

IT.Integrator



Що таке Cisco SASE та навіщо це потрібно?

Володимир Ілібман
Cisco



Agenda



- ▶ What is SASE & SSE
- ▶ Core Components of SASE
- ▶ SASE Use Cases
- ▶ SASE Customers Case Studies

Networks We Used To Build - Historic Traffic Flows

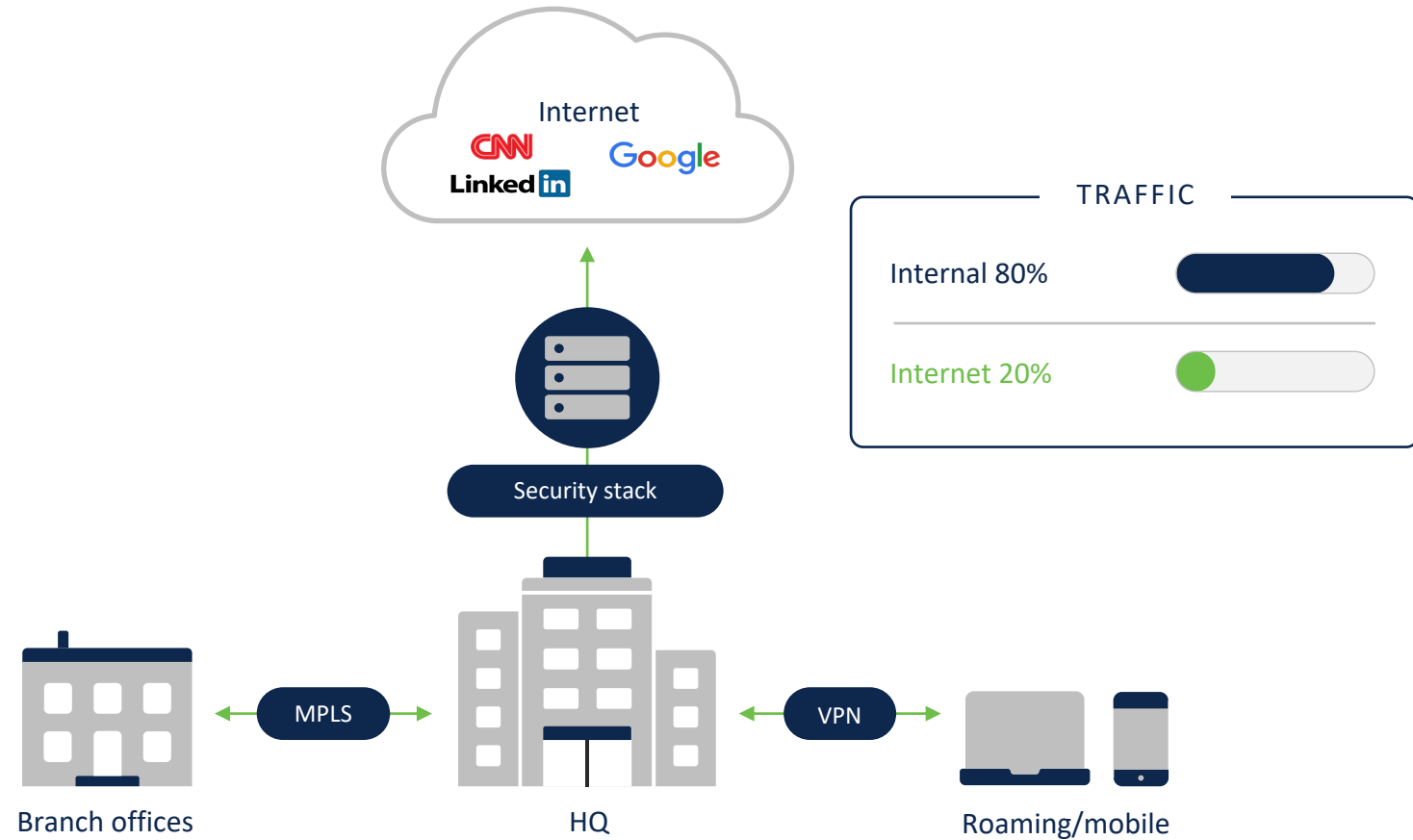
Led to the age of perimeter-based security and networking

Network

Centralized

Security

Single, on-premise security stack

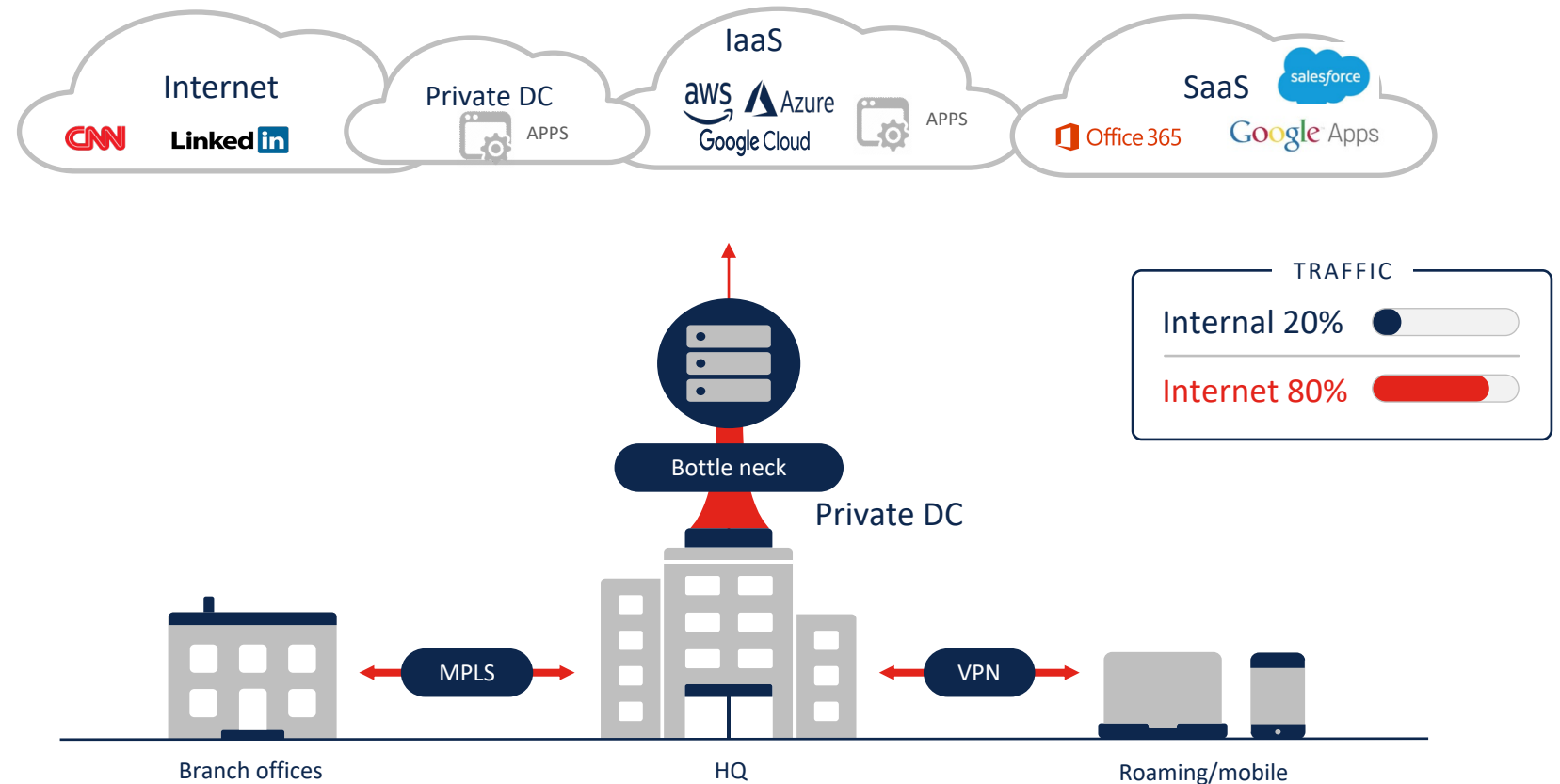


What Has Changed?

Problems:

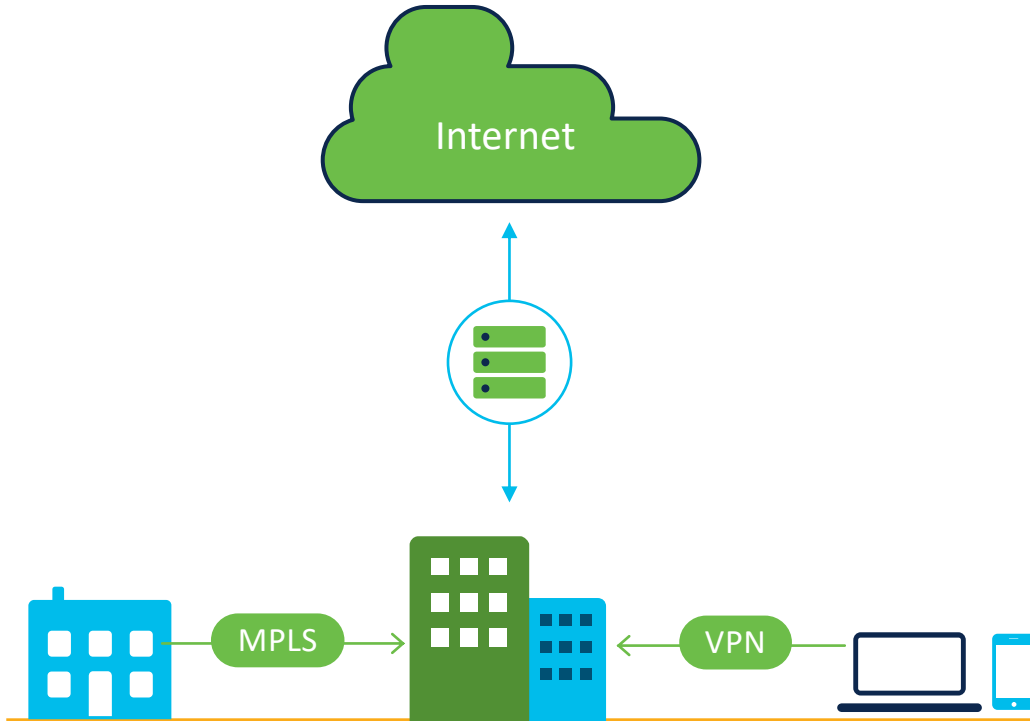
- Bandwidth requirements
- Application Performance (Latency)
- User experience
- Costs
- # Tools/Vendors

- Cyber Security efficacy
 - HTTPS Decryption
 - Protection of Remote Users
 - Security Updates
 - Complexity/Alarm fatigue
 - Experts' shortage



Network & Security transformation

Centralized

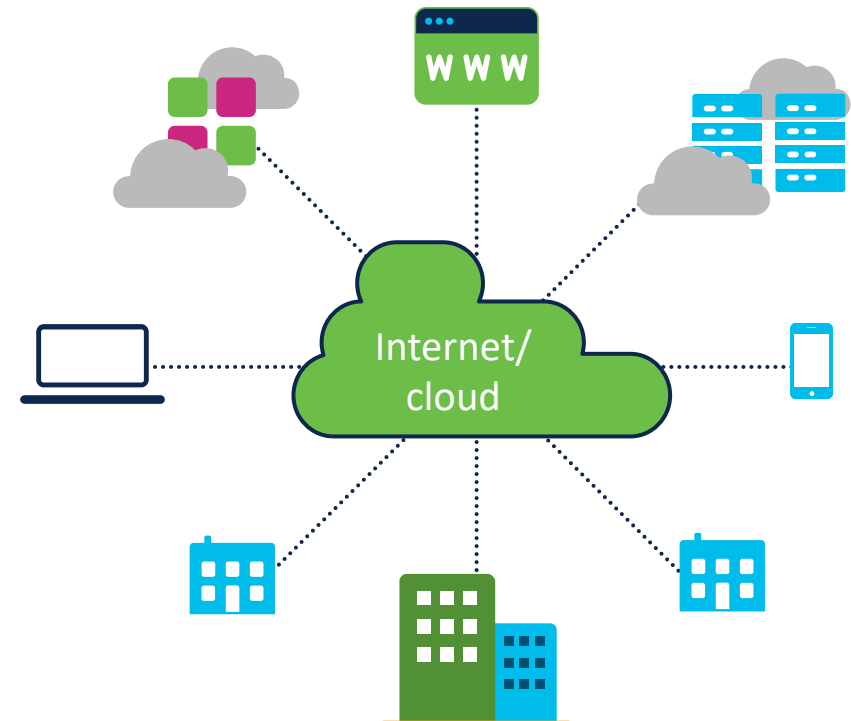


Poor Application Performance
Poor User Experience
Complex

Expensive
No scalability
Insecure



Decentralized



Simple, Agile,
Flexible Performance
Exceptional User Experience
State of the Art Cyber Security
Reduced Total Cost of Ownership (TCO)

“*The enterprise perimeter is no longer a location; it is a set of dynamic **edge** capabilities delivered when needed as a **service** from the cloud.*”

Gartner: The Future of Network **Security** is in the Cloud,
Neil MacDonald, Lawrence Orans, Joe Skorupa, 2019

Secure **A**ccess **S**ervices **E**dge

🔊 /'sæsi/

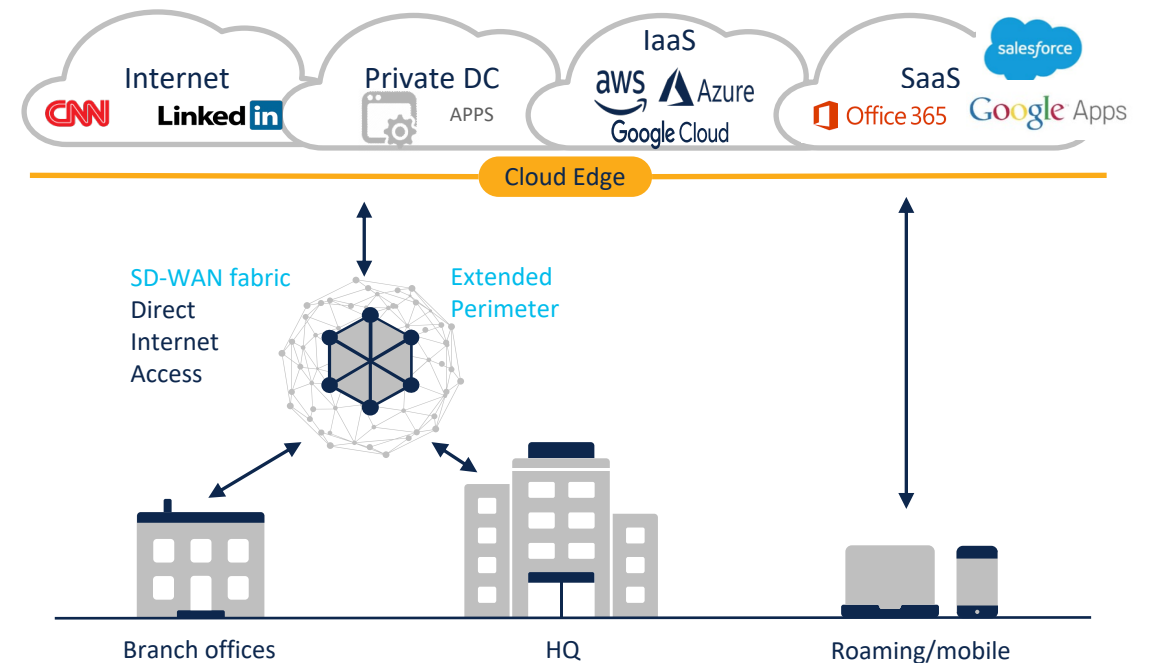
A **consolidated** architectural solution that provides effective & homogenous levels of **security** and **network access** for users from anywhere on any device.

Secure Access Service Edge (SASE) Architecture

Addresses the challenges in cloud centric and hybrid network environments

What is SASE:

- Combines
 - **Security** - Enforced at the cloud edge
 - **Network** - Optimized routing from anywhere to the cloud



Security Services Edge (SSE): It's SASE without the "A"

The SSE category was first introduced by Gartner in the “2021 Roadmap for SASE Convergence” report in March of 2021 (where it was named “Security Services Edge” with service in the plural.

SSE is the half of secure access service edge (SASE) focusing on the convergence of Cloud Security Services.

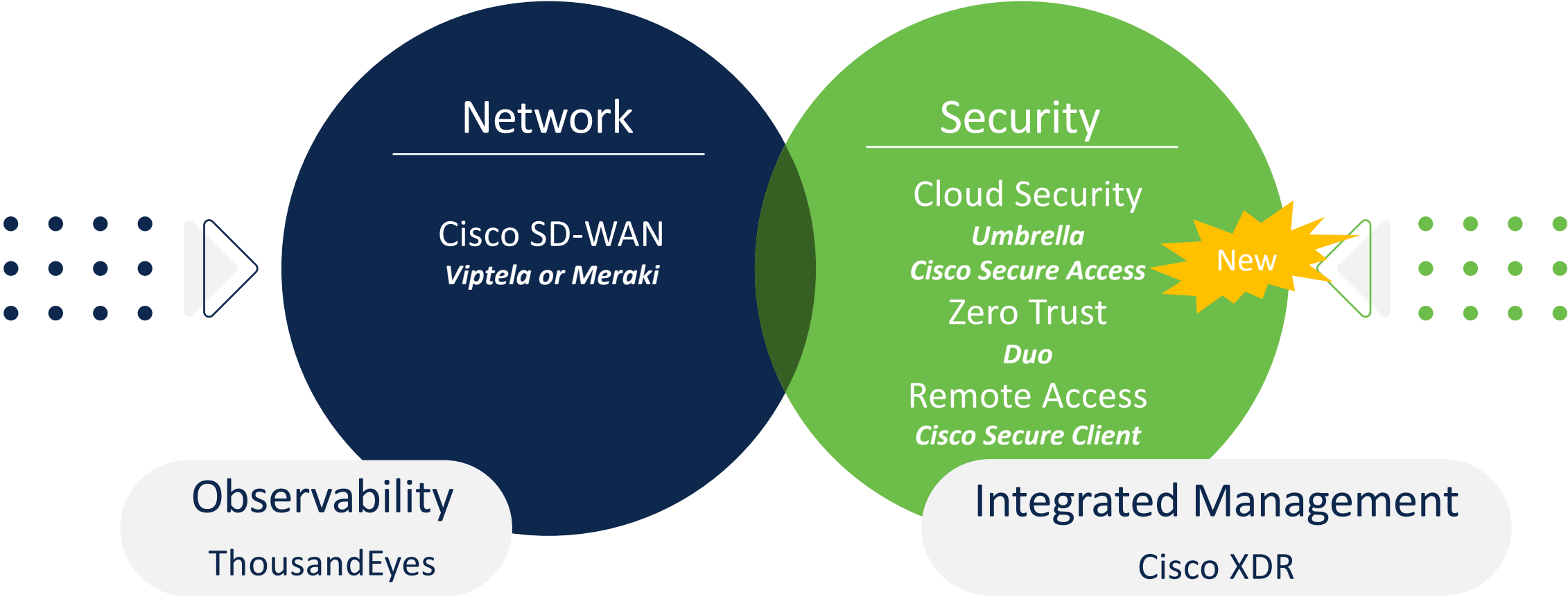
Networking convergence forms the other half of SASE.

Why Now?

- By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access using a SASE/SSE architecture, up from 20% in 2021.
- By 2025, one-third of new SASE deployments will be based on a integrated single-vendor SASE offering, up from 10% in 2022.

Gartner: Market Guide for Single-Vendor SASE, September 2022

Components of Cisco SASE Architecture



Cisco Umbrella : Security Services Edge (SSE) for Internet access



| | | | |
|---------------------------------|-----------------------------------|----------------------|------------------------------|
| DNS-layer security | Cloud-delivered firewall (w/ IPS) | Secure web gateway | Cloud access security broker |
| Interactive threat intelligence | Remote browser isolation | Data loss prevention | Cloud malware detection |

Combines multiple security capabilities into one simple, effective, cloud-native service

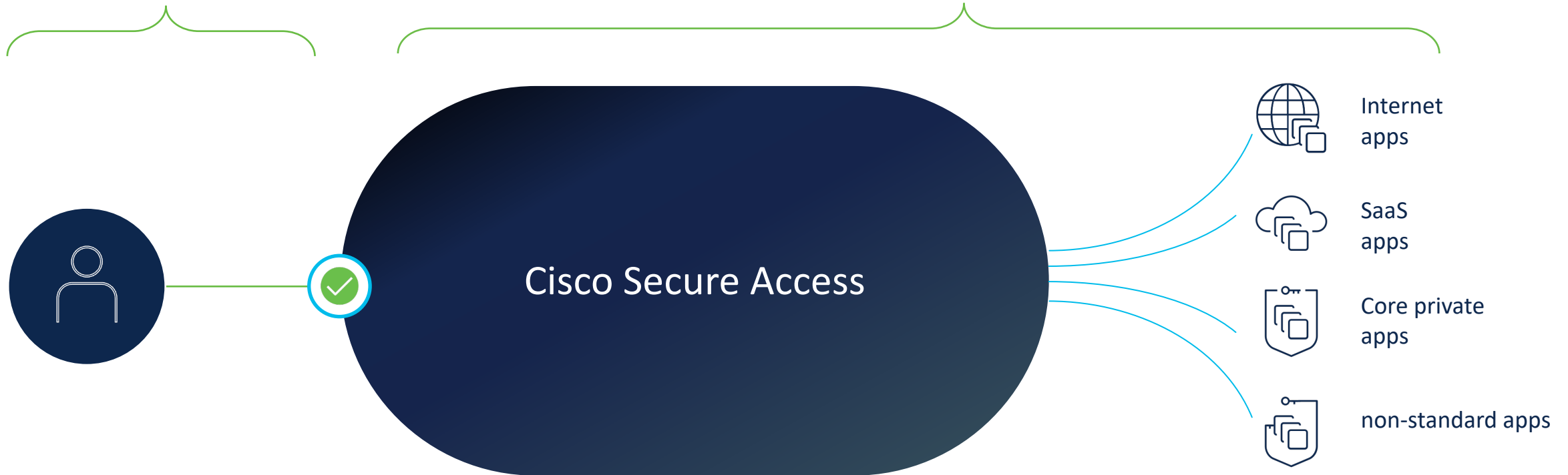
Block more threats earlier

Cisco Secure Access

Easy, frictionless user experience

1 Connect to a network

2 Get to work



Cisco Secure Access

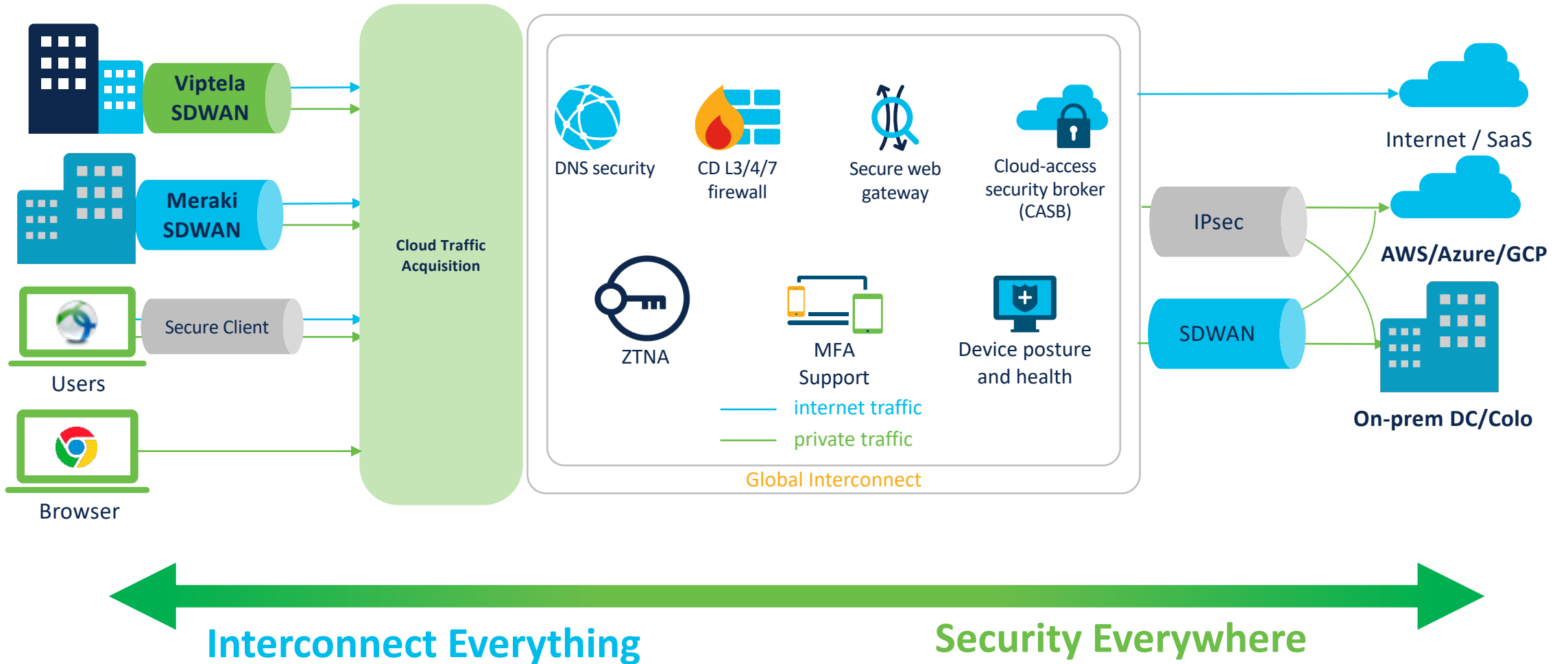
Go beyond core Secure Service Edge (SSE) to better connect and protect your business



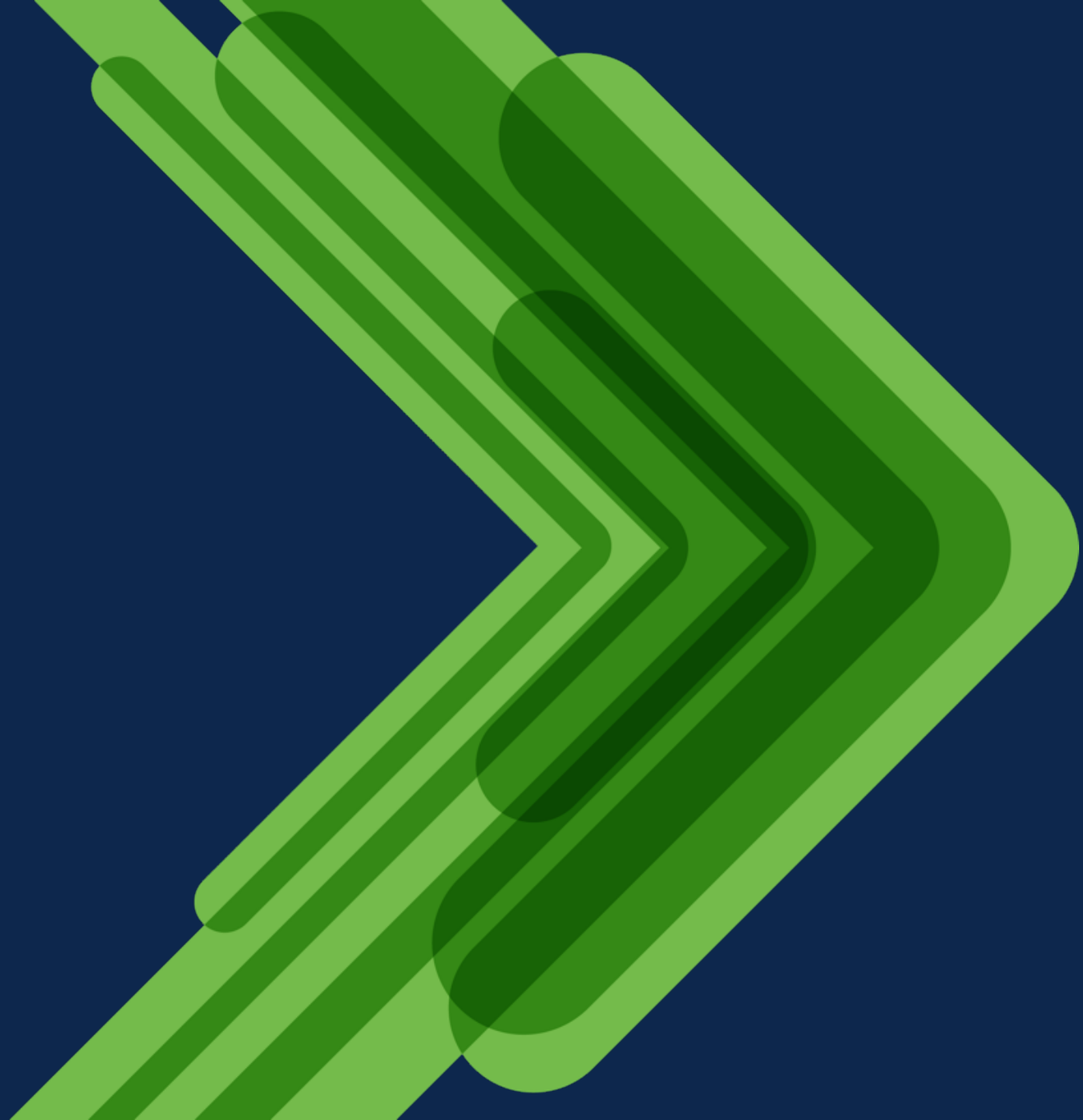
Combines multiple security capabilities into one simple, effective, cloud-native service

Cloud-Native service with state-of-the-art cybersecurity capabilities delivered out of data centers worldwide, interconnected with private and public peerings to provide the fastest route and lower latency.

Cisco Secure Access - Unlocking the power of SASE



SASE Use Cases



Use Case 1 – Remote Workers

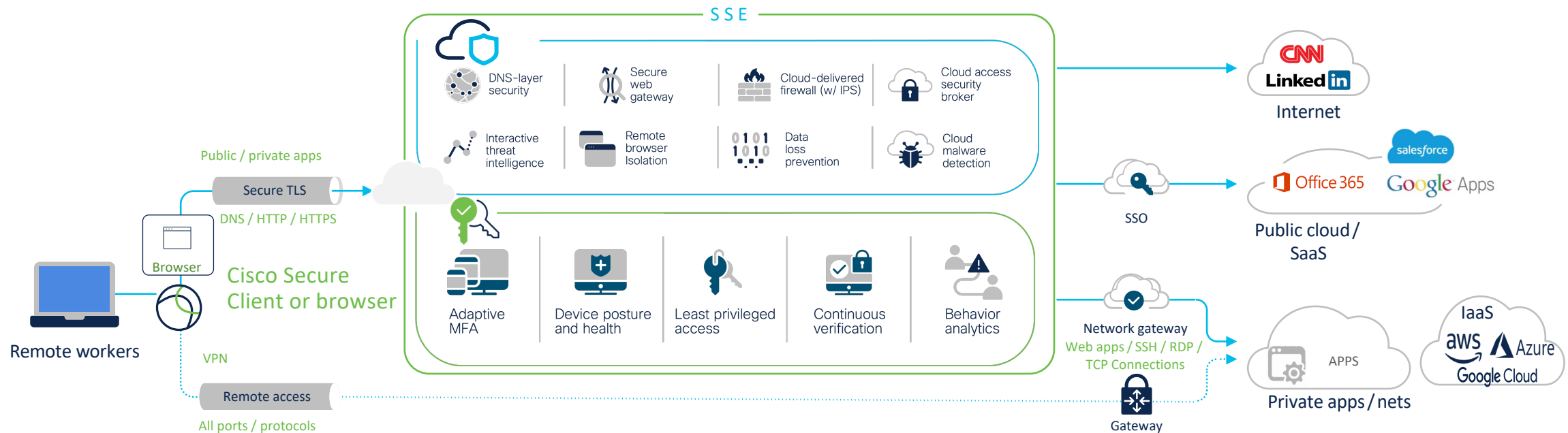
No Branch Network

Advanced application experience with comprehensive security

Use Case 1 – Remote Workers

No Branch Network

Advanced application experience with comprehensive security

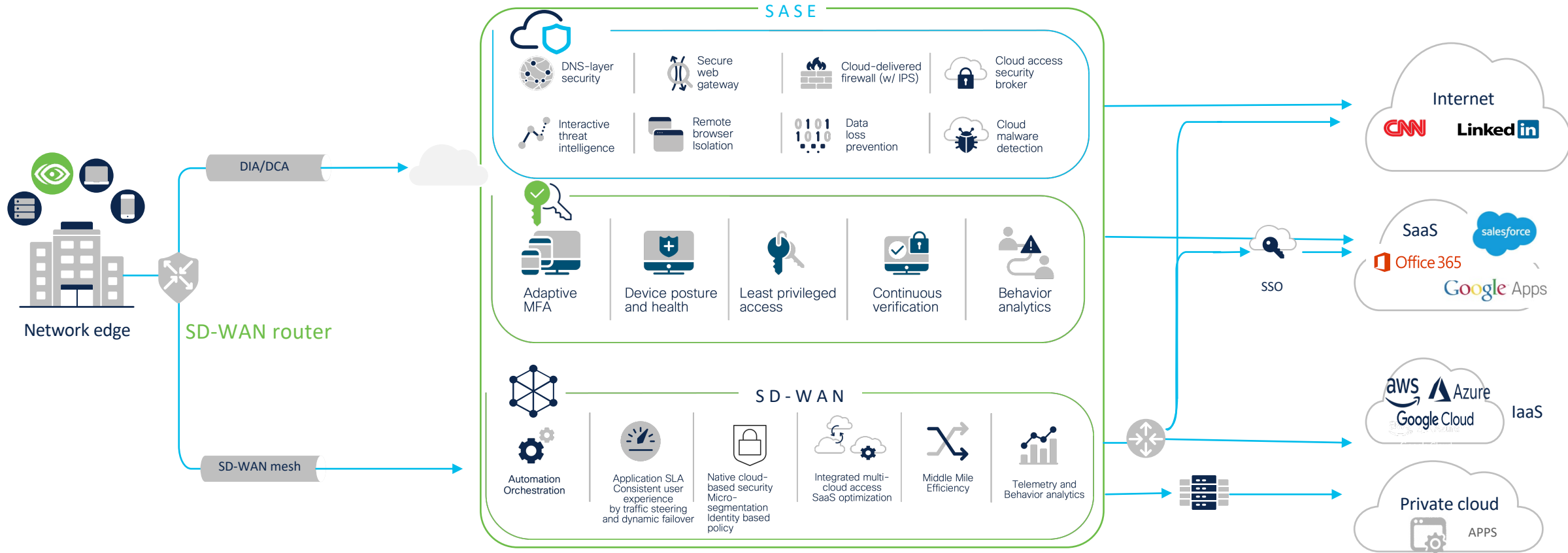


Use Case 2

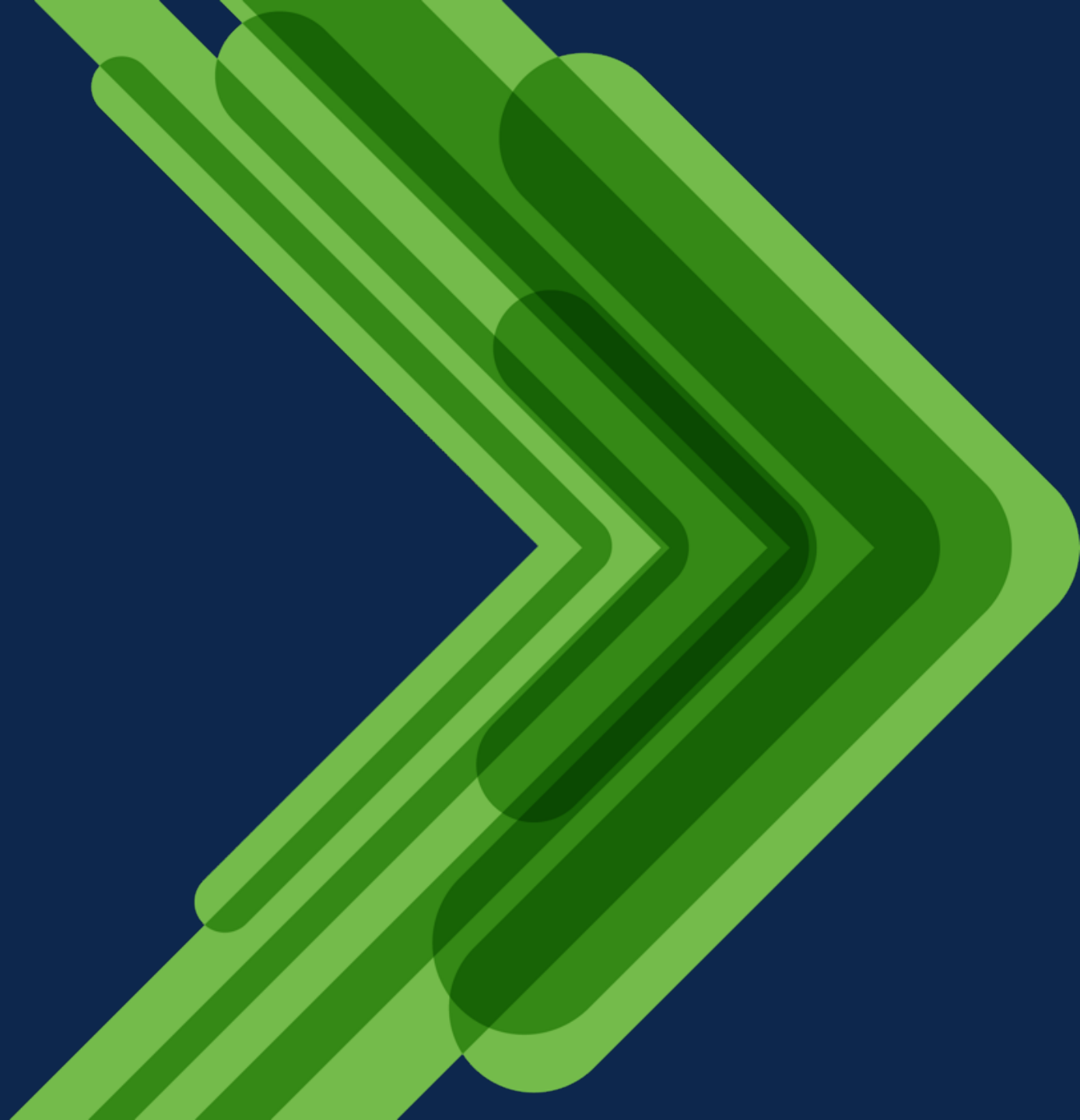
Secure Edge & Branch Infrastructure

Remote workers

Secure Edge



SASE Cases Study



Use Case 1 – Віддалений доступ для співробітників банку

SASE для віддаленого доступу

Другий етап
2021 р

2023

2019 рік

Перший етап
2020 р

Послуга AnyConnect VPN для керівників та IT/InfoSec на базі міжмережевого екрану та системи авторизації Cisco попереднього покоління

Впровадження AnyConnect для всього банку (2500 співробітників)

Збільшення ємності та виділення спеціалізованих пристроїв

Використання багатофакторної аутентифікації Cisco DUO

Контроль Інтернет-доступу мобільних співробітників через Cisco Umbrella

Використання всіх переваг Cisco Secure Client, перевірка відповідності кінцевих пристроїв політикам

Що було до COVID-19

Розширення VPN

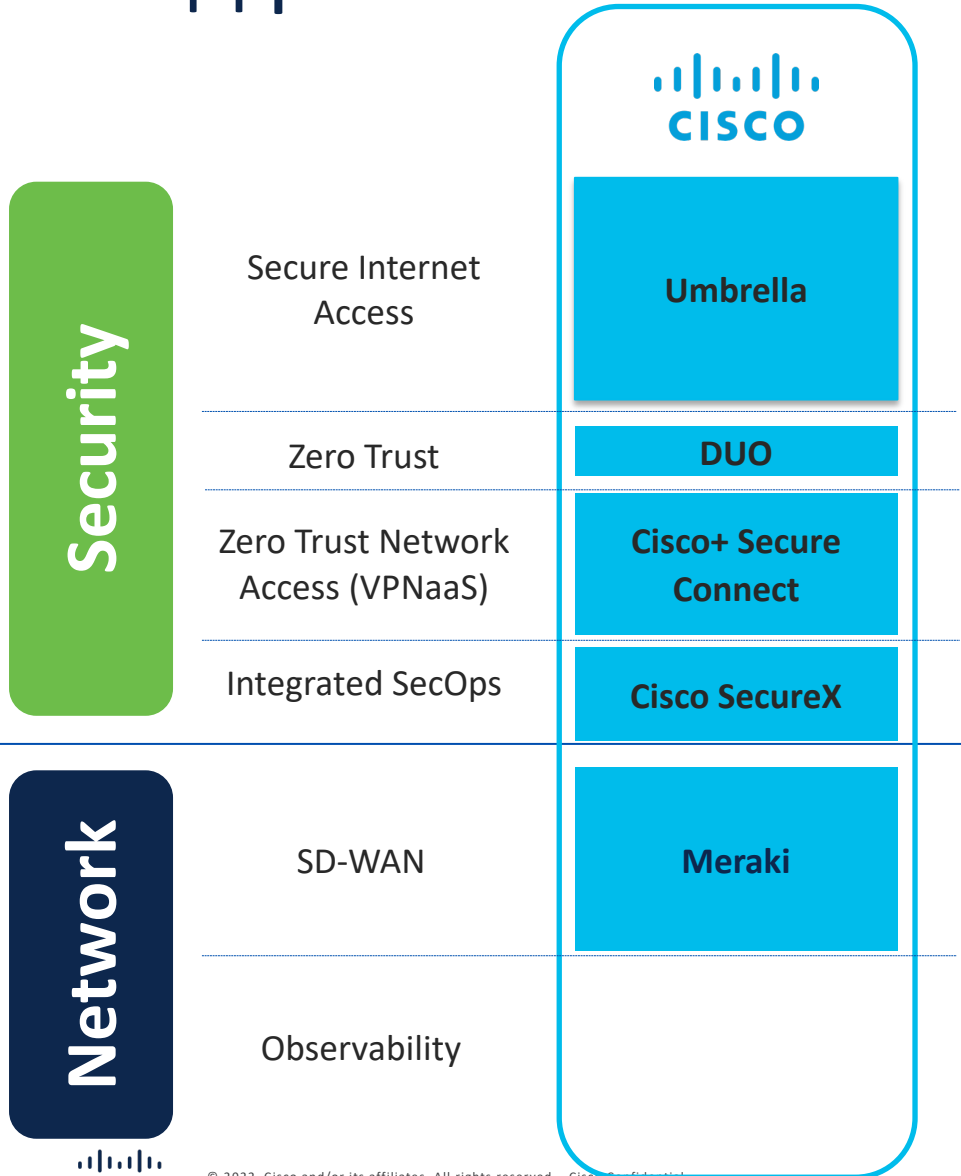
Підвищення безпеки

Передові послуги захисту

Use Case 2 – Хмарний захист Інтернет доступу філіалів розподіленого холдінгу

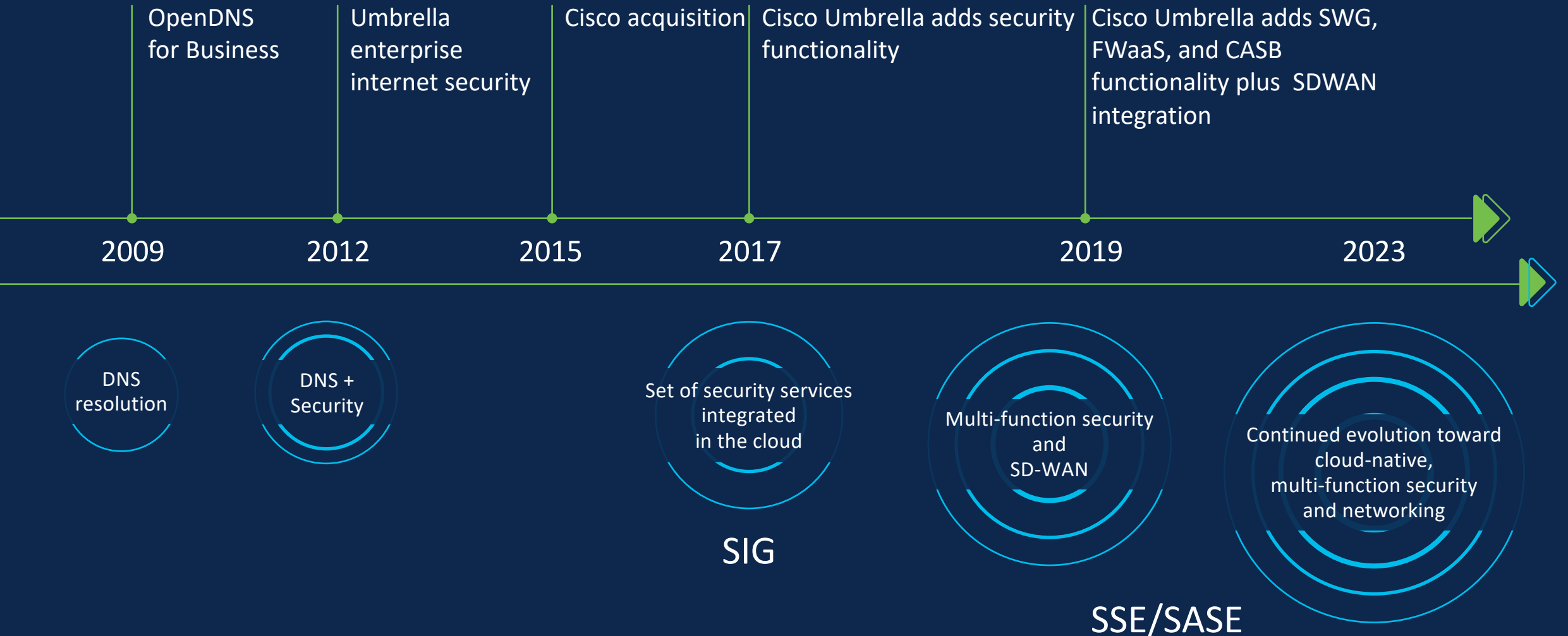
- **Хмарна стратегія та Microsoft Azure**
- **Потреба захисту віддалених користувачів та користувачів у філіалах**
- **Багаторівневий захист центрального офісу холдінгу**
- **Існують обмеження централізованого доступу в Інтернет для філіалів (особливо для закордонних)**
- **Деякі користувачі мають підвищений ризик цільових атак під час роботи в Інтернеті**

Огляд рішення



- **Інтеграція Umbrella до Meraki MX для захисту філіалів**
- **Cisco Secure Client для захисту віддалених робочих місць**
- **DUO для багатофакторки**
- **Remote Browser Isolation для захисту критичних користувачів від Інтернет-ризиків**
- **Cisco SecureX як оркестратор**

Cisco Umbrella evolution





SECURE

