

Cisco SASE and Universal ZTNA



Julien Hernandez
Technical Solution Architect
Security/SASE

Nicolas Boursier
Technical Solution Architect
SD-WAN/SASE

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.

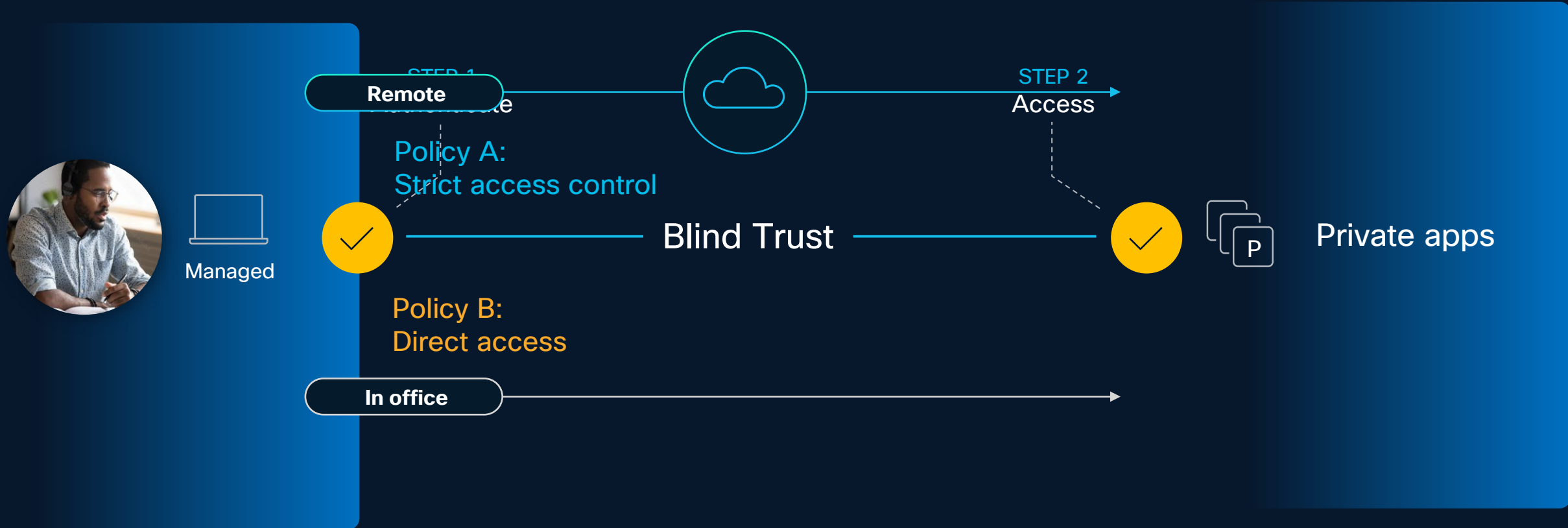
SD-WAN as a key building block of SASE Evolution

- 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

The collage features three overlapping screenshots of press releases. The top-right screenshot is from Zscaler, with a dark blue background and white text, titled "Eliminate Lateral Threat Movement with Zero Trust SD-WAN". The middle-left screenshot is from Netskope, with a white background and dark blue text, titled "Press Release" and "Netskope Acquires Infiot, Will Deliver Fully Integrated, Single-Vendor SASE Platform". The bottom-right screenshot is from Palo Alto Networks, with a white background and green text, titled "Software Defined WAN (SD-WAN)" and "Palo Alto Networks Completes Acquisition of CloudGenix".

Le Universal ZTNA c'est quoi?

Traditional ZTNA: Work from home solution



Managed devices,
private apps

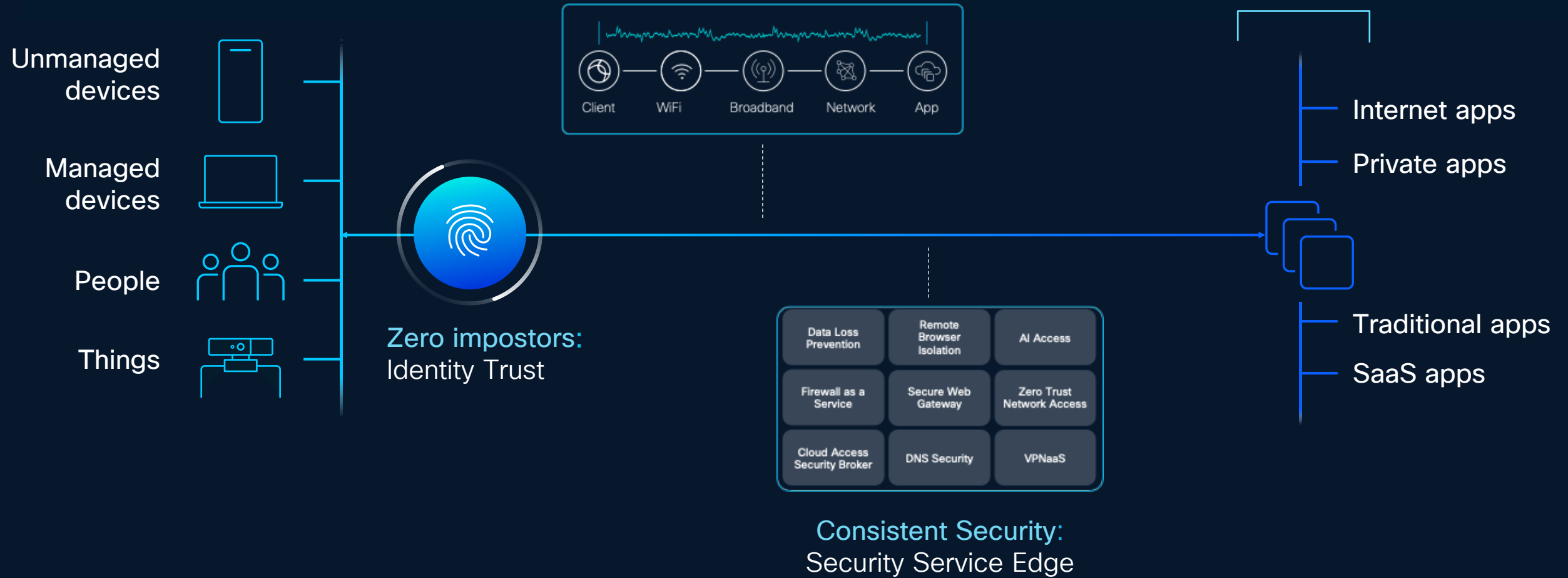
Different policies
for home versus office

Blind trust between
authentication and access

Universal ZTNA from Cisco

Zero downtime:
Experience and Policy Assurance

Zero friction



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

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



USERS



MACHINES



SERVICES



HRIS



DATA



APPS



PLATFORMS

↑ Identity Providers ↑ ↑ ↑ User Context

SailPoint

Dragos

CrowdStrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

Amazon

Cisco's Identity Intelligence | Dynamic User Trust Scores

Provide in-session risk evaluation in the Secure Access dashboard

User Trust Score



Authentication

Authenticate:

- Basic log-in?
- Strong MFA?
- Is this a known device or location?

User Activities and Application Access

Ongoing Evaluation:

- What is this user's trust score?
- Have risky activities occurred during the session?
- Has the trust score changed?

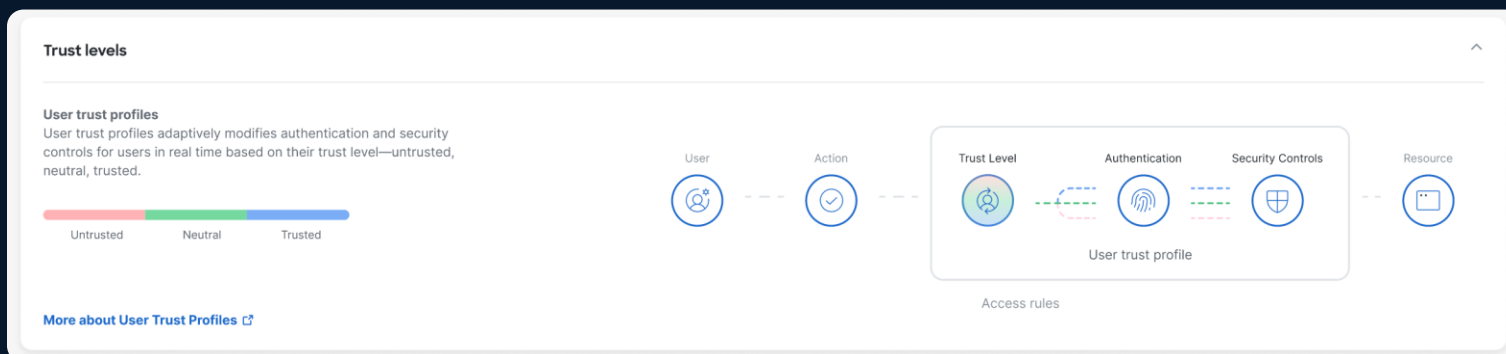


Cisco Identity Intelligence s'intègre à Secure Access pour analyser le comportement dans l'ensemble de l'écosystème d'identité, en attribuant un score de confiance dynamique qui détecte et bloque de manière proactive les activités malveillantes pendant les sessions actives.

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

Trust level	Authentication controls	Security Controls
Trusted	Single Sign On	IPS: Connectivity Over Security
Neutral	Reauthenticate Every 24hrs	IPS: Security Over Connectivity Geolocation: US only
Untrusted	Block	-



Etude de cas Universal ZTNA

Etude de cas Universal ZTNA

Julien



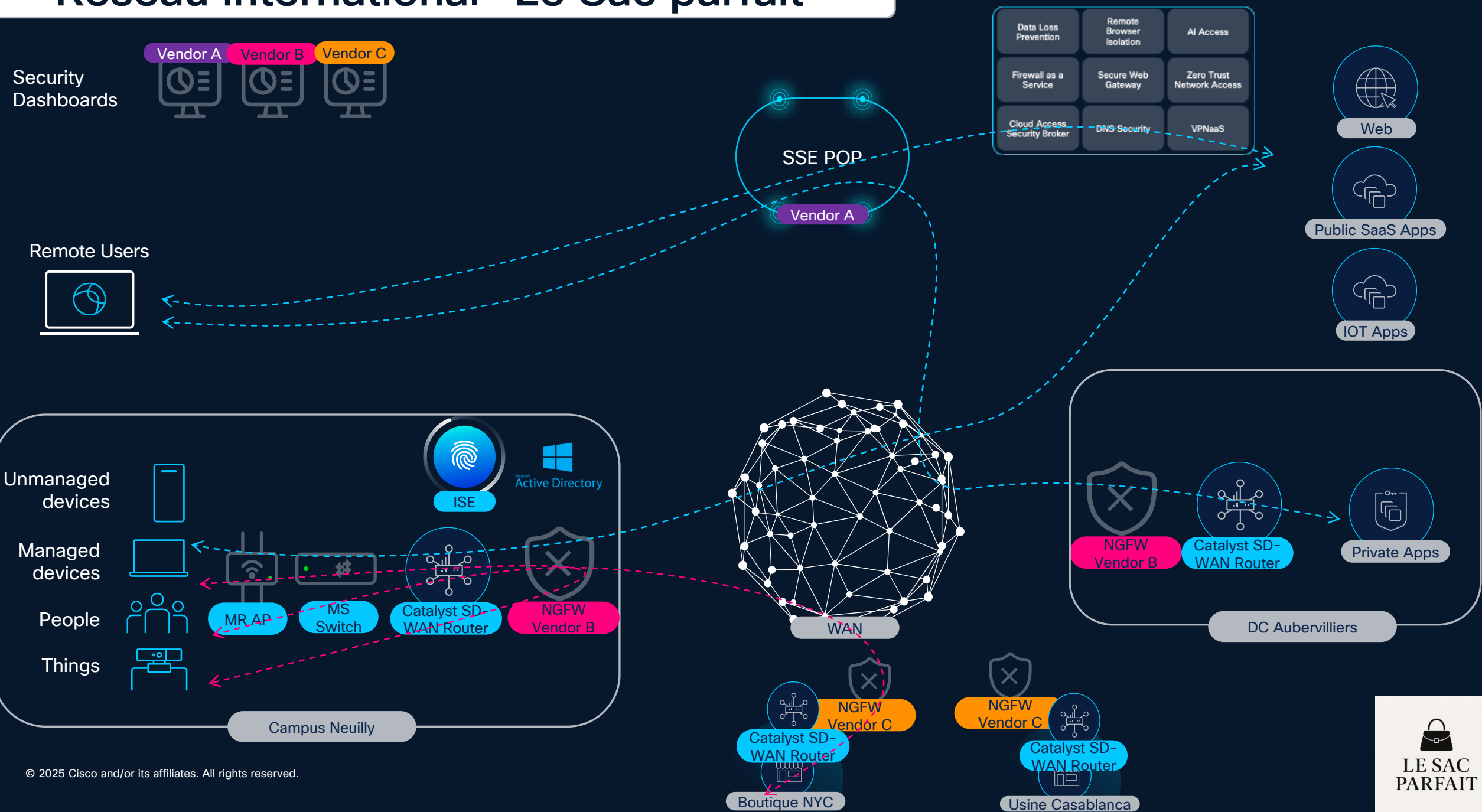
CIO Entreprise “Le Sac Parfait”

Nicolas

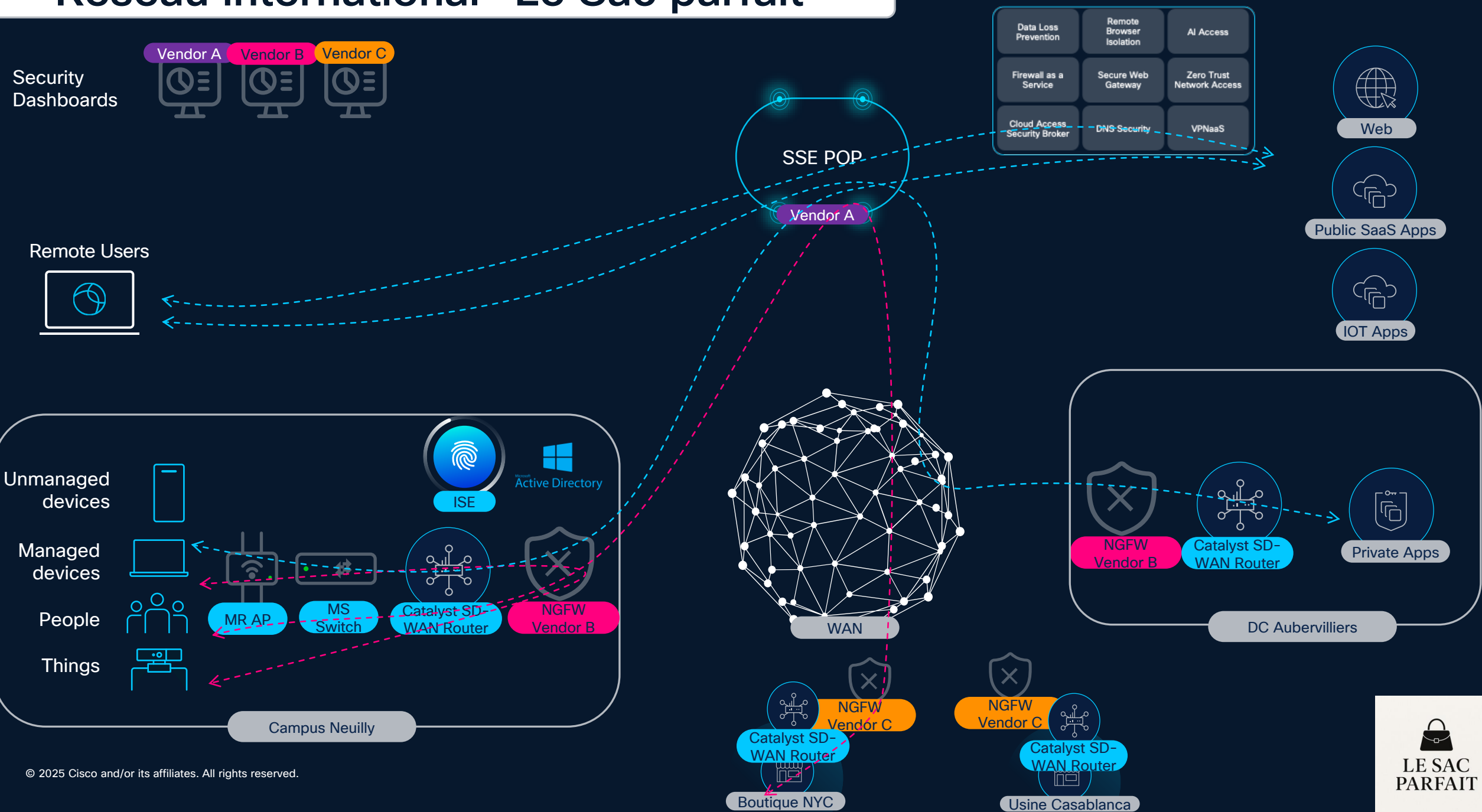


Solution Engineer Cisco

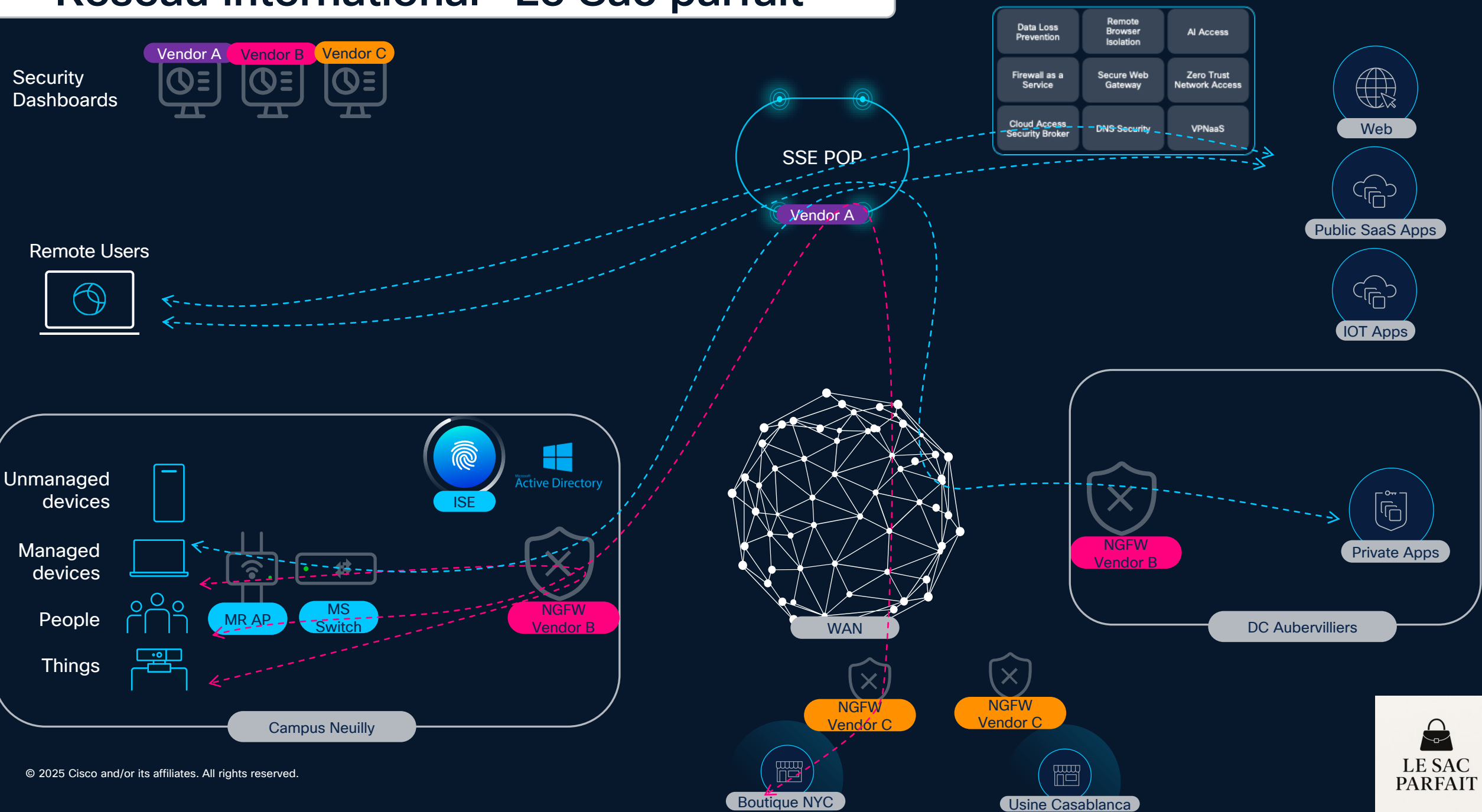
Réseau international "Le Sac parfait"



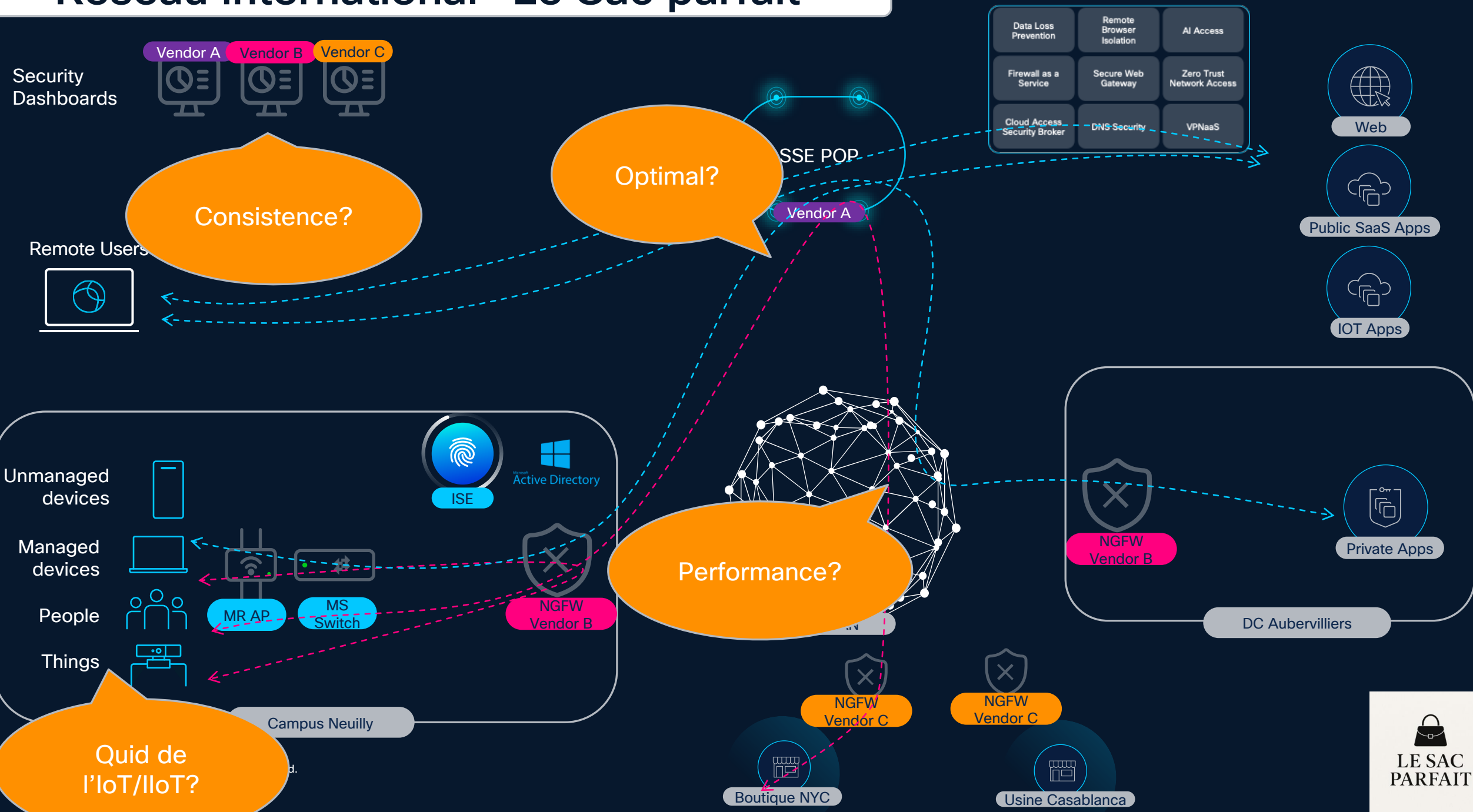
Réseau international "Le Sac parfait"



Réseau international "Le Sac parfait"



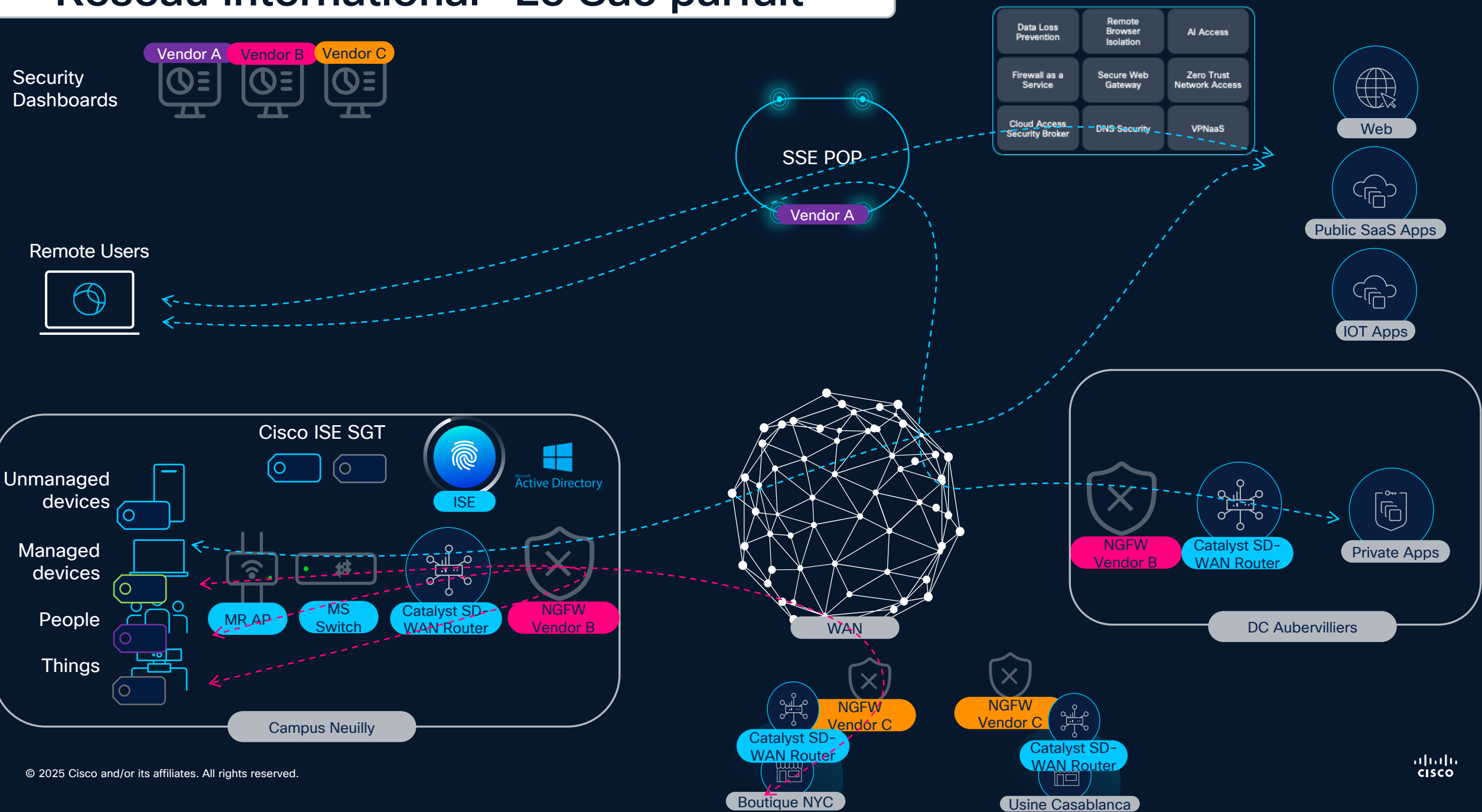
Réseau international "Le Sac parfait"



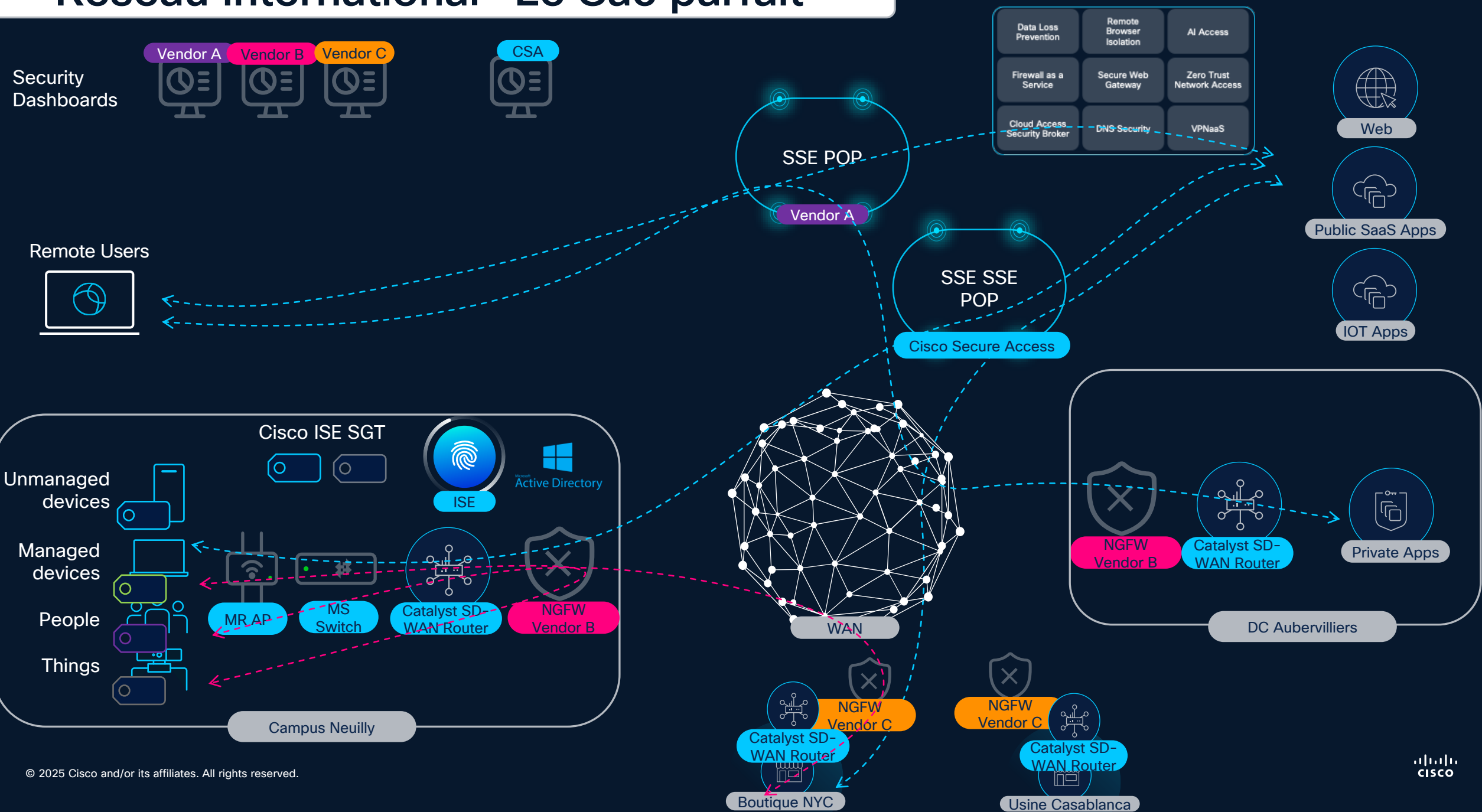
Objectifs CIO/CTO “Le Sac Parfait”

- Réduire les coûts et la complexité
 - Réduire le nombre d'équipements
 - Consistance 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

Réseau international "Le Sac parfait"



Réseau international "Le Sac parfait"



Cisco Secure Access: Extended SSE protection

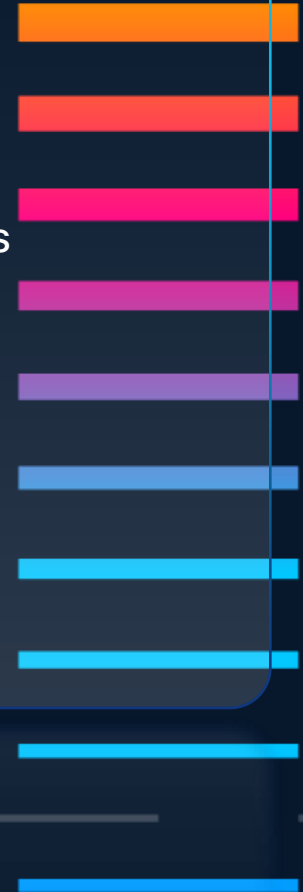
SSE core capabilities

- 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

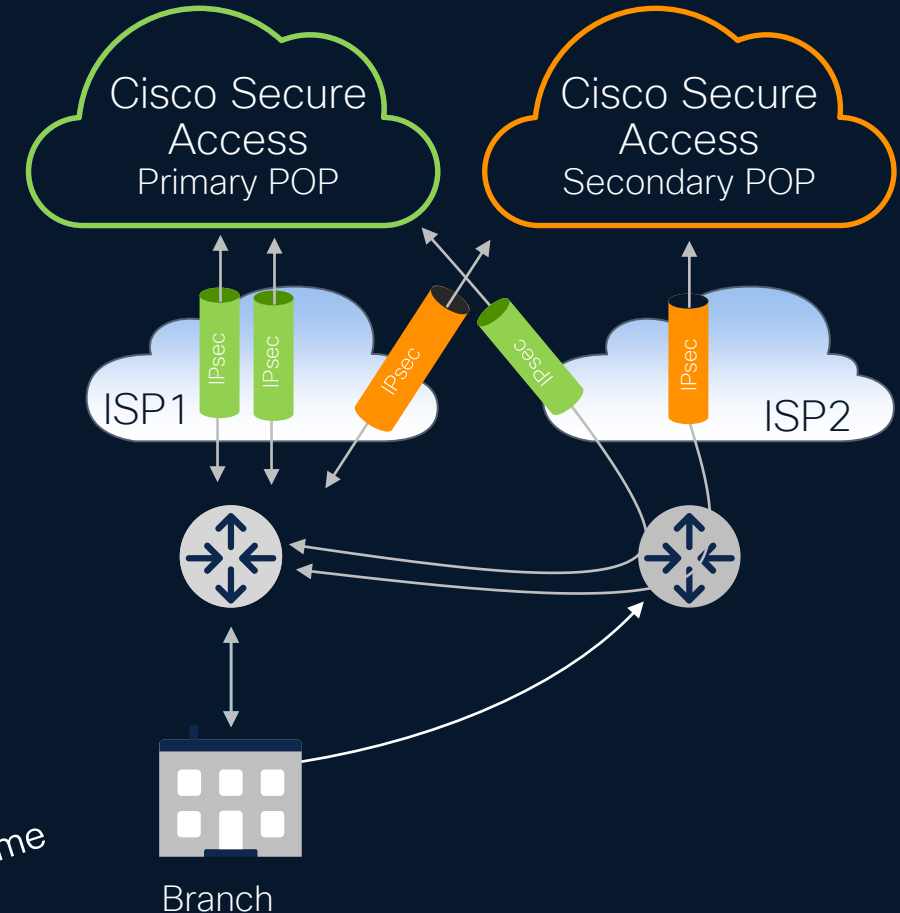
- Automated IPSEC tunnel creation from both sides
- up to 15X* faster than manual tunnel creation*

Automated failover

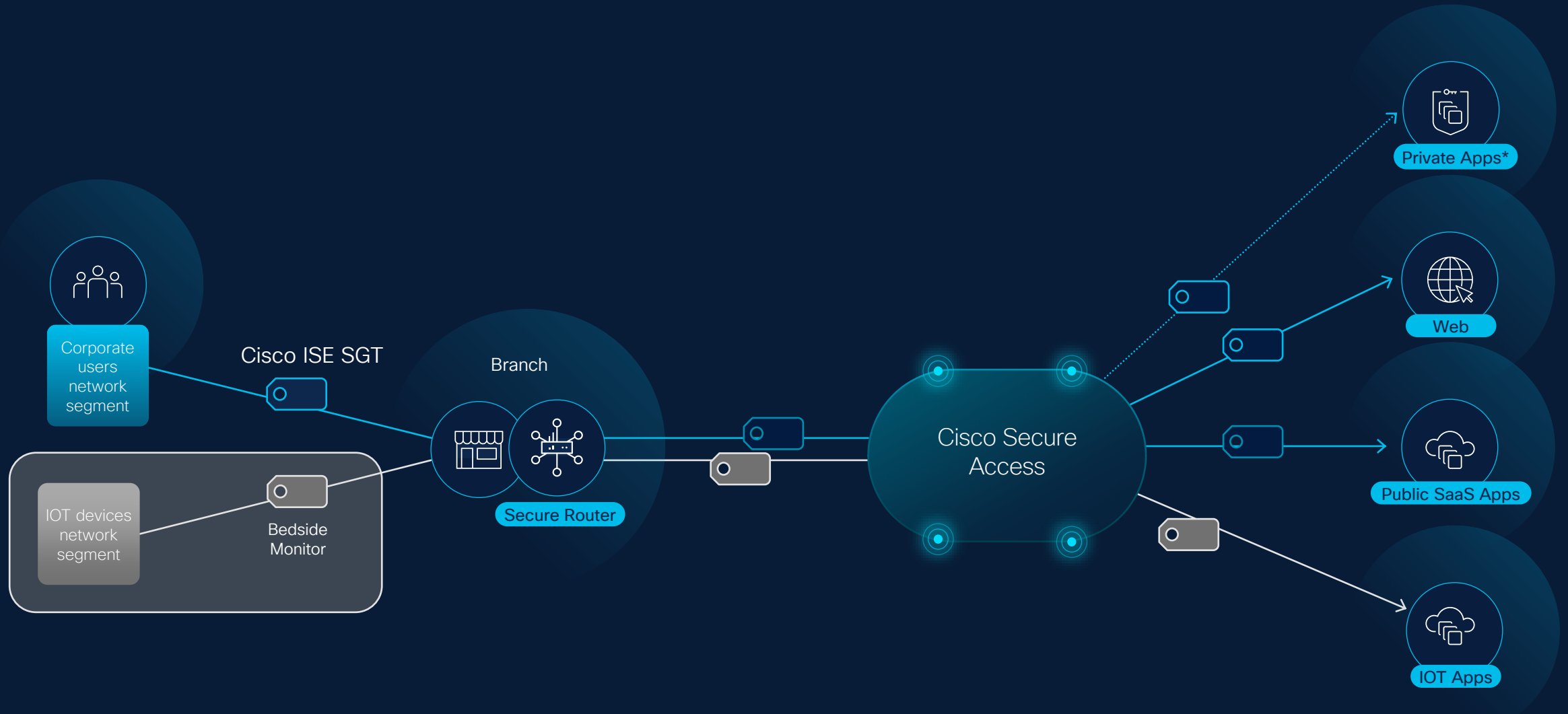
- Automated HA Design
 - Active/Standby
 - Active/Active
 - Failover to secondary DC
 - ECMP load balancing on SIG tunnels is based on source IP

End-to-end visibility and faster troubleshooting

- Performance routing on CSA tunnels
 - Tunnel performance monitoring
- up to 10X* reduction in detection/investigation time*



Catalyst SD-WAN + Cisco Secure Access unique integration



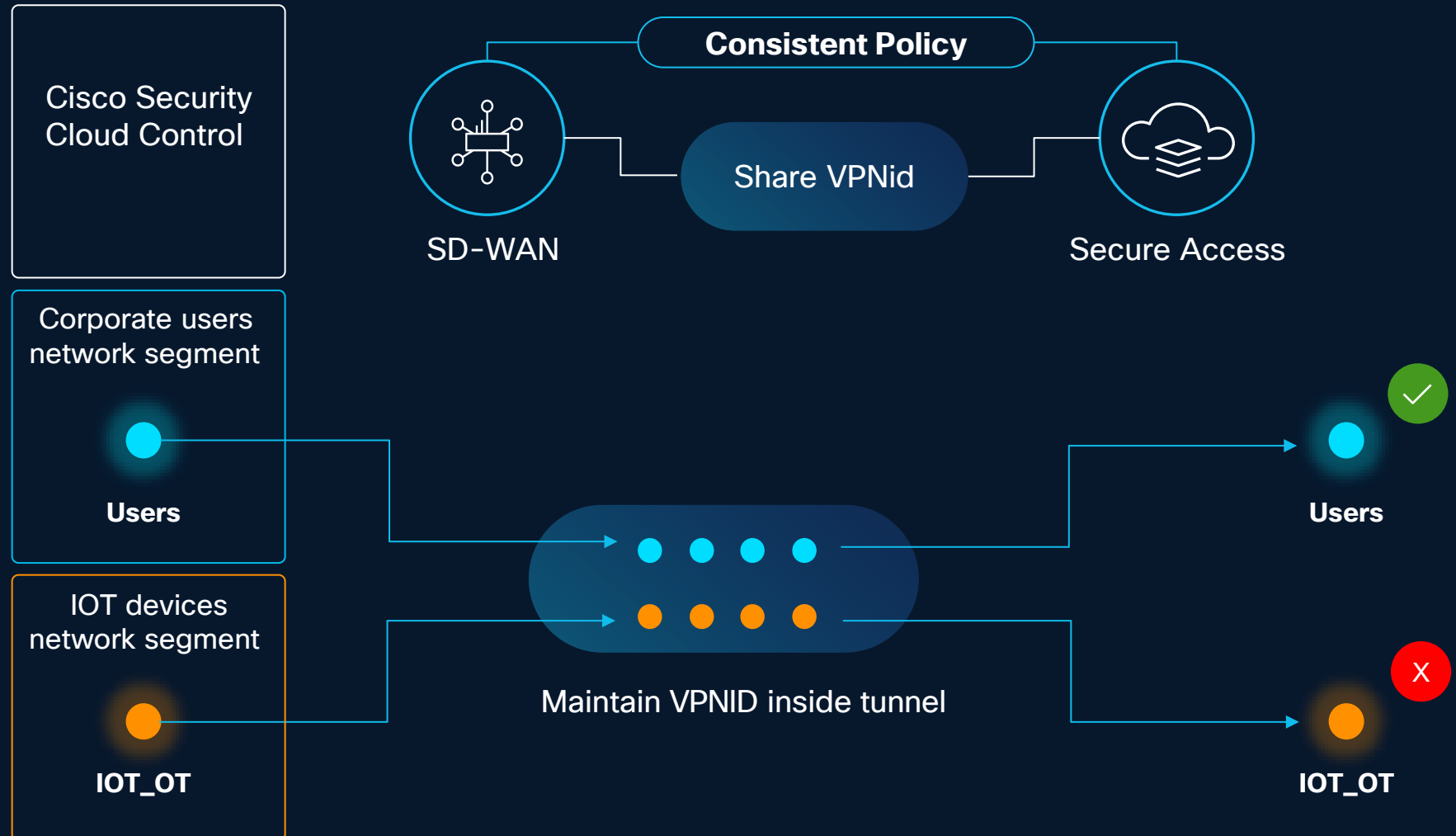
SGT inline transport over CSA IPSEC tunnels

Catalyst SD-WAN

VPNid support for consistent segmentation

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

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



Catalyst SD-WAN and Cisco Secure Access SGT integration

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The browser address bar indicates the URL is `ise.dcloud.cisco.com/admin/#context_dir/context_dir_devices/endpointDetails`. The page title is "Context Visibility / Endpoints".

The main content area displays details for an endpoint with MAC address `00:1D:9C:B8:13:2E`. The details are organized into two columns:

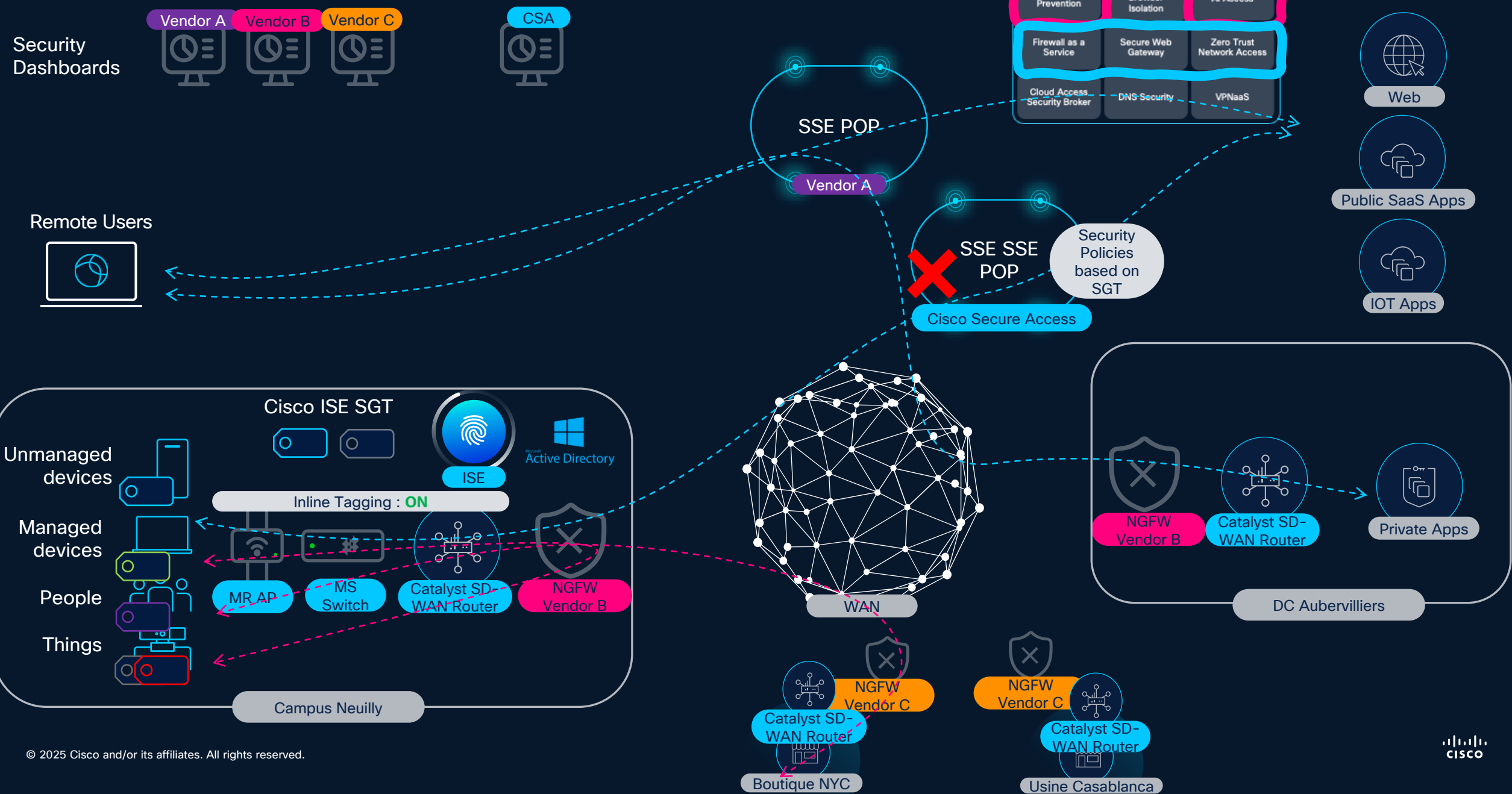
- Left Column:**
 - Username: `00-1D-9C-B8-13-2E`
 - Endpoint Profile: `Cell1`
 - Current IP Address: `10.10.1.10`
 - Location: `Manufacturing`
- Right Column:**
 - MFC Endpoint Type: `Operator Panel, Rockwell Automation`
 - MFC Hardware Manufacturer: `Rockwell Automation`
 - MFC Hardware Model: `-`
 - MFC Operating System: `-`

Below the details, there are tabs for "Applications", "Attributes", "Authentication", "Threats", and "Vulnerabilities". The "Attributes" tab is active, showing a table of attributes:

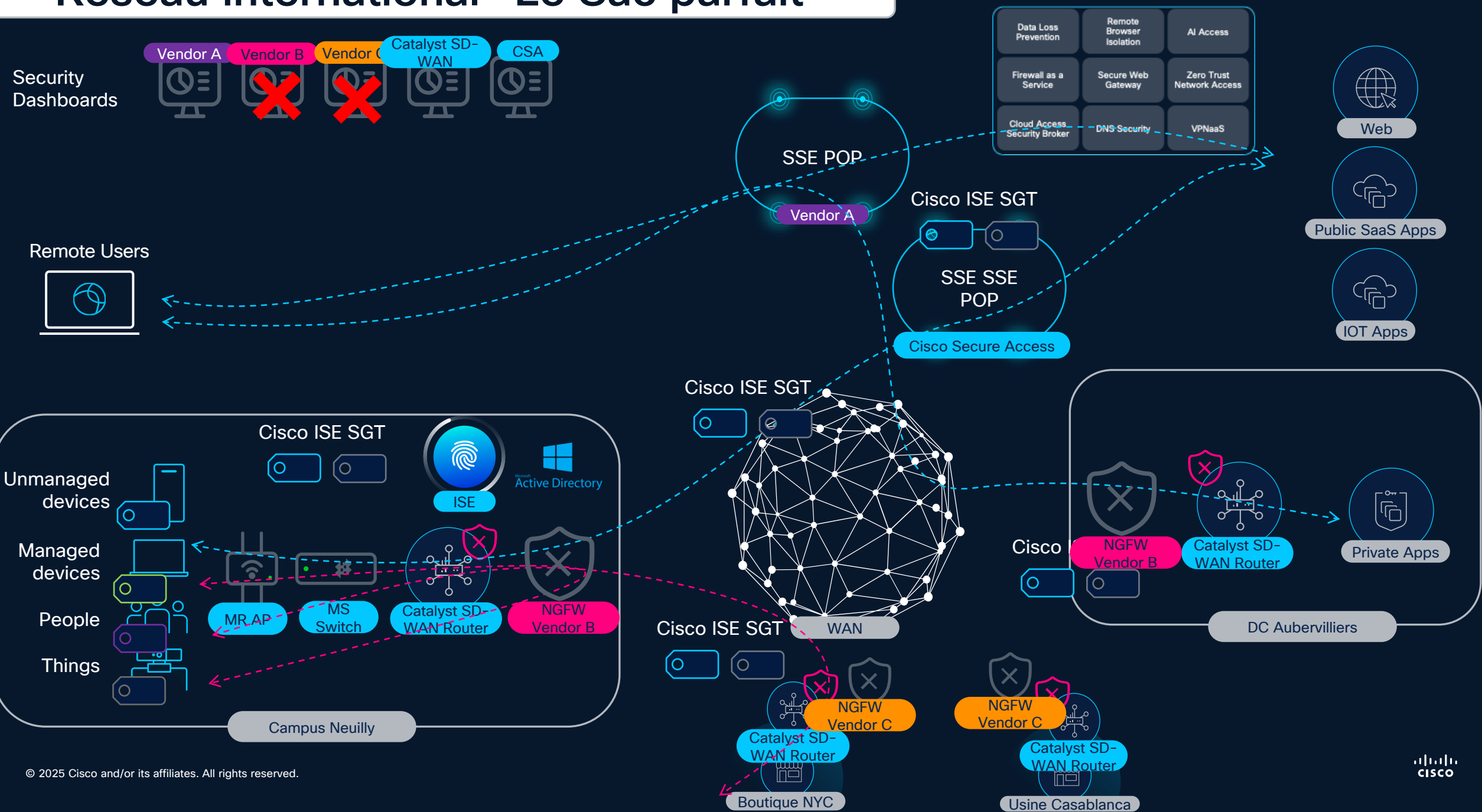
General Attributes	Custom Attributes	Other Attributes
AAA-Server		ise
AllowedProtocolMatchedRule		MAB
AuthenticationIdentityStore		Internal Endpoints
AuthenticationMethod		Lookup
AuthenticationStatus		AuthenticationPassed
AuthorizationPolicyMatchedRule		Cell1
PVODRegistration		Unknown

The Windows taskbar at the bottom shows the system time as 10:22 AM on 8/22/2025.

Réseau international "Le Sac parfait"



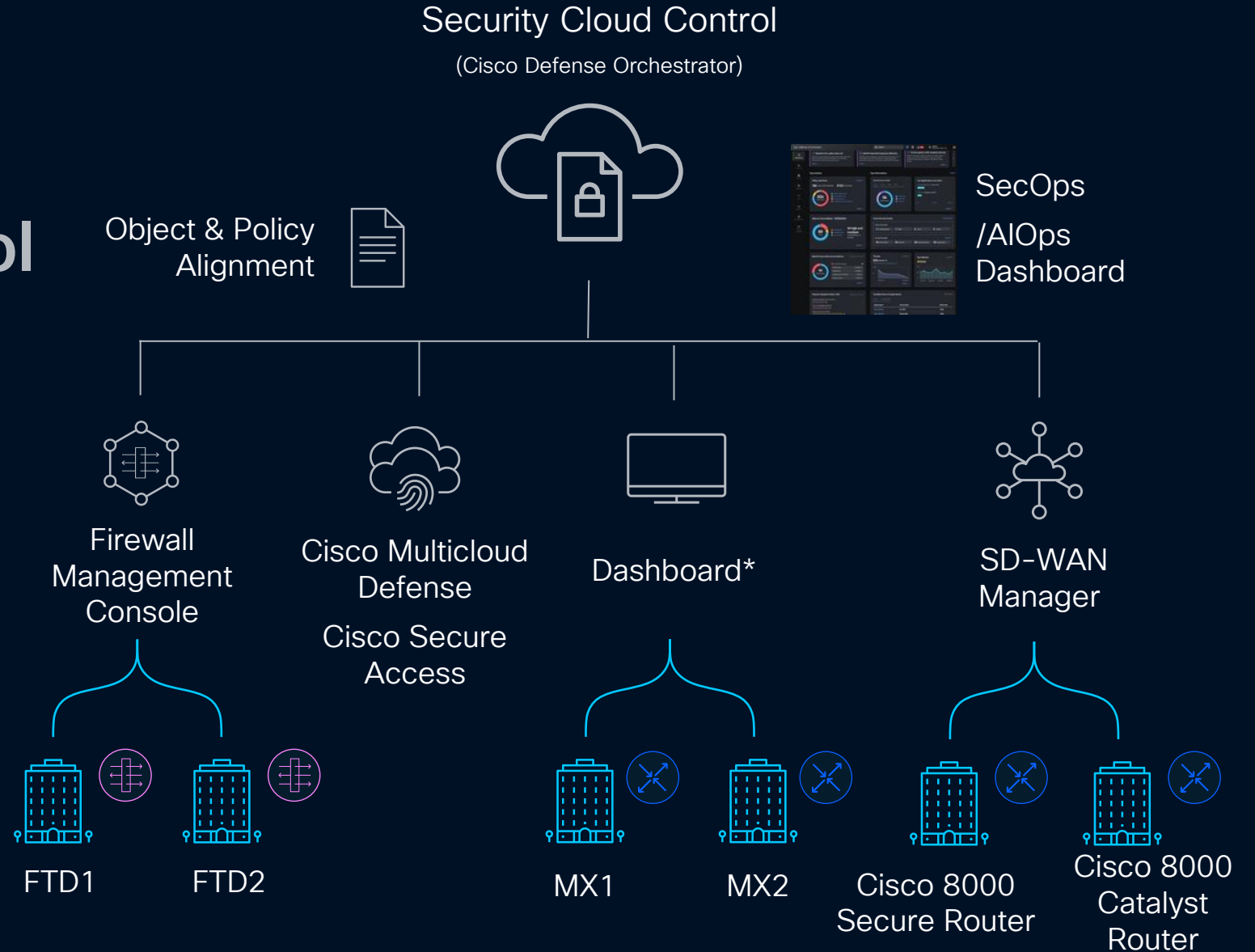
Réseau international "Le Sac parfait"



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



SCC – Single dashboard for Catalyst SDWAN NGFW and CSA

- Organization: dcloud-ss-cdo
- Home
- Products
 - AI Defense
 - Firewall**
 - Hypershield
 - Multicloud Defense
 - Secure Access
 - Secure Workload
- Platform services
 - Favorites
 - Identity Intelligence
 - Security Devices
 - Shared Objects
 - Platform Management

Home

Top Insights & Alerts 10 Active Insights

[All Insights](#)

<p>Best practices and recommendations</p> <p>Data source: SanJose-DC2-Ftd2</p> <p>AIOps has detected 7 needs review checks.</p> <p>Last 24h Details</p>	<p>Best practices and recommendations</p> <p>Data source: France-Spoke-FTD1</p> <p>AIOps has detected 7 needs review checks.</p> <p>7d ago Details</p>	<p>Best practices and recommendations</p> <p>Data source: SanJose-DC2-Ftd1</p> <p>AIOps has detected 7 needs review checks.</p> <p>Last 23h Details</p>
--	---	--

Multicloud Defense Multicloud Defense

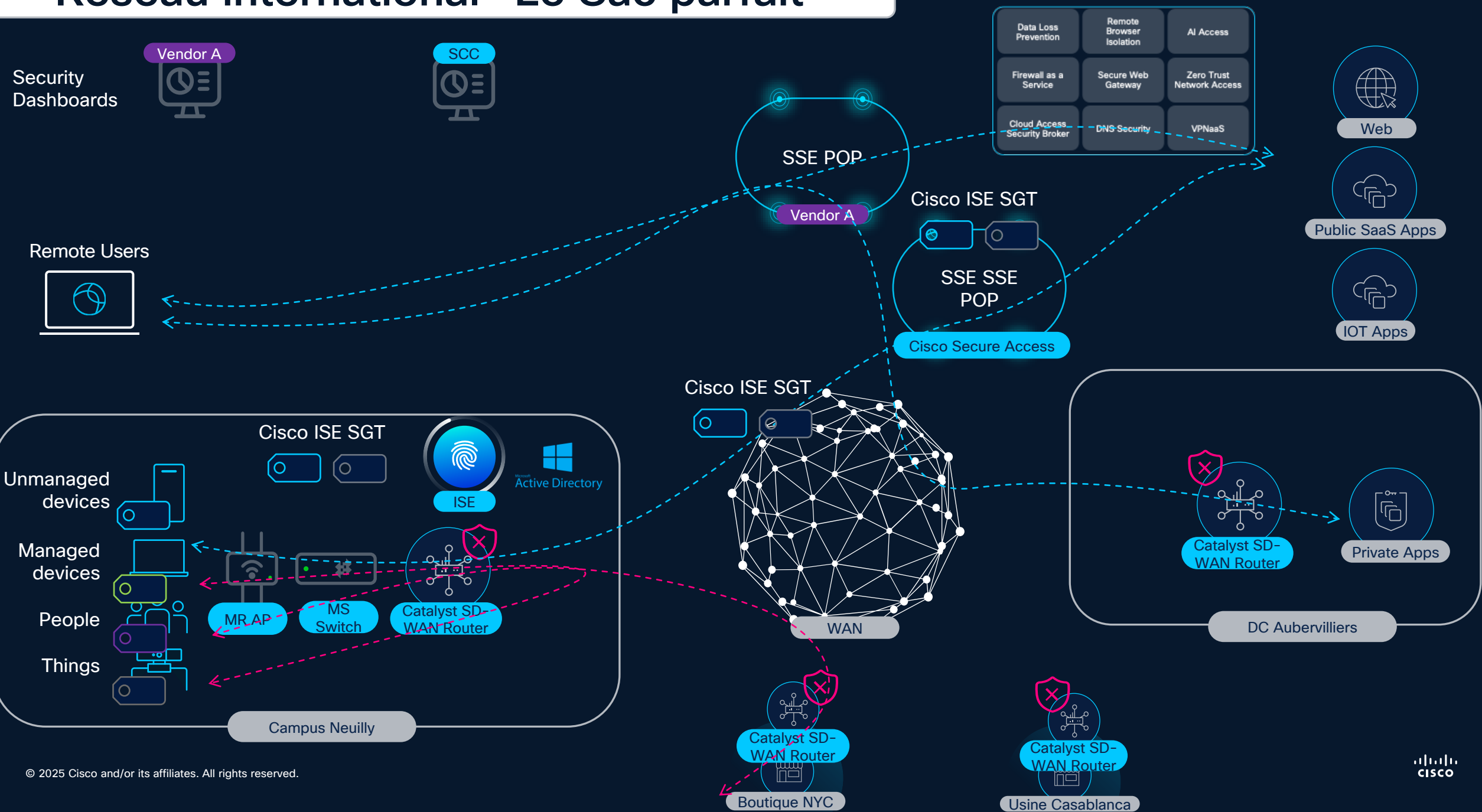
Account Resources

27 VPCs/ VNETs	69 Security Groups	45 Route Tables	94 Subnets
34 Instances	5 Load Balancers	0 Tags	5 Applications

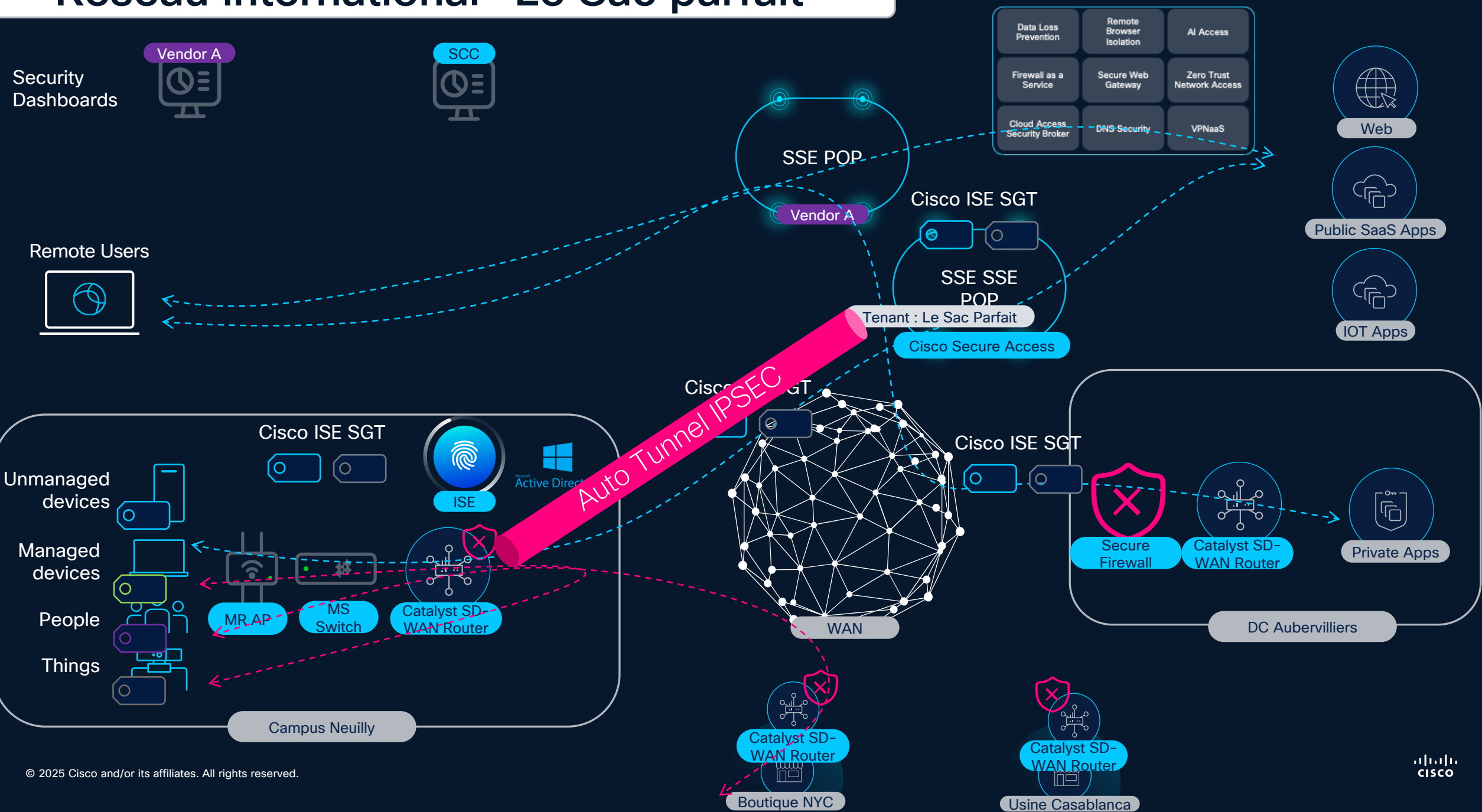
Security Considerations

5 Applications not protected	24 VPCs/VNETs not protected	0 Service VPC/VNETs without Gateways
-------------------------------------	------------------------------------	---

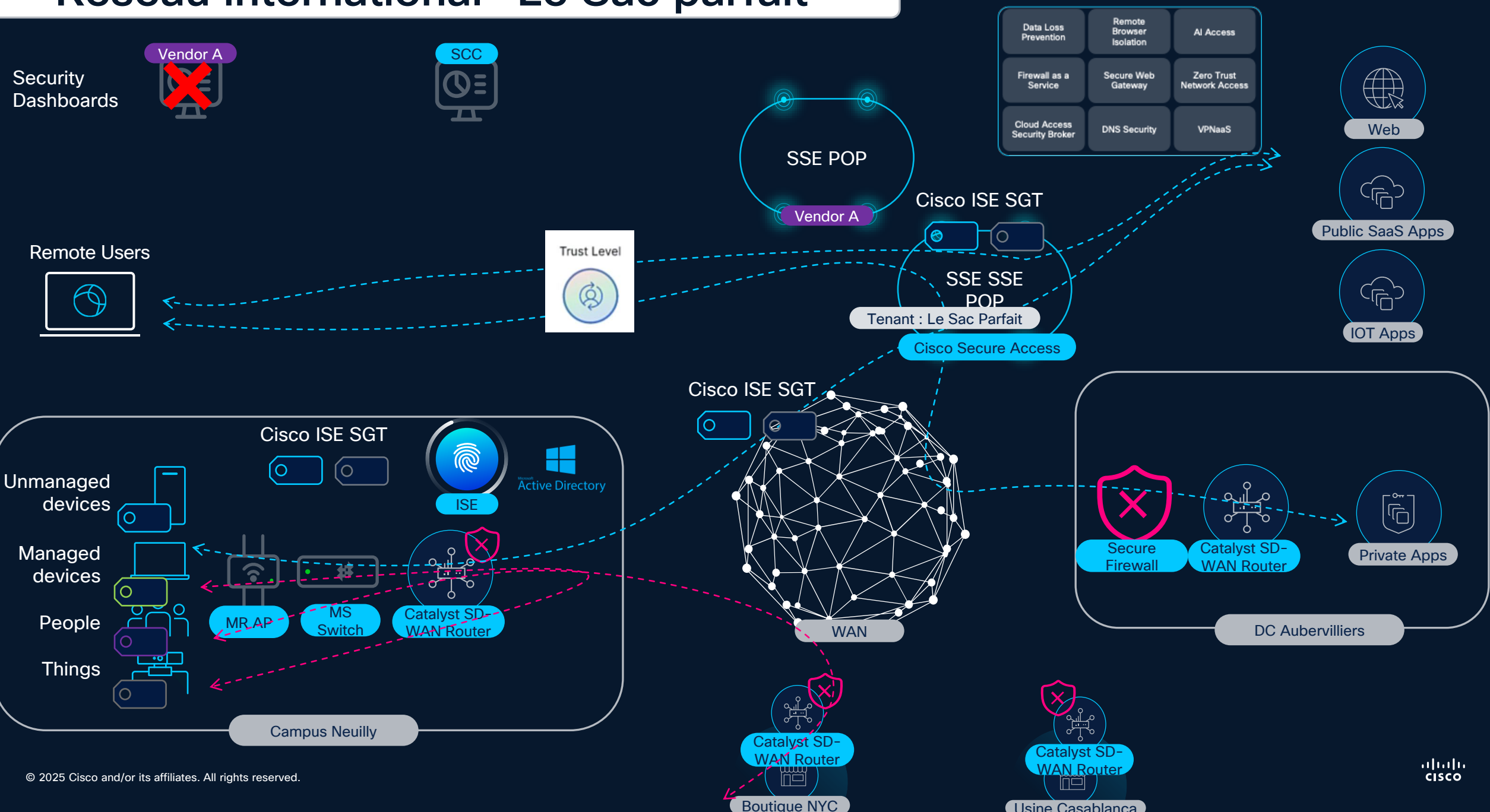
Réseau international "Le Sac parfait"



Réseau international "Le Sac parfait"



Réseau international "Le Sac parfait"



Conclusion approche uZTNA Cisco

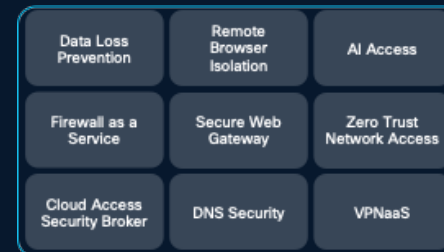
Security Dashboards



Consistence et simplicité

Haut niveau de performance et de disponibilité

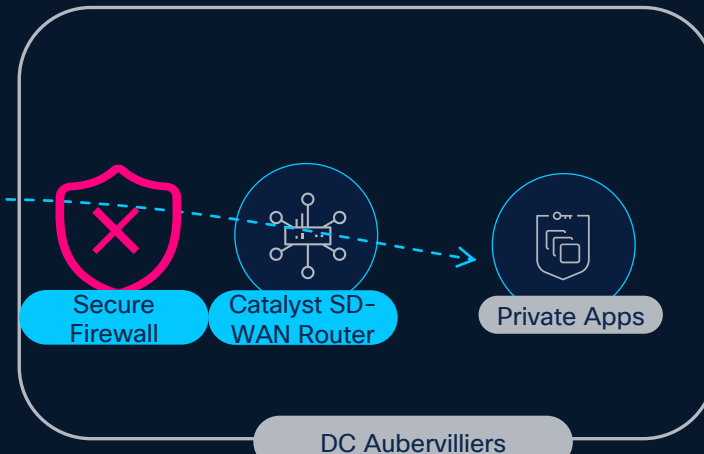
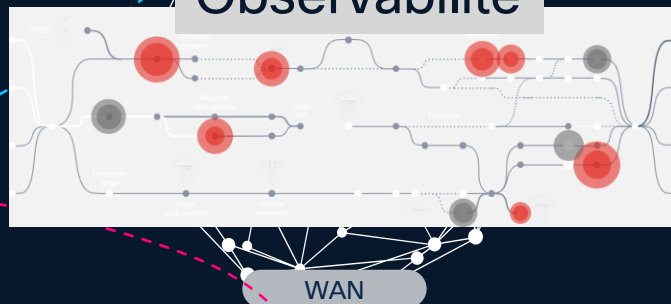
Remote Users



Identité and Posture

Cisco ISE SGT

Observabilité

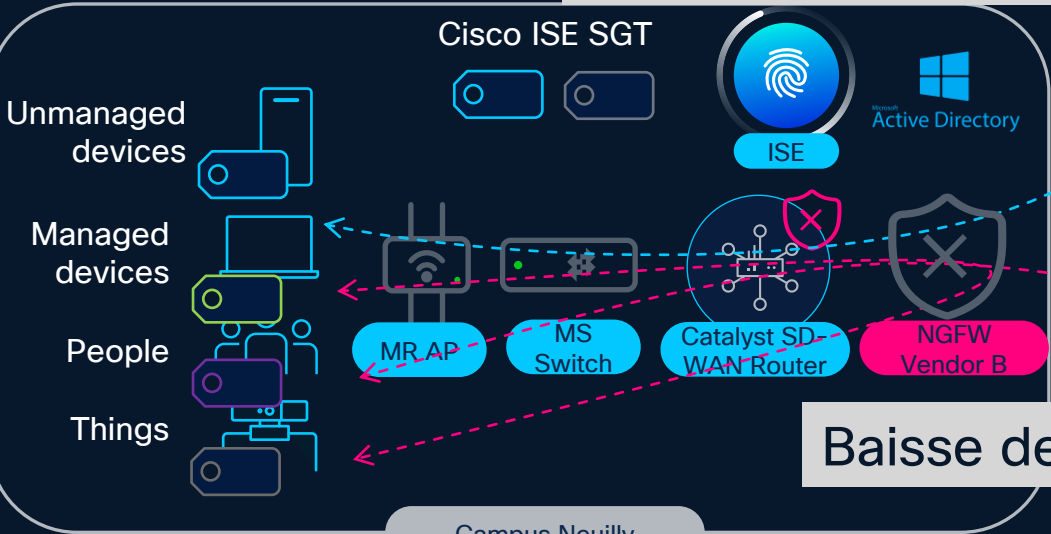


Unmanaged devices

Managed devices

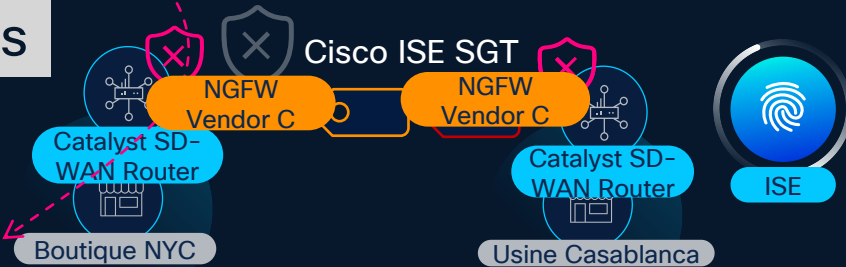
People

Things



Baisse des coûts

Campus Neuilly



Merci

