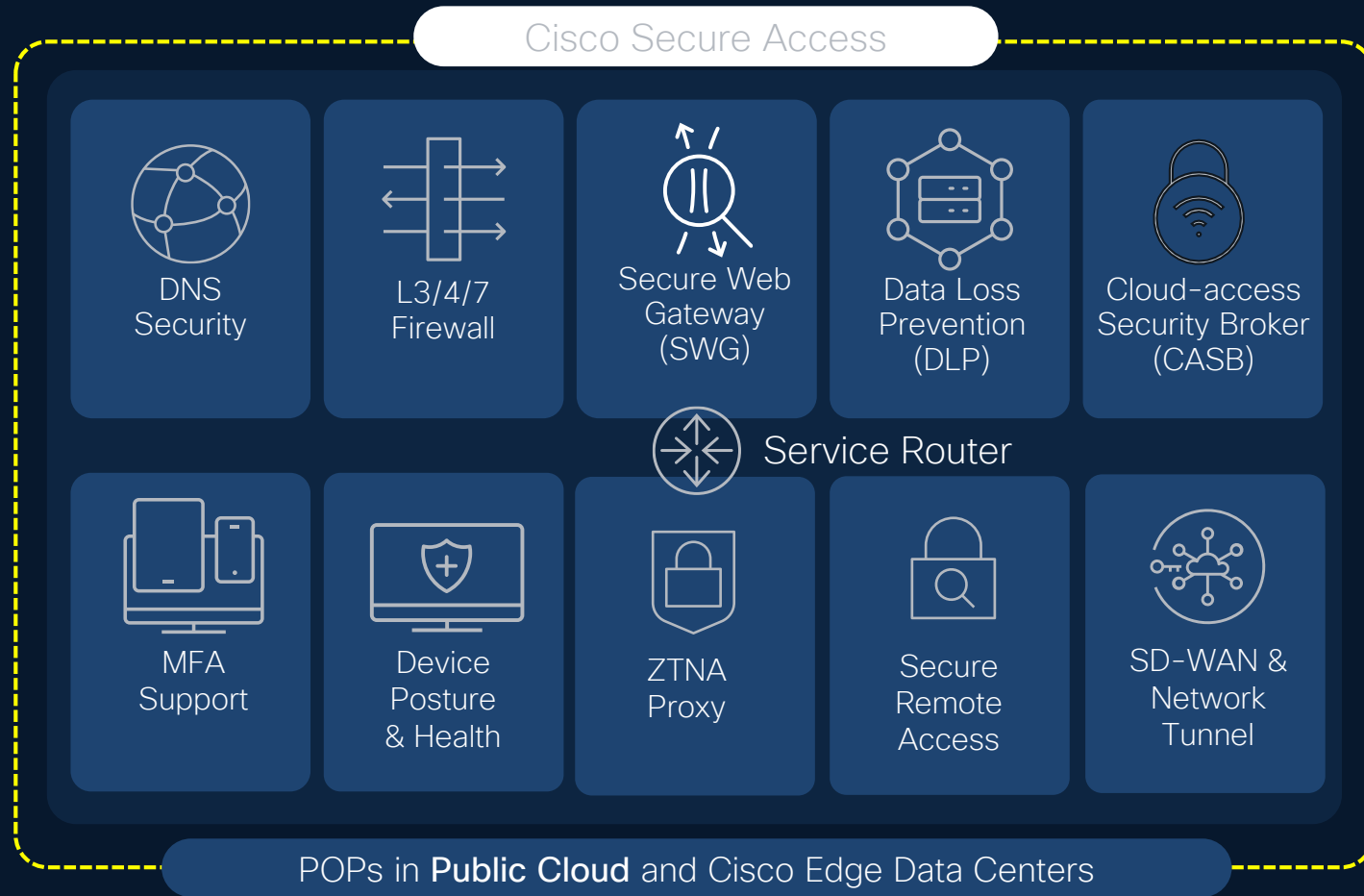
Site Reliability Engineering

Automation

Capacity

Tooling

Practices



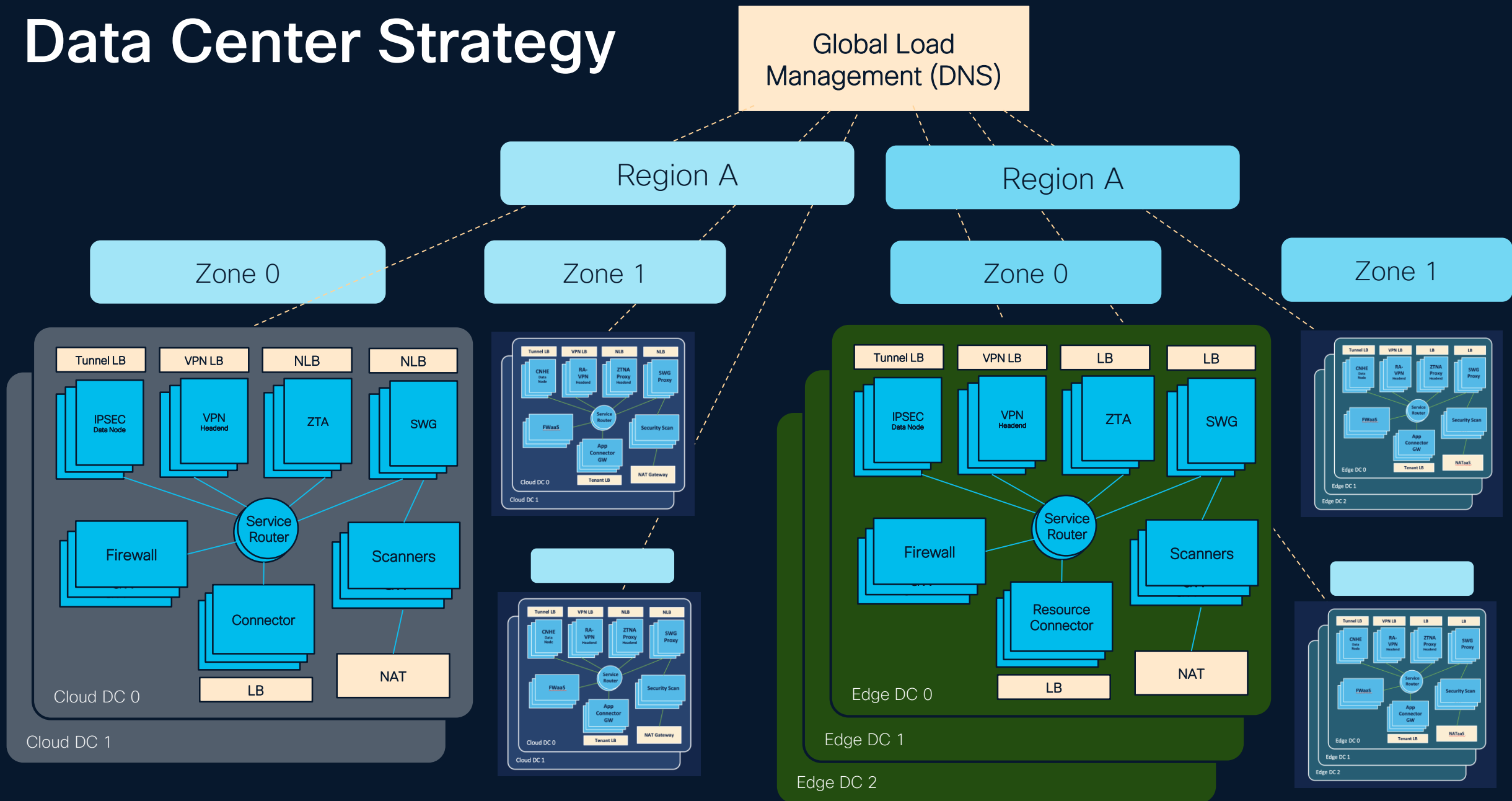
Deployments

SLIs / SLOs

Region Buildouts

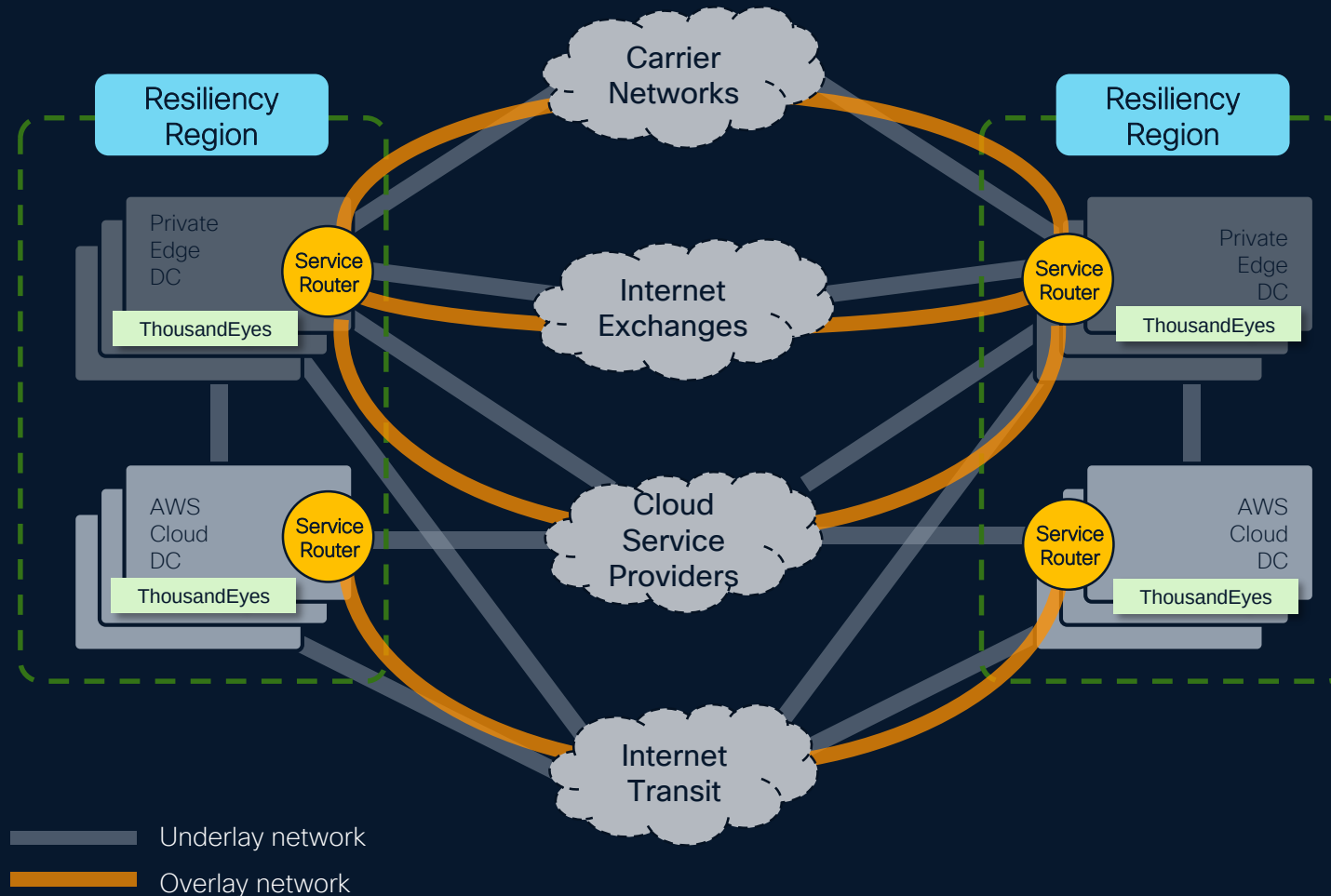
Experience Monitoring

Data Center Strategy

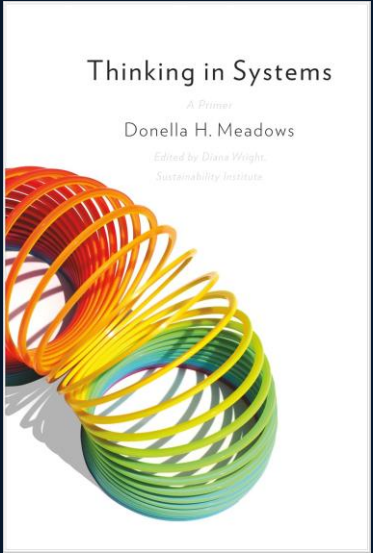


Global Scale Backbone

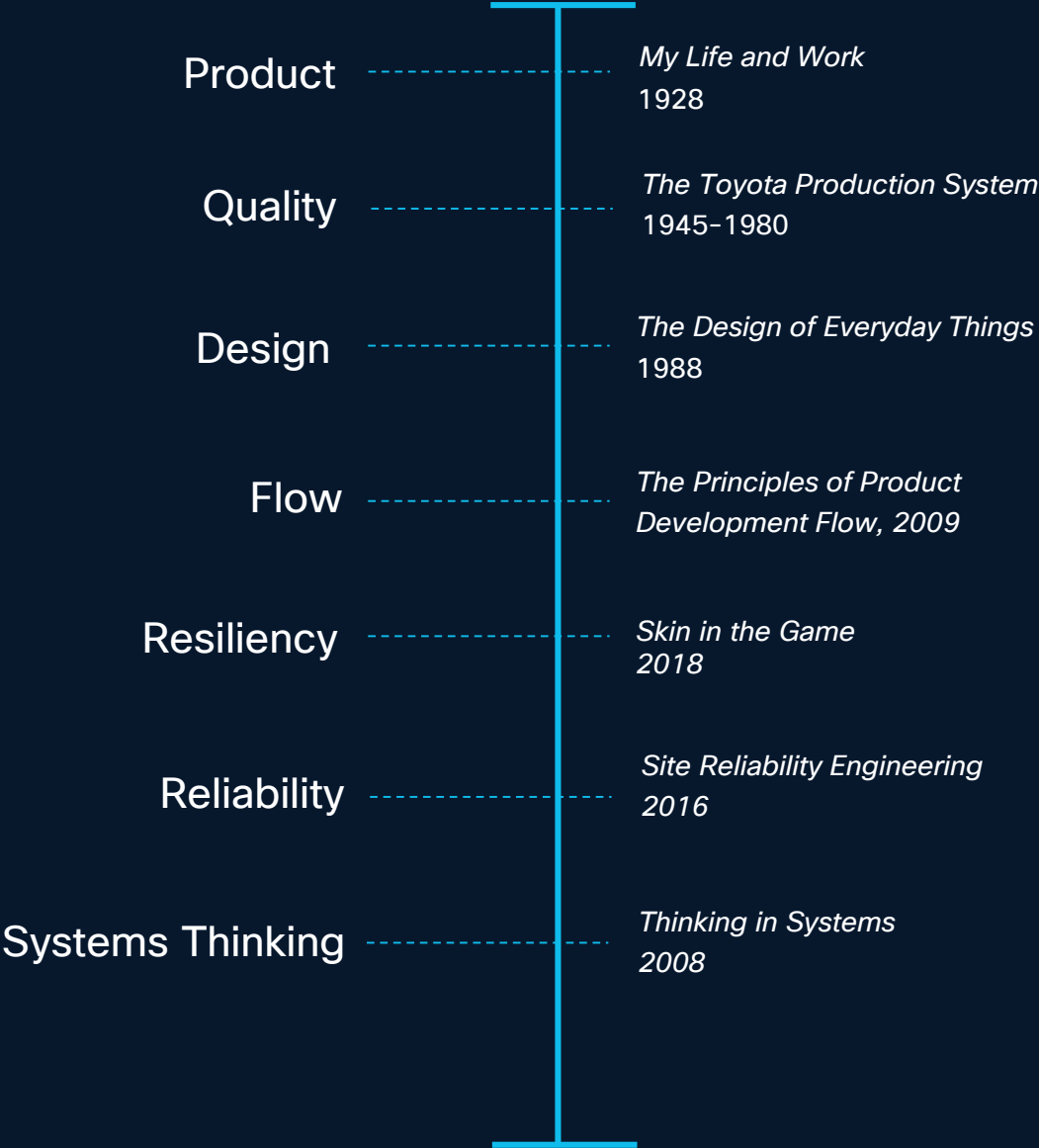
Connecting users and apps from anywhere to anywhere,
with low latency and high availability



Pattern 7: Systems Thinking

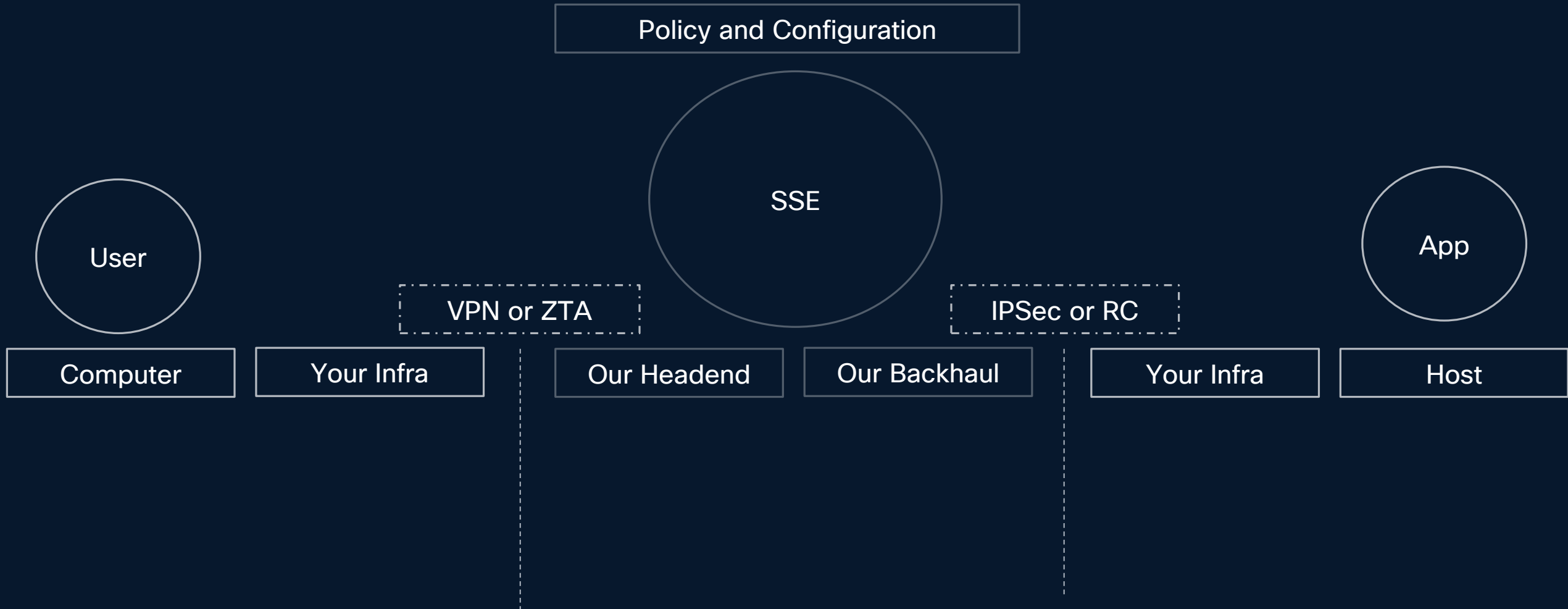


“The world is a continuum. Where to draw a boundary around a system depends on the purpose of the discussion”



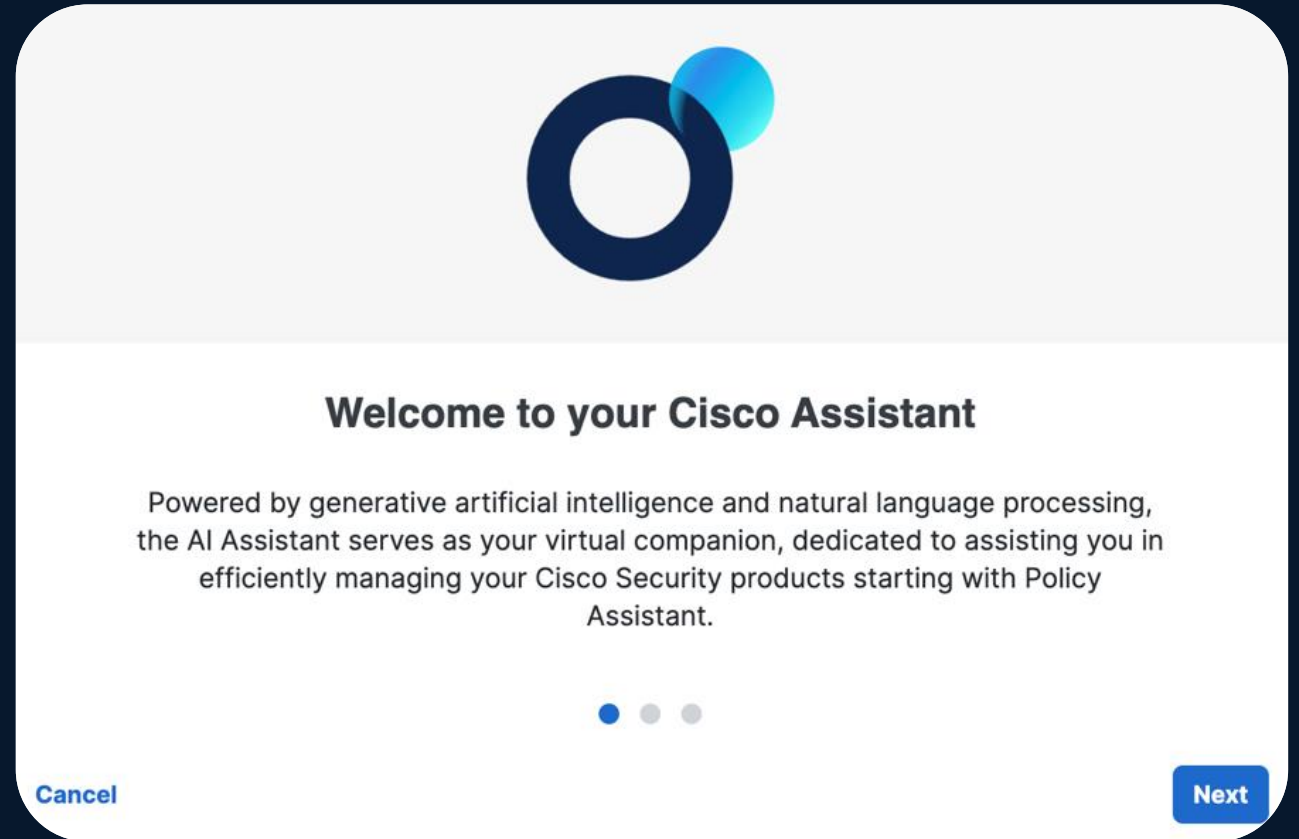
Troubleshooting

Narrowing down the problem across the system



The AI Assistant

- Policy Creation
- Documentation Summarization
- Experience Insights
- Troubleshooting



Troubleshooting Assistant

Cisco AI Assistant

You

Why can't Solomon access netx-private-app?

AI Assistant

Verify settings in the event details section and then click Analyze event.

Event details

Sources:

solomon huang (solhuang@...)

Destinations:

netx-private-app

Connection Type:

ZTA

Device type:

All Device Types

Devices:

solhuang-tia

Analyze event

Add a rule or ask the AI Assistant a question

The AI Assistant may make mistakes. Confirm information by reviewing the source.

ZTA Access failure analysis

1 Issue and 2 Warnings

9/9 checks

Device Enrollment

The user Solomon is successfully enrolled for Zero Trust device enrollment in the network.

System Resources

Network Connectivity

Resource Reachability

Network Connections

App Access

Warning

User Access

Warning

Policy

Issue

There was a blocked event. The ZTNA block reason is: "failure in connection to DNS server."

Navigate to Activity Search for Client Based ZTA

DNS

Experience Insights Assistant

Edit default test target

Synthetic tests allow you to identify performance issues with user journeys to destinations. Change the default test target that will apply to all endpoints and view the results in various dashboards. You chose the default target during onboarding.

Zero Trust Access

RAVPN

SWG Roaming Module

Custom target

Target type

Private resource

zta-private-app (10.207.47.48:80)

Choose a VPN or ZTA private resource.

Public application

Port

80

Test interval

1 minute

Determines the data refresh rate on dashboards.

Network traffic calculator (optional)

Ensure your network can support the maximum throughput for private resources considering the number of endpoints that will be registered. For high traffic management strategies, see [Help](#).

Registered endpoints

Estimated maximum throughput ⓘ

25

Calculate

25 KB/s

Cancel

Save

AI Assistant

Event Analysis:

Based on the information provided, here are the possible failure reasons why **Rusty Shackleford** cannot access **CHCLASEN-DC**:

- Failure in connection to the DNS server preventing Rusty Shackleford's access to CHCLASEN-DC.
- ZTA enforcement blocked the attempted connection for policy reasons.
- ZTA DNS issue causing Rusty Shackleford's inability to access CHCLASEN-DC.
- Rusty Shackleford was blocked access to CHCLASEN-DC 90 times due to the reason "User is not allowed access to this application".

Note that these are possible reasons only, and further investigation may be required to determine the exact cause.

ZTA Access failure analysis

1 Issue and 2 Warnings

9/9 checks

✓

Device Enrollment

✓

System Resources

The device associated with Rusty Shackleford, 'Win11-2', is not configured in Experience Insights. Therefore, I am unable to retrieve system resource data for this device.

✓

Network Connectivity

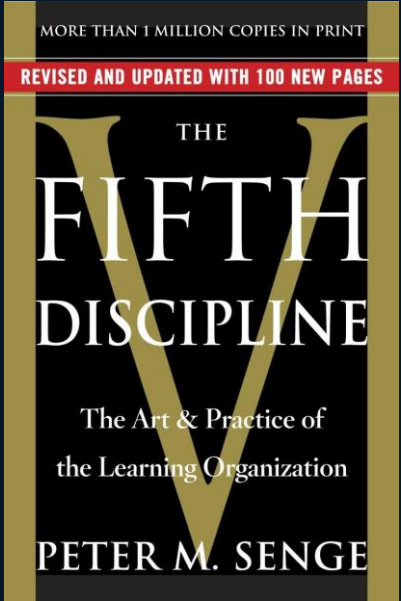
The device associated with Rusty Shackleford, identified as 'Win11-2', is not configured in Experience Insights. Therefore, I am unable to retrieve network status data for this device.

© 2025 Cisco and/or its affiliates. All rights reserved.

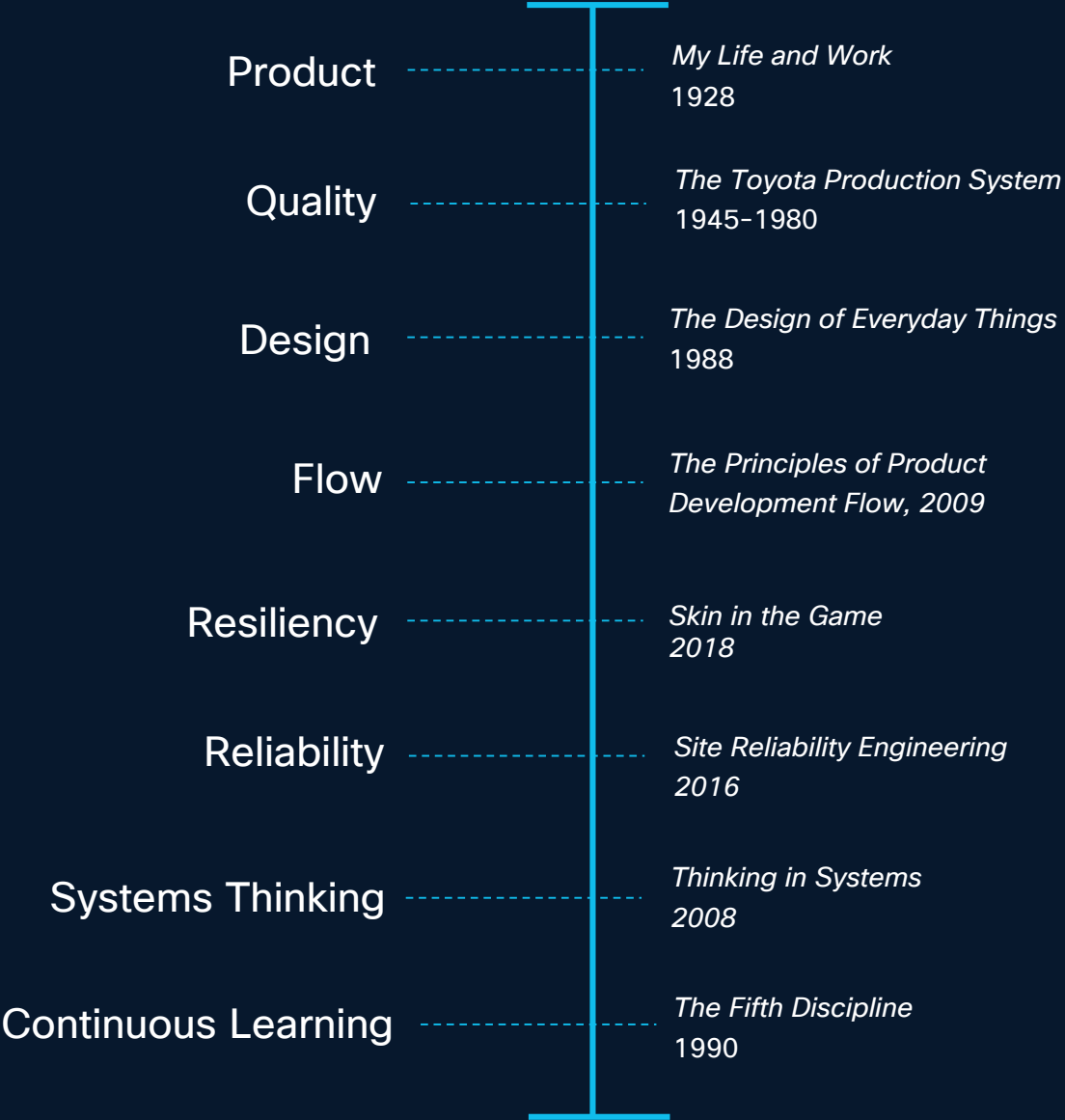
BRKSEC-2885

37

Pattern 8: Learning

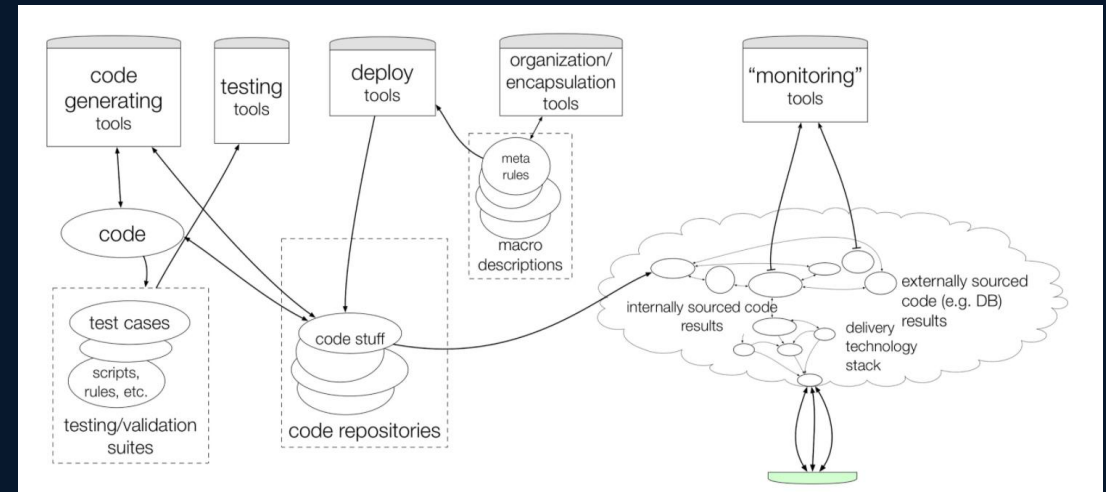
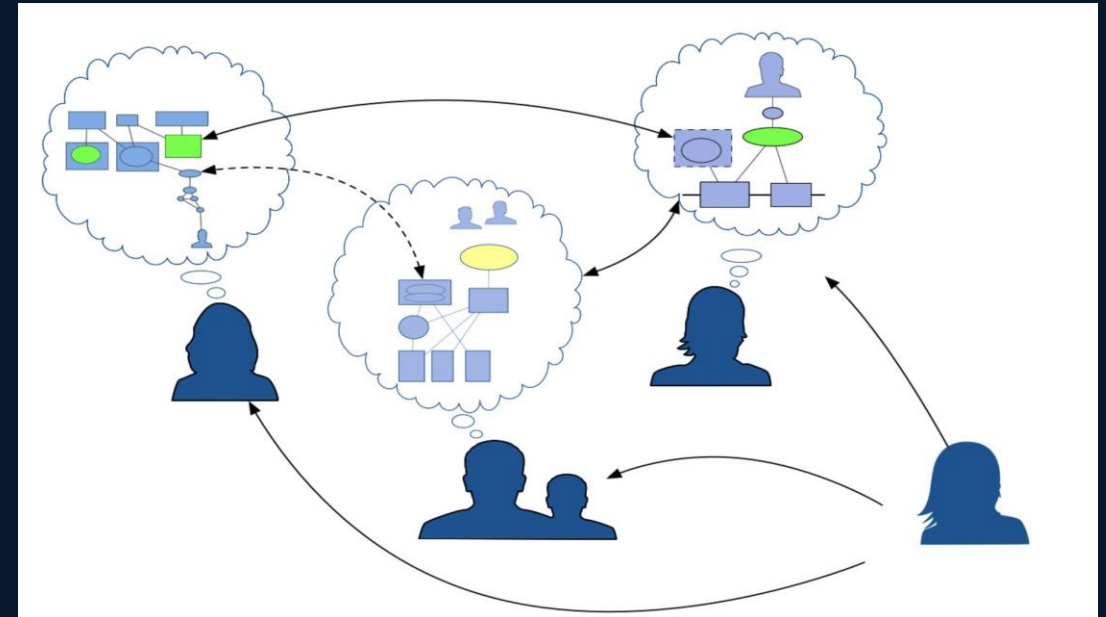


“A learning organization is a place where people are continually discovering how they create their reality. And how they can change it.”



Incidents

- Incident Response is a muscle that the org needs to constantly exercise
- Incident Analysis as a skill that an organization learn and develop
- Two sides of the system:
 - The system and what went wrong
 - The people and what they understood
- Two analytical approaches:
 - Root Cause Analysis (RCA)
 - Learning From Incidents (LFI)
 - John Allspaw, Dr. David Woods

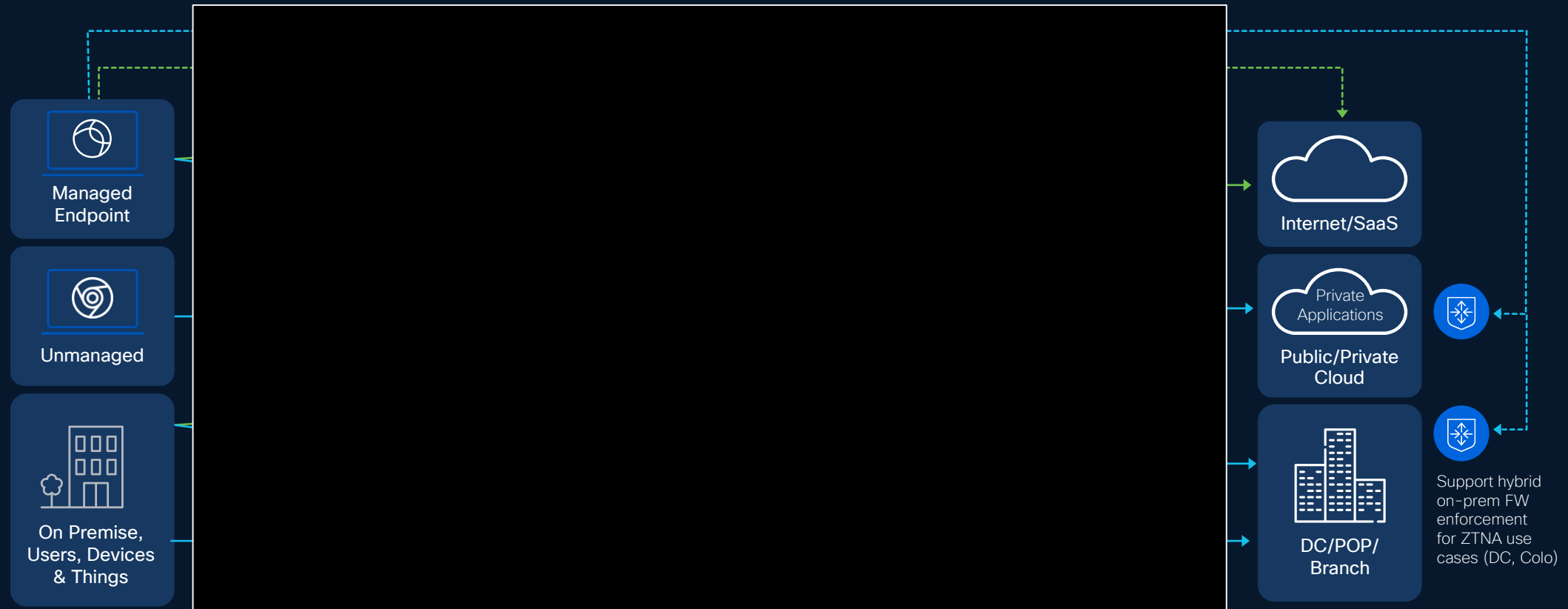


<https://snafucatchers.github.io>

Conclusion

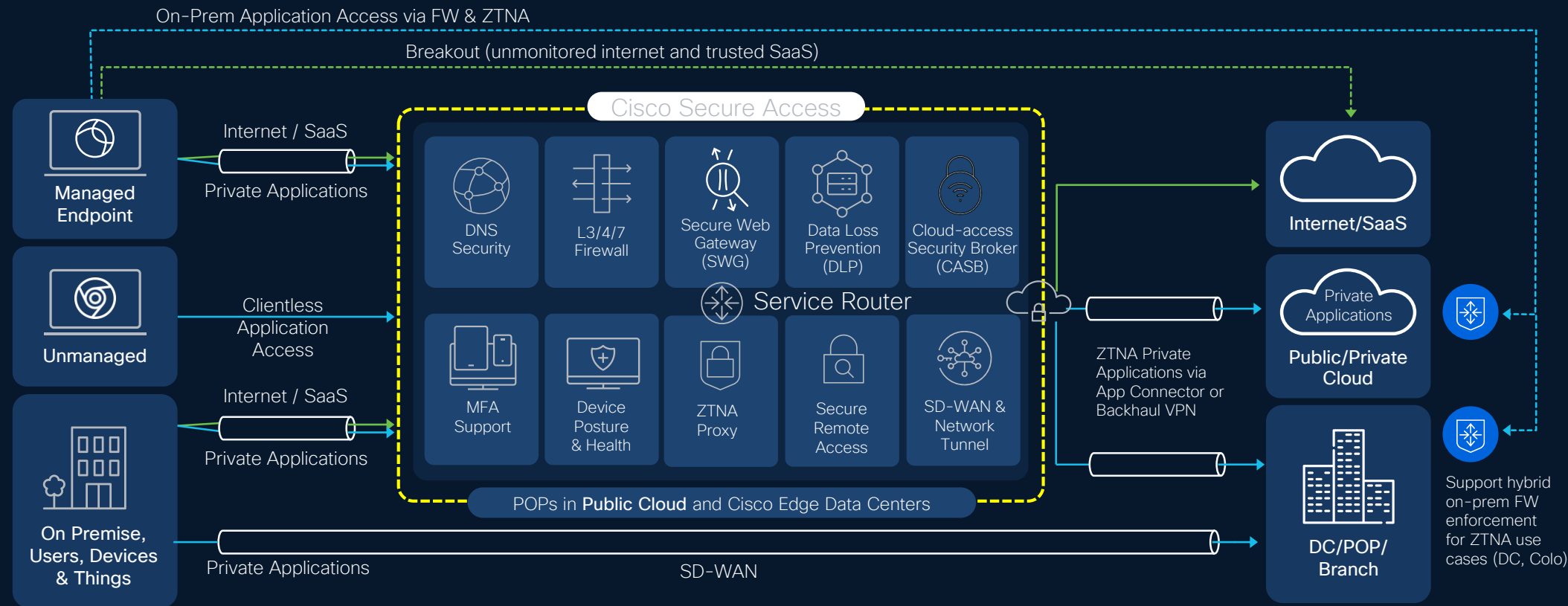
Cisco Secure Access

Overlay security service network with intelligent interconnect



Cisco Secure Access

Overlay security service network with intelligent interconnect



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 2026.



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:

Email: jrauser@cisco.com

LinkedIn: @jrause

Thank you

CISCO Live !

