Secure Service Edge og SDWAN

Når denne session er ovre ved du

- **Hvad er :**

  - **Secure Internet Access**
  - **Secure Private Access**
  - **SSE**
  - **SDWAN**
  - **SASE**
  - **Cisco+ Secure connect**
  - **Cisco Secure Access**
  - **SD-Routing**

- **Hvorfor Cisco Secure Access**

What is SSE (Gartner)

Secure Internet Access

🌐 Internet apps

☁️ SaaS apps

🔑 Zero trust Network Access

+

Secure Private Access

🛡️ Private apps

=

Security Service Edge (SSE)

Secure Access from anywhere to everywhere
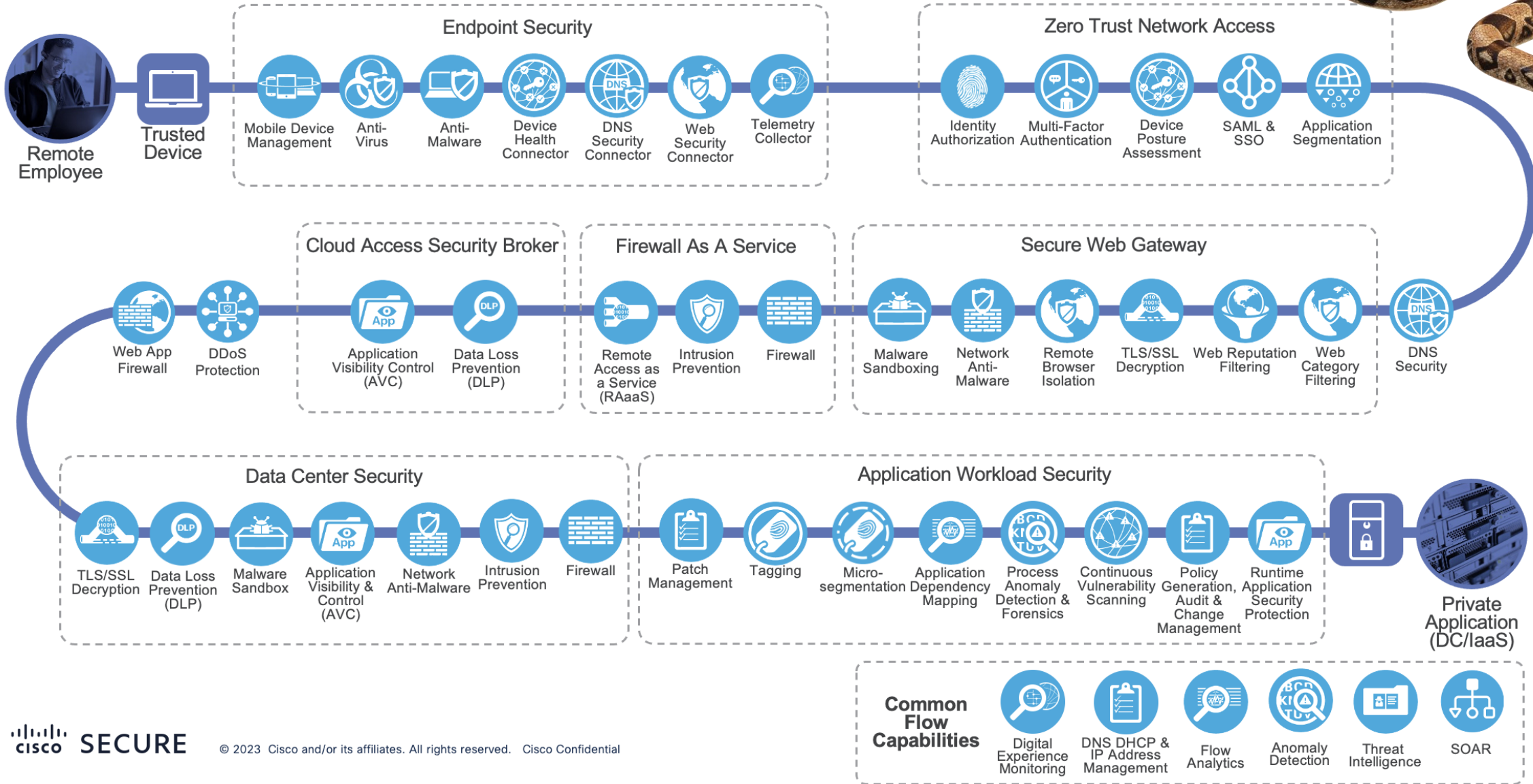
cisco

What is Cisco Secure Access (Cisco+ Secure Connect)

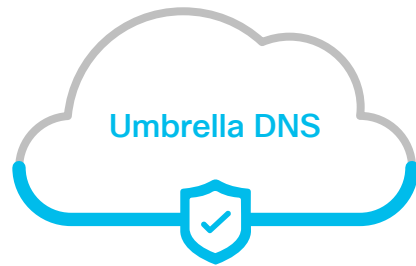## Go beyond core Secure Service Edge (SSE) to better connect and protect your business

Core SSE

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB) and DLP

Zero Trust Network Access (ZTNA)

Firewall as a Service (FWaaS) and IPS

Cisco Secure Access er super simpelt

Umbrella – Cisco Secure Access Evolution

1.0

Umbrella DNS

2.0

Cisco Umbrella SIG
Full Security cloud proxy

- DNS-layer security
- Secure web gateway
- Cloud-delivered firewall
- Cloud access security broker (CASB)
- Data loss prevention
- Remote browser Isolation
- Interactive threat intel

3.0

Cisco Secure Access (SSE)
Cisco+ Secure Connect (Unified S

- DNS-layer security
- Secure web gateway
- Cloud-delivered firewall
- Cloud access security broker (CASB)
- Data loss prevention
- Interactive threat intel
- VPN & ZTNA Private Application Access
- Unified Dashboard Experience
- Digital Experience Management

Secure web access
Provide users with safe access to websites and cloud applications from any location and block malicious activity and threats

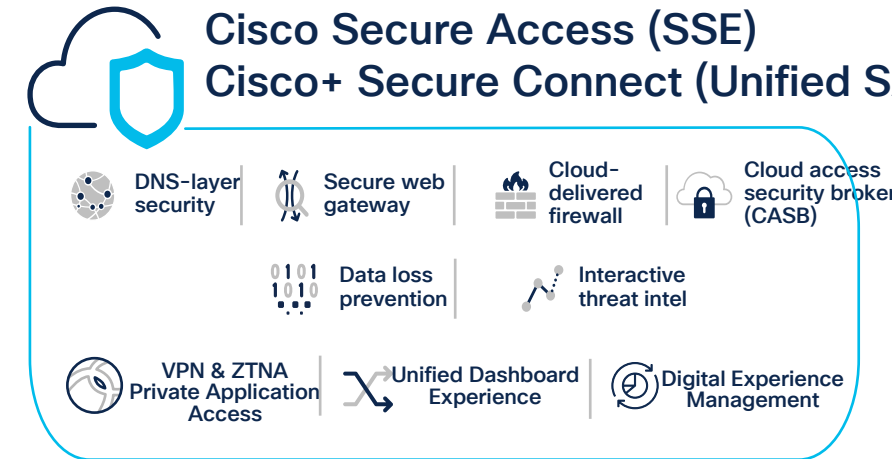### Secure internet access
Provide users with safe access to the internet and cloud applications from any location and block malicious activity and threats

Secure internet access
Provide users with safe access to the internet and cloud applications from any location and block malicious activity and threats
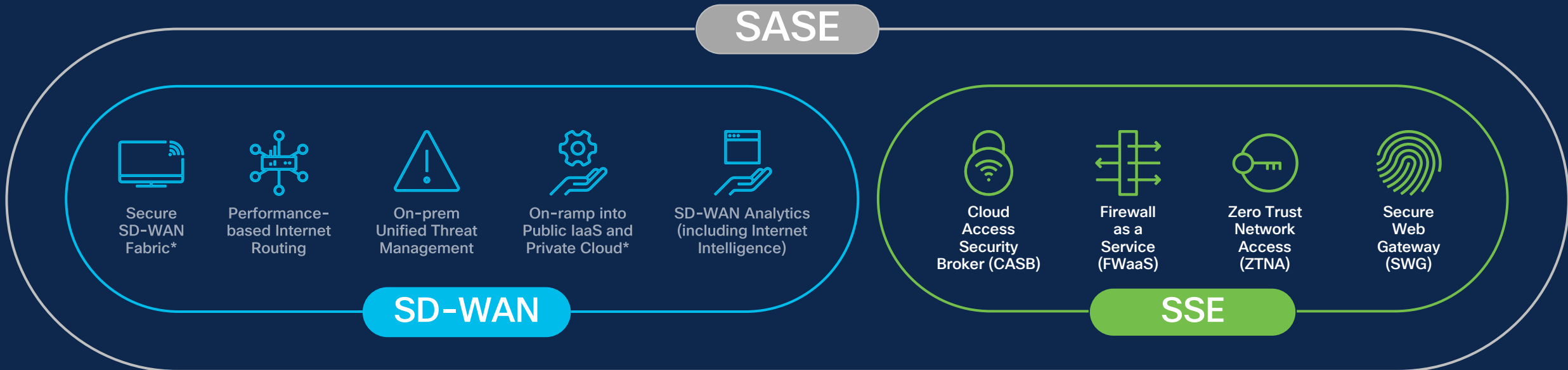
Secure private access leveraging Zero-Trust Principles
Deliver secure connections to company assets in private data centers or in the private cloud.

Interconnect
Dramatically simplify architecture and configuration by inherently interconnecting anything you connect to the SASE Fabric

CISCO SECURE

What is SASE

SASE

SD-WAN

- Secure SD-WAN Fabric*
- Performance-based Internet Routing
- On-prem Unified Threat Management
- On-ramp into Public IaaS and Private Cloud*
- SD-WAN Analytics (including Internet Intelligence)

SSE

- Cloud Access Security Broker (CASB)
- Firewall as a Service (FWaaS)
- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)

CISCO

Så nu har vi lært at :

Secure Internet Access + Secure Private Access = SSE

SSE+SDWAN = SASE

SSE done the right way = Cisco+ Secure connect and Cisco Secure Access

Funktionalitetsmæssigt er Cisco+ Secure connect = Cisco Secure Access

Eliminate unnecessary decisions

How would you like your water delivered?

Users

VPN
ZTNA
Direct
SaaS

Private apps
Internet apps
Traditional apps
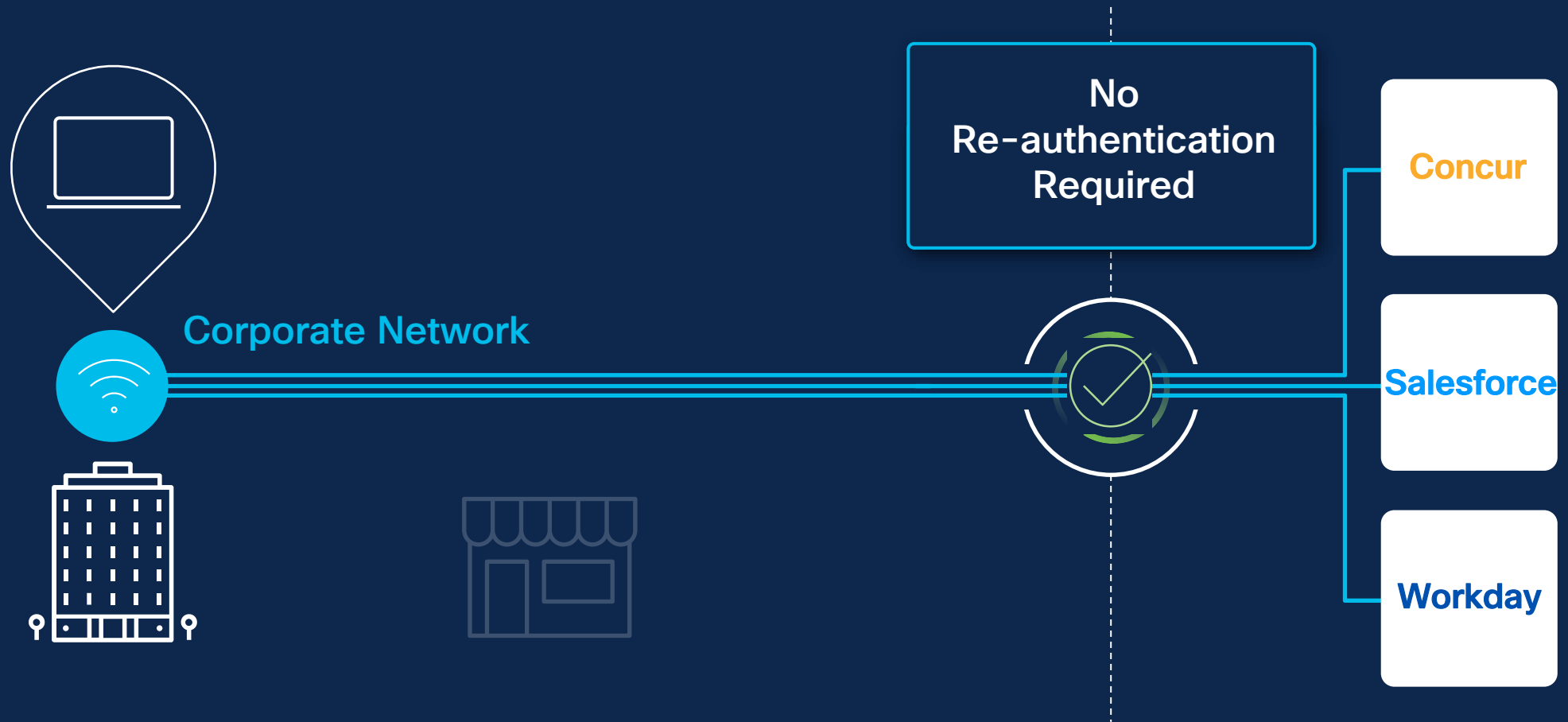SaaS apps

CISCO

Seamless user to app Zero Trust
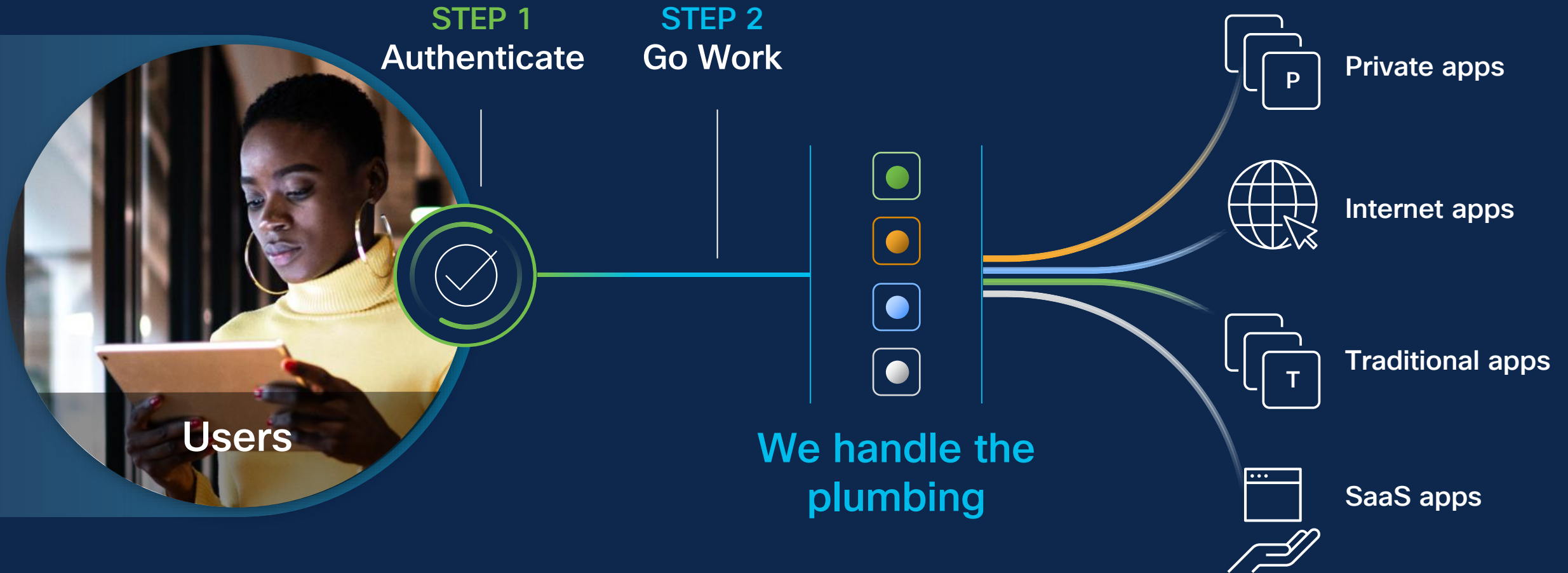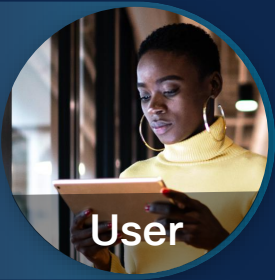
Centralized policy management simplifies security

Cisco Security Cloud
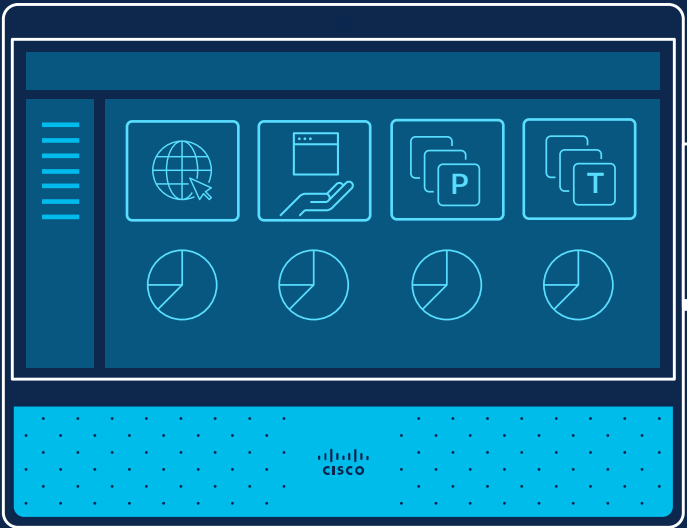
Single central, cloud-based console
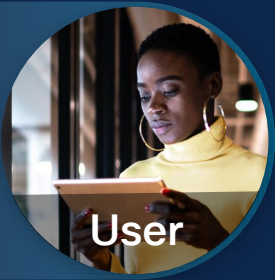
Private apps

Internet apps

Traditional apps

SaaS apps

IT

Data protected | Malware stopped | Policies unified | Experience monitored

Cisco ensures a great user experience

User

ThousandEyes

Client   WiFi   Broadband   Network   Application

Built into Cisco SD-WAN

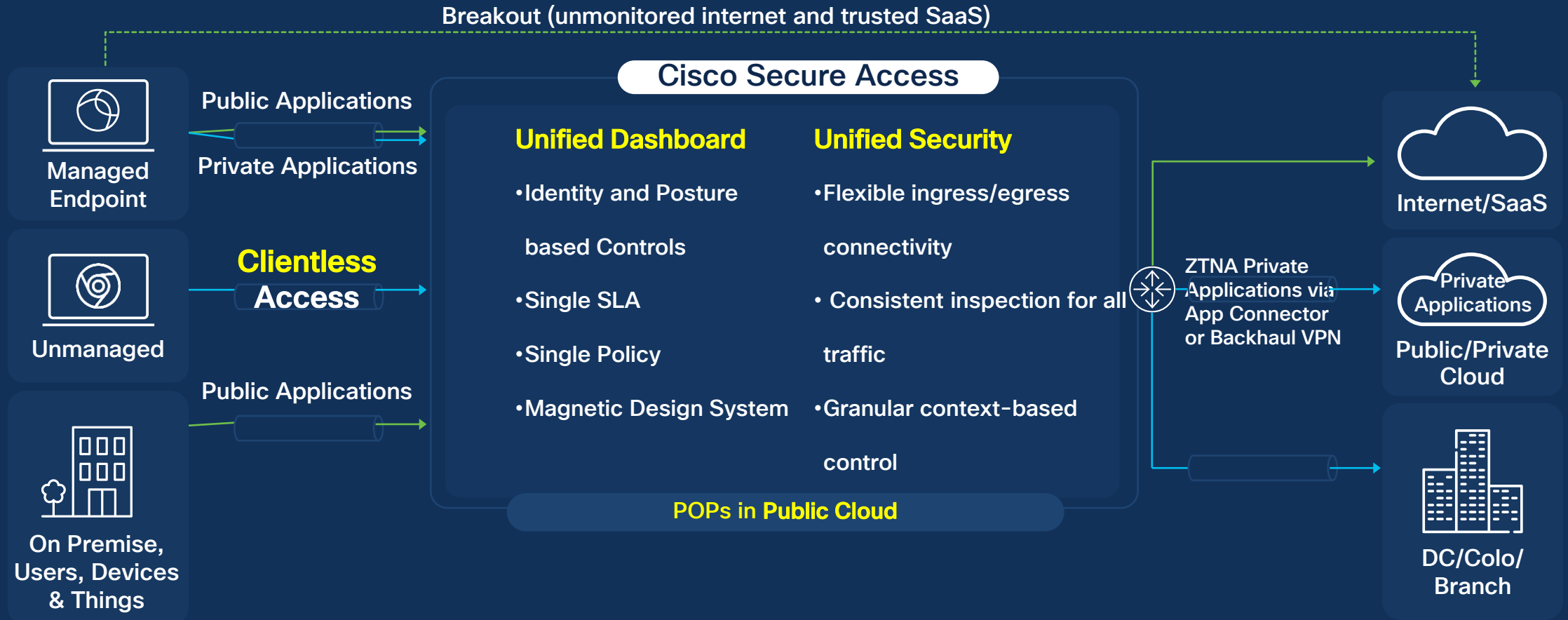Robust, fault tolerant global network

Target latency of ~40ms or less for 99% of users

Built on industry leading QUIC protocol

Architecture Overview

Breakout (unmonitored internet and trusted SaaS)

Cisco Secure Access

Public Applications

Private Applications

Managed Endpoint

Clientless Access

Unmanaged

Public Applications

On Premise, Users, Devices & Things

Unified Dashboard

- Identity and Posture based Controls
- Single SLA
- Single Policy
- Magnetic Design System

Unified Security

- Flexible ingress/egress connectivity
- Consistent inspection for all traffic
- Granular context-based control

POPs in Public Cloud

ZTNA Private Applications via App Connector or Backhaul VPN

Internet/SaaS

Private Applications

Public/Private Cloud

DC/Colo/ Branch

Users & Devices

How

Apps

One Dashboard

Overview [👁 read-only]

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to ad

Get started with Cisco Secure Access

to start protecting your organization's users and then follow the tasks listed here

Sources and destinations

Policy	Profiles	Settings

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

Profiles

Endpoint Posture Profiles

Configure requirements for end-user devices connecting to private resources

IPS Profiles

Configure settings for intrusion prevention

Web Profiles

Configure web security settings for use in internet access rules

Settings

Threat Categories

Choose types of harmful destinations to restrict access to

Notification Pages

Configure notifications to present to end users who try to access blocked or warned destinations.

Do Not Decrypt Lists

Specify destinations for traffic that must never be decrypted

Certificates

Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate

Sidebar Navigation

- Overview
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

Overview

Connect

Resources

Secure

Monitor

Admin

Workflows

Overview 👁 read-only

The Overview dashboard displays status, usage, and health metrics for your or

✨ **Get started with Cisco Secure Access**

Choose how you want to start protecting your organization's users a

0/3 steps complete

Reports	Management
Remote Access Logs	**Exported Reports**
Activity Search Traffic logs	**Scheduled Reports**
Security Activity Security events and top threats	**Admin Audit Log**
App Discovery Discover and analyze network applications	
Top Destinations Top domains visited by DNS	
Top Categories Top security and content categories by DNS	
Data Loss Prevention Data violations detected through the Real Time and SaaS API rules	
Cloud Malware View and manage detected malware events	

Nu ved DU hvad forskellen er på disse ting :

- Secure Internet Access
- Secure Private Access
- SSE
- SDWAN
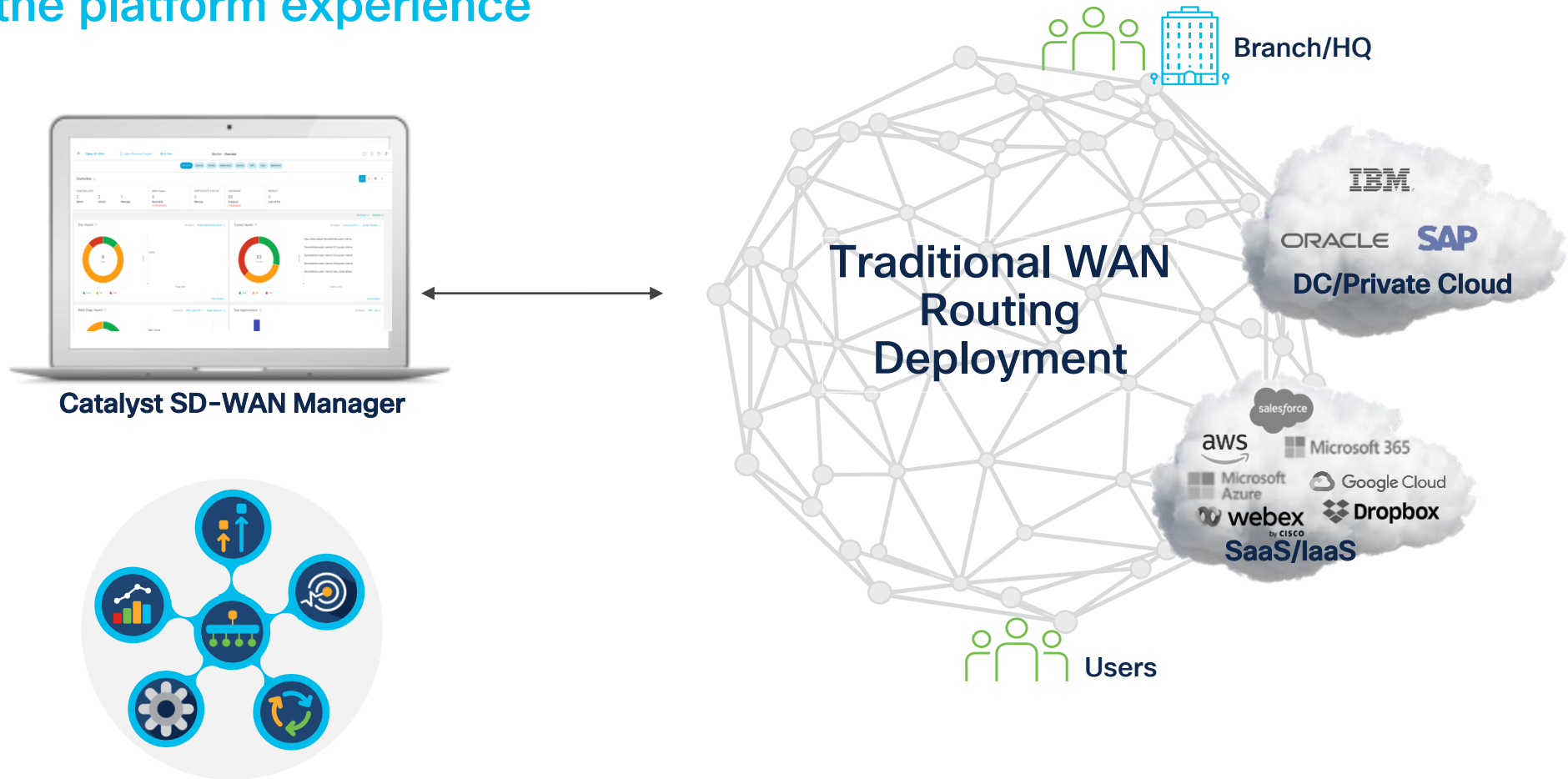- SASE
- Cisco+ Secure connect
- Cisco Secure Access

**Cisco Secure Access
Simplify / Unify**

Introducing SD-Routing
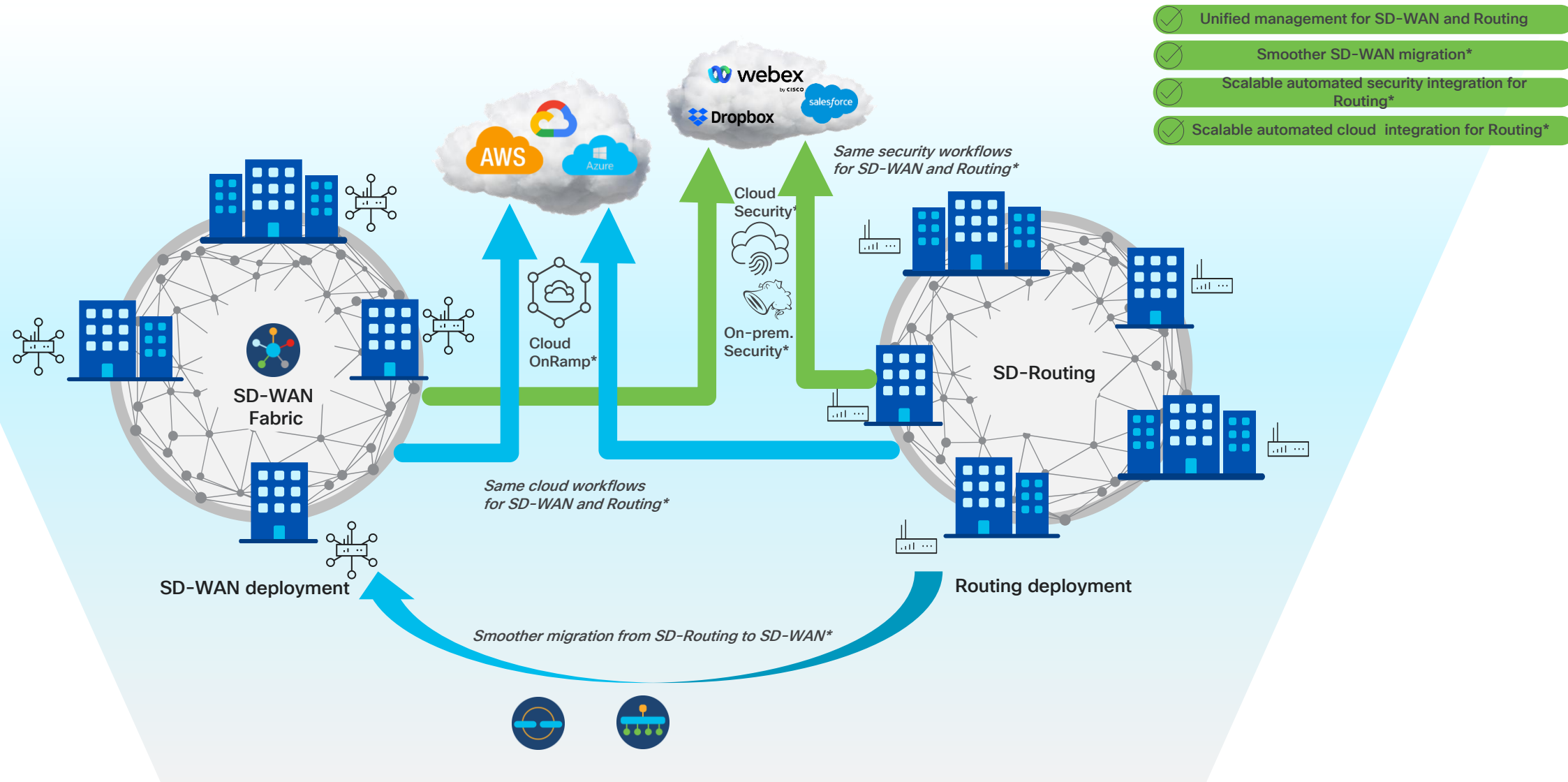
Transform the platform experience

Catalyst SD-WAN Manager

Traditional WAN Routing Deployment

Branch/HQ

DC/Private Cloud

SaaS/IaaS

Users

| Simplicity and Agility | OpEx Reduction | Future-Ready WAN | Multi-layered Security |

Unified Management for your WAN

Unified management for SD-WAN and Routing

Smoother SD-WAN migration*

Scalable automated security integration for Routing*

Scalable automated cloud integration for Routing*

Same security workflows for SD-WAN and Routing*

Cloud Security*

On-prem. Security*

Cloud OnRamp*

SD-WAN Fabric

SD-Routing

Same cloud workflows for SD-WAN and Routing*
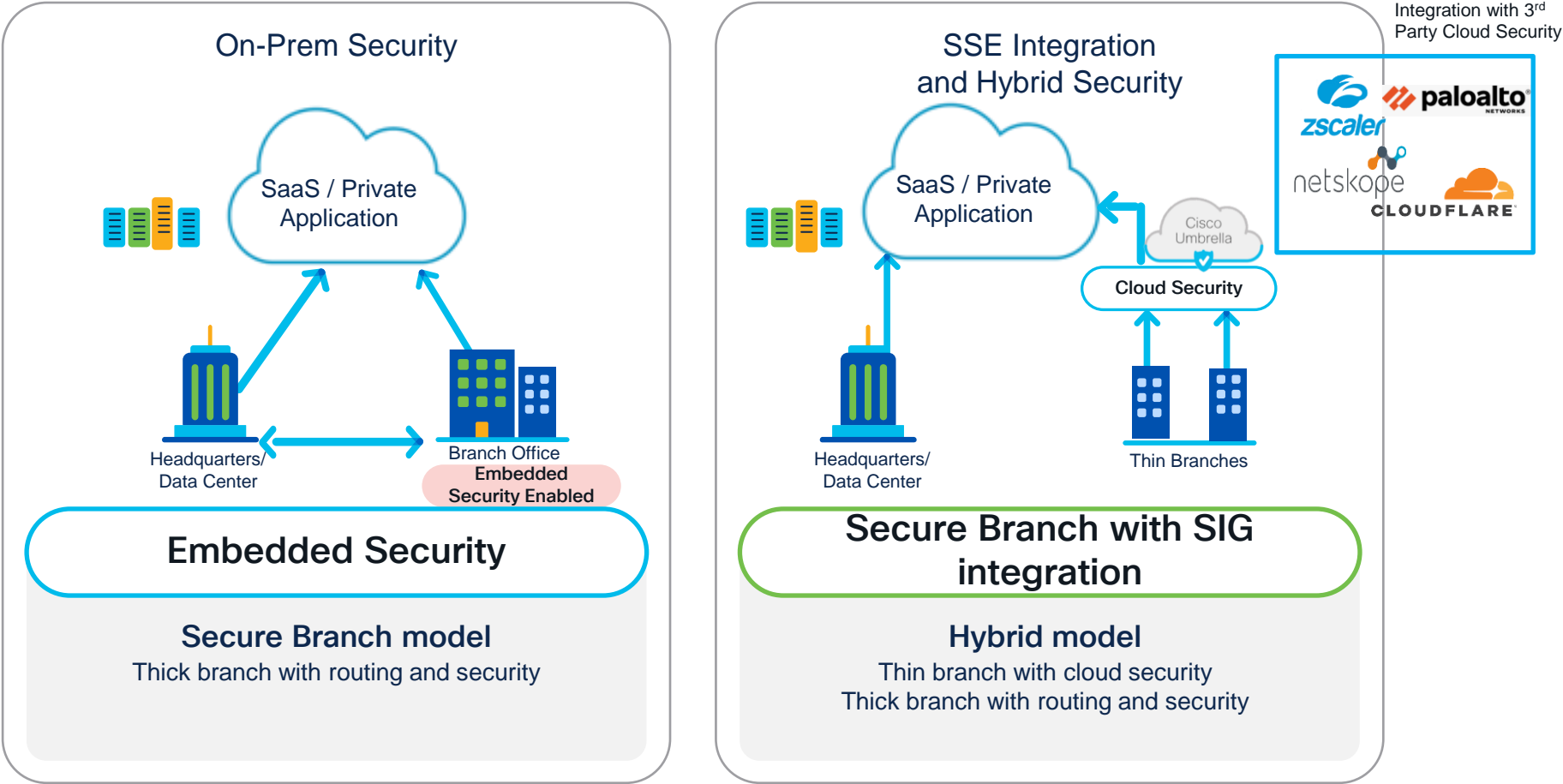
SD-WAN deployment

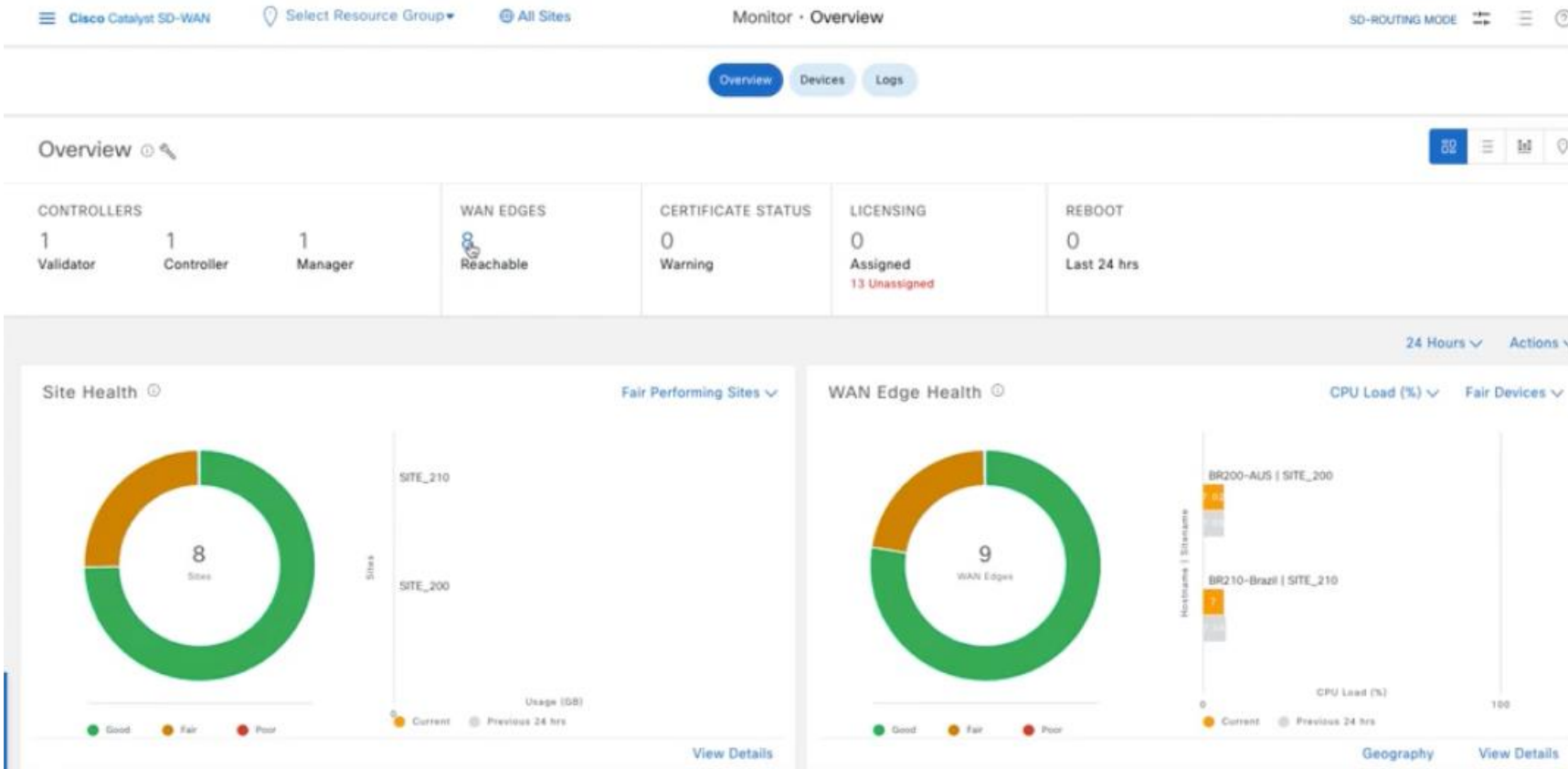Routing deployment

Smoother migration from SD-Routing to SD-WAN*

* On Roadmap for Routing. Fully supported with SD-WAN today.

Consistent Security Across SD-WAN and SD-Routing

What's available with 20.12/17.12 for SD-Routing

Device onboarding

Monitoring

Troubleshooting

Lifecycle management

SD-Routing (roadmap)

Key takeaways

Simplicity and Agility
Eliminate CLI and reduce potential configuration errors on individual devices

OpEx Reduction
Avoid dispatching IT staff onsite for routine operational tasks with a single dashboard for all use cases

Future-Ready WAN
Easily migrate to Catalyst SD-WAN with familiar UI and workflows

---

Experience scalable and unified manageability for both traditional routing and SD-WAN

Device Lifecycle Management

Intelligent Monitoring

On-Prem Security Workflows

Multicloud Integration

Nu ved DU hvad :
- SD-Routing

Thank you

The bridge to possible

CISCO

CISCO Live!

#CiscoLive