CISCO Connect

Le réseau d'accès : Premier rempart d'une stratégie Zero-Trust

Jérôme DURAND
Solutions Engineer Networking - CISCO

Jeremy KESSLER
Senior CyberSecurity Architect - CISCO

Sébastien CIELOCH
Administrateur Réseau - LIEBHERR

21 mai 2026

Agenda

La sécurité fusionnée au réseau
Pourquoi ?

La sécurité fusionnée au réseau
Comment ?

Sébastien CIELOCH
Témoignage LIEBHERR

La sécurité fusionnée au réseau
Pourquoi ?

Souvenez-vous... en 2017

Hackers stole a casino's high-roller database through a thermometer in the lobby fish tank

Et depuis...

Data from charities stolen in ransomware attack

North London school closed due to cyber attack

School IT network held to ransom in cyber attack

RANSOMWARE

Southern Water customers hit by cyber attack

Spider-Man 2 maker angered by massive hack

Weeks of disruption after council 'cyber incident'

SUPPLY CHAIN ATTACKS

SPYWARE/MALWARE

DATA/IP THEFT

Cyber attack affecting museum's system one year on

Poland investigates cyber-attack on rail network

British Library's hacked customer data on dark web

MALVERTISING

UNPATCHED SOFTWARE

Health board fears hackers have stolen patient data

MAN IN THE MIDDLE

ROGUE SOFTWARE

DRIVE BY DOWNLOADS

Cyber-attack on electoral registers revealed

'Worrying precedent' as hackers target water firm

Council facing 10,000 cyber attacks a day

BOTNETS

Cyber attack continues to hit NHS trust's services

WIPER ATTACKS

DDOS

Scottish university targeted by cyber attackers

CREDENTIAL COMPROMISE

NHS IT supplier held to ransom by hackers

Australia phones cyber-attack exposes personal data

Nato investigates hacker sale of missile firm data

ADVANCED PERSISTENT THREATS

PHISHING

Network complexity is increasing security risk

Identities are changing

Explosion of IoT, OT, and unmanaged devices raises risk of lateral movement

Workloads are everywhere

Remote work, SaaS, and cloud adoption erode the traditional security perimeter

Threats from AI are here

Rise of AI-powered attacks overwhelm network and security teams

MORE USERS. MORE DEVICES. SMARTER THREATS.

What's happening in the workplace?

1:5

1:5 managed to **unmanaged endpoint ratio**

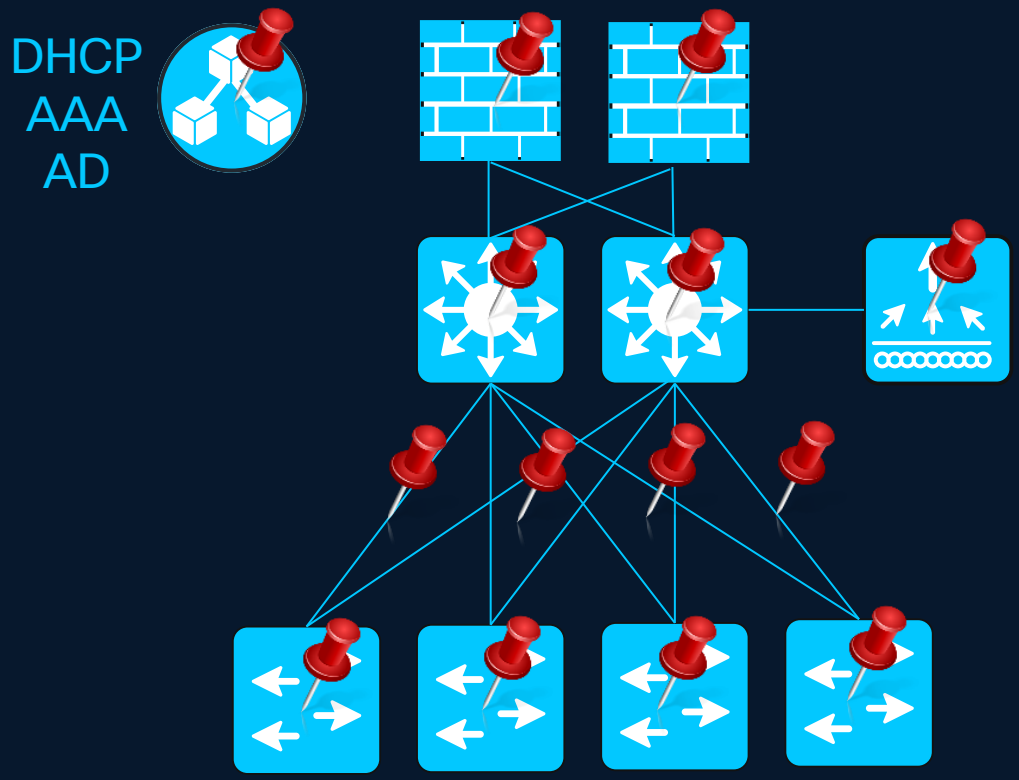
Unmanaged endpoints are difficult to patch and **most vulnerable to cyber attacks.**

Secure authentication mechanisms unusable on unmanaged endpoints

Open, unsegmented networks with IOT devices put organizations at risk

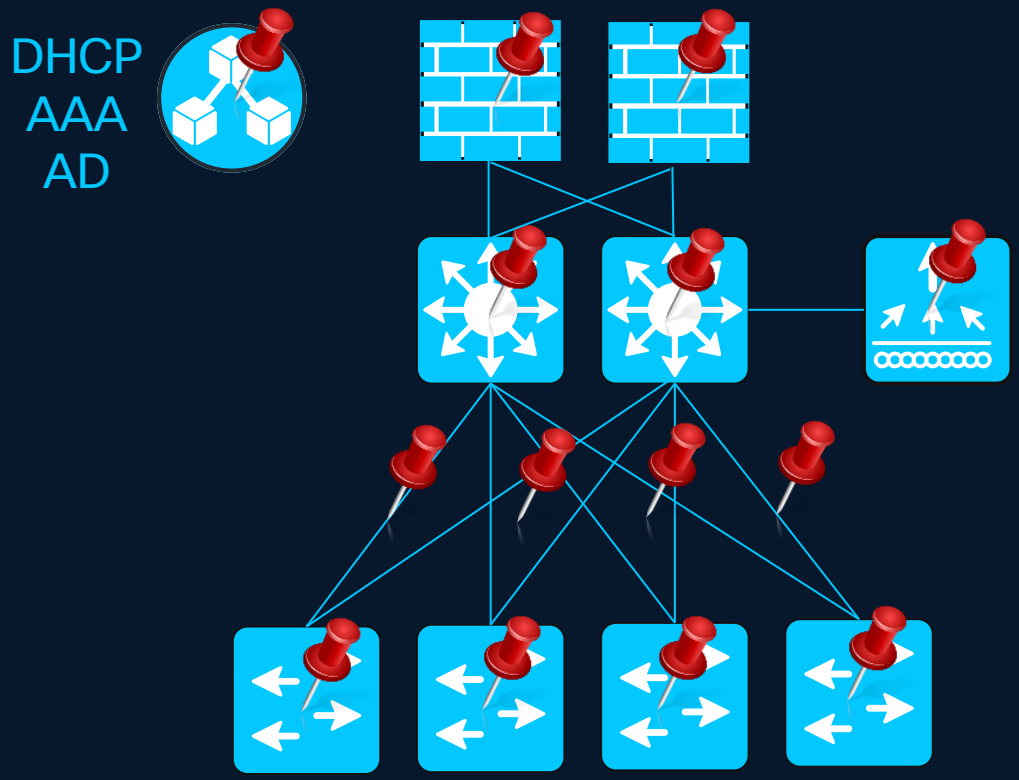
Old methods don’t scale anymore...

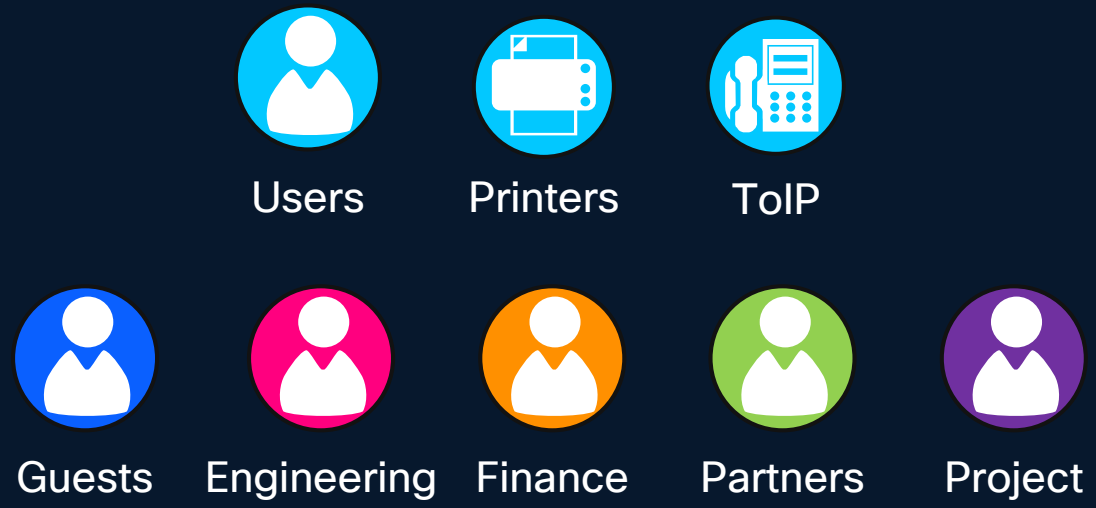
One VLAN per group



Old methods don’t scale anymore...

One VLAN per group

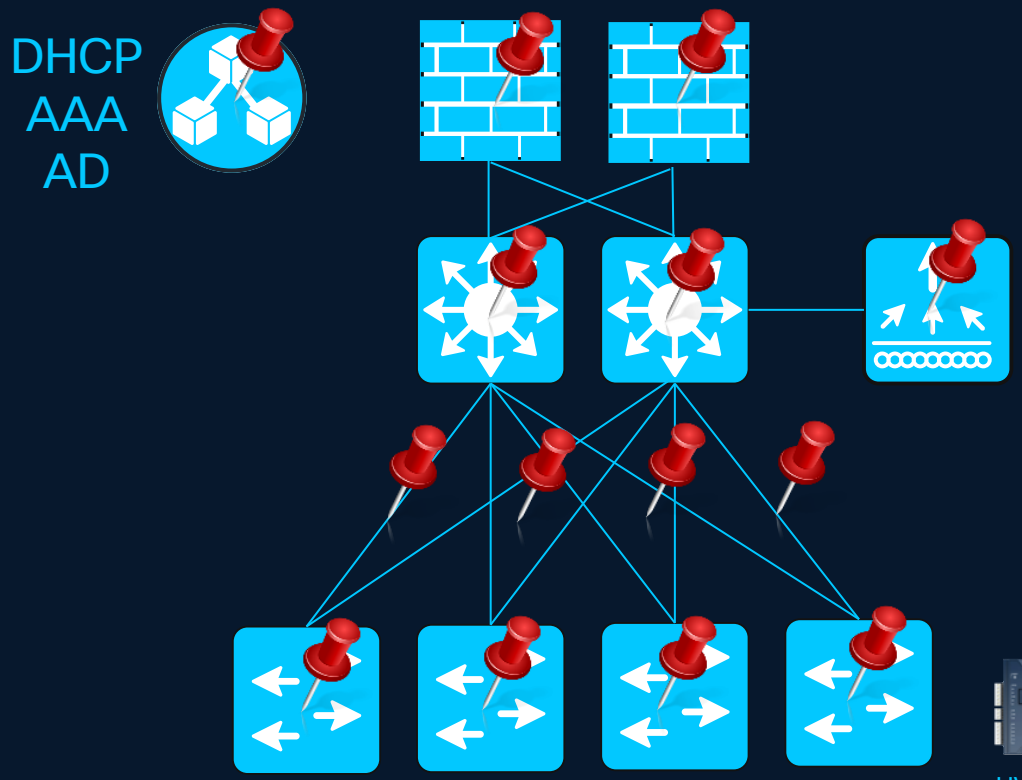




cisco

Old methods don’t scale anymore...

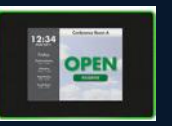
One VLAN per group




Light fixtures


Surveillance cameras

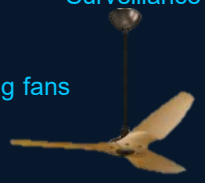

Biometric door locks



Meeting room nameplates

PoE displays


HVAC VAV controllers


Ceiling fans


Facial recognition systems


Entry barriers and turnstiles

Status signs

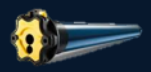

Smoke alarms


Power meters

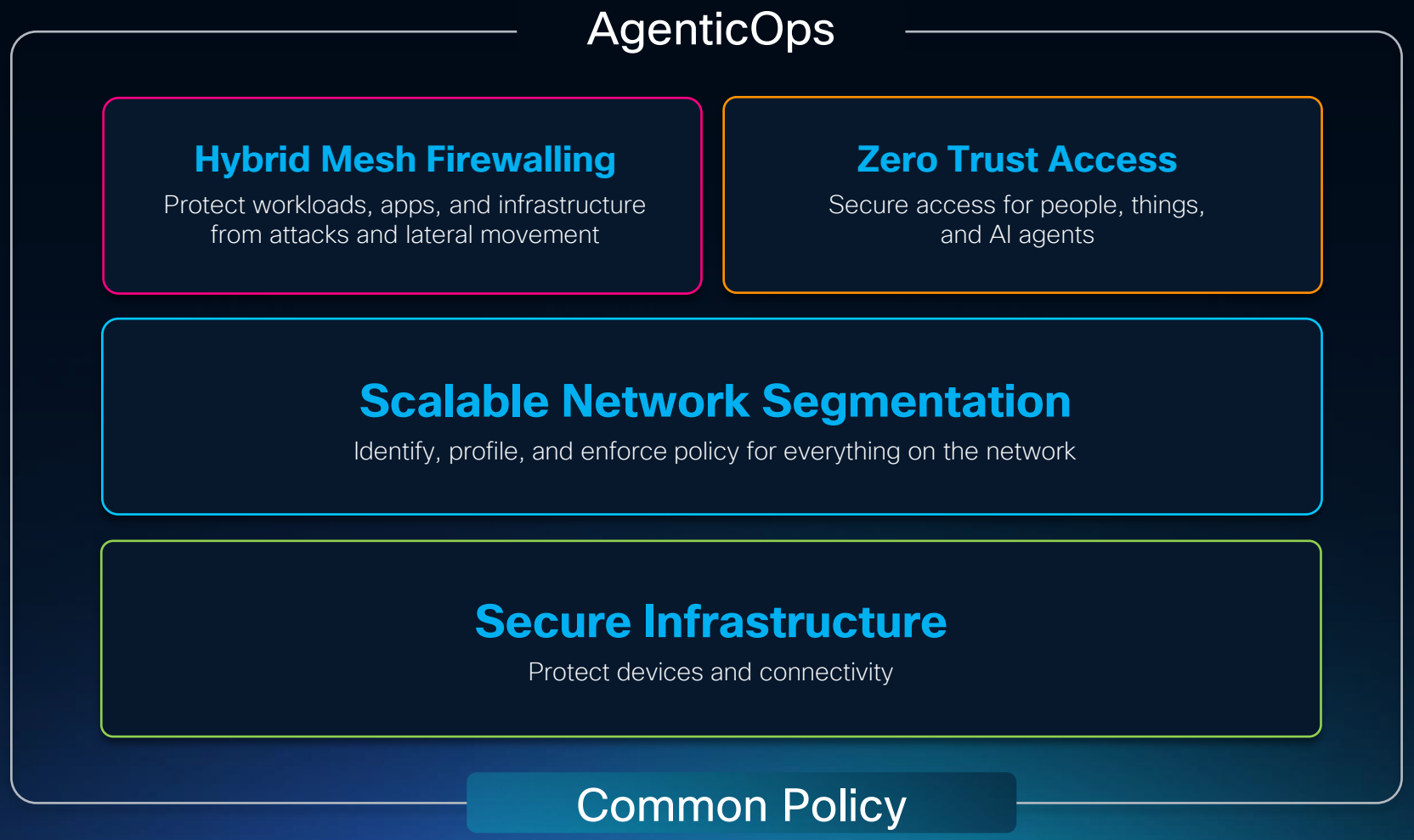

Badge readers


IP call towers

Environmental sensor hubs

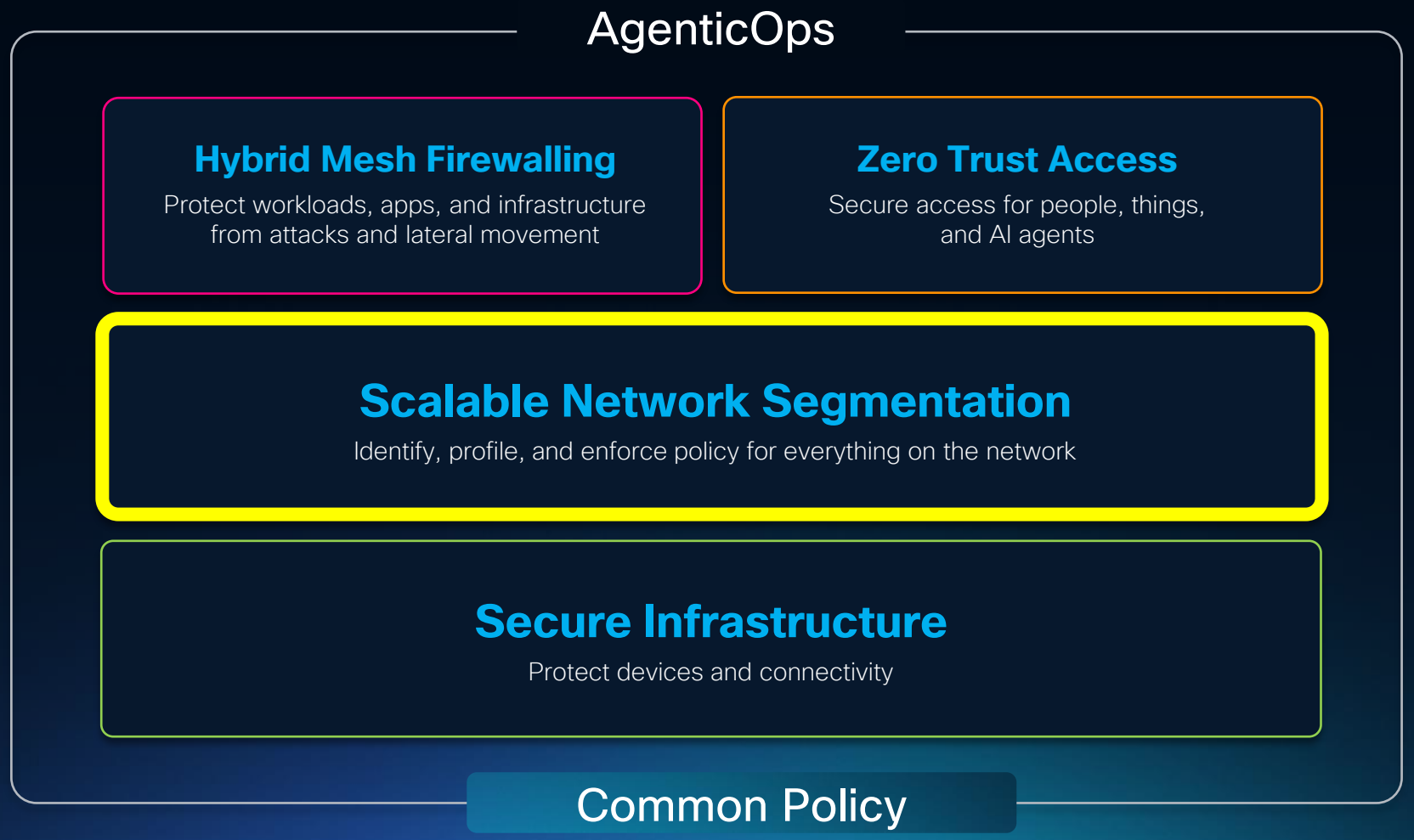

Blind motors

Introducing Cisco's approach to secure networking



Source: Zeus Kerravala, ZK Research, 2025

Introducing Cisco's approach to secure networking



Source: Zeus Kerravala, ZK Research, 2025

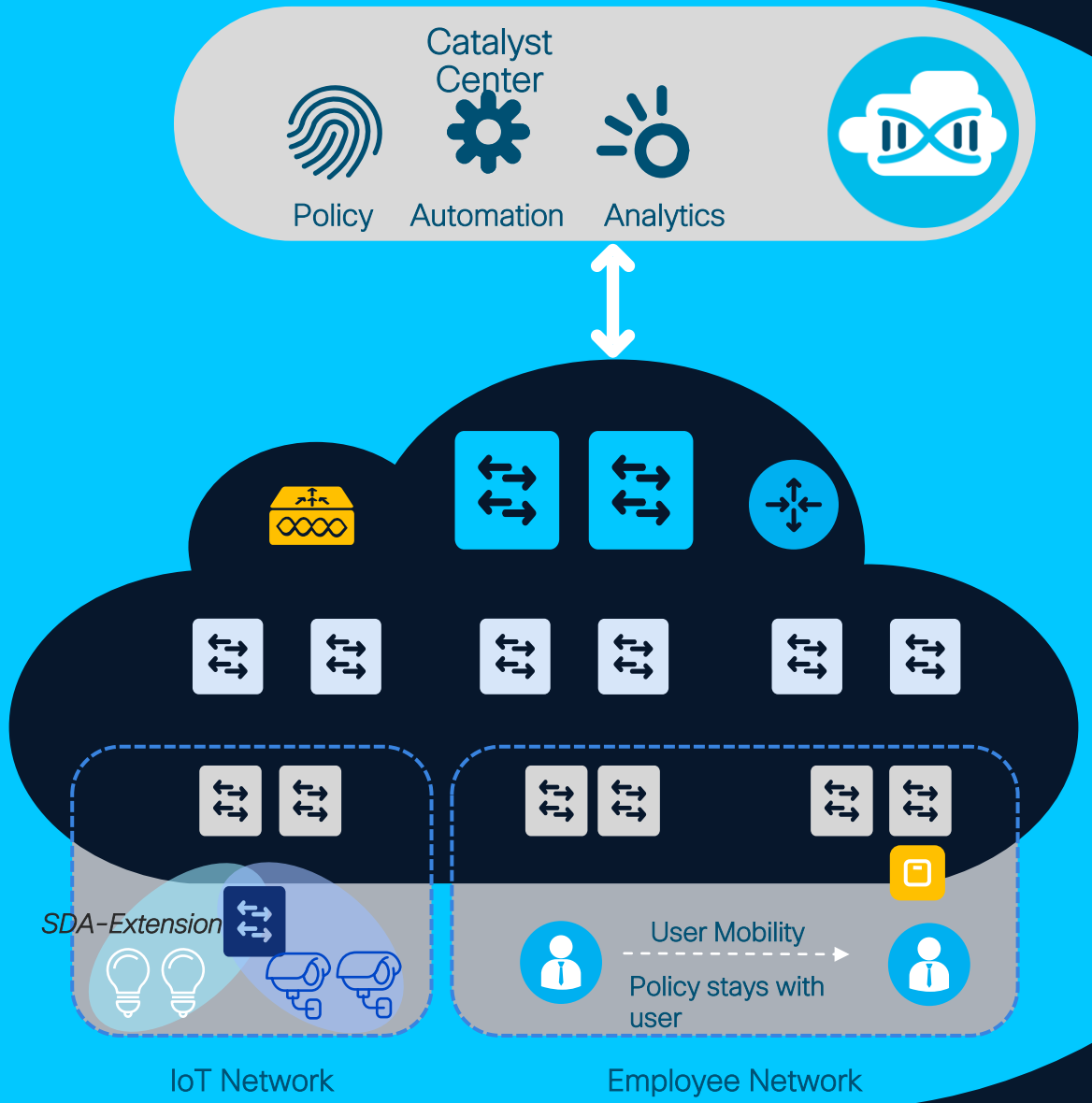
Micro-Segmentation – Group-Based policies with Trustsec SGT

Traditional Segmentation
Centralized on few dedicated enforcement points (firewalls...)

```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

Micro-Segmentation with Group-Based Policies / SGT Fused into the Network

Cisco Software-Defined Access



Identity-based Policy & Segmentation

Decoupled security policy definition from VLAN and IP Address

Automated Network Fabric

Single Fabric for Wired & Wireless with Workflow-based Automation

Insights & Telemetry

Analytics and insights into user and application behavior

SD-Access LISP: Proven. Global. Mission-Critical.

Automated fabric / Integrated Segmentation / Assurance

Deployments	Customers	Site Scale	Device Scale
5465 → *+26% YoY*	2900 → *+12% YoY*	40K+ → *+41% YoY*	2.8M → *+37% YoY*

51% EMEA | 27% AMER | 21% APJC

Massive Scale. Driving Intent-based transformation

Healthcare

UCLA Health
5300 devices
15K+endpoints

Stanford HEALTH CARE
6200 devices
10K+endpoints

Higher Ed + Energy

Yale
6500 devices
66K+endpoints

PETROBRAS
5300 devices
57K+endpoints

Manufacturing + Transportation

Ford
4500 devices
10K+endpoints

TOYOTA
16k devices
98K+endpoints

Kempegowda International Airport Bengaluru
2500 devices
16.8+endpoints

FINANCIAL

CIBC

1200+ Sites 10k+ Devices

185k Endpoints

Managed by a lean team of 5

PARTNER VALIDATED

CDW CANADA

World Wide Technology

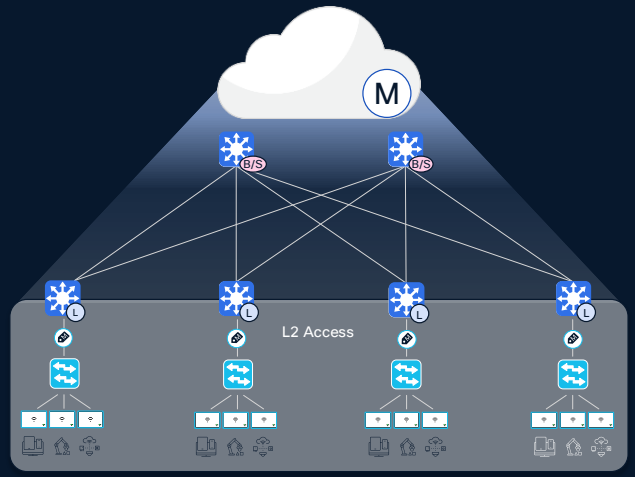
“proven enterprise solution.”

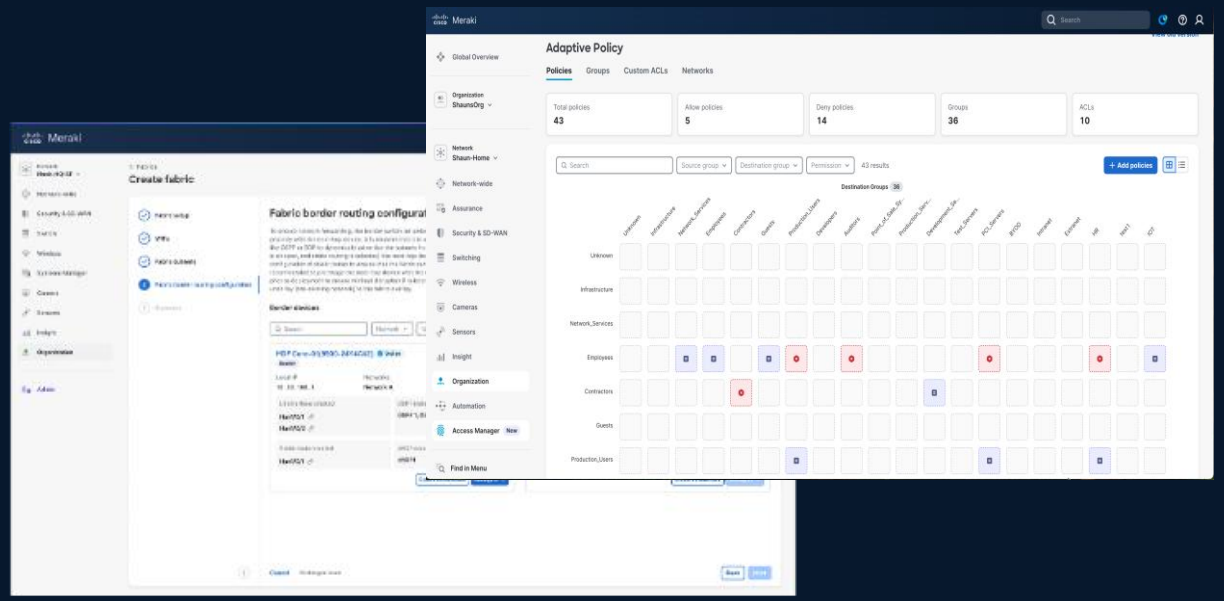
“a mature, scalable, secure architecture”

cisco

Microsegmentation also in Meraki Dashboard

With Adaptive Policies and Cloud Fabric





Benefit from Cloud Simplicity

Build and manage large sites from an intuitive cloud networking platform

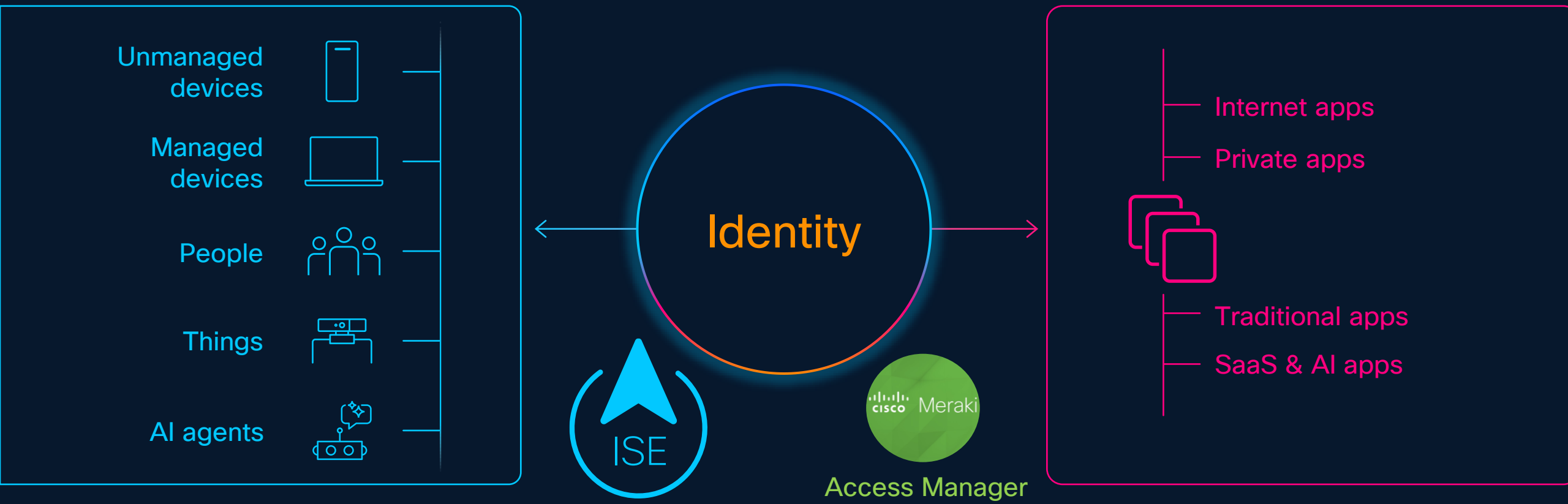
Leverage Existing Investments

Modernize the network while utilizing existing C9K infrastructure

Migrate at Your Own Pace

Incrementally migrate devices and subnets to the cloud over time

Identity is the new control plane



Remote	Enterprise	Campus	Branch	Data Center	IIoT	Field	...

La sécurité fusionnée au réseau
Comment ?

Identity is the new control plane

With Cisco Identity Services Engine

Remote	Enterprise	Campus	Branch	Data Center	IIoT	Field	...

cisco

ISE's role in Zero Trust

Establish Trust

User/Machine Authentication, Health Assessment

Enforce Trust Based Access

Network Segmentation enabled by Granular Context

Continuously Verify Trust

With Integrated Intelligence

Respond to change in trust

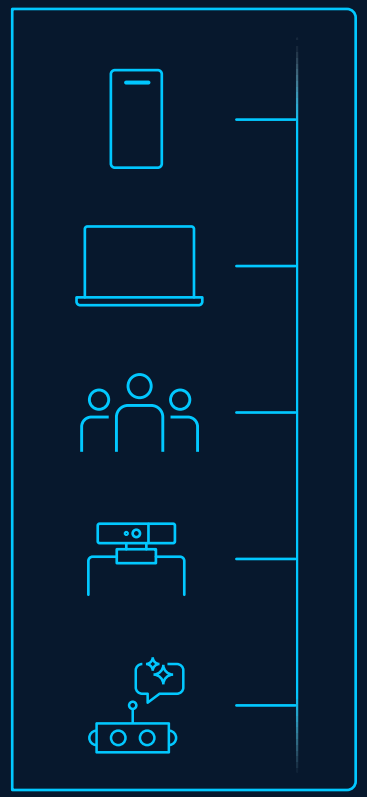
With Adaptive Network Control

cisco

Establish Trust

Remote	Enterprise	Campus	Branch	Data Center	IIoT	Field	...

Establish Trust



Identifies an classifies the endpoint

AuthN

IBNS 2.0

RADIUS

RADIUS

ISE

Authentication

Dot1x

MAB

WebAuth

Authorization

VLAN

URL_Redirect

ACL / dACL

Reauth Timer

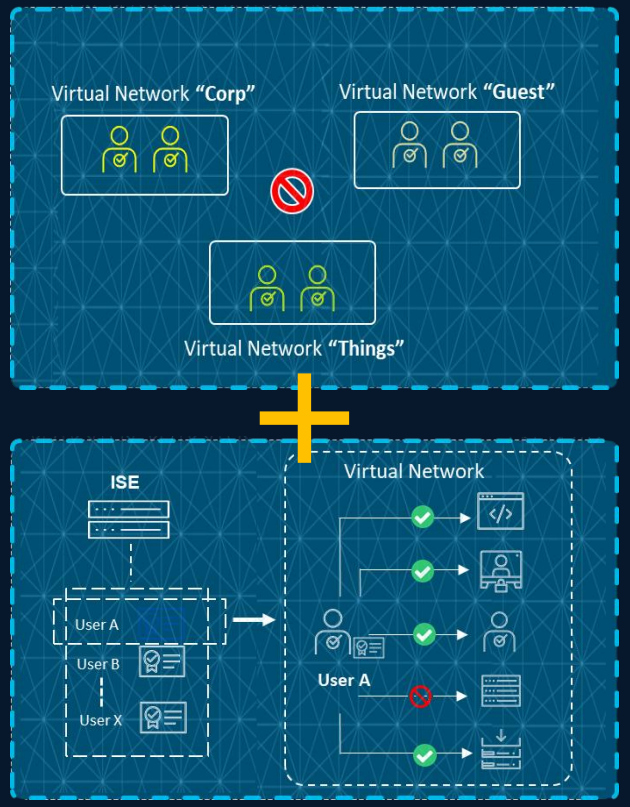
Interface template

SGT

Tells what the endpoint has access to

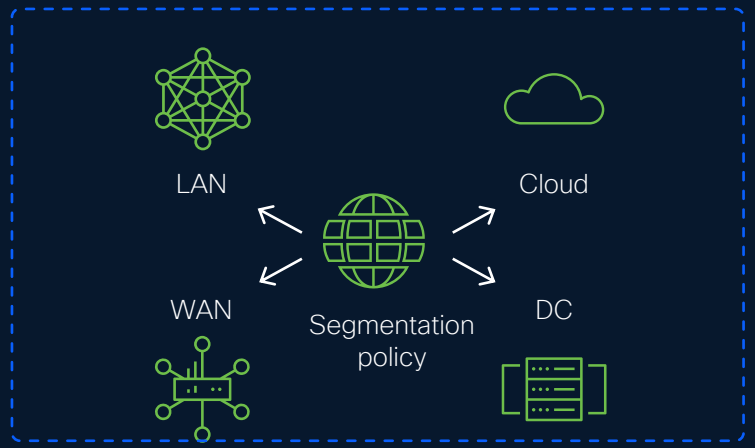
cisco

Enforce Trust Based Access (1)



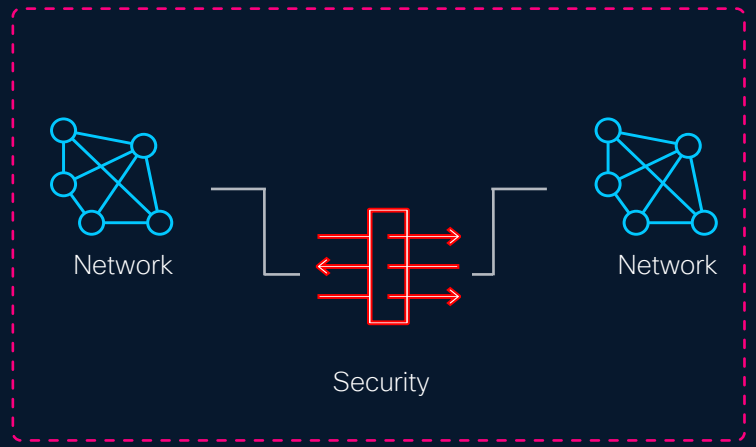
Macro & Micro Segmentation

VRF boundaries + identity rules inside



Common Policy to

LAN / WAN / SSE / DC / Cloud

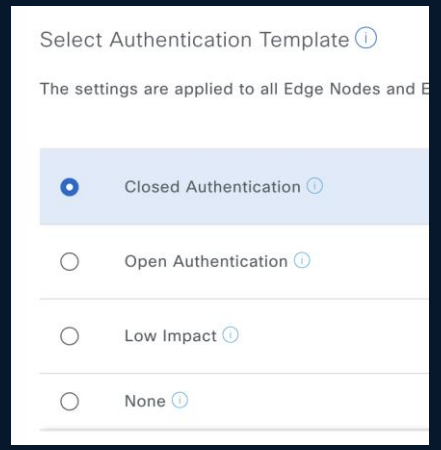


Steering Traffic to security services for stateful inspection or IPS/IDS

cisco

Automation is a MUST for Identity Networking

```
policy-map type control subscriber NAC
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template
DEFAULT_CRITICAL_VOICE_TEMPLATE
   20 pause reauthentication
   30 authorize
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  …
```



Catalyst Center

Without controller

Error prone, deviations, heterogenity

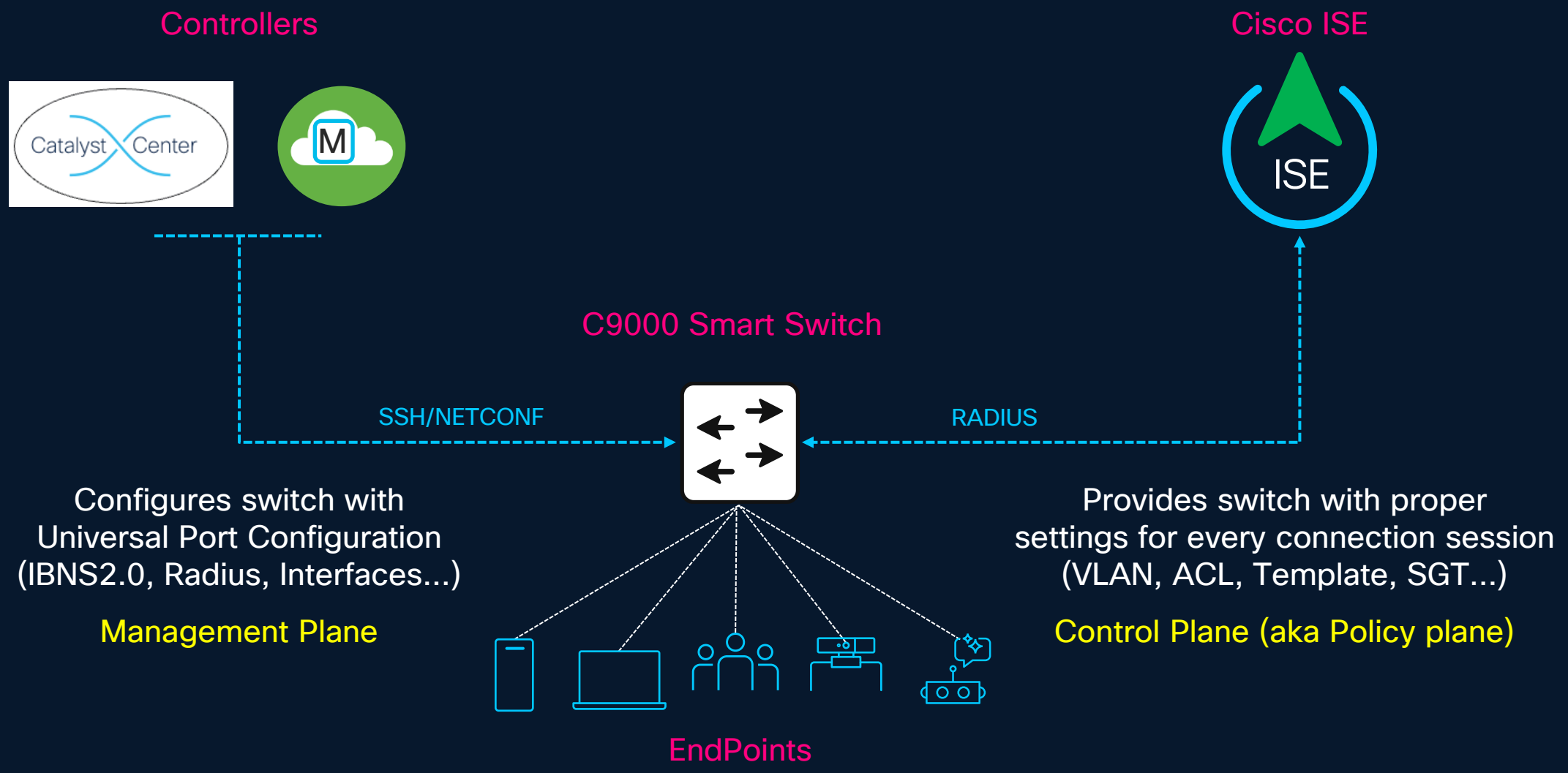
Time wasted on Configuration management

With controller

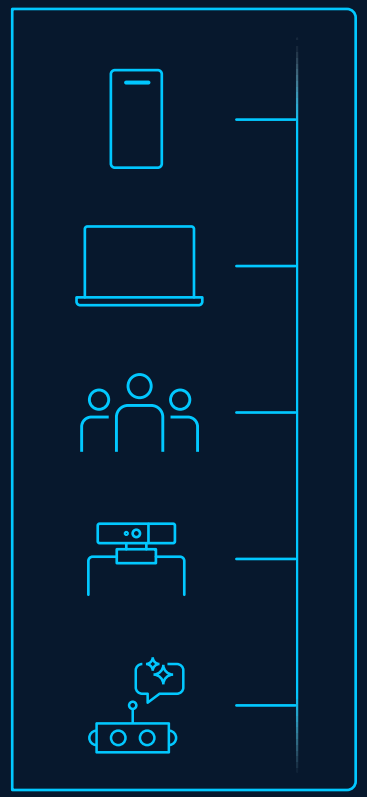
Compliance, Continuous Optimizations

Focus on Identities, Policies and Use Cases

Architecture components



Establish Trust



Identifies an classifies the endpoint

AuthN

IBNS 2.0

RADIUS

RADIUS

ISE

Authentication

Dot1x

MAB

WebAuth

Authorization

VLAN

URL_Redirect

ACL / dACL

Reauth Timer

Interface template

SGT

Tells what the endpoint has access to

cisco

Interface Templates for Automation and Compliance

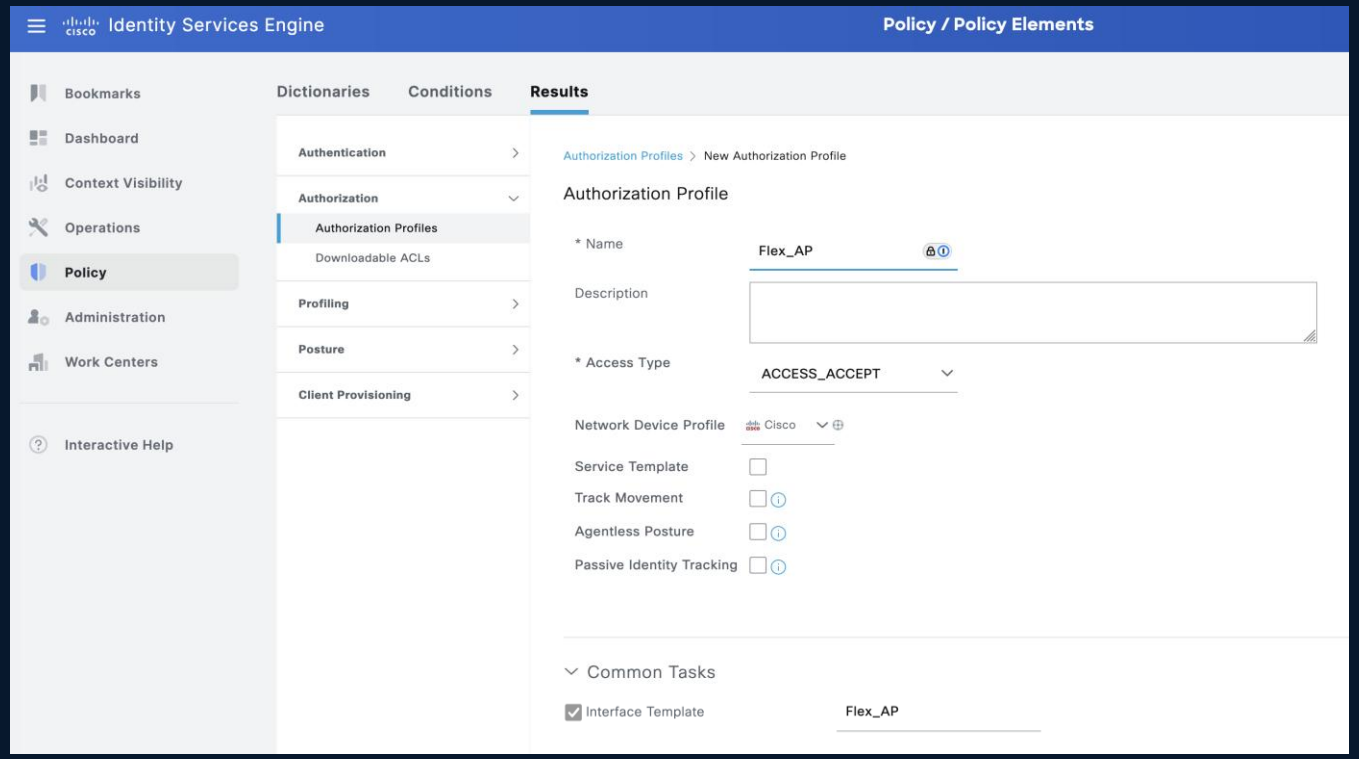
Stop modifying access port configuration

Doesn't modify the running-config

- Apply to the interface not the session
- Bound to the session
- Revert automatically to source template when session teardown

Precedence order

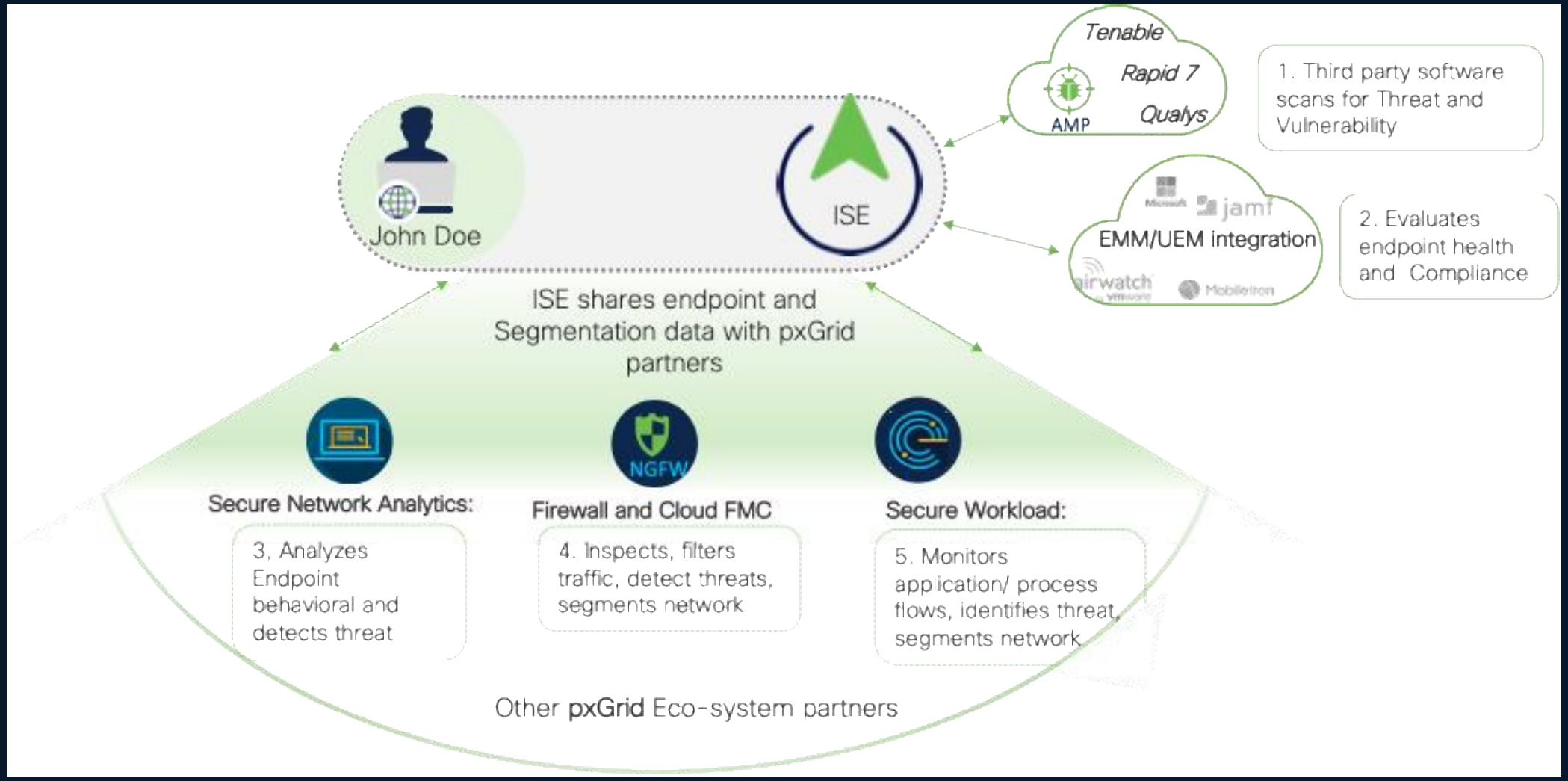
1. Dynamic interface template
2. Interface configuration
3. Static interface template



Start relying on derived configuration with ISE dynamic attributes

Continuously Verify Trust

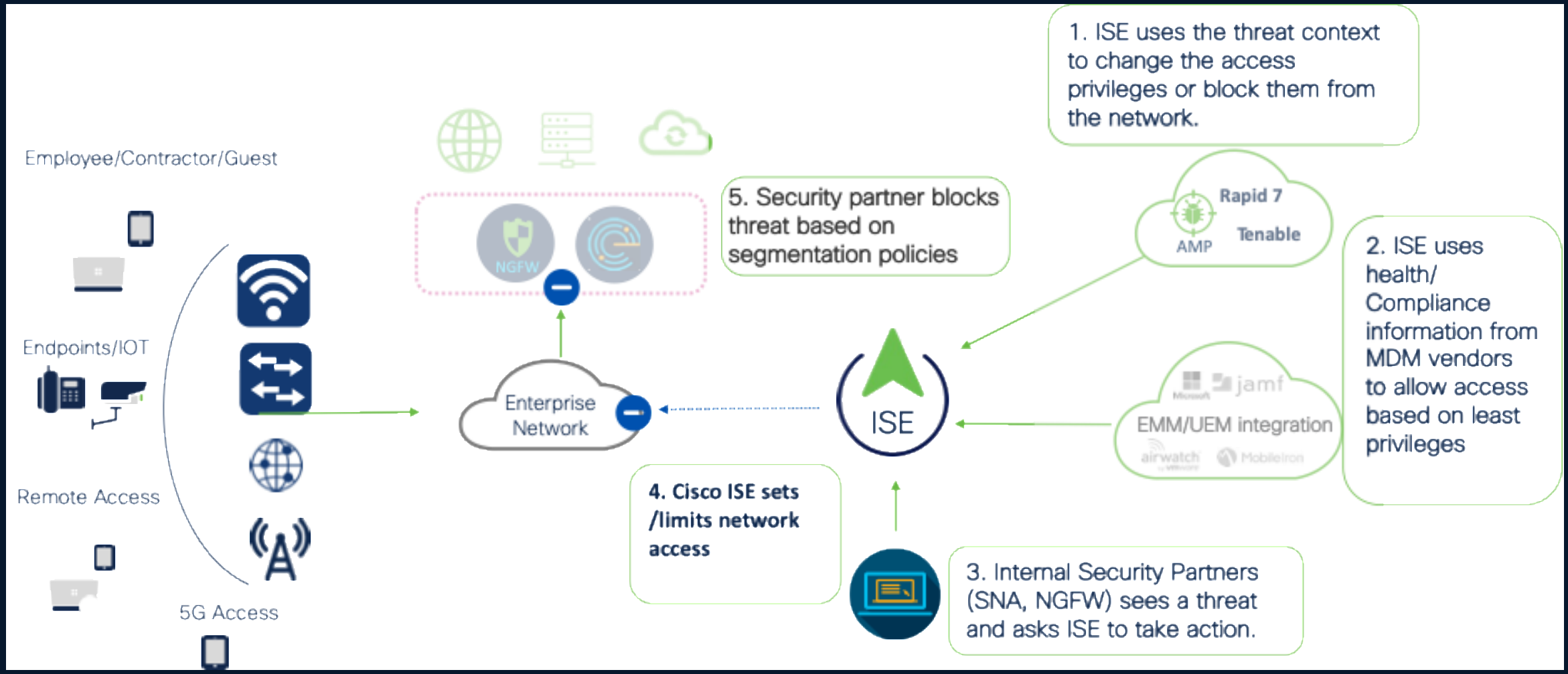
With ISE integrations across variety of vendors to gather deeper context and take actions



cisco

Respond to change in trust

Threat Containment and Response



Cisco Professional Services (CX)

Accélérer les projets

- Faire les bons choix en amont
- Ne pas perdre de temps grâce à notre expérience mondiale

Mitiger les risques

- Accès à des experts reconnus
- Le fameux tampon du constructeur, l'assurance qu'une solution sera trouvée
- Médiateur de confiance pour débloquer les conflits

Optimiser les coûts

- Engager CX le plus tôt possible
- Le prix du service ne doit être comparé qu'au gain qu'il apporte

Rendre les clients autonomes

- Transfert de compétences

Cisco CX travaille main dans la main avec les partenaires engagés

Cisco CX accélère les roadmaps pour mieux répondre à vos besoins

Témoignage

Sébastien CIELOCH
LIEBHERR

Liebherr – une entreprise familiale

1949

Fondation par le Dr.-Ing. E.h. Hans Liebherr à Kirchdorf an der Iller (DE)

Holding:
Liebherr-International SA à Bulle (Suisse)

Liebherr est une entreprise technologique familiale

Une structure

décentralisée

et des unités opérationnelles

indépendantes

et

autonomes

55 963

Employé(e)s

> 40

Sites de production

14 772

Million d’euros de chiffre d’affaires (2025)

>150

Sociétés

Organisation des divisions Liebherr-International AG


Terrassement


Technique du béton


Réfrigération et congélation


Secteur minier


Grues maritimes


Composants


Grues mobiles et sur chenilles


Fondations spéciales


Hôtels


Grues à tour


Aerospace et ferroviaire


Technologie de manutention


Techniques d’engrenages et systèmes d’automatisation

Les produits Liebherr sont regroupés en 13 divisions différentes.

LIEBHERR

La division terrassement – la gamme de produits

Pelles sur pneus

Pelles sur chenilles

Tombereaux articulés

Chargeuses sur pneus

Bouteurs sur chenilles

Chargeuses sur chenilles

Chariots télescopiques

Poseurs de canalisations

Pelles sur pontons

Pelle à câbles

Outils

La division terrassement – les sites de production

Liebherr-France SAS

Colmar (France)

Création : 1961

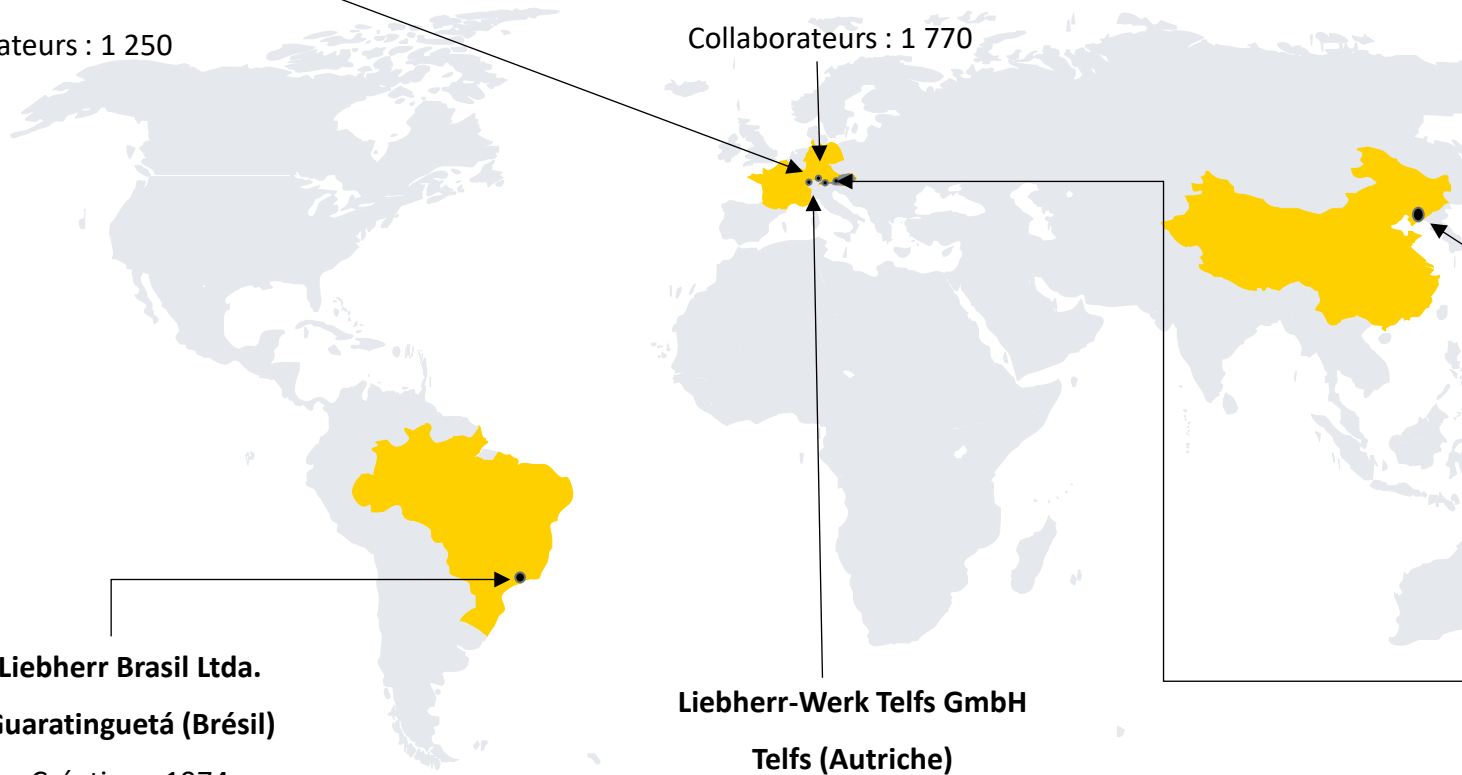
Collaborateurs : 1 250

Liebherr-Hydraulikbagger GmbH

Kirchdorf an der Iller (Allemagne)

Création : 1949

Collaborateurs : 1 770



Liebherr Machinery (Dalian) Co., Ltd.

Dalian (Chine)

Création : 2002

Collaborateurs : 267

Liebherr Brasil Ltda.

Guaratinguetá (Brésil)

Création : 1974

Collaborateurs : 1 070

Liebherr-Werk Telfs GmbH

Telfs (Autriche)

Création : 1976

Collaborateurs : 850

Liebherr-Werk-Bischofshofen Gmbh

Bischofshofen (Autriche)

Création : 1960

Collaborateurs : 1 300

Visibilité / exploitation

Manque de visibilité sur incidents et les tendances. Outils de dépannage complexes

---

Convergence IT/OT : nos outils de cybersécurité réseau ne suffisent plus (pas de firewall, trop peu de segmentation)

Segmentation réseau

Aucune possibilité technique de « micro-segmentation »

Challenges et objectifs de Liebherr France SAS

Standardiser, harmoniser nos technologies

Shared services, Groupe…

Maitrise des coûts

L'architecture doit continuer d'héberger l'IT et l'OT.

Capitaliser sur les licences

Automatisation et efficacité

Via des outils permettant de limiter le risque d'erreurs humaines

---

Conformité et sécurité accrue

Des attaques Cyber touchent Liebherr, les équipes Cyber mobilisent davantage l'IT

LIEBHERR

Merci !


CISCO