CISCO Connect

Cisco SASE and Universal ZTNA

Julien Hernandez
Technical Solution Architect
Security/SASE

Nicolas Boursier
Technical Solution Architect
SD-WAN/SASE

Mai 2026

Julien Hernandez

Technical Solution Architect
Security/SASE

Nicolas Boursier

Technical Solution Architect – Partner Org
SD-WAN/SASE

Agenda

01 Tendances de Marché SASE

02 Le UZTNA c’est quoi?

03 Etude de cas UZTNA

Tendances de Marché SASE

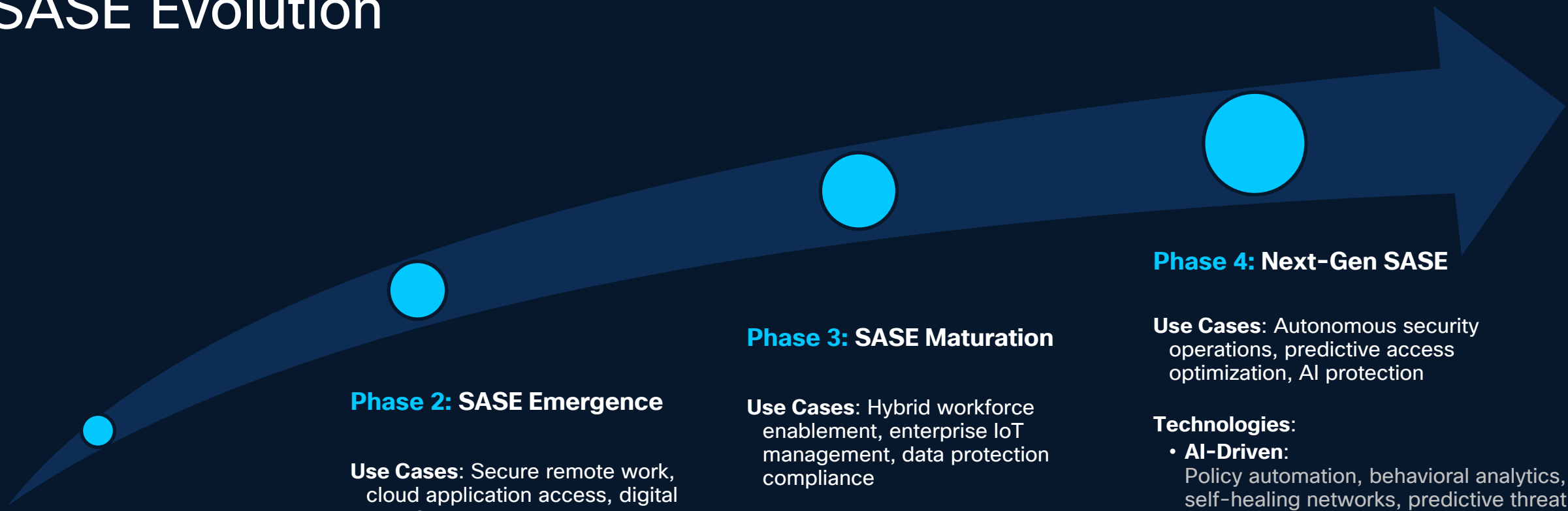
What we hear from customers

"There are too many disparate security tools creating blind spots and risk."

"Security can't get in the way of productivity for my employees."

"I need security that can keep up with evolving threats and new AI risks."

SASE Evolution



Phase 1: Legacy Era

Use Cases: Hub-and-spoke connectivity, perimeter-based security, basic remote access

Technologies:
MPLS, hardware firewalls, VPN concentrators, point solutions, basic network access control

Phase 2: SASE Emergence

Use Cases: Secure remote work, cloud application access, digital transformation enablement

Technologies:

- **Core SASE**:
  SD-WAN, SWG, CASB, basic ZTNA, FWaaS
- **Data Protection**:
  Early cloud data classification and DLP integration

Phase 3: SASE Maturation

Use Cases: Hybrid workforce enablement, enterprise IoT management, data protection compliance

Technologies:

- **Converged Platform**:
  SASE platforms, Universal ZTNA, DEM, Enterprise browser
- **Data Security**:
  Posture DSPM for real-time data discovery, classification, and protection

Phase 4: Next-Gen SASE

Use Cases: Autonomous security operations, predictive access optimization, AI protection

Technologies:

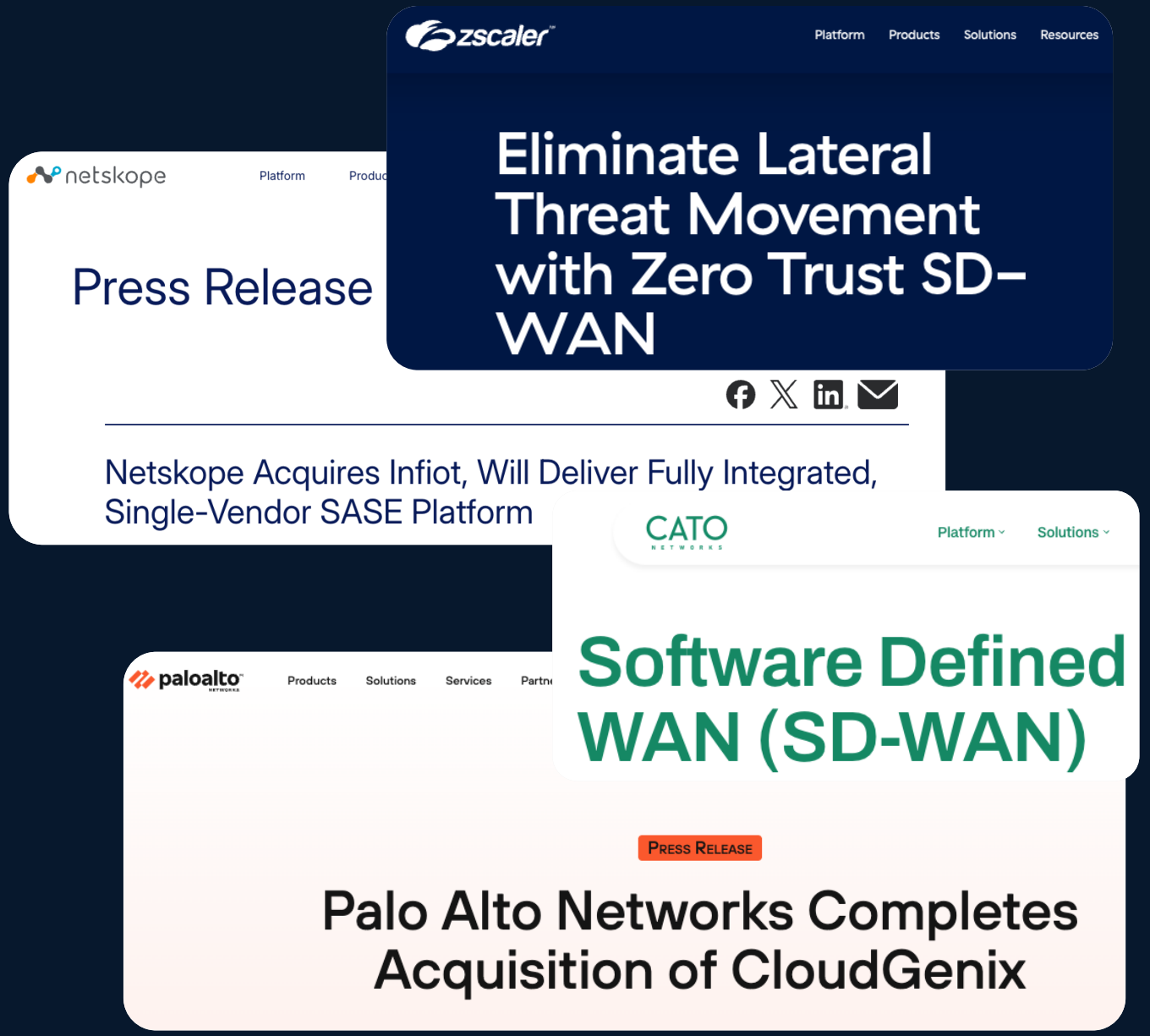
- **AI-Driven**:
  Policy automation, behavioral analytics, self-healing networks, predictive threat detection
- **Intelligent Data Protection**:
  Autonomous DSPM with AI for real-time risk remediation
- **Quantum Ready Security**:
  Effective security and privacy in a post-quantum world.

cisco

SD-WAN as a key building block of SASE Evolution

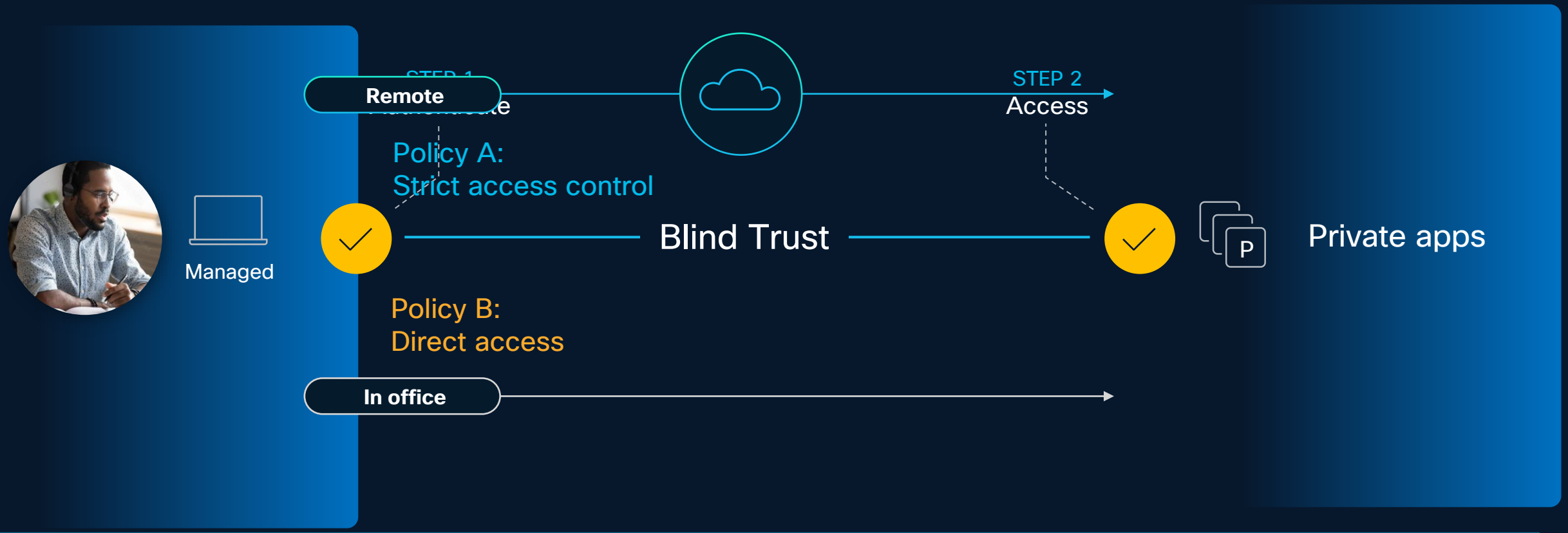
- Every SSE vendor has invested in SD-WAN to complete its SASE solution

- SD-WAN ensures
  - Secured connectivity (Post Quantum era)
  - Best Application performance
  - Digital Experience Monitoring and Troubleshooting
  - Simple Cloud and SSE connectivity



Le Universal ZTNA c’est quoi?

Traditional ZTNA: Work from home solution



Managed devices, private apps

Different policies for home versus office

Blind trust between authentication and access

Universal ZTNA from Cisco

Zero downtime:
Experience and Policy Assurance

Unmanaged devices

Managed devices

People

Things

Zero impostors:
Identity Trust

Zero friction

Internet apps

Private apps

Traditional apps

SaaS apps

Data Loss Prevention	Remote Browser Isolation	AI Access
Firewall as a Service	Secure Web Gateway	Zero Trust Network Access
Cloud Access Security Broker	DNS Security	VPNaaS

Consistent Security:
Security Service Edge

Cisco Universal ZTNA

Zero downtime | Consistent Security | Zero impostors

Secure SD-WAN		Security Services Edge		Trusted Identity Edge
Catalyst SD-WAN Meraki SD-WAN FTD SD-WAN	+	Secure Access	+	Duo Identity Intelligence ISE

SINGLE VENDOR SASE

End-to-end assurance with ThousandEyes

cisco

Role of identity in a Universal ZTNA approach

Gouvernance des identités : pierre angulaire du modèle Zero Trust

une **gouvernance améliorée de l'identité** (l'accès aux ressources est contingenté à l'identification de l'utilisateur et de l'équipement utilisé, du statut de l'actif et de facteurs environnementaux tels que l'heure et la géolocalisation de la demande de connexion). En tant qu'éléments clés du modèle *Zero Trust*, le ou les référentiels d'identité doivent être assainis avec une politique stricte de mise à jour lors des arrivées, départs et mobilités. Ils doivent refléter fidèlement la situation courante des utilisateurs

https://cyber.gouv.fr/publications/le-modele-zero-trust

Cisco Identity Intelligence

Identity Providers

User Context

SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

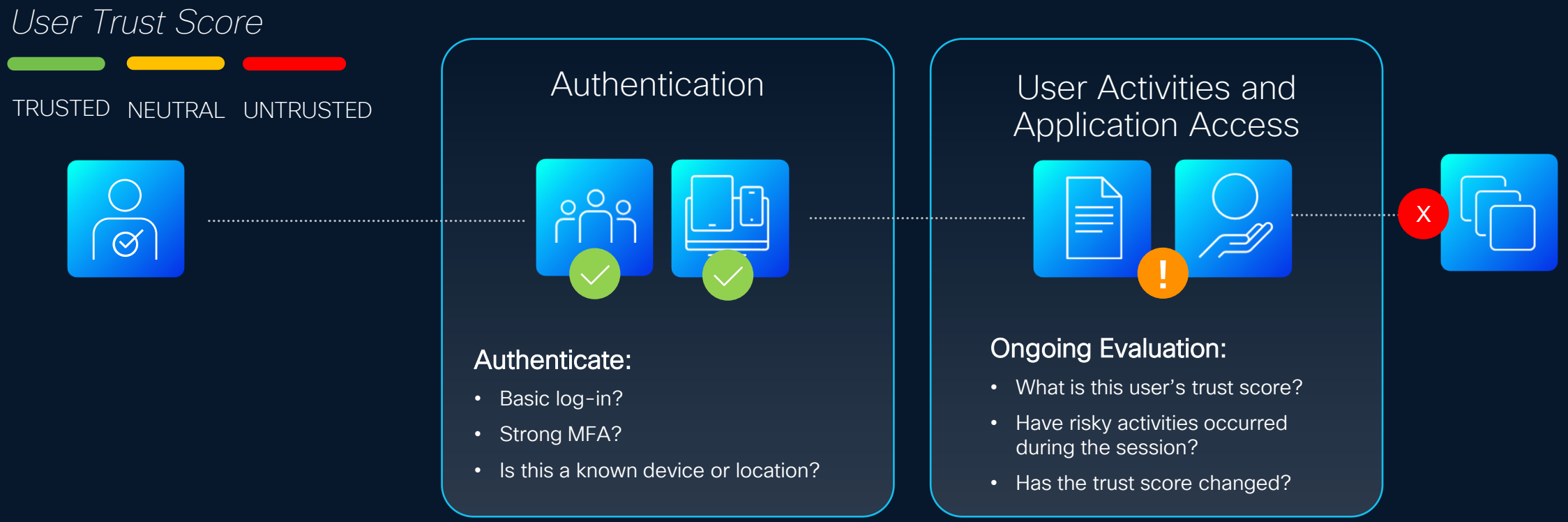
Cyberark

Amazon

Identity posture

Cisco’s Identity Intelligence | Dynamic User Trust Scores

Provide in-session risk evaluation in the Secure Access dashboard



Cisco Identity Intelligence s'intègre à Secure Access pour analyser le comportement dans l'ensemble de l'écosystème d'identité, en attribuant un score de confiance dynamique qui détecte et bloque de manière proactive les activités malveillantes pendant les sessions actives.

Additional User Context augmented Zero Trust

Source Criteria					Destination Criteria:			Result
IP Addr	**User / Groups**	**SGT**	**Device Trust**	**Trust Level**	**App**	**SGT**	**IPS**	**Action**
any	Executives	VIPs	Compliant	Favorable	SAP	ERP	Enabled	permit
any	any	Employees	Compliant	Untrusted	any	Ordering	-	deny

Etude de cas Universal ZTNA

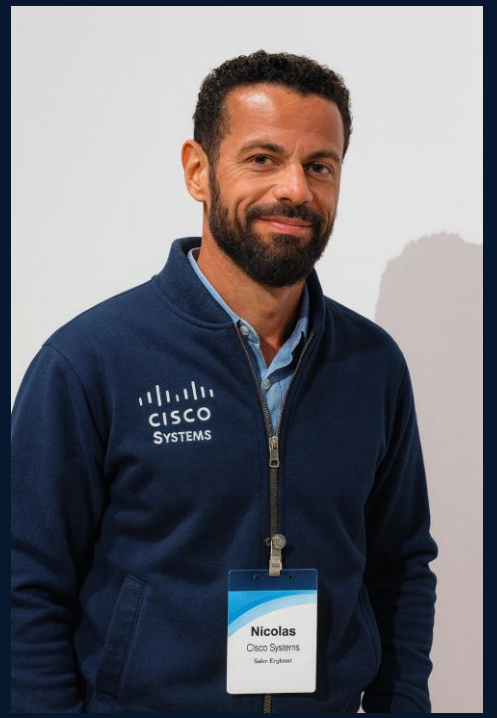
Etude de cas Universal ZTNA

Julien

LE SAC PARFAIT

CIO Entreprise “Le Sac Parfait”

Nicolas

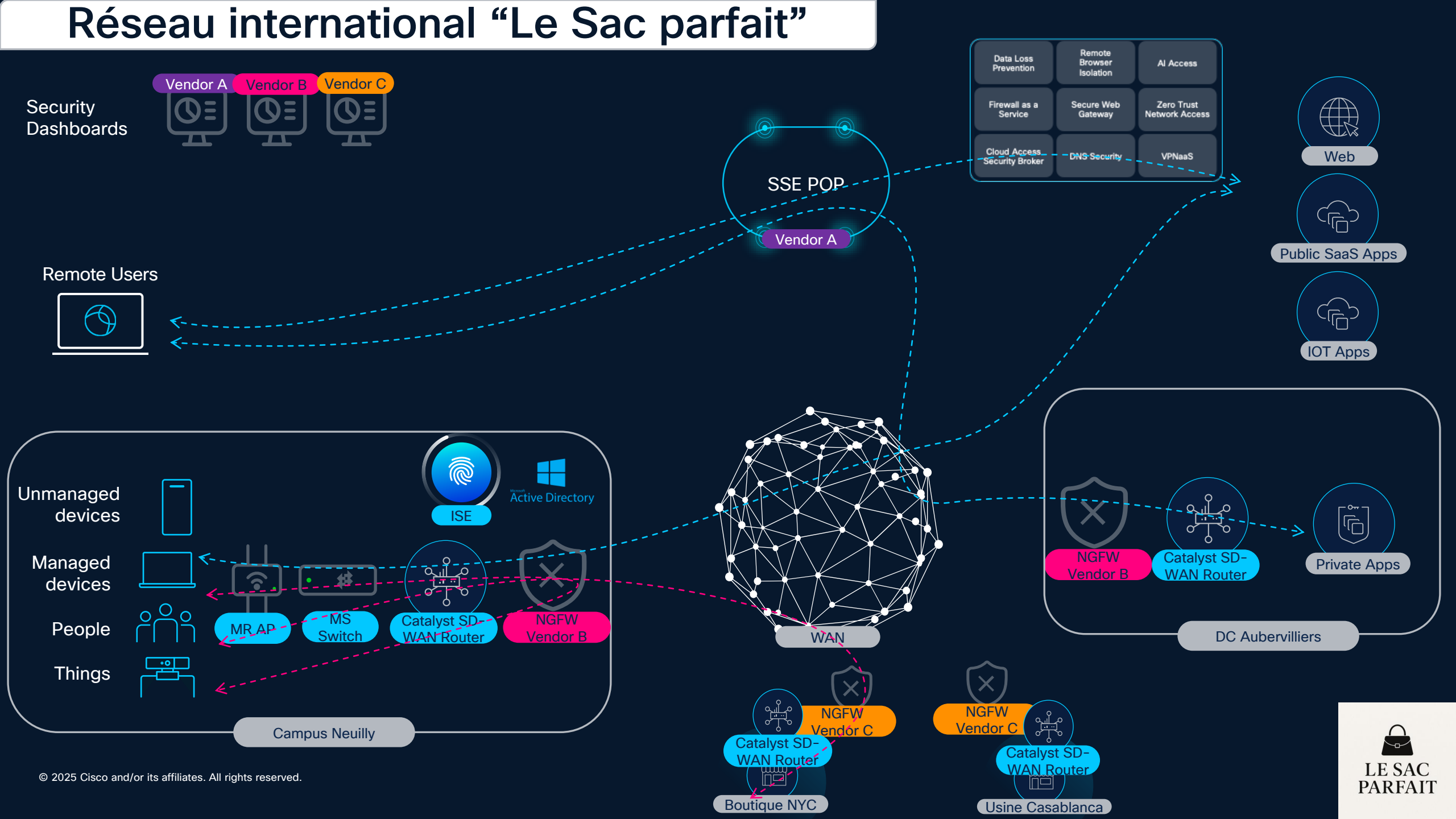


CISCO

Solution Engineer Cisco

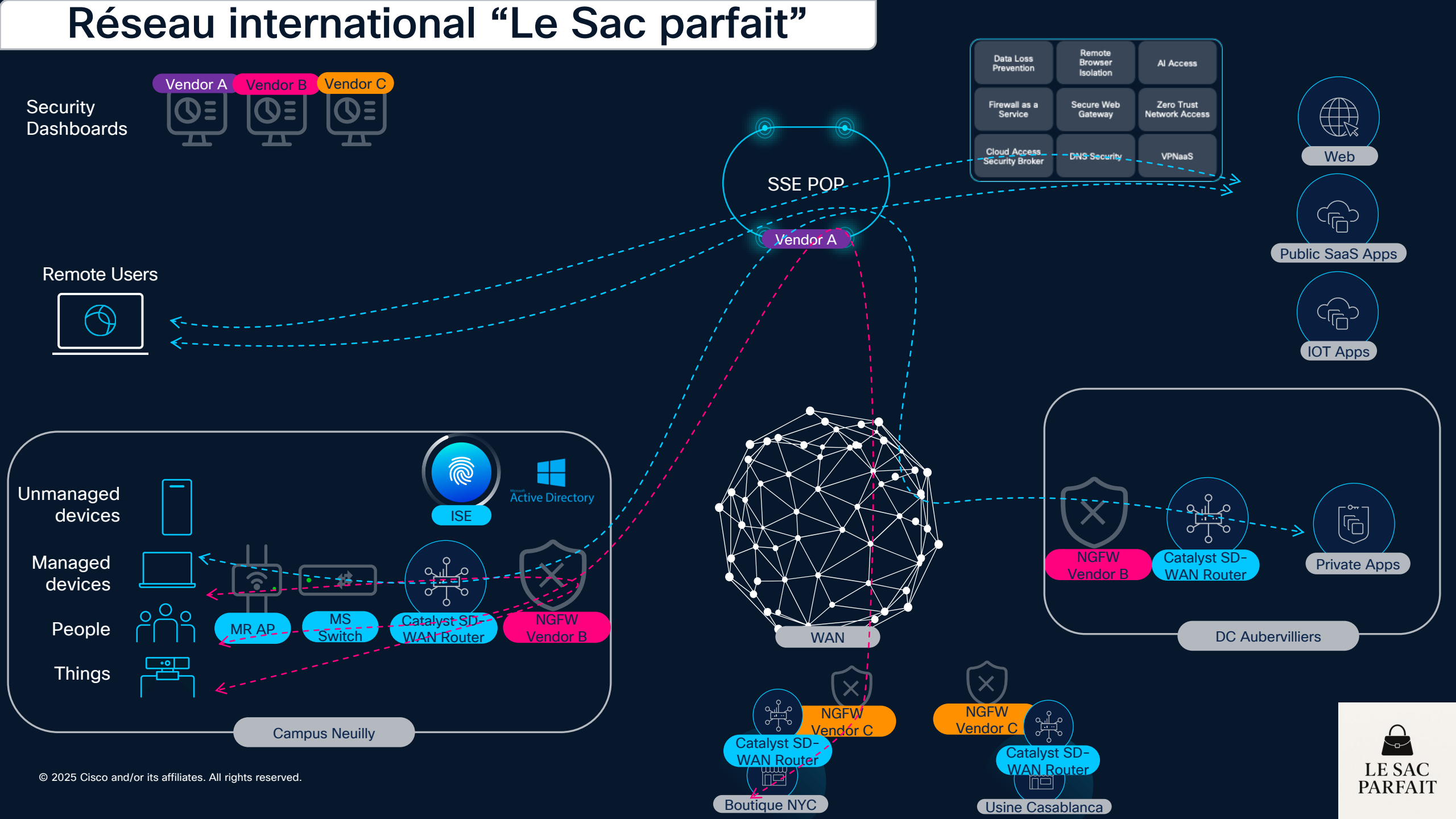
cisco

Réseau international “Le Sac parfait”



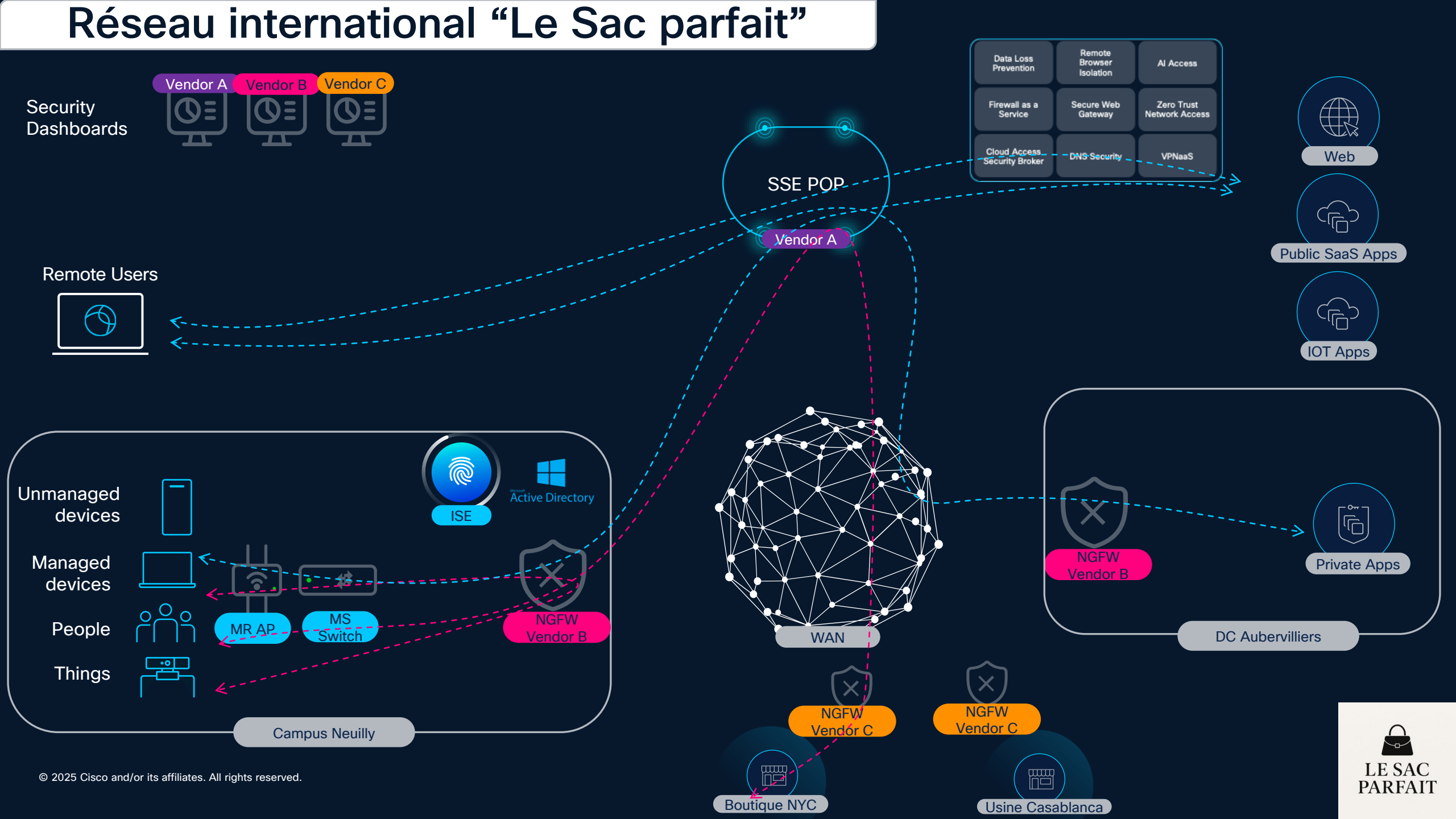
LE SAC PARFAIT

Réseau international “Le Sac parfait”



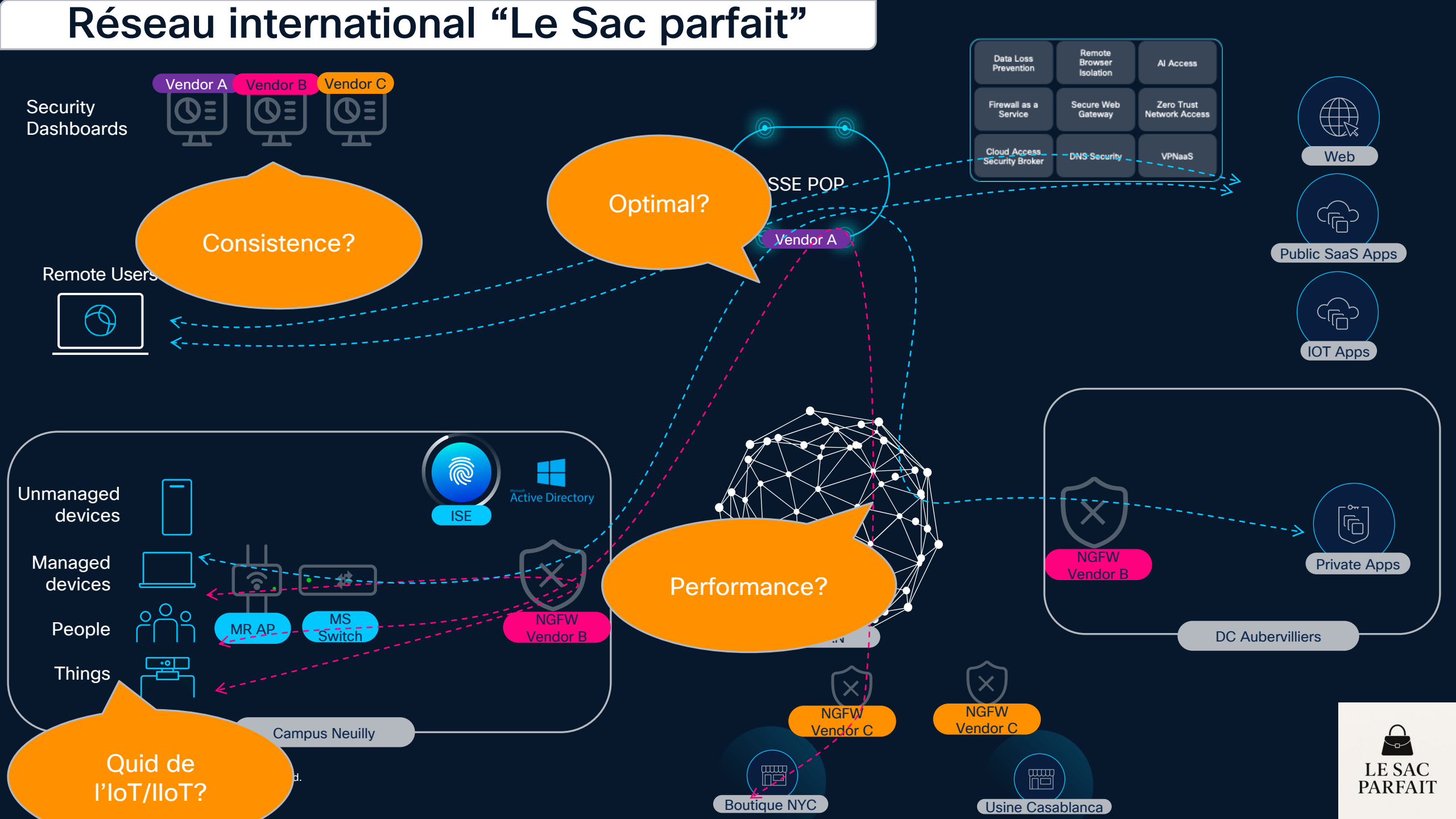
LE SAC PARFAIT

Réseau international “Le Sac parfait”



LE SAC PARFAIT

Réseau international “Le Sac parfait”



LE SAC PARFAIT

Objectifs CIO/CTO “Le Sac Parfait”

- Réduire les coûts et la complexité
  - Réduire le nombre d’équipements
  - Consistence multi domaine (LAN, WAN, DC, Cloud)

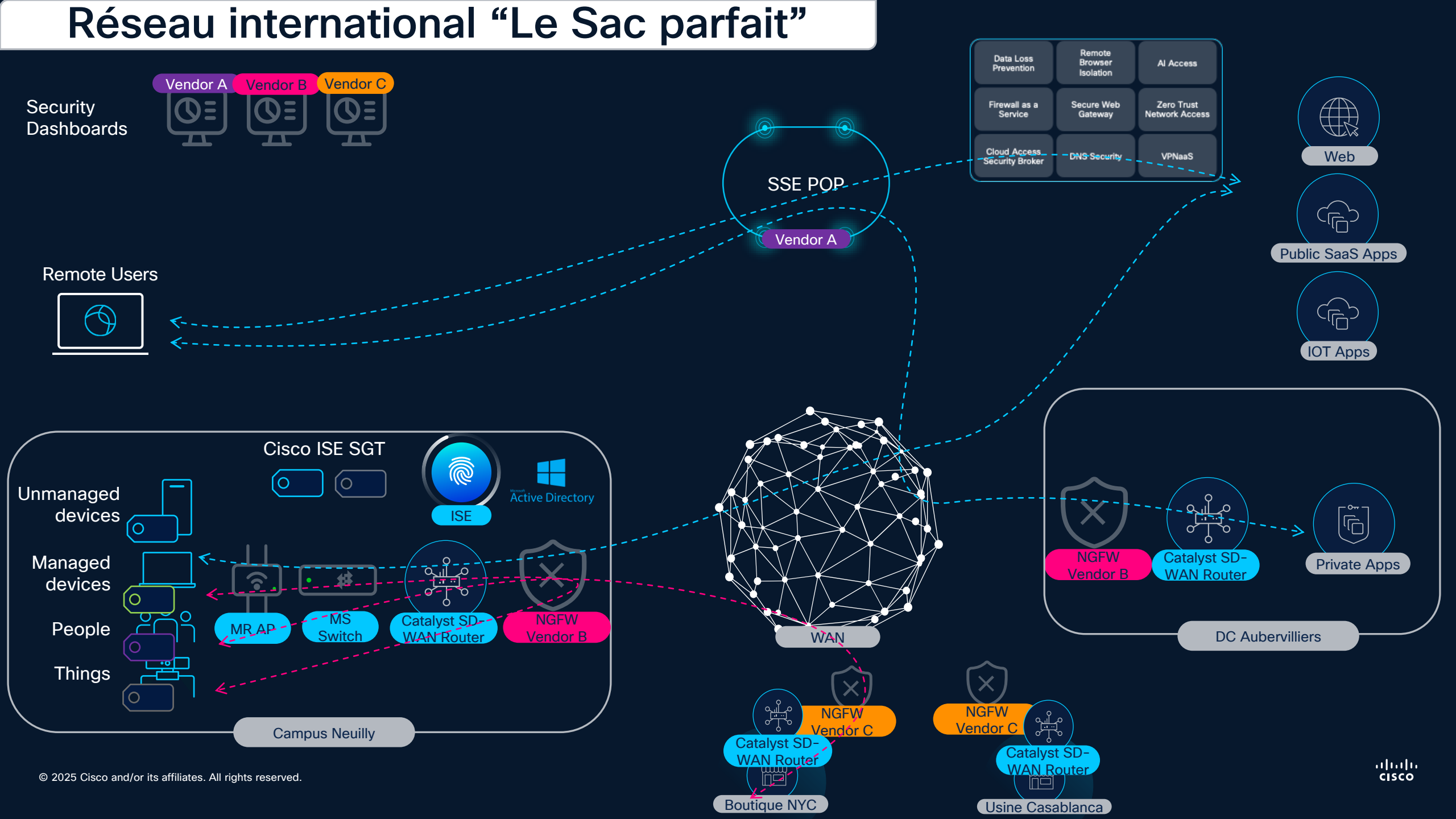
- Appliquer une politique de sécurité consistente
  - Quelque soit le type d’utilisateur/device
  - Quelque soit le mode de connexion

- Gestion de la sécurité à travers des identités et de la posture plutôt que des pools d’adresses IP

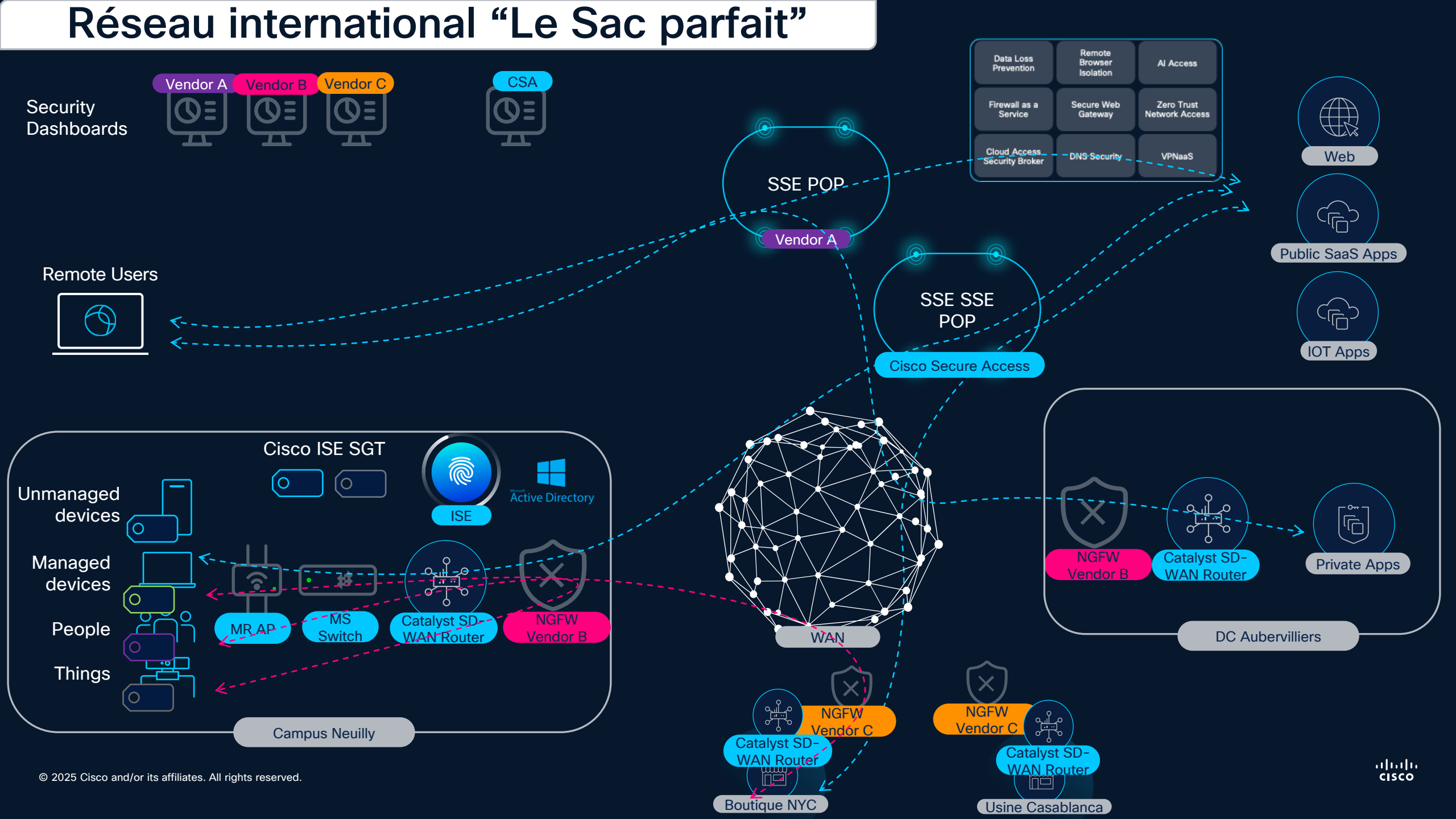
- Maintenir un haut niveau de performance et de disponibilité de son infrastructure

LE SAC PARFAIT

Réseau international “Le Sac parfait”



Réseau international “Le Sac parfait”



Cisco Secure Access: Extended SSE protection

SSE core capabilities

Secure web gateway

Zero trust network access

Firewall as-a-service

Cloud access security broker

Data loss prevention

Advanced malware protection

Sandbox

+ So much more

VPN as-a-service

Digital experience monitoring

AI Access and usage controls

Local ZTNA enforcement options

IPS with Talos threat intelligence

Enterprise browser integration

Remote browser isolation

Policy verification

DNS security

Catalyst SD-WAN + Cisco Secure Access unique integration

Simplified onboarding

- Automated IPSEC tunnel creation from both sides

up to 15X* faster than manual tunnel creation

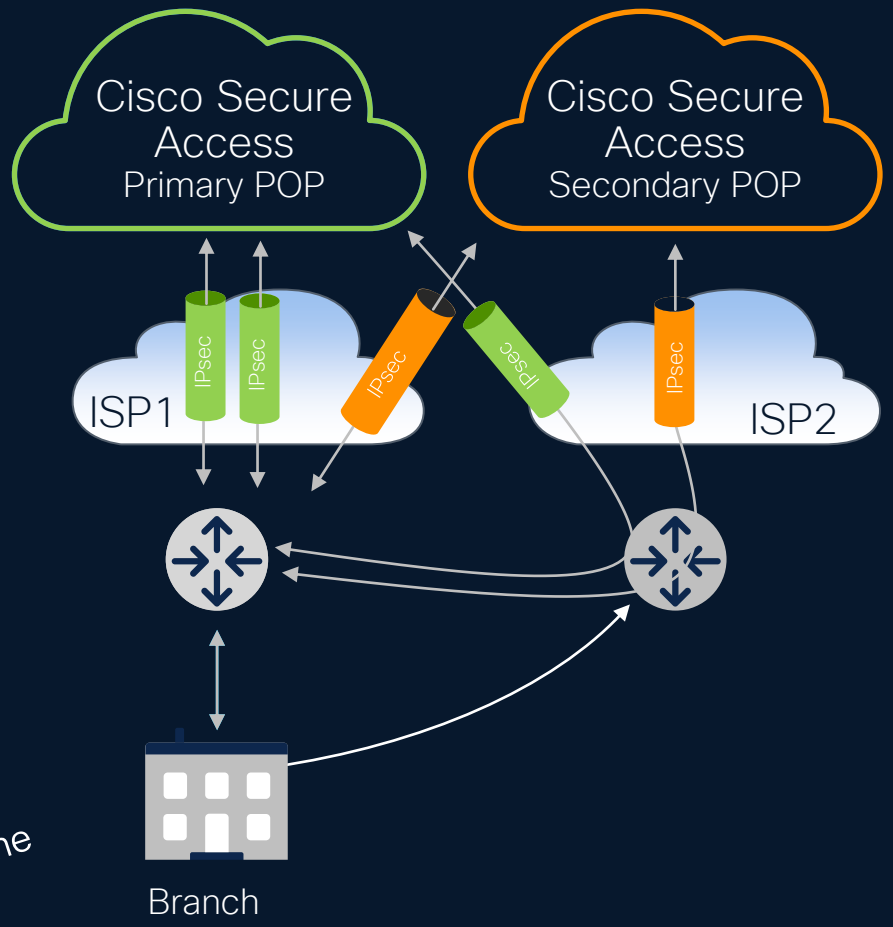
Automated failover

- Automated HA Design
  - Active/Standby
  - Active/Active
  - Failover to secondary DC
  - ECMP load balancing on SIG tunnels is based on source IP

End-to-end visibility and faster troubleshooting

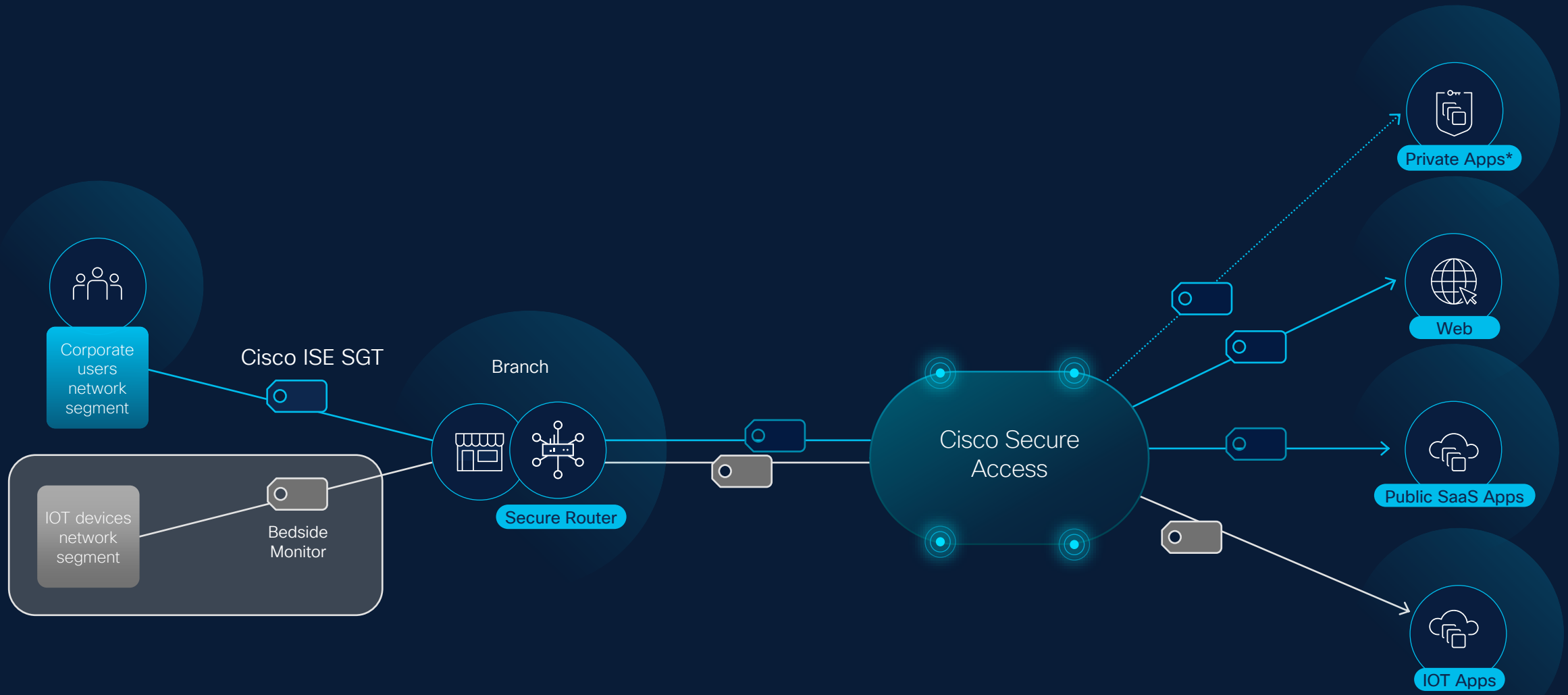
- Performance routing on CSA tunnels
- Tunnel performance monitoring

up to 10X* reduction in detection/investigation time



Fast, simple, and resilient

Catalyst SD-WAN + Cisco Secure Access unique integration



SGT inline transport over CSA IPSEC tunnels

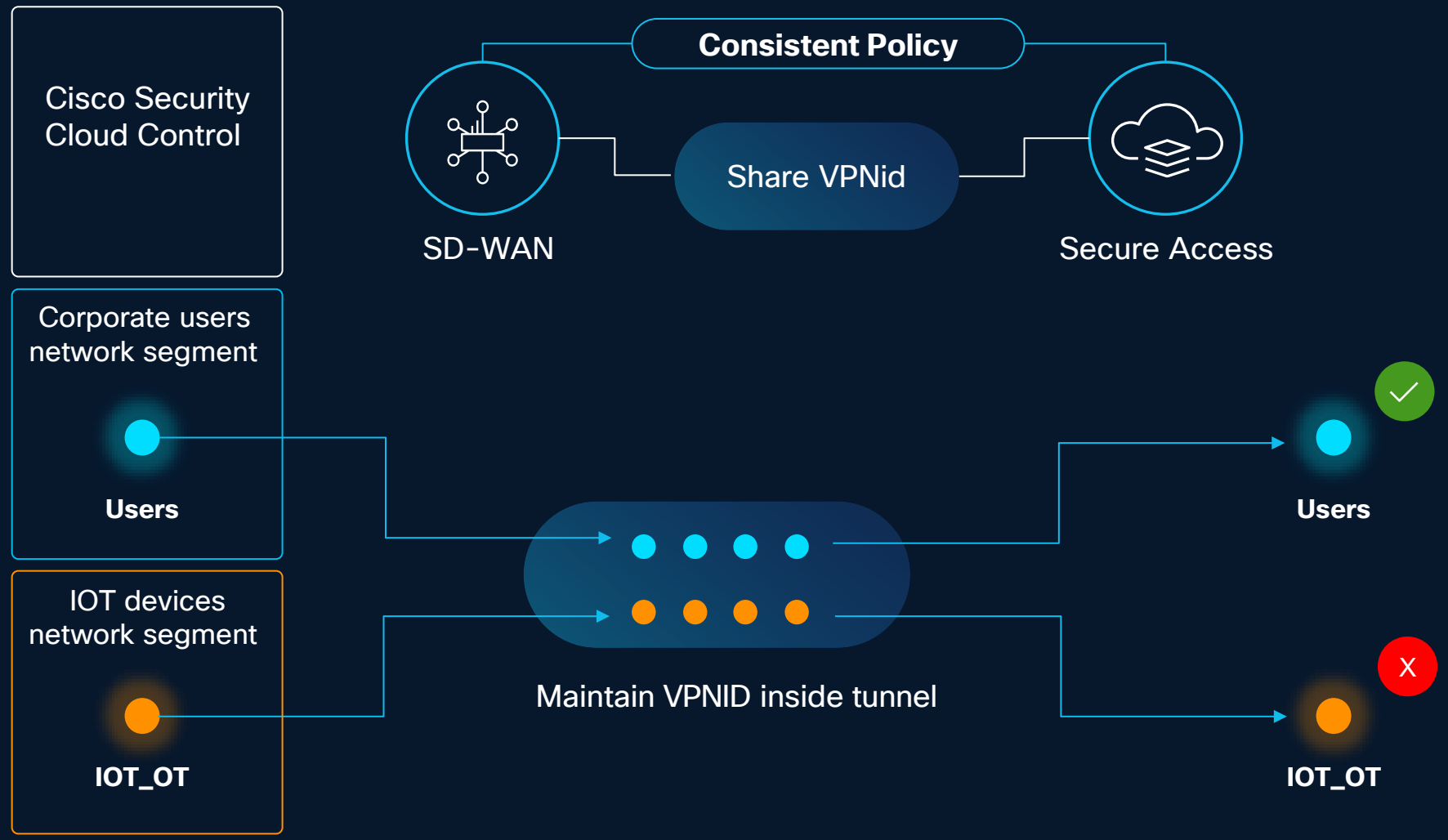
* Capabilities are planned but not yet available or guaranteed.

Catalyst SD-WAN

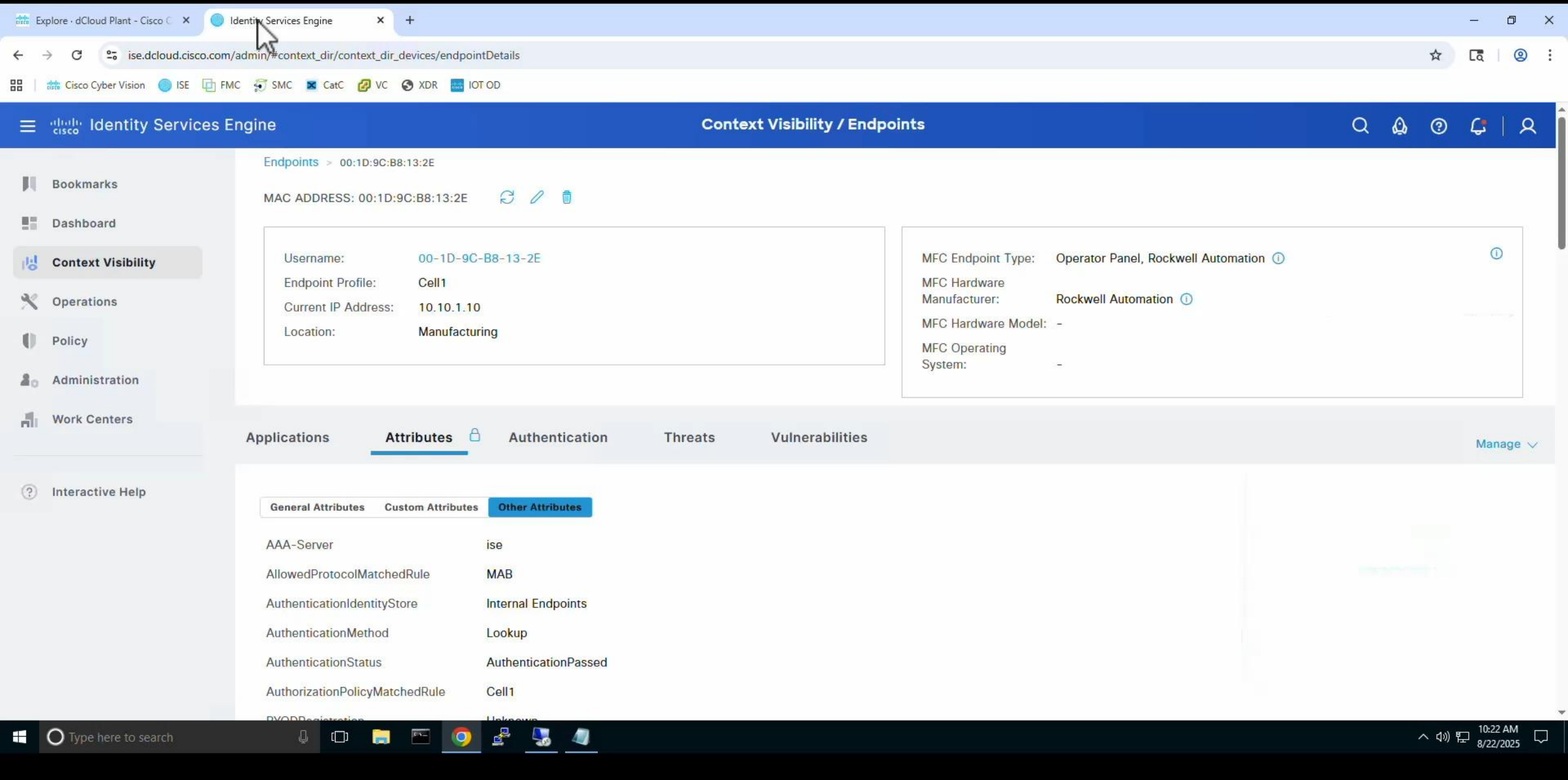
VPNid support for consistent segmentation

- ✓ VPN ID (VRF) is carried over additional headers
- ✓ Only for automated tunnels (outbound only for now)

- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



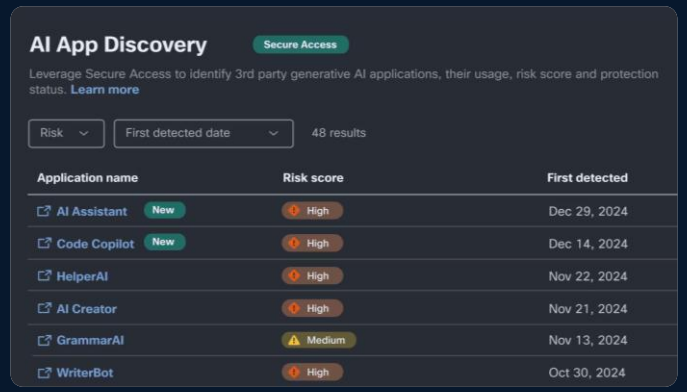
Catalyst SD-WAN and Cisco Secure Access SGT integration



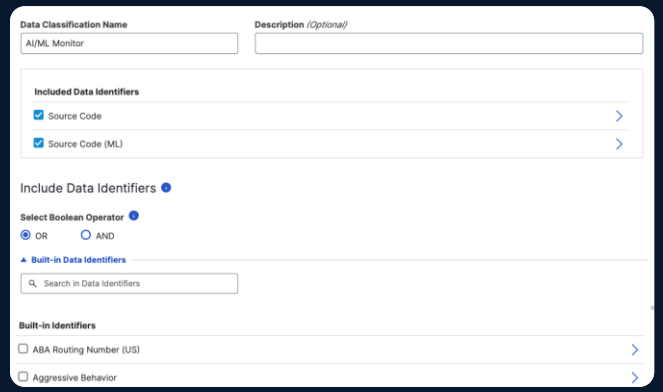
AI Access : Secure access for AI users

AI Access protection that goes beyond discovery

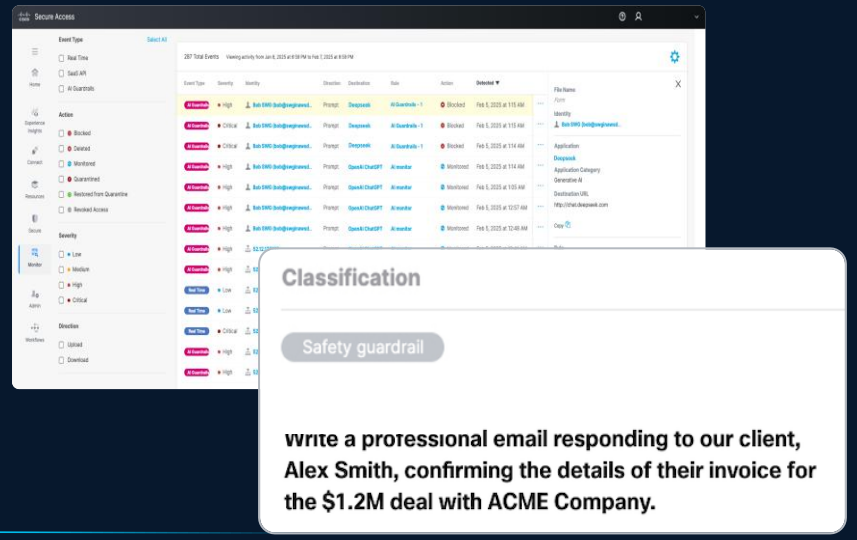
Discover shadow AI & block specific apps



Advanced AI/ML DLP controls



Enforce guardrails for AI queries: Security, Privacy, Safety

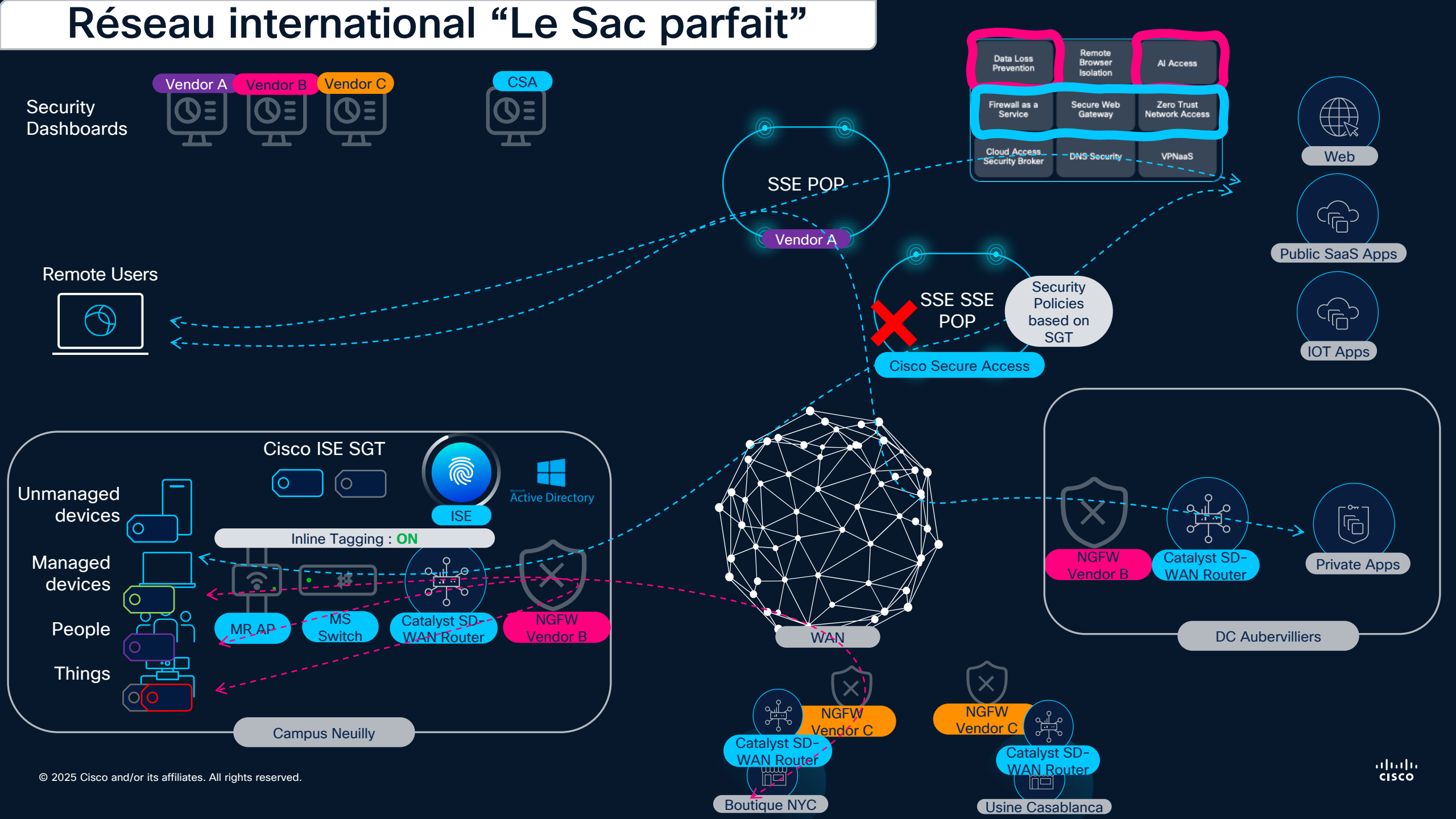


1200+
AI Apps Protected

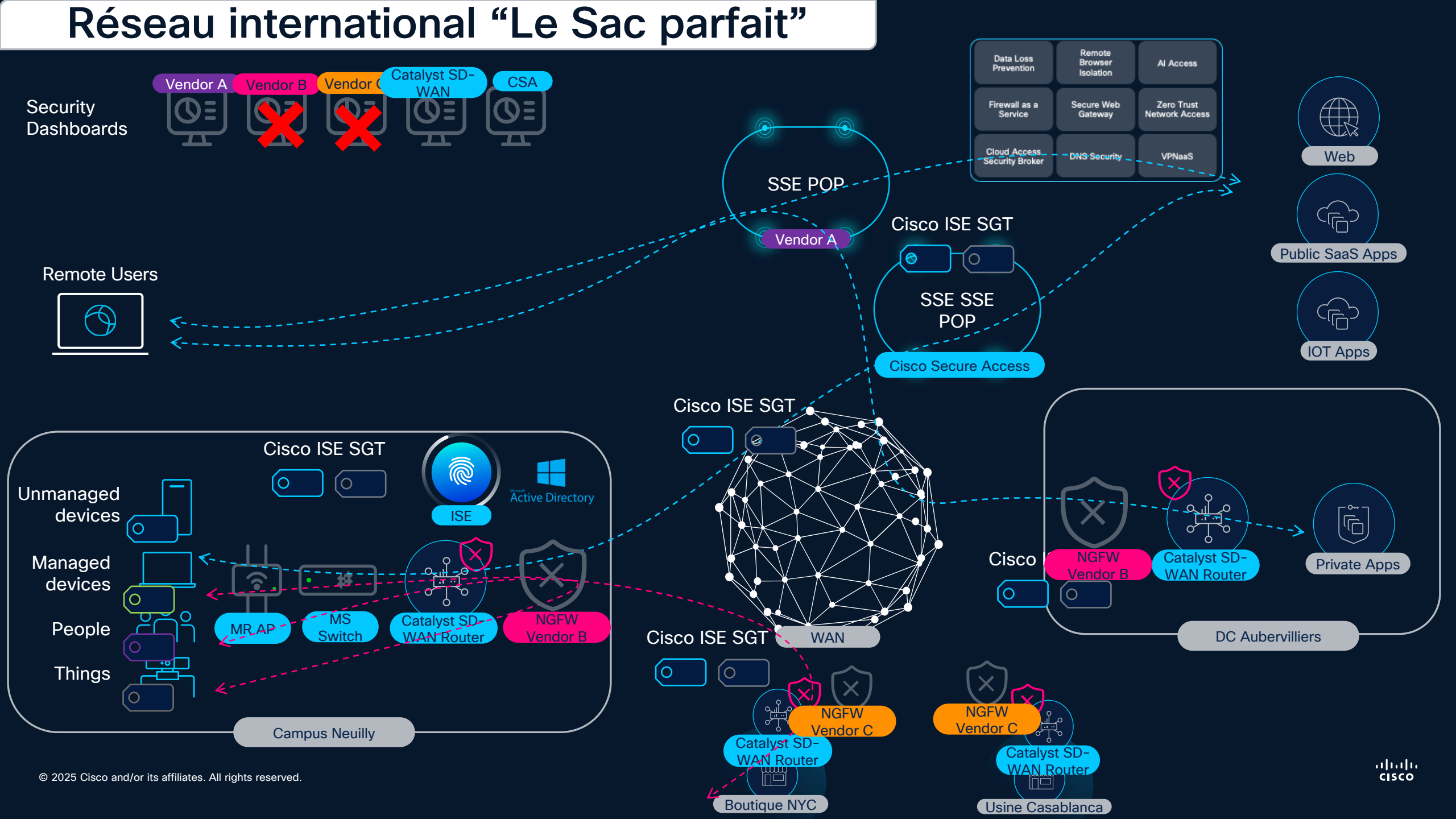
100%
Guardrails for top AI Apps

1
Unified Security Platform

Réseau international “Le Sac parfait”



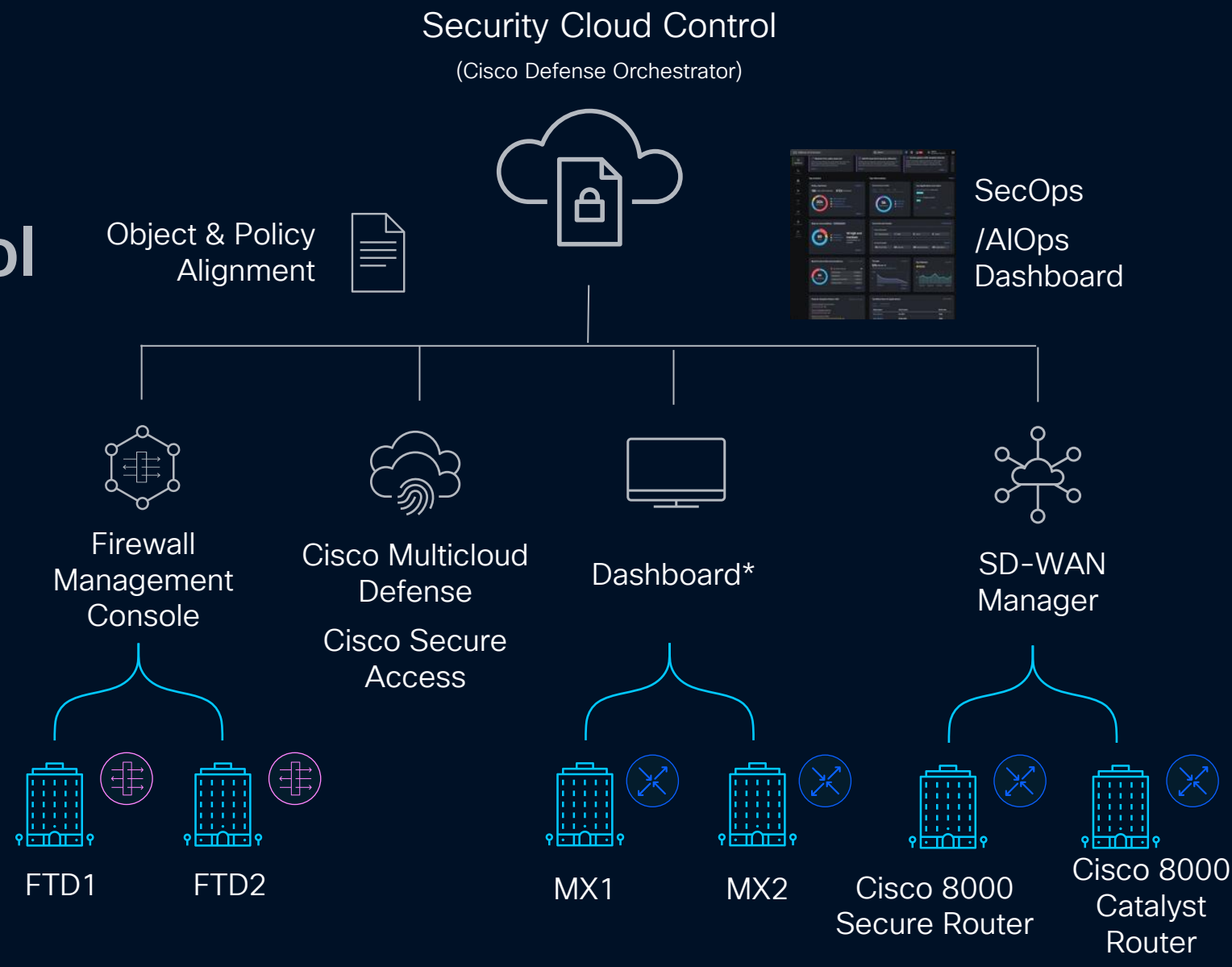
Réseau international “Le Sac parfait”



Cisco Security innovations

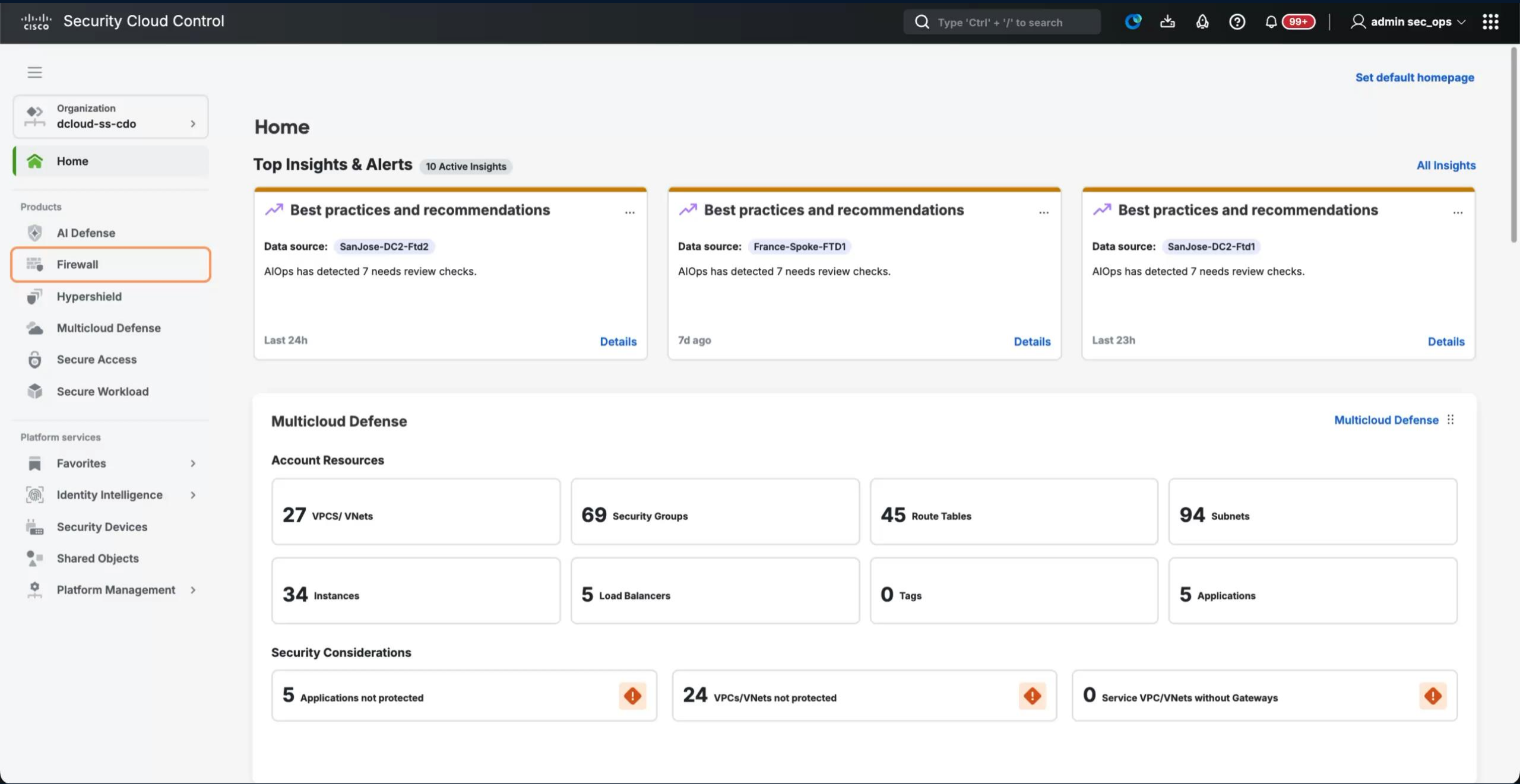
Centralized security management in Security Cloud Control

Providing SecOps admins with rich, **centralized management** with policy optimization, vulnerability management, and best practice recommendations

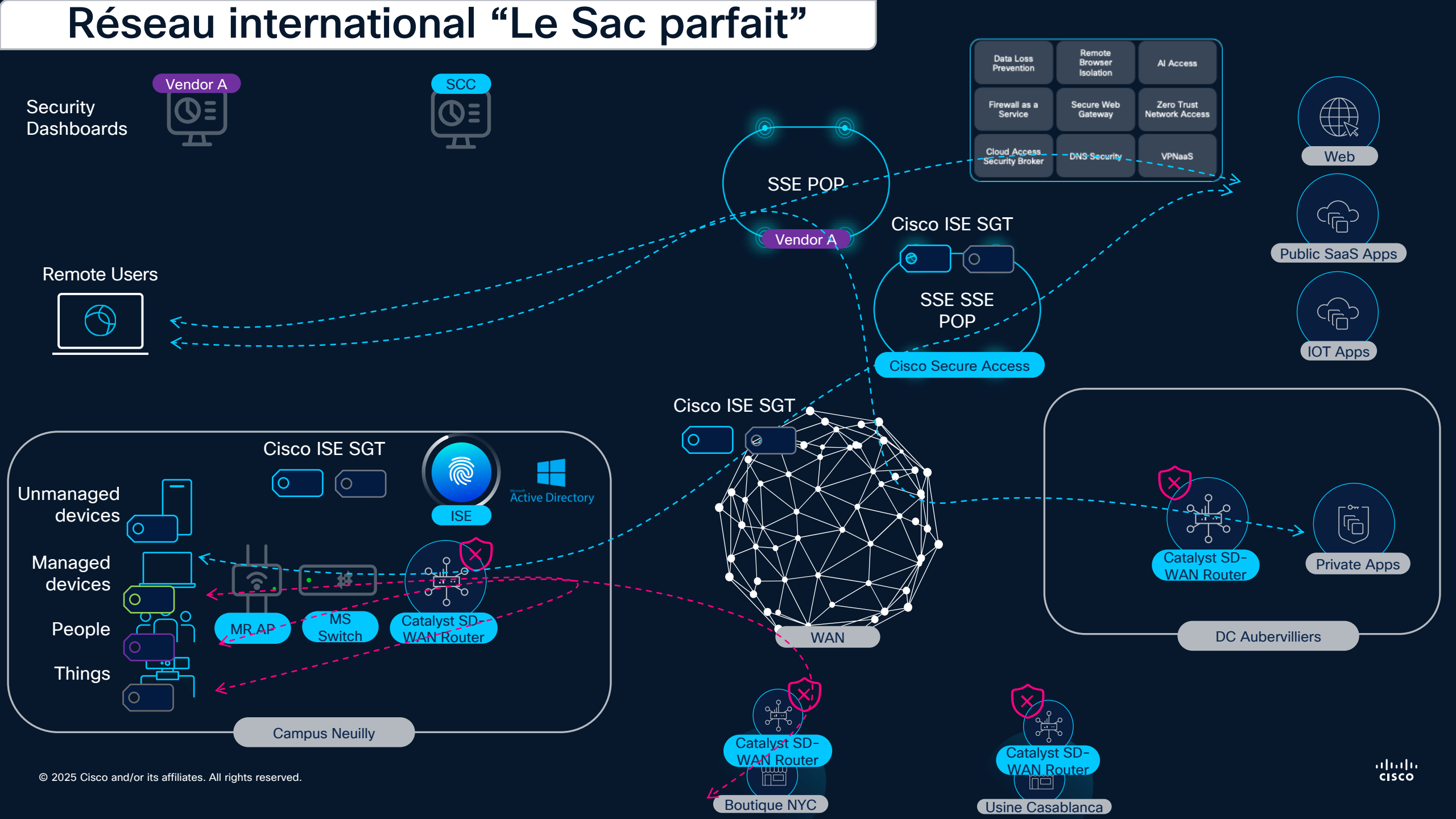


*Roadmap

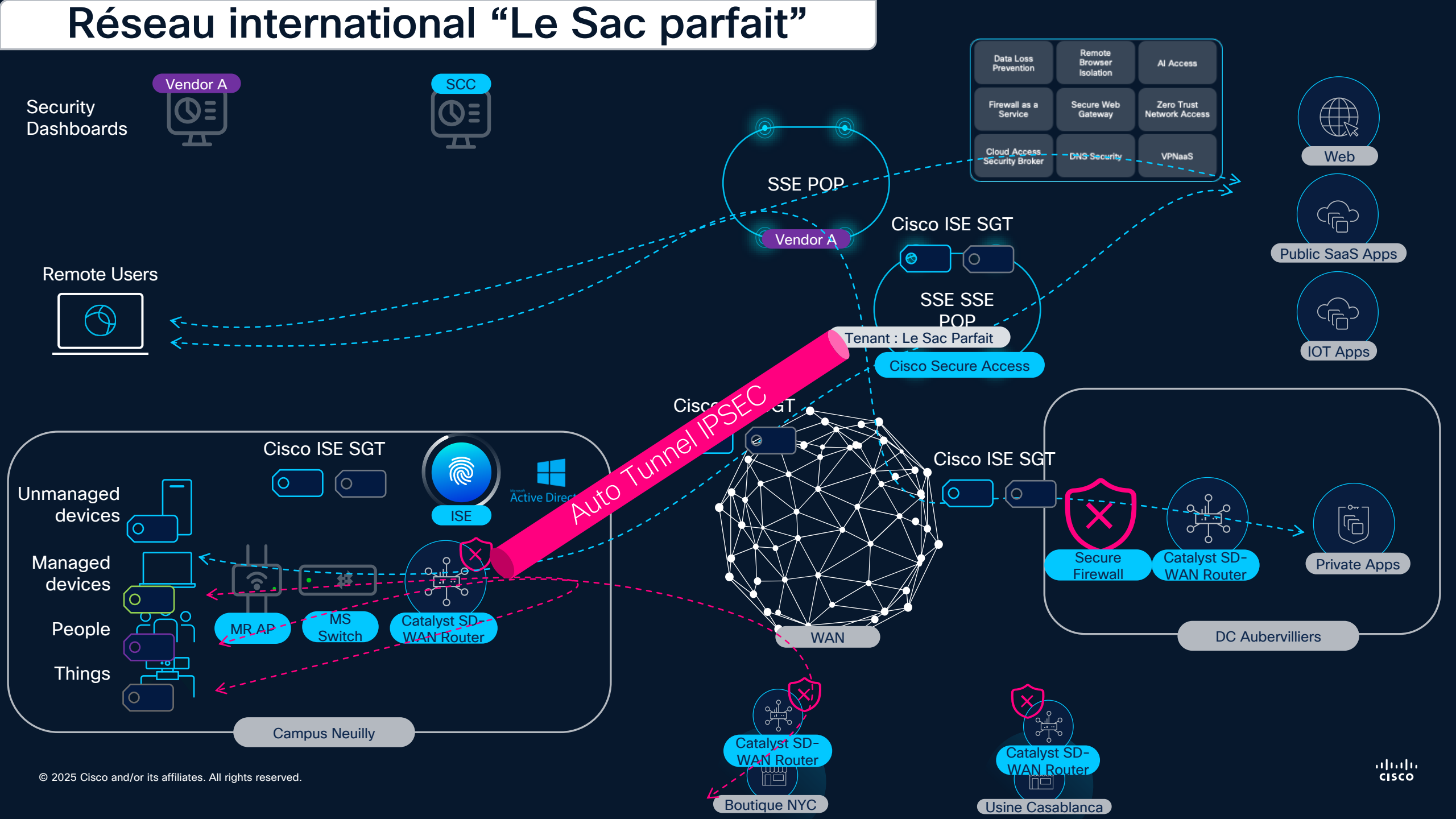
SCC – Single dashboard for Catalyst SDWAN NGFW and CSA



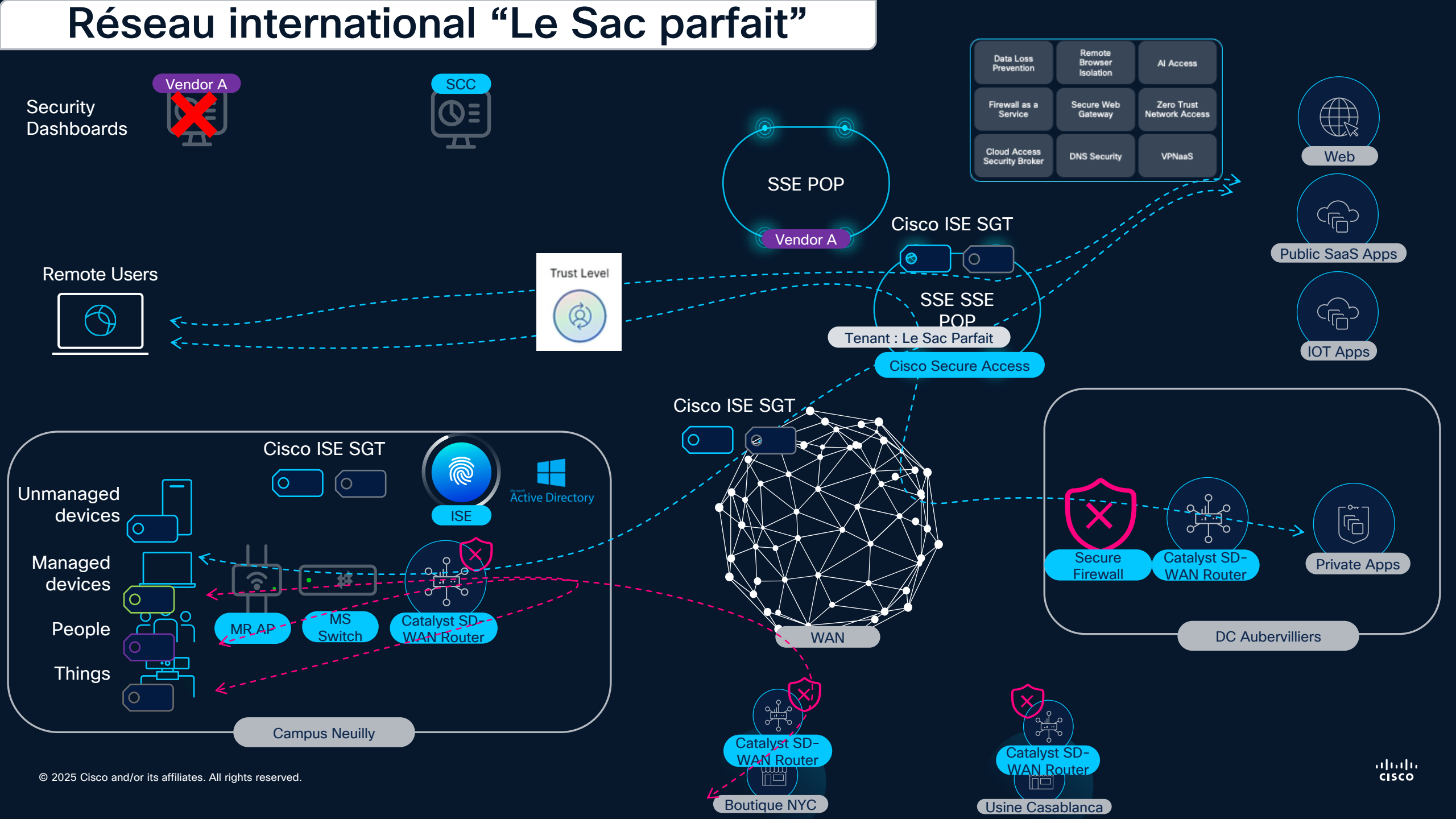
Réseau international “Le Sac parfait”



Réseau international “Le Sac parfait”



Réseau international “Le Sac parfait”



Conclusion approche uZTNA Cisco

Security Dashboards

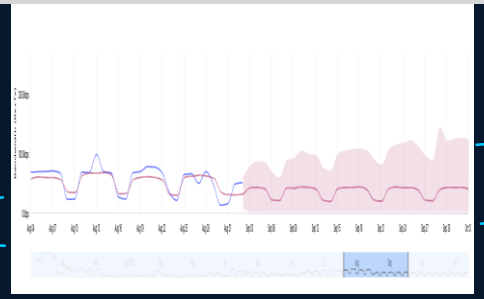
Vendor A Vendor B Vendor C SCC

Consistence et simplicité

Data Loss Prevention | Remote Browser Isolation | AI Access
Firewall as a Service | Secure Web Gateway | Zero Trust Network Access
Cloud Access Security Broker | DNS Security | VPNaaS

Web
Public SaaS Apps
IOT Apps

Haut niveau de performance et de disponibilité



Remote Users

Cisco ISE SGT

SSE SSE POP

Cisco Secure Access

Identité and Posture

Cisco ISE SGT

ISE

Active Directory

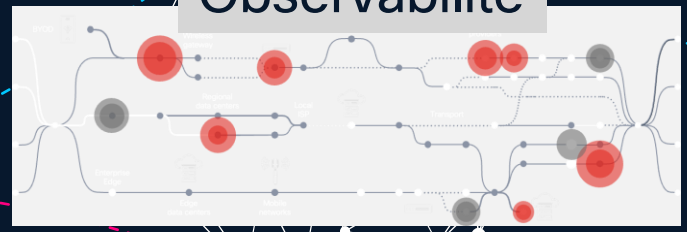
Unmanaged devices
Managed devices
People
Things

MR AP | MS Switch | Catalyst SD-WAN Router | NGFW Vendor B

Campus Neuilly

Cisco ISE SGT

Observabilité



WAN

Secure Firewall | Catalyst SD-WAN Router | Private Apps

DC Aubervilliers

Baisse des coûts

Cisco ISE SGT

NGFW Vendor C | NGFW Vendor C

Catalyst SD-WAN Router

Boutique NYC

Catalyst SD-WAN Router

Usine Casablanca

ISE

cisco

Merci